

Microsoft.MS-500.v2023-11-28.q273

試験コード:	MS-500
試験名称:	Microsoft 365 Security Administration
認定資格:	Microsoft
無料問題数:	273
バージョン:	v2023-11-28
アクセス数:	963
ページビュー数:	2730
https://www.jpnpdf.com/Microsoft.MS-500.v2023-11-28.q273-mondaishu.html	

最新問題: 1

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Microsoft 365 テナントがあります。Microsoft Azure Information Protection で

CompanyConfidential という名前のラベルを作成します。

CompanyConfidential をグローバル ポリシーに追加します。

ユーザーは CompanyConfidential を使用して電子メール メッセージを保護し、ラベルを複数の外部受信者に送信します。外部受信者は、電子メール メッセージを開けないと報告しています。

外部の受信者が、自分に送信された保護された電子メール メッセージを開けられるようにする必要があります。

解決策: グローバル ポリシーで新しいラベルを作成し、ユーザーに電子メール メッセージを再送信するように指示します。

これは目標を達成していますか?

A. いいえ

B. はい

Answer: ([解答を表示する](#))

最新問題: 2

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 サブスクリプションがあります。Site1 には、次の表に示すフォルダーが含まれています。

Name	File in folder
Folder1	File1
Folder2	File2

09:00 に、次の図に示すように、Policy1 という名前の Microsoft Cloud App Security ポリシーを作成します。

Create a filter for the files this policy will act on

Apply to:

selected folders

Currently supports Box, SharePoint, Dropbox, OneDrive.

Folder1 (Microsoft SharePoint Online) x

[Add more folder\(s\)](#)

Apply to:

all file owners

Microsoft

Inspection method

None

Alerts

Create an alert for each matching file [Restore default settings](#)

Daily alert limit 5

Send alert as email ⓘ

Send alert as text message ⓘ

[Save as default settings](#)

Send alerts to Flow

[Create a playbook in Flow](#)

Policy1 を作成した後、次の表に示すようにファイルを Site1 にアップロードします。

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
File1 triggers an alert from Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

説明

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

参照：

<https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

最新問題: 3

Microsoft 365 サブスクリプションをお持ちです。

次のデータ損失防止 (DLP) 要件を特定します。

- * ユーザーが EU 社会保障番号を含む添付ファイルを送信しようとした場合に通知を送信します
- * クレジットカード番号を含む電子メールメッセージが組織外に送信されないようにする
- * EU パスポート番号を含む Microsoft OneDrive コンテンツの外部共有をブロックします
- * ルールの一致が発生した場合、管理者に電子メールアラートを送信します。

要件を満たすために作成する必要がある DLP ポリシーとルールの最小数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: 正しく選択するたびに 1 ポイントの価値があります。

Policies:

1	V
2	
3	

Rules:

1	V	
2		
3		Microsoft
4		

Answer:

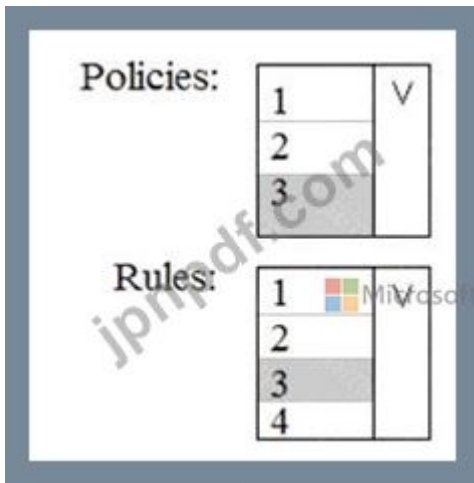
Policies:

1	V
2	
3	

Rules:

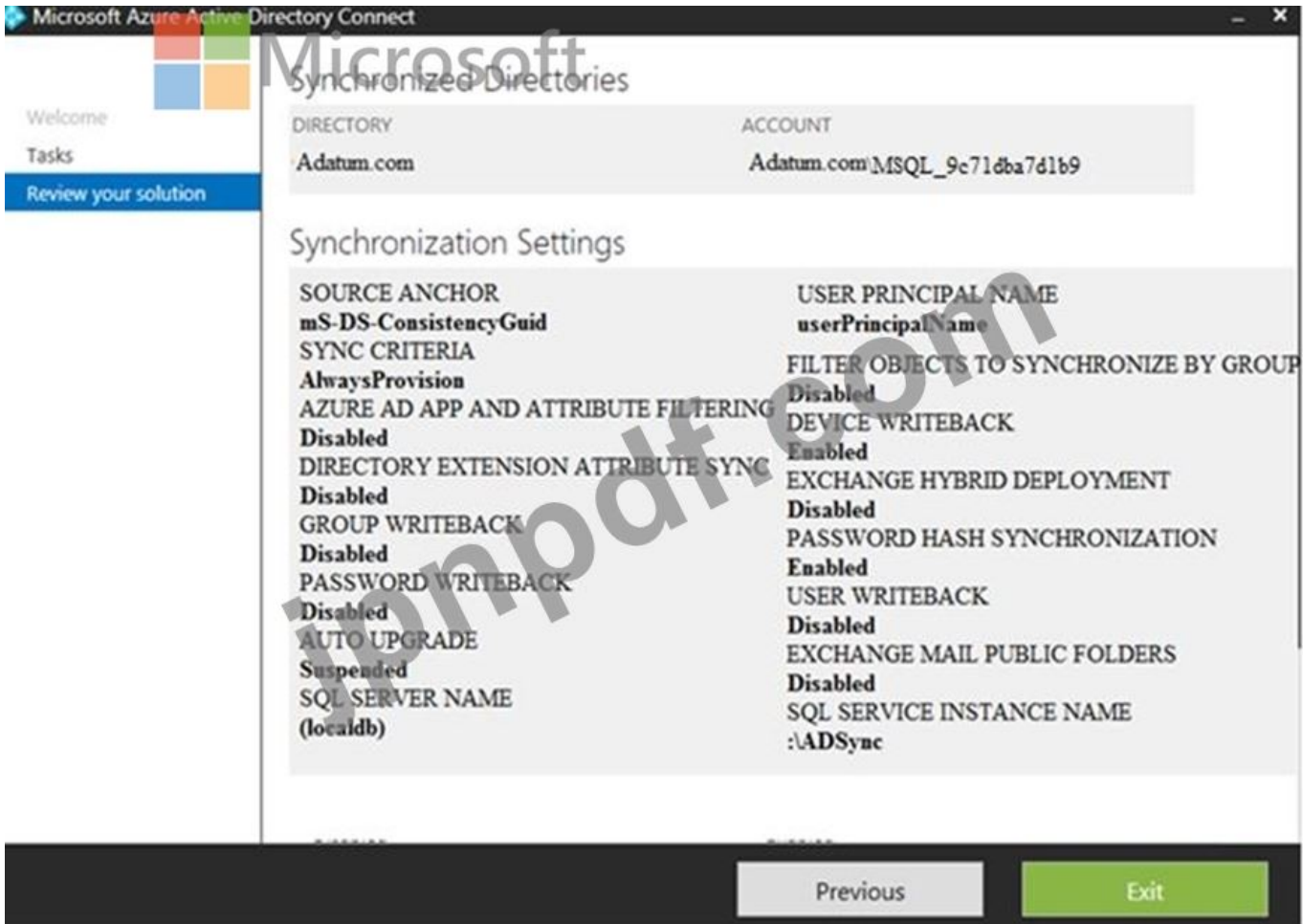
1	V
2	
3	1
4	

説明



最新問題: 4

次の図に示すように、Microsoft Azure Active Directory (Azure AD) Connect を構成します。



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

注: 正しく選択するたびに 1 ポイントの価値があります。

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

Answer:

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

説明

Microsoft

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

最新問題: 5

ユーザーが Microsoft Office 365 ProPlus アプリケーションまたは Android デバイスからドキュメントまたは電子メール メッセージ内のリンクを選択するタイミングを管理するソリューション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す必要があります。

fabrikam.com という名前のドメインへのアクセスをブロックする

ユーザーが fabrikam.com へのリンクを選択したときに情報を保存します。

このタスクを完了するには、Microsoft 365 ポータルにサインインします。

Answer:

安全なリンク ポリシーを構成する必要があります。

Office 365 セキュリティとコンプライアンス管理センターに移動します。

[脅威管理] > [ポリシー] > [安全なリンク] に移動します。

[組織全体に適用するポリシー] セクションで、[デフォルト] を選択し、[編集] アイコンをクリックします。

[次の URL をブロックする] セクションに「f.fabrikam.com」と入力します。これは質問の最初の要件を満たしています。

[電子メール以外のコンテンツに適用する設定] セクションで、[ユーザーが安全なリンクをクリックしたときは追跡しない] チェックボックスをオフにします。これは質問の 2 番目の要件を満たしています。

保存」をクリックして変更を保存します。

参照：

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide>

最新問題: 6

デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。
次の図に示すように、Microsoft OneDrive で共有設定を構成します。

Links Microsoft

Choose the kind of link that's selected by default when users share items.

Default link type

- Shareable: Anyone with the link
- Internal: Only people in your organization
- Direct: Specific people

External sharing

Users can share with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can create shareable links that don't require sign-in

New and existing external users
External users must sign-in

Existing external users
Only users already in your organization's directory

Only people in your organization
No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

Allow or block sharing with people on specific domains

Allow only these domains Contoso.com, Adatum.com [Add domains](#)

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

注: 正しく選択するたびに 1 ポイントの価値があります。

A user who has an email address of user1@fabrikam.com [answer choice]

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

Answer:

A user who has an email address of user1@fabrikam.com [answer choice]

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

説明

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

参考文献:

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

最新問題: 7

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

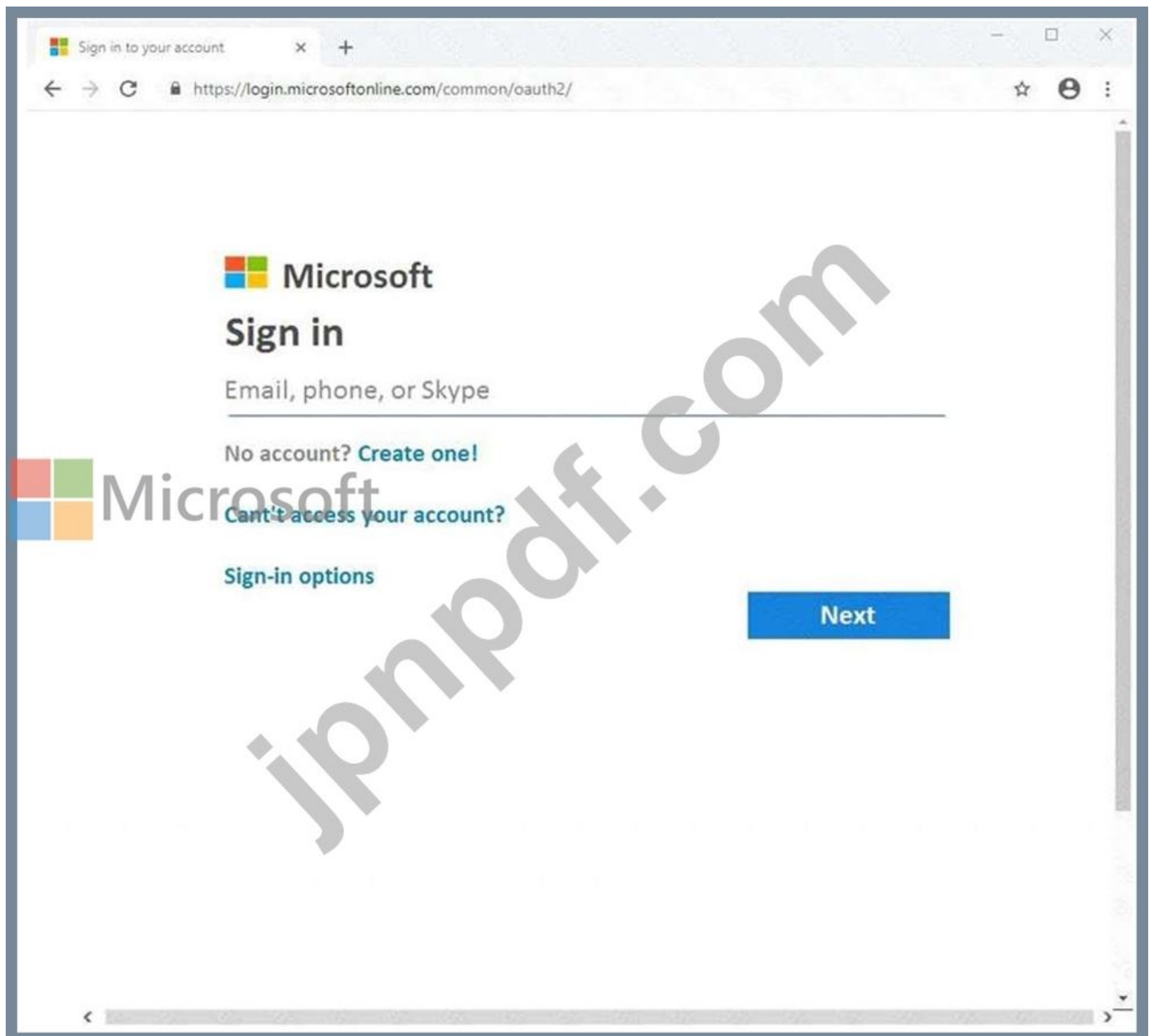
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308

Microsoft



Microsoft



Get your work done
with **Office 365**



jpnpdf.com

Microsoft



Microsoft

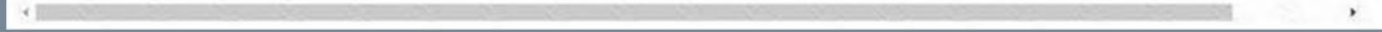
Brainstorm
together in **Word**



Microsoft



Stay on top of what matters with **Outlook**





Access Office 365 apps and documents in one place with

Office.com



Microsoft Office Home | office.com/?auth=2

Contoso electronics | Office 365

Good morning | Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint

OneNote | Skype | Calendar | People | All apps

Recommended

You edited this Jan 15

Excel

Integrated Team Sales Process

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart
lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15

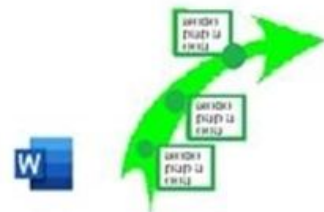


Contoso Electronics Outdoor...

lodse000198.sharepoint.co...



You edited this Jan 15



AD Slogans

lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

↑ Upload and open...

New ▾

Go to OneDrive →



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →

SharePoint

Frequent sites

Following

SM Sales and Marketing

R Retail

Cs Communication Site

SharePoint

Frequent sites

Following

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

Go to SharePoint →

Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

英国データ保護法の対象となるデータを含む電子メールメッセージが、adatum.com という名前の外部ドメインに送信される場合を除き、組織外の受信者に送信されないようにする必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

1. Microsoft 365 管理センターにサインインした後、Exchange 管理センターのコンプライアンス管理に移動します。
2. 「データ損失防止」オプションをクリックします。
3. 新しいカスタム DLP ポリシーを追加するには、(+) プラス ボタンをクリックしてコンテキストメニューを表示します。
4. [新しいカスタム DLP ポリシー] オプションをクリックすると、新しいウィンドウが表示され、ポリシー名、説明、状態、および要件の詳細のモードを入力する必要があります。保存ボタンをクリックしてポリシーを作成し、続行します...
5. 「データ損失防止」画面に戻り、新たにポリシー情報が追加されます。
6. 追加された行をダブルクリックしてポリシーの詳細を開き、図に示すように画面の左側にあるルール オプションをクリックします。
7. (+) プラス ボタンをクリックして、新しいルールを追加します。機密情報を含むメッセージをブロックする」ルールを選択します。
8. 次の画面で、条件、アクション、例外、ルールのアクティブ化および非アクティブ化の日付を追加できます。

new rule

Name:
Sent to scope Outside the organization

*Apply this rule if...

× The recipient is located... Outside the organization

and

× The message contains any of these sensitive information types... Select sensitive information types...

add condition

*Do the following...

× Generate incident report and send it to... Send incident report to: *Select one... with content: Custom content

and

× Notify the sender with a Policy Tip... Block the message

add action

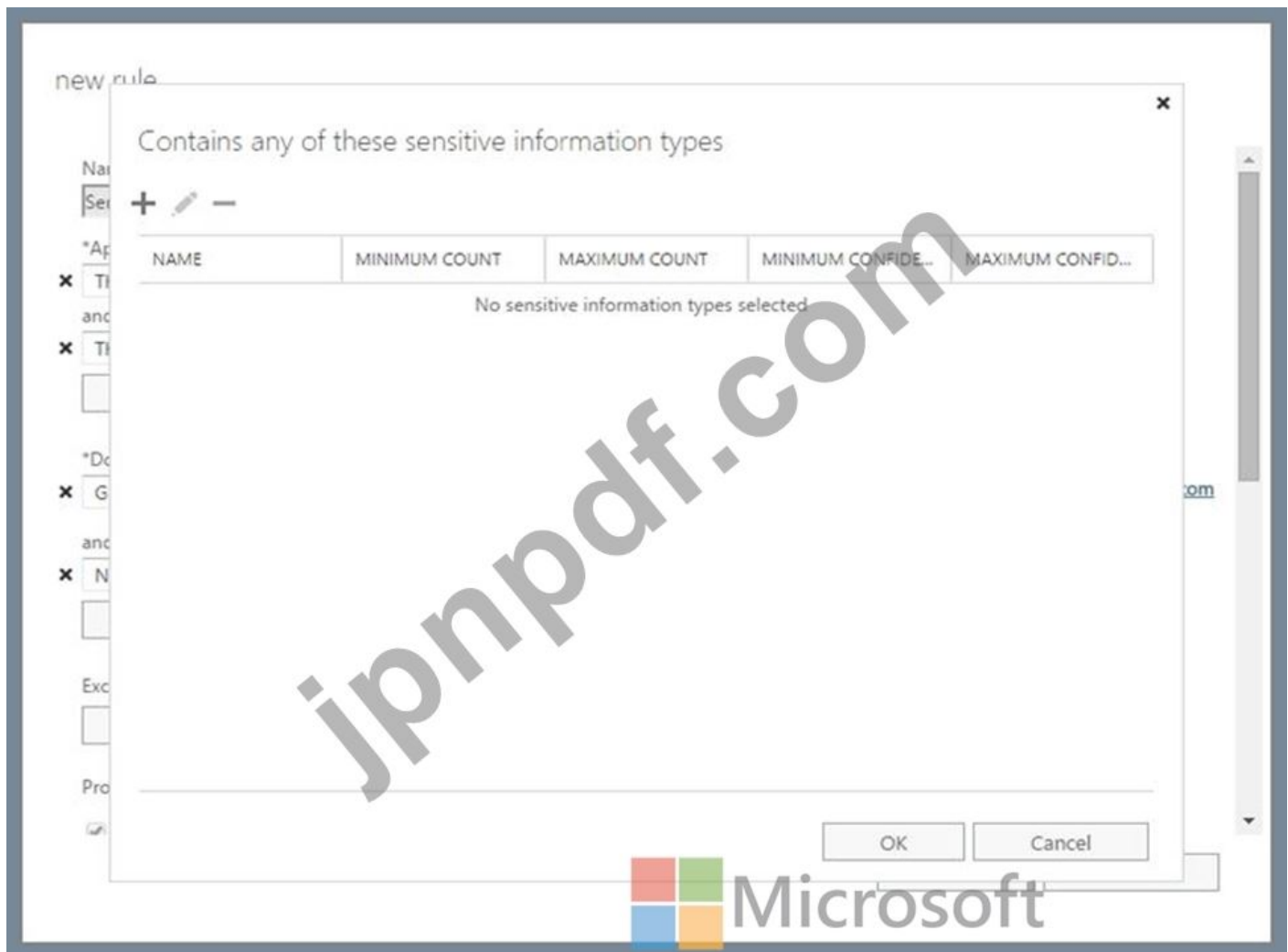
Except if...

add exception

Properties of this rule:

Save Cancel

9. [機密情報の種類を選択] をクリックして、機密情報の詳細を指定します。



10. (+) プラス ボタンをクリックし、次の機密情報の種類を追加します。

* 英国国民保険番号 (NINO)

* 米国/英国のパスポート番号

* スウィフトコード

11. OK」をクリックします。

12. adatum.com ドメインの受信者に対する例外を追加します

13. インシデントレポートの受信者を追加し、OK」をクリックします。

14. 保存」をクリックします。

15. 保存」をクリックします。

参照：

<https://events.collab365.community/configure-data-loss-prevention-policies-in-exchange-online-in-office-365/>

最新問題: 8

デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。

次の図に示すように、Microsoft OneDrive で共有設定を構成します。

Choose the kind of link that's selected by default when users share items.

Default link type

- Shareable: Anyone with the link
- Internal: Only people in your organization
- Direct: Specific people

External sharing

Users can share with:



Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

- Allow or block sharing with people on specific domains
 - Allow only these domains Contoso.com, Adatum.com
 - [Add domains](#)

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

注: 正しく選択するたびに 1 ポイントの価値があります。

A user who has an email address of user1@fabrikam.com [answer choice]

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

Answer:

A user who has an email address of user1@fabrikam.com [answer choice]

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

説明

A user who has an email address of user1@fabrikam.com [answer choice]

Microsoft

If a new guest user is created for user2@contoso.com [answer choice]

cannot access OneDrive content
 can access OneDrive content after a link is created
 must be added to be a group before the user can access shared files

the user cannot access OneDrive content
 the user can access OneDrive content after a link is created
 must be added to a group before the user can access shared files

参考文献:

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

最新問題: 9

Microsoft 365 E5 サブスクリプションをお持ちです。

一部のユーザーは、Microsoft SharePoint Online にアクセスするために認証アプリを使用する必要があります。

SharePoint Online にアクセスするために認証アプリを使用したユーザーを表示する必要があります。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。

あなたは何をするべきか？

- A. セキュリティとコンプライアンス管理センターからレポートをダウンロードします。
- B. Azure Log Analytics からログをクエリします。
- C. セキュリティとコンプライアンス管理センターから、監査ログ検索を実行します。
- D. Azure Active Directory 管理センターのエンタープライズ アプリケーション ブレードから、サインインを表示します。

Answer: D (メッセージを残す)

ユーザー サインイン レポートは、ユーザーのサインイン パターン、1 週間にサインインしたユーザーの数、およびこれらのサインインのステータスに関する情報を提供します。

ノート:

試験ではこの問題にはいくつかのバージョンがあります。この質問には 2 つの正解が考えられません。

1. Azure Active Directory 管理センターのエンタープライズ アプリケーション ブレードから、サインインを表示します。
2. Azure Active Directory 管理センターから、サインインを表示します。

試験で表示される可能性のあるその他の不正解の選択肢には次のものがあります。

1. Azure Active Directory 管理センターのエンタープライズ アプリケーション ブレードから、監査ログを表示します。
2. Azure Active Directory 管理センターから、監査ログを表示します。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

最新問題: 10

Group1 および Group2 という名前の 2 つのグループと、次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Role	Member of
Admin1	Global Administrator	None
User1	Global reader	Group1
User2	Global reader	Group2

次の図に示すように、特権アクセス設定が構成されています。



次の設定を持つ特権アクセス ポリシーがあります。

* ポリシー名: 新しいトランスポート ルール

* ポリシーの種類: タスク

* ポリシーの範囲 交換

※承認タイプ :マニユアル

※承認者グループ :グループ1

User1 は、新しいトランスポート ルール ポリシーへの 2 時間のアクセスを要求します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ]を選択します。

注: 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 

Statements	Yes	No
Admin1 can approve the request.	<input type="radio"/>	<input type="radio"/>
User1 can approve the request.	<input type="radio"/>	<input type="radio"/>
User2 can approve the request.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area 

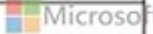
Statements	Yes	No
Admin1 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 11

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

Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を実装します。PIM から、アプリケーション管理者の役割を確認し、次の表に示すユーザーを検出します。

Name	Assignment type
UserA	Permanent
UserB	Eligible 
UserC	Eligible

アプリケーション管理者の役割は、PIM で次の設定を使用するように構成されています。

- * 最大アクティベーション時間: 1 時間
- * 通知: 無効にする
- ※ インシデント/リクエストチケット: 無効
- * 多要素認証: 無効にする
- * 承認が必要: 有効
- * 選択した承認者: 結果はありません

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 12

ワークロード管理者のセキュリティ要件を満たすようにアクセス レビューを構成する予定です。アクセス レビュー ポリシーを作成し、スコープとグループを指定します。他にどのような設定を構成する必要がありますか? 回答するには、回答領域で適切な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。

Set the frequency to:

One time	▼
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	▼
Advanced settings	
Programs	
Reviewers	

Answer:

Set the frequency to:

One time	<input type="checkbox"/>
Weekly	<input checked="" type="checkbox"/>
Monthly	<input type="checkbox"/>

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	<input checked="" type="checkbox"/>
Advanced settings	<input type="checkbox"/>
Programs	<input type="checkbox"/>
Reviewers	<input type="checkbox"/>

説明

Set the frequency to:

One time	<input type="checkbox"/>
Weekly	<input checked="" type="checkbox"/>
Monthly	<input type="checkbox"/>

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	<input checked="" type="checkbox"/>
Advanced settings	<input type="checkbox"/>
Programs	<input type="checkbox"/>
Reviewers	<input type="checkbox"/>

最新問題: 13

Microsoft 365 サブスクリプションをお持ちです。

次の例に示すように、Label1 という名前の保持ラベルを作成します。

Create a label to help users classify their content.

- Name your label
- Label settings
- Review your settings

Review your settings

Name: Label1 [Edit](#)

Descriptions for admins [Edit](#)

Description for users [Edit](#)

Retention [Edit](#)

2 years
Retain and Delete
Based on when it was created
Use Label to classify content as a "Record"


[Back](#) [Create this label](#) [Cancel](#)

Label1 を SharePoint サイトに公開します。

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


注: 正しく選択するたびに 1 ポイントの価値があります。

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].	<input type="text"/>
	▼ never delete the file. delete the file before January 1, 2021. delete the file after January 1, 2021.
If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].	<input type="text"/>
	▼ always remain in the library. remain in the library until you delete the file. be deleted automatically on March 15, 2021.



Answer:

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].	<input type="text"/>
	▼ never delete the file. delete the file before January 1, 2021. delete the file after January 1, 2021.
If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].	<input type="text"/>
	▼ always remain in the library. remain in the library until you delete the file. be deleted automatically on March 15, 2021.



参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/labels>

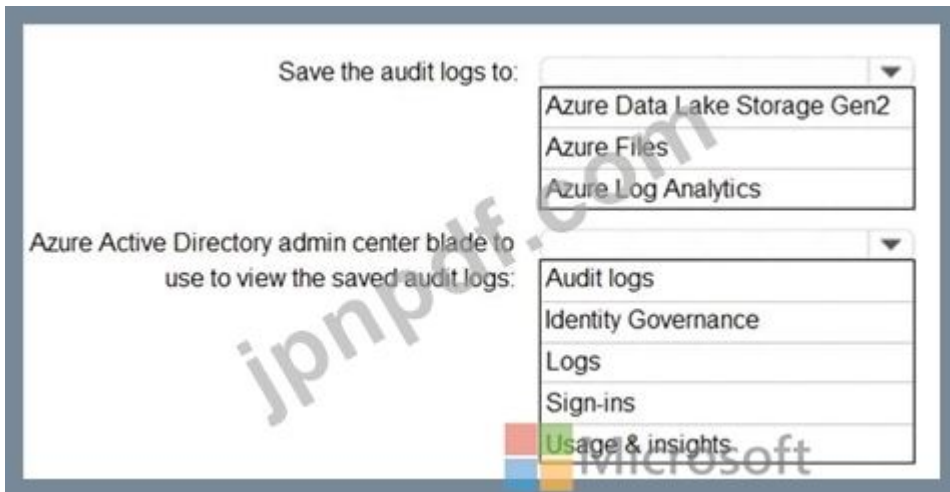
最新問題: 14

Microsoft 365 テナントがあります。

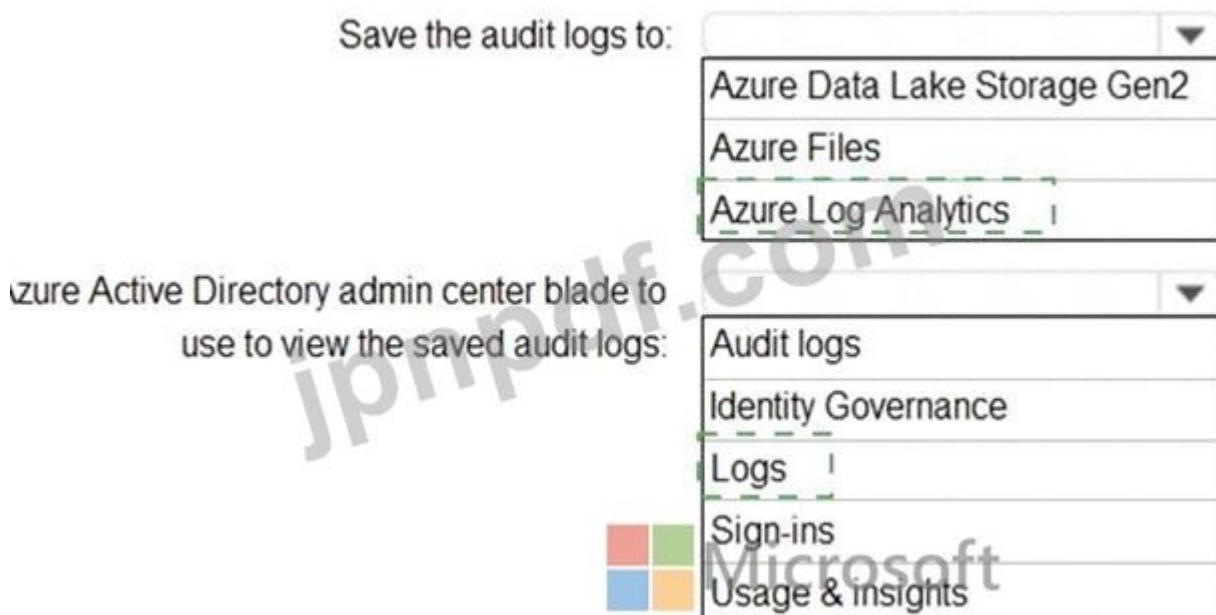
Azure Active Directory (Azure AD) 監査ログは 2 年間保持する必要があります。管理者は、Azure Active Directory 管理センターを使用して監査ログ情報をクエリできる必要があります。

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。

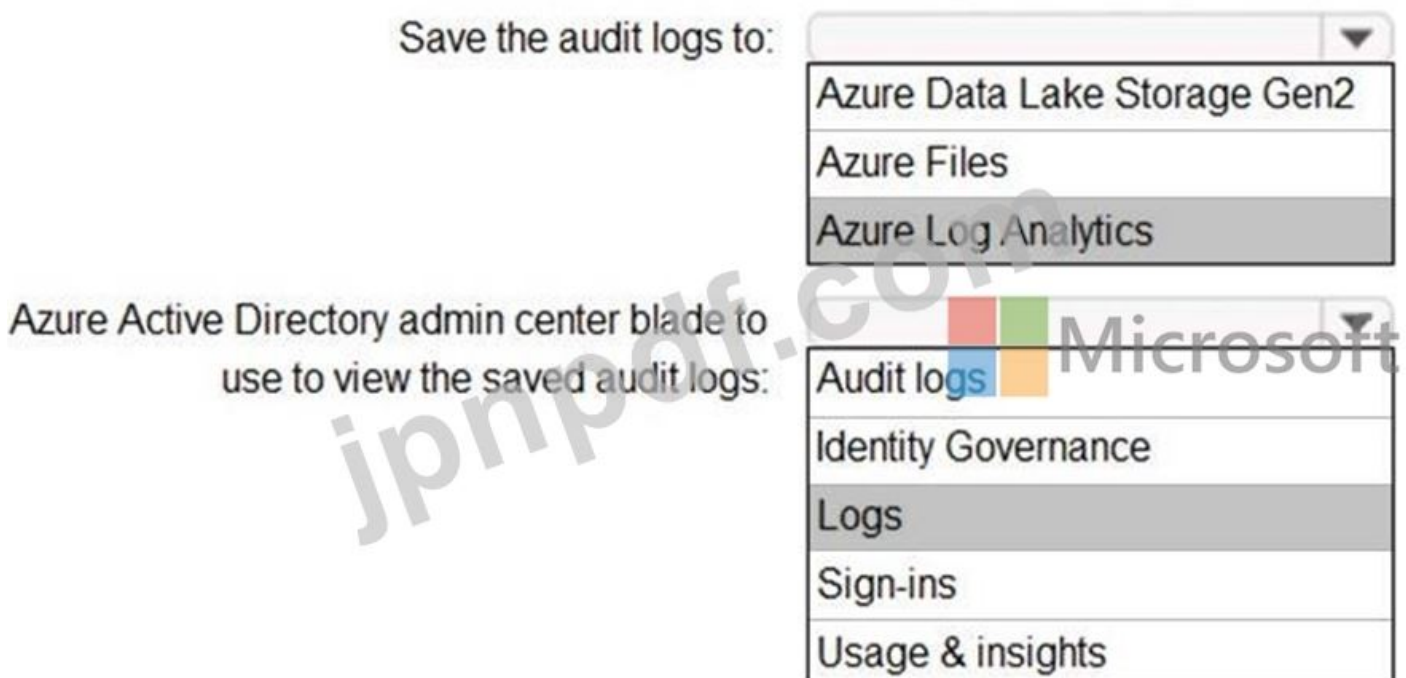


Answer:



説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーションの説明が自動生成される



参照 :

<https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-anal>

最新問題: 15

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Microsoft 365 E5 サブスクリプションがあります。

contoso.com の Azure AD Identity Protection アラートは、次のように構成されています。

 Save  Discard  Download


Alert on user risk level at or above

Low **Medium** High

Emails are sent to the following users. ⓘ

INCLUDED

1 selected

 Add additional emails to receive alert notifications (Preview). ⓘ

User1 という名前のユーザーは、Azure AD Identity Protection からアラートを受信するように構成されています。

次の表に示すように、contoso.com にユーザーを作成します。

Name	Role
User2	Security reader
User3	User administrator
User4	None
User5	None

ユーザーは、次の表に示すサインインを実行します。

Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>

説明

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>

ボックス 1: いいえ

User1 は、中以上に分類される 2 つのアラートを受信します。

感染したデバイスからのサインインは低として分類されます。このリスク検出では、ユーザーのデバイスではなく、IP アドレスが識別されます。

複数のデバイスが1つのIPアドレスの背後にあり、その一部のみがボットネットワークによって制御されている場合、他のデバイスからのサインインによってこのイベントが不必要にトリガーされる可能性があるため、このリスク検出は「低」に分類されます。

ボックス 2: いいえ

User2 は、中以上に分類される2つのアラートを受信します。

電子メールアラートは、すべてのグローバル管理者、セキュリティ管理者、およびセキュリティ閲覧者に送信されます。感染したデバイスからのサインインは低として分類されます。このリスク検出では、ユーザーのデバイスではなく、IPアドレスが識別されます。

複数のデバイスが1つのIPアドレスの背後にあり、その一部のみがボットネットワークによって制御されている場合、他のデバイスからのサインインによってこのイベントが不必要にトリガーされる可能性があるため、このリスク検出は「低」に分類されます。

ボックス 3: いいえ

User3 は変更を受け取りません。

電子メールアラートは、すべてのグローバル管理者、セキュリティ管理者、およびセキュリティ閲覧者に送信されます。

参照：

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

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-r>

最新問題: 16

ユーザーは次のファイルを Microsoft OneDrive に保存します。

- * ファイル.docx
- * 重要ファイル.docx
- * ファイル_重要.docx

次の例に示すフィルターを持つ Microsoft Cloud App Security ファイル ポリシー Policy1 を作成します。

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

File name contains words File

Apply to: all files

Apply to: all file owners 

Policy1 はどのファイルに適用されますか?

- A. ファイル_重要.docx のみ
- B. ファイル.docx、重要ファイル.docx、およびファイル_重要.docx
- C. ファイル.docx のみ
- D. 重要ファイル.docx のみ
- E. File.docx および File_Minimum.docx のみ

Answer: B ([メッセージを残す](#))

参照 :

<https://docs.microsoft.com/en-us/cloud-app-security/file-filters>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 17


Azure ATP センサーをドメインコントローラーにインストールします。

Domain Admins グループにメンバーを追加します。Azure ATP のタイムラインを表示すると、メンバーシップの変更に関する情報が欠落していることがわかります。

Azure ATP レポートのセキュリティ要件を満たす必要があります。

何を設定すればよいでしょうか? 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。

Policy to edit:  Microsoft ▼

Default Domain Controllers Policy
Default Domain Policy
A local policy on one domain controller


Audit setting to configure: ▼

Audit User Account Management
Audit Computer Account Management
Audit Other Account Management Events
Audit Security Group Management

Answer:

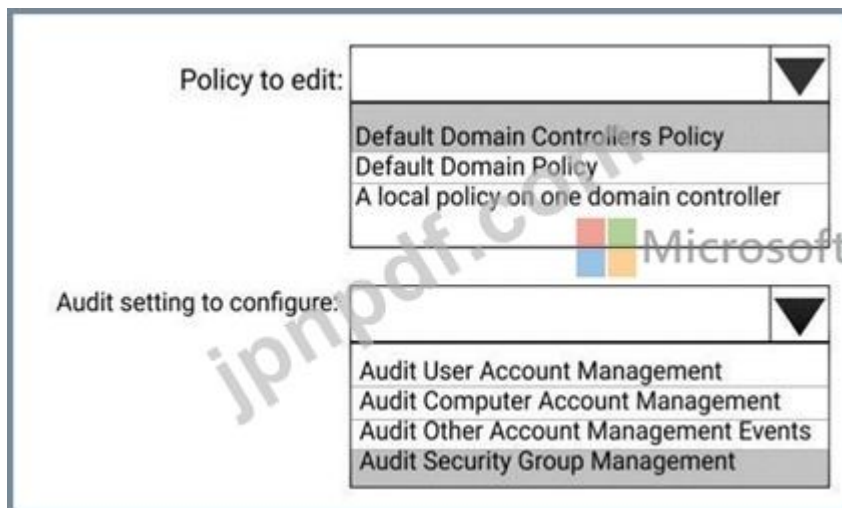
Policy to edit: ▼

Default Domain Controllers Policy
Default Domain Policy
A local policy on one domain controller

Audit setting to configure:  Microsoft ▼

Audit User Account Management
Audit Computer Account Management
Audit Other Account Management Events
Audit Security Group Management

説明



参考文献:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy>

最新問題: 18

Group3を作成する必要があります。

グループを作成するには2つの方法がありますか?

- A. Microsoft 365 管理センターの Office 365 グループ
- B. Microsoft 365 管理センターのメールが有効なセキュリティ グループ
- C. Microsoft 365 管理センターのセキュリティ グループ
- D. Microsoft 365 管理センターの配布リスト
- E. Azure AD 管理センターのセキュリティ グループ

Answer: A,D (メッセージを残す)

トピック 3、Contoso, Ltd

既存の環境

インフラストラクチャー

ネットワークには、Microsoft Azure Active Directory (Azure AD) テナントに同期されている contoso.com という名前の Active Directory ドメインが含まれています。パスワードライトバックが有効になっています。

ドメインには、Windows Server 2016 を実行するサーバーが含まれています。ドメインには、Windows 10 Enterprise を実行するラップトップおよびデスクトップコンピューターが含まれています。

各クライアントコンピュータには1つのボリュームがあります。

各オフィスはNATデバイスを使用してインターネットに接続します。オフィスのIPアドレスは次の表に示されています。

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

名前付きロケーションは、次の表に示すように Azure AD で定義されます。

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

[多要素認証] ページから、198.35.3.0/24 のアドレス スペースが信頼できる IP リストに定義されます。

Azure Multi-Factor Authentication (MFA) は、財務部門のユーザーに対して有効になっています。テナントには、次の表に示すユーザーが含まれます。

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

テナントには、次の表に示すグループが含まれています。

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

カスタマー ロックボックスは Microsoft 365 で有効になっています。

Microsoft Intune の構成

Intune に登録されているデバイスは、次の表に示すように構成されています。

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

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

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

デバイス コンプライアンス ポリシーには、次の表に示す割り当てがあります。

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

[コンプライアンス ポリシーが割り当てられていないデバイスをマークする] 設定が [準拠] に設定されます。

要件

技術的要件

Contoso は次の技術要件を特定します。

最小特権の原則を使用する

User1 がレポート閲覧者の役割をユーザーに割り当てられるようにする

User6 がカスタマー ロックボックスの要求をできるだけ早く承認するようにする User9 が

Azure AD Privileged Identity Management を実装できるようにする

最新問題: 19

Microsoft 365 サブスクリプションをお持ちです。セキュリティとコンプライアンス管理センターから、次の表に示す保持ポリシーを作成します。

Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

次の図に示すように構成されている場合の Policy1。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 1 years ▾

No, just delete content that's older than ⓘ

1 years ▾

Delete the content based on when it was created ▾ ⓘ

Need more options?

Use advanced retention settings ⓘ

Back

Next

Cancel

Policy2 は次のように構成されています。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 3 years ▾

Retain the content based on when it was created ▾ ⓘ

Do you want us to delete it after this time?

Yes No

No, just delete content that's older than ⓘ

1 years ▾

Need more options?

Use advanced retention settings ⓘ

Back  Next Cancel

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

Answer Area

Yes	No
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

- If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019
- If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019
- If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022

Answer:

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input checked="" type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input checked="" type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input checked="" type="radio"/>

説明

Answer Area



Microsoft

Yes

No

If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019

If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019

If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen->

最新問題: 20

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Microsoft 365 サブスクリプションがあります。


次の要件を満たす Azure AD Privileged Identity Management (PIM) ソリューションを推奨する必要があります。

* セキュリティ管理者ロールがアクティブ化されると、管理者に通知する必要があります。

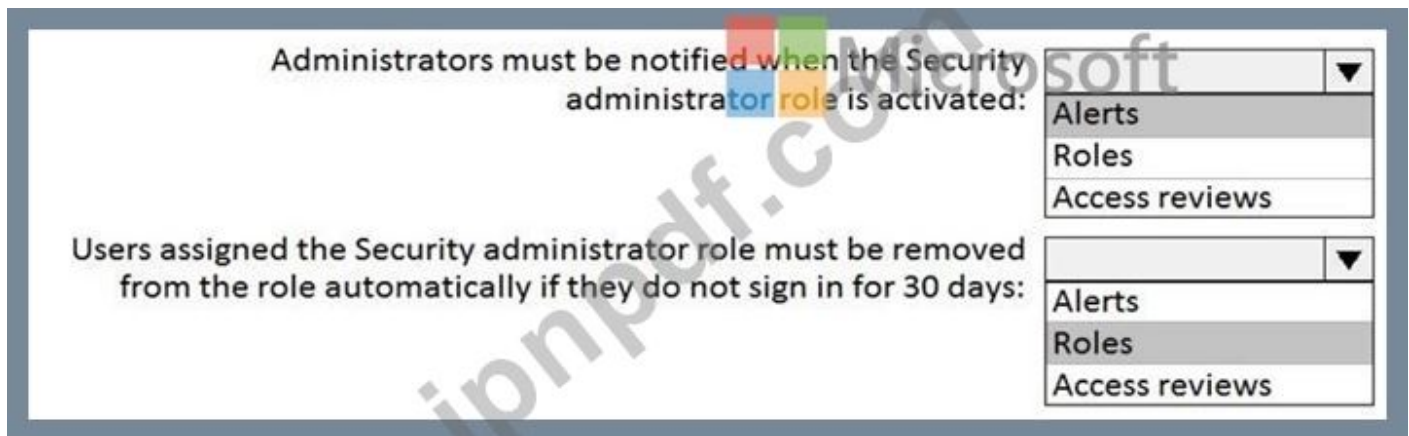
* セキュリティ管理者ロールを割り当てられたユーザーは、30 日間サインインしない場合、そのロールから自動的に削除される必要があります。

各要件に対してどの Azure AD PIM 設定を構成することを推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

	Administrators must be notified when the Security administrator role is activated:	<input type="radio"/>	▼
		Alerts	
		Roles	
		Access reviews	
	Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days:	<input type="radio"/>	▼
		Alerts	
		Roles	
		Access reviews	

Answer:



参照 :

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-config>

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-change>

最新問題: 21

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



ExamUser

Sign in

jnpdf.com

必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

Exchange Online の電子メール メッセージと SharePoint Online のドキュメントが 8 年間保持されるようにする必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

注意: 当社の目的上、保存期間は 8 年間となります。Exchange Online で電子メール メッセージを保持する

には:

ステップ 1: 保持タグを作成する

1. Exchange 管理センターに移動します。
2. コンプライアンス管理 + に移動します
3. 次のオプションのいずれかを選択します。

* メールボックス全体に自動的に適用 (デフォルト): デフォルトのポリシー タグ (DPT) を作成するには、このオプションを選択します。DPT を使用して、メールボックス内のすべてのアイテムに適用されるデフォルトの削除ポリシーとデフォルトのアーカイブ ポリシーを作成できます。

* 特定のフォルダーに自動的に適用: 受信トレイや削除済みアイテムなどの既定のフォルダーに保持ポリシー タグ (RPT) を作成するには、このオプションを選択します。

* ユーザーがアイテムとフォルダーに適用 (個人): 個人タグを作成するには、このオプションを選択します。これらのタグを使用すると、Outlook および Outlook on the web (以前の Outlook Web App) ユーザーは、親フォルダーまたはメールボックス全体に適用される設定とは異なるアーカイブまたは削除の設定をメッセージまたはフォルダーに適用できます。

4. [新しい保持タグ] ページのタイトルとオプションは、選択したタグの種類によって異なります。次のフィールドに入力します。

* 名前: 保持タグの名前を入力します。タグ名は表示目的であり、タグが適用されるフォルダーやアイテムには影響しません。ユーザーにプロビジョニングした個人タグは、Outlook および Web 上の Outlook で利用できることを考慮してください。

* このタグを次のデフォルト フォルダーに適用します: このオプションは、[特定のフォルダーに自動的に適用] を選択した場合にのみ使用できます。

* 保持アクション: アイテムが保持期間に達した後に実行されるアクションを次のいずれか選択します。

* 削除して回復を許可: アイテムを削除しますが、Outlook または Web 上の Outlook の [削除済みアイテムの回復] オプションを使用してユーザーがアイテムを回復できるようにするには、このアクションを選択します。アイテムは、メールボックス データベースまたはメールボックス ユーザーに対して構成された削除済みアイテムの保存期間に達するまで保持されます。

* 完全に削除: メールボックス データベースからアイテムを完全に削除するには、このオプションを選択します。

* アーカイブに移動: このアクションは、DPT または個人タグを作成している場合にのみ使用できます。アイテムをユーザーのインプレース アーカイブに移動するには、このアクションを選択します。

* 保存期間: 次のオプションのいずれかを選択します。

* 決してしない: アイテムを決して削除したり、アーカイブに移動したりしないことを指定するには、このオプションを選択します。

* アイテムが次の経過日数 (日数) に達した場合: このオプションを選択し、アイテムが移動または削除されるまでにアイテムを保持する日数を指定します。カレンダーとタスクを除くすべてのサポートされているアイテムの保存期間は、アイテムが受信または作成された日から計算されます。カレンダーとタスクのアイテムの保存期間は終了日から計算されます。

* コメント: このオプションのフィールドを使用して、管理上のメモやコメントを入力します。このフィールドはユーザーには表示されません。

ステップ 2: 保持ポリシーを作成する

1. [コンプライアンス管理] に移動します [追加 +]

2. [新しい保持ポリシー] で、次のフィールドに入力します。

* 名前: 保持ポリシーの名前を入力します。

* 保持タグ: [追加 +] をクリックして、この保持ポリシーに追加するタグを選択します。

保持ポリシーには次のタグを含めることができます。

* アーカイブに移動アクションを持つ 1 つの DPT。

* 削除および回復の許可または完全に削除のアクションを持つ 1 つの DPT。

* 削除および回復の許可または完全に削除のアクションを含むボイス メール メッセージ用の 1 つの DPT。

* アイテムを削除するには、受信トレイなどのデフォルト フォルダーごとに 1 つの RPT が必要です。

* 任意の数の個人タグ。

ステップ 3: メールボックス ユーザーにアイテム保持ポリシーを適用する

アイテム保持ポリシーを作成したら、それをメールボックス ユーザーに適用する必要があります。異なるユーザーのセットに異なる保持ポリシーを適用できます。

* [受信者] > [メールボックス] に移動します。

* リスト ビューでは、Shift キーまたは Ctrl キーを使用して複数のメールボックスを選択します。

* 詳細ペインで、[その他のオプション] をクリックします。

* [保持ポリシー] で、[更新] をクリックします。

* [保持ポリシーの一括割り当て] で、メールボックスに適用する保持ポリシーを選択し、[保存] をクリックします。

SharePoint Online でドキュメントを保持する場合

セキュリティとコンプライアンス管理センターにアクセスする

1. Office 365 管理センターに移動します。

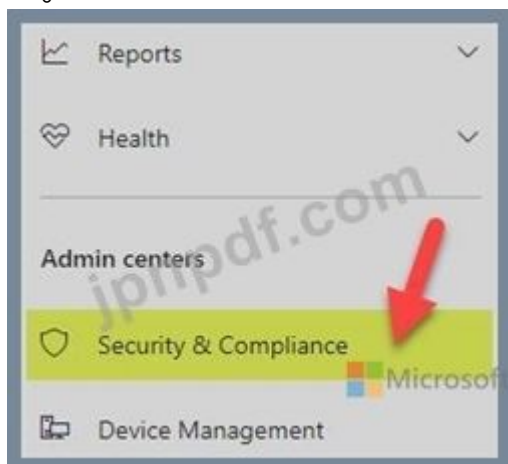


Office 365

Apps

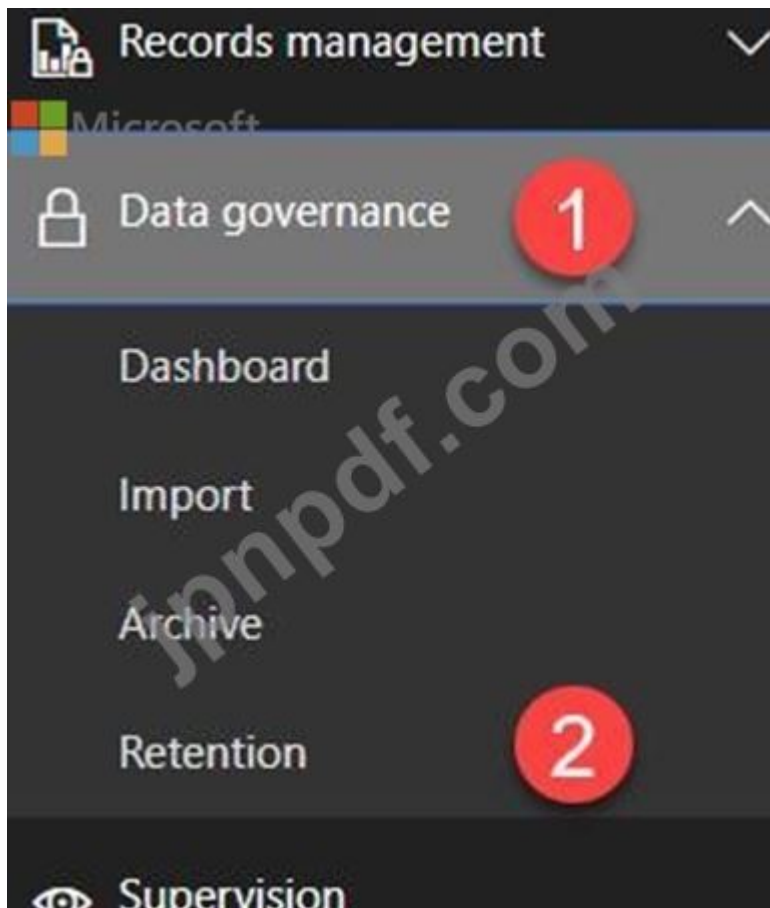


2. 利用可能な管理センターのリストから、「セキュリティとコンプライアンス」をクリックします。



SharePoint サイトで保持ポリシーを作成して公開する方法

セキュリティとコンプライアンス管理センターに移動したので、SharePoint サイトで保持ポリシーを作成して公開する準備が整いました。



1. [作成] ボタンをクリックして、新しい保持ポリシーを作成します。

Home > Retention

Email, documents, Skype and Teams conversations. Your users generate a lot of content every day. Take control of it by setting up retention policies to get rid of what you don't. [Learn more about retention](#)

Labels

Create labels to let users manually classify and retain their own content (email, docs, folders, and more). You can also auto-apply labels to specific content.

Label policies

Create label policies to publish or automatically apply existing labels to your users apps (Outlook, SharePoint, OneDrive, and more).

+ Create Refresh Search ...

<input type="checkbox"/> Name	Created by	Last modified
<input type="checkbox"/> 3-day retention	Gregory Zelfond	September 9, 2019

2. ポリシーに名前と説明を付けます。

Create a policy to retain what you want and get rid of what you don't.

- Name your policy
- Settings
- Choose locations
- Review your settings

Name your policy

Name * ⓘ

Retain for 2 days, then delete 1

Description ⓘ

This policy retains documents for 2 days after they were last modified and then deletes the 2

3

Next Cancel

3. 次の画面では、ロジックを設定します。コンテンツを保持する日数、月数、または年数を構成したり、計算 (保持期間) を作成日または最終変更日から計算するかどうかを指定したりできます。最後に、保存期間の終了後にコンテンツを保持するか削除するかを指定することもできます。次へ」をクリック

Create a policy to retain what you want and get rid of what you don't.

- Name your policy
- Settings
- Choose locations
- Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 2 days 1

Retain the content based on when it was last modified ⓘ 2

Do you want us to delete it after this time? ⓘ

Yes No 3

At this time, creating a policy to delete Teams content that's less than 30 days old is not supported. If you want this policy to apply to Teams content, specify a retention period that's equal to or more than 30 days.

No, just delete content that's older than ⓘ

1 years

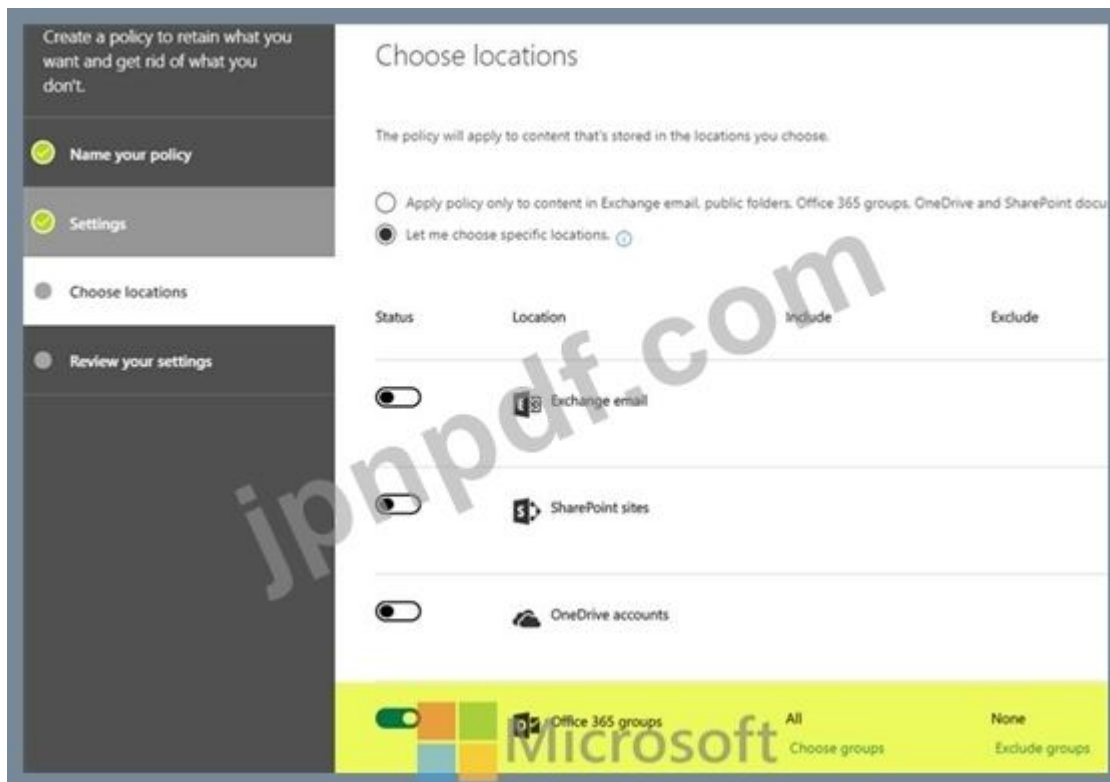
Need more options?

Use advanced retention settings ⓘ

4

Back Next Cancel

4. 次の画面で、ポリシーを適用する場所を選択します。これは、電子メール (Exchange)、SharePoint サイト、OneDrive アカウント、および Office 365 グループに適用できます。



5. 私の場合、単一の Office 365 グループ サイトにポリシーを適用しました。



6. 最後の画面で、設定を確認して「このポリシーを作成」ボタンをクリックする必要があります。下部に表示されるメッセージに注意することが重要です。前の手順で設定したロジックに従ってポリシーが有効になるとすぐに、コンテンツが削除される可能性があることが警告されます。

Create a policy to retain what you want and get rid of what you don't.

- ✓ Name your policy
- ✓ Settings
- ✓ Choose locations

● Review your settings



Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name Edit

Retain for 2 days, then delete

Description Edit

This policy retains documents for 2 days after they were last modified and then deletes them

Applies to content in these locations Edit

SharePoint sites

Settings Edit

Retention period

Keep content, and delete it if it's older than 2 days

⚠ Content that's currently older than this will be deleted after you turn on the policy.

Back

Save for later

Create this policy

Cancel

参考文献:

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-re>

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-reten>

<https://sharepointmaven.com/how-to-set-a-retention-policy-on-a-sharepoint-site/>

最新問題: 22

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

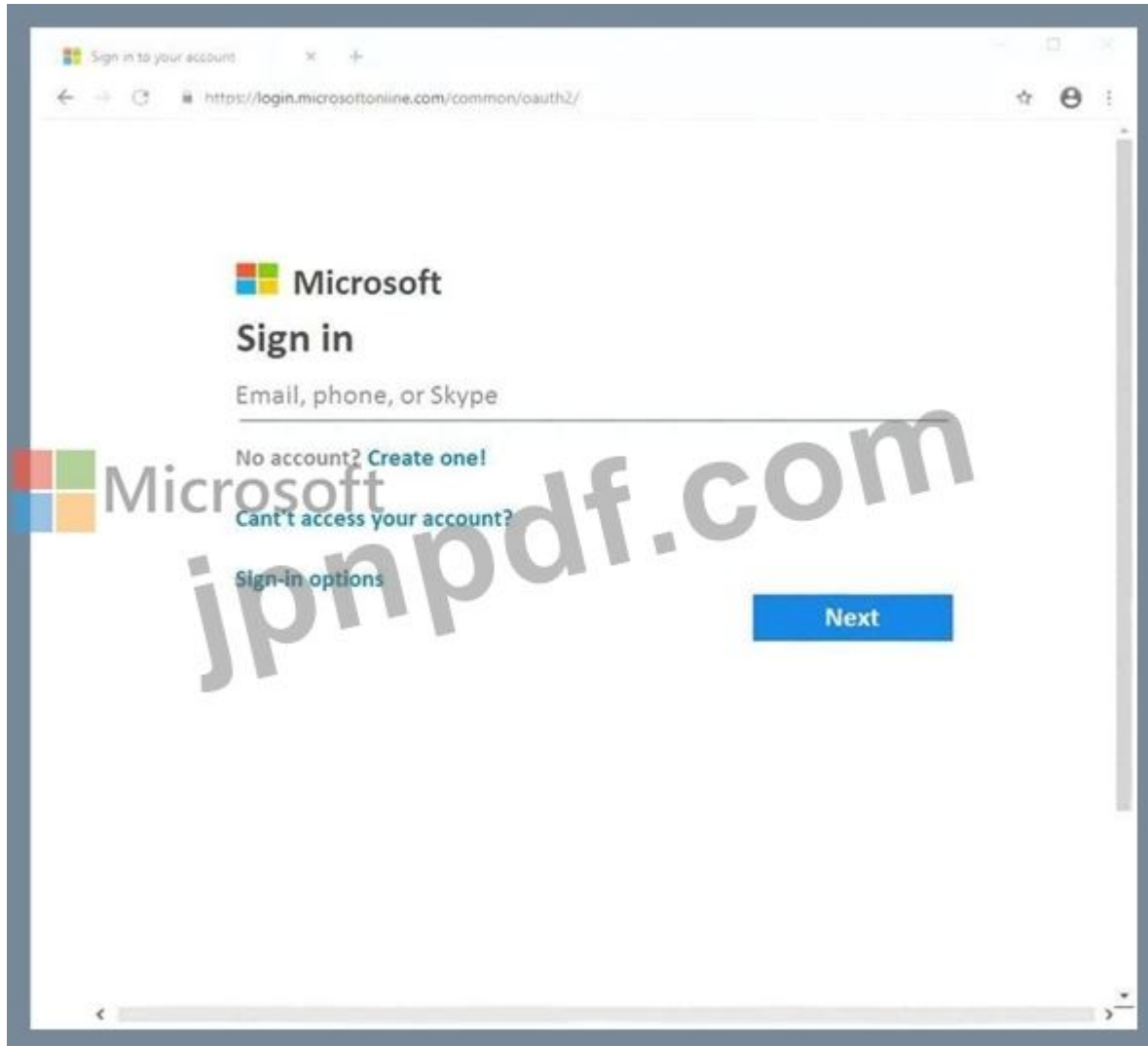
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

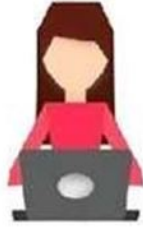
Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308





jpnpdf.com

Brainstorm
together in **Word**





jpnpdf.com

Stay on top of what matters with Outlook



Microsoft



Microsoft



Access Office 365 apps and documents in one place with **Office.com**



jbnpdf.com

Good morning

Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint | OneNote | Skype | Calendar | People | All apps

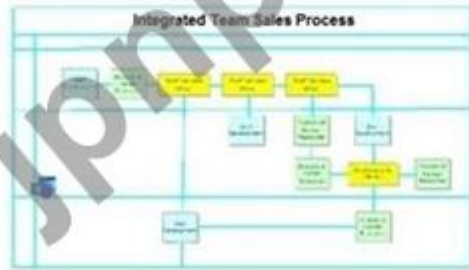
Recommended

You edited this Jan 15



Excel

You edited this Jan 15



Sales Process

lodse000198.sharepoint.co...

You edited this Jan 15



Org Chart

lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recommended



You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

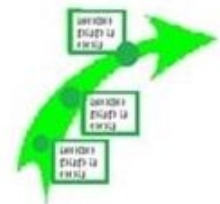
You edited this Jan 15

Ad Slogans



AD Slogans

lodse000198.sharepoint.co...



Recent | Pinned | Shared with me | Discover

Recent Pinned Shared with me Discover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

↑ Upload and open...

New ▾

Go to OneDrive →



Recent Pinned Shared with me Discover



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →

SharePoint

Frequent sites Following

SM Sales and Marketing

R Retail

Cs Communication Site

Go to SharePoint →

SharePoint

Frequent sites **Following**

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

Allan Deyoung という名前のユーザーのメールボックスを保留する電子情報開示ケースを作成する必要があります。保留には、件名に「merger」または「Contoso」という単語が含まれる電子メールメッセージを保持する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

1. セキュリティ & コンプライアンス センターの [電子情報開示] に移動し、[ケースの作成] をクリックします。
2. [新しいケース] ページで、ケースに名前を付け、必要に応じて説明を入力し、[保存] をクリックします。ケース名は組織内で一意である必要があります。

新しいケースは、電子情報開示ページのケースのリストに表示されます。ケース名の上にカーソルを置くと、ケースのステータス (アクティブまたはクローズ)、ケースの説明 (前のステップで作成されたもの)、ケースが最後に変更された日時など、ケースに関する情報が表示されます。そしてそれを変えたのは誰なのか。

電子情報開示ケースの保留を作成するには:

1. セキュリティ/コンプライアンス センターで、[電子情報開示] > [電子情報開示] をクリックして、組織内のケースのリストを表示します。
2. 保留を作成するケースの横にある [開く] をクリックします。
3. ケースのホームページで、保留」タブをクリックします。

4. [保留] ページで、[作成] をクリックします。
5. [保留に名前を付ける] ページで、保留に名前を付けます。保留の名前は組織内で一意である必要があります。

Name your hold

Name *

Enter a friendly name

Description

Enter a friendly description for your policy

Microsoft

Next Cancel

6. (オプション) [説明] ボックスに、保留の説明を追加します。

7. 「次へ」をクリックします。

8. 保留するコンテンツの場所を選択します。メールボックス、サイト、パブリック フォルダを保留にすることができます。

Choose locations

Location	Include
Exchange email	None Choose users, groups, or teams
Office 365 group email	<input type="checkbox"/> A
Skype for Business	
Teams messages	<input type="checkbox"/> Microsoft
To-Do	
Yammer conversations	
SharePoint sites	None Choose sites
OneDrive accounts	<input type="checkbox"/> B
Office 365 group sites	
Teams sites	
Yammer networks	
Exchange public folders	None <input type="checkbox"/> C

Back Next Cancel

- * 電子メールの交換 - [ユーザー、グループ、またはチームの選択] をクリックし、次に [ユーザー、グループ、またはチームの選択] をクリックします。
 - * また、保留するメールボックスを指定します。検索ボックスを使用して、保留するユーザーのメールボックスと配布グループを検索します (グループメンバーのメールボックスを保留する場合)。Microsoft チーム、Yammer グループ、または Office 365 グループに関連付けられたメールボックスを保留することもできます。ユーザー、グループ、チームのチェック ボックスをオンにし、[選択] をクリックして、[完了] をクリックします。
- ノート

[ユーザー、グループ、またはチームの選択] をクリックして保留にするメールボックスを指定すると、表示されるメールボックス ピッカーは空になります。これはパフォーマンスを向上させるための設計によるものです。このリストにユーザーを追加するには、検索ボックスに名前 (最低 3 文字) を入力します。

9. クエリベースの保持を設定したら、[次へ] をクリックします。

10. 設定を確認し、[この保留を作成] をクリックします。

参照：

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-cases?view=o365-worldwide#step-4-pla>

最新問題: 23

Microsoft 365 E5 サブスクリプションとハイブリッド Microsoft Exchange Server 組織があります。

Executive という名前のグループの各メンバーには、オンプレミスメールボックスがあります。エグゼクティブグループのみ

メンバーは多要素認証 (MFA) が有効になっています。研究というグループの各メンバーは Exchange Online のメールボックス。

Microsoft Office 365 攻撃シミュレーターを使用して、攻撃者を基準とするピアフィッシング攻撃をモデル化する必要があります。

研究グループのメンバー

あなたが偽装しようとしている電子メールアドレスは、エグゼクティブグループのメンバーに属しています。

あなたは最初に何をすればいいですか？

A. Azure ATP 管理センターから、プライマリワークスペース設定を構成します。

B. Microsoft Azure ポータルから、Azure AD Identity Protection でユーザー リスク設定を構成します。

C. 研究グループのメンバーに対して MFA を有効にする

D. Executive グループのメンバーを Exchange Online に移行します。

Answer: C (メッセージを残す)

説明/参照：

参照：

<https://docs.microsoft.com/ja-jp/office365/securitycompliance/攻撃シミュレーター>

最新問題: 24

Microsoft 365 テナントがあります。

ユーザー属性は、会社の人事 (HR) システムから Azure Active Directory (Azure AD) に同期されません。

同社には 4 つの部門があり、それぞれに独自の Microsoft SharePoint Online サイトがあります。

各サイトには、それぞれの部門のユーザーのみがアクセスする必要があります。

次の要件を持つアクセス管理ソリューションを設計しています。

ユーザーは、自分の部門のセキュリティ グループに自動的に追加される必要があります。
すべてのセキュリティ グループ所有者は、四半期に 1 回、自分の部門内のユーザーのみが自分の
グループに属していることを確認する必要があります。

要件を満たすためにどのコンポーネントを推奨する必要がありますか? 回答するには、適切なコ
ンポーネントを正しい要件にドラッグします。各コンポーネントは 1 回だけ使用することも、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
で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

Components

- Access packages
- Access reviews
- Azure AD Privileged Identity Management (PIM) role assignments
- Conditional access policies
- Data loss prevention (DLP) policies
- Groups that have a Membership type of Assigned
- Groups that have a Membership type of Dynamic User

Answer Area

Users must be automatically added to the security group for their department.

Group owners must verify membership of departmental groups.

Components

Components

Answer:

Components

- Access packages
- Access reviews
- Azure AD Privileged Identity Management (PIM) role assignments
- Conditional access policies
- Data loss prevention (DLP) policies
- Groups that have a Membership type of Assigned
- Groups that have a Membership type of Dynamic User

Answer Area

Users must be automatically added to the security group for their department:

Group owners must verify membership of departmental groups:

Groups that have a Membership type of Assigned

Access reviews

参照 :

<https://cloudbuild.co.uk/tag/create-a-dynamic-security-group-in-azure-ad/>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

最新問題: 25

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

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

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

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

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

Policy1 を適用する必要があります。

どのグループに Policy1 を適用できますか? 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: 正しく選択するたびに 1 ポイントの価値があります。

On-premises Active Directory groups:

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

Azure AD groups:

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

Answer:

On-premises Active Directory groups:

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

Azure AD groups:

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

説明

On-premises Active Directory groups:

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

Azure AD groups:

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

参照 :

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

最新問題: 26

User 1 と User2 という名前のユーザーを含む Microsoft 165 ES サブスクリプションをお持ちですか？

次の表に示す監査ログの保存要件があります。

User	Action	Retention period
User1	Rename a Microsoft SharePoint Online site.	12 months
User1	Perform all actions in Microsoft Dynamics 365.	6 months
User2	Create a Microsoft SharePoint Online site collection.	12 months
User2	Perform all Microsoft Exchange Online administrative actions.	10 years

要件を満たすために監査保持ポリシーを作成する必要があります。ソリューションでは、コストとポリシーの数を最小限に抑える必要があります。

作成する必要がある監査保持ポリシーの最小数はどれくらいですか？

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

Answer: B ([メッセージを残す](#))

最新問題: 27

ハイブリッド Microsoft 365 環境があります。すべてのコンピューターは Windows 10 を実行し、Microsoft Intune を使用して管理されます。

準拠としてマークされた Windows 10 コンピューターのみがオンプレミス ネットワークへの VPN 接続を確立できるようにする Microsoft Azure Active Directory (Azure AD) 条件付きアクセス ポリシーを作成する必要があります。

まず何をすべきでしょうか？

- A. Azure Active Directory 管理センターから、新しい証明書を作成します。
- B. Azure AD でアプリケーション プロキシを有効にする
- C. Active Directory 管理センターから、動的アクセス制御ポリシーを作成します。
- D. Azure Active Directory 管理センターから、認証方法を構成します。

Answer: ([解答を表示する](#)**)**

参照：

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivitywindows10>

最新問題: 28

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Permanent role assignment
User1	Global Administrator
User2	Security Administrator
User3	Privileged Role Administrator
User4	None

ユーザー管理者ロールは、次の図に示すように、Azure AD Privileged Identity Management (PIM) で構成されます。

User Administrator



Save Discard

Activations

Maximum activation duration (hours) ⓘ

4

Notifications

Send email notifying admins of activation ⓘ

Enable Disable

Incident/Request ticket

Require incident/request ticket number during activation ⓘ

Enable Disable

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation ⓘ

Enable Disable

Require approval

Require approval to activate this role ⓘ

Enable Disable



If no approvers are selected, Privileged Role Administrators will be approvers by default.

SELECTED APPROVER

ACTION

No results

Select approvers

No approver selected



User4 にユーザー管理者ロールの資格を与えます。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input type="radio"/>
User2 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input type="radio"/>
User3 receives an email notification when User4 requests activation of the User Administrator role.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
User3 receives an email notification when User4 requests activation of the User Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 29

どのポリシーがどのデバイスに適用されますか? 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。

DevicePolicy1:	<input type="checkbox"/> None
	<input type="checkbox"/> Device1 only
	<input type="checkbox"/> Device3 only
	<input type="checkbox"/> Device2 and Device3 only
	<input type="checkbox"/> Device1 and Device3 only
	<input type="checkbox"/> Device1, Device2, and Device3
DevicePolicy2:	<input type="checkbox"/> None
	<input type="checkbox"/> Device4 only
	<input type="checkbox"/> Device2 and Device4 only
	<input type="checkbox"/> Device2, Device3, and Device 4 only

Answer:

On VPN1:

Configure an authentication provider.	V
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port

443	V
1723	
1813	
8080	
8531	

説明

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

最新問題: 30

User 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。

Name	Platform	Group
Device1	Android	Group1, Group3
Device2	iOS	Group1, Group2
Device3	Android	Group3

次の表に示すように、Microsoft Intune にデバイスを登録します。

各デバイスには、App1 と App2 という名前の 2 つの基幹業務アプリがインストールされています。

Name	Platform	Deployed to	Protected apps
Policy1	Android	Group3	App2
Policy2	iOS	Group2	App2
Policy3	Android	Group1	App1

次の表に示すように、Microsoft エンドポイント マネージャーですべてのアプリの種類を対象としたアプリケーション コントロール ポリシーを作成します。

Name	Platform	Deployed to	Protected apps
Policy1	Android	Group3	App2
Policy2	iOS	Group2	App2
Policy3	Android	Group1	App1

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 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

Microsoft

Statements

Statements	Yes	No
Policy1 applies to Device1.	<input type="radio"/>	<input type="radio"/>
When User1 signs in to Device1, App1 is protected.	<input type="radio"/>	<input type="radio"/>
When User1 signs in to Device2, App1 is protected.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Microsoft

Statements

Statements	Yes	No
Policy1 applies to Device1.	<input checked="" type="radio"/>	<input type="radio"/>
When User1 signs in to Device1, App1 is protected.	<input checked="" type="radio"/>	<input type="radio"/>
When User1 signs in to Device2, App1 is protected.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 31

カスタム ネットワーク インジケーターがオンになっている Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) 展開があります。Microsoft Defender ATP は、Windows を実行する 2 台のコンピューターを保護します

以下の表に示すように、10。

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender ATP には、次の表に示すマシン グループがあります。

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp
Last	Ungrouped machines (default)	None

Microsoft Defender セキュリティ センターから、次の表に示す URL/ドメイン インジケーターを作成します。

URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	<input type="radio"/>	<input type="radio"/>
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	<input type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	<input checked="" type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input type="radio"/>	<input checked="" type="radio"/>

説明

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	<input checked="" type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input type="radio"/>	<input checked="" type="radio"/>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 32

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

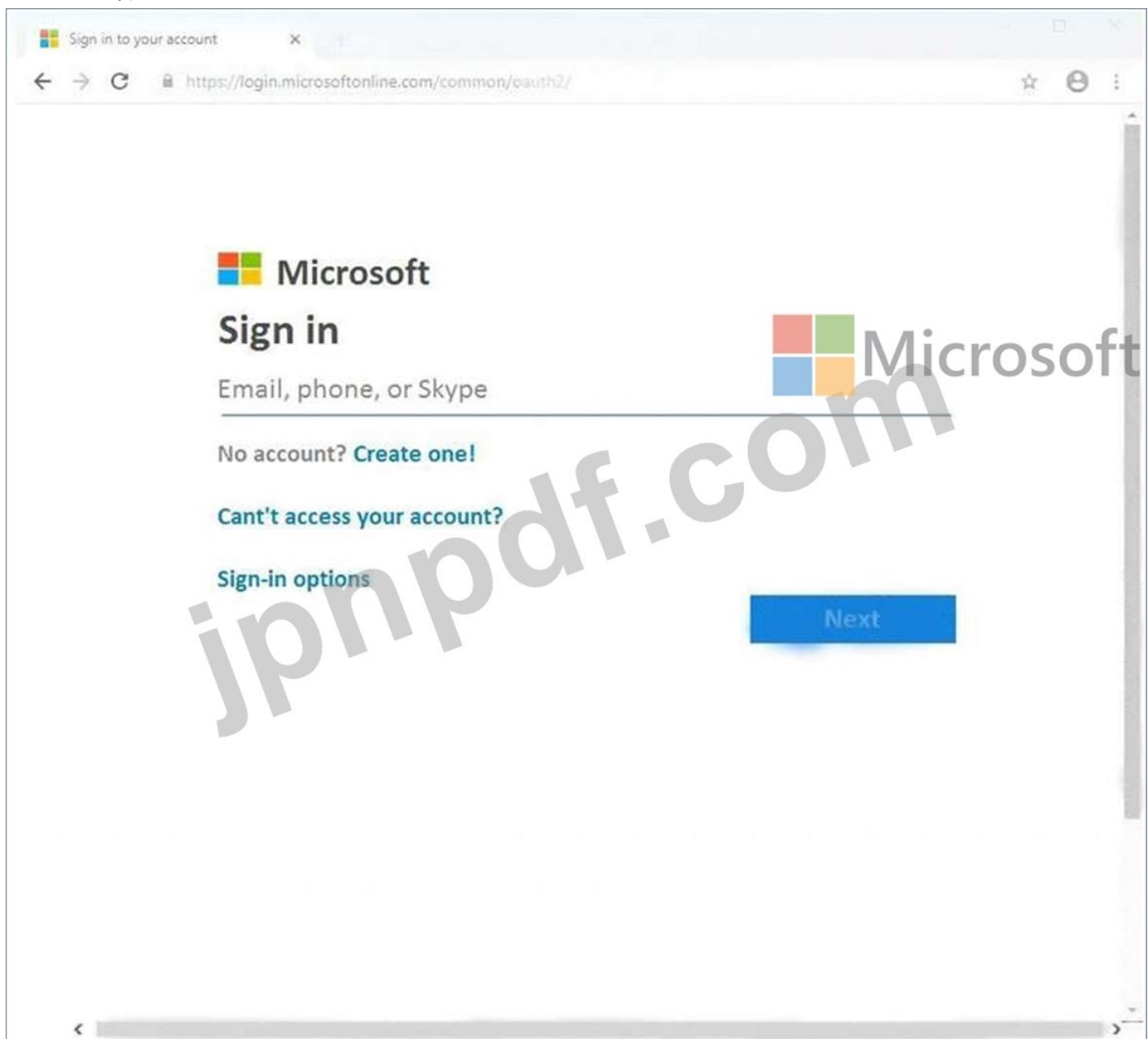
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。


ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



Sign in to your account

https://login.microsoftonline.com/common/oauth2/

 Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

[Next](#)

必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308



Microsoft

Microsoft ×



jpnpdf.com

Brainstorm
together in Word



Microsoft



Stay on top of what matters with Outlook



Microsoft



Microsoft



Microsoft



Access Office 365 apps and documents in one place with

Office.com



jpnpdf.com

Microsoft Office Home | office.com/tauliv-2 | Contoso electronics | Office 365


Good morning Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint

OneNote | Skype | Calendar | People | All apps

Recommended


You edited this Jan 15



Excel

Sales Results Overview
lodse000198.sharepoint.co...


You edited this Jan 15



Excel

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15



Org Chart
lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recommended

You edited this Jan 15



Excel

P and L Summary
lodse000198.sharepoint.co...

You edited this Jan 15



Word

Contoso Electronics Outdoor...
lodse000198.sharepoint.co...

You edited this Jan 15



Word

AD Slogans
lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recent

Pinned

Shared with me

Discover



Microsoft



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

Upload and open...

New

[Go to OneDrive](#) →

Recent

Pinned

Shared with me

Discover



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

[Go to OneDrive](#) →

SharePoint

Frequent sites

Following

Sales and Marketing

Retail

Communication Site

[Go to SharePoint](#) →

SharePoint

Frequent sites

Following

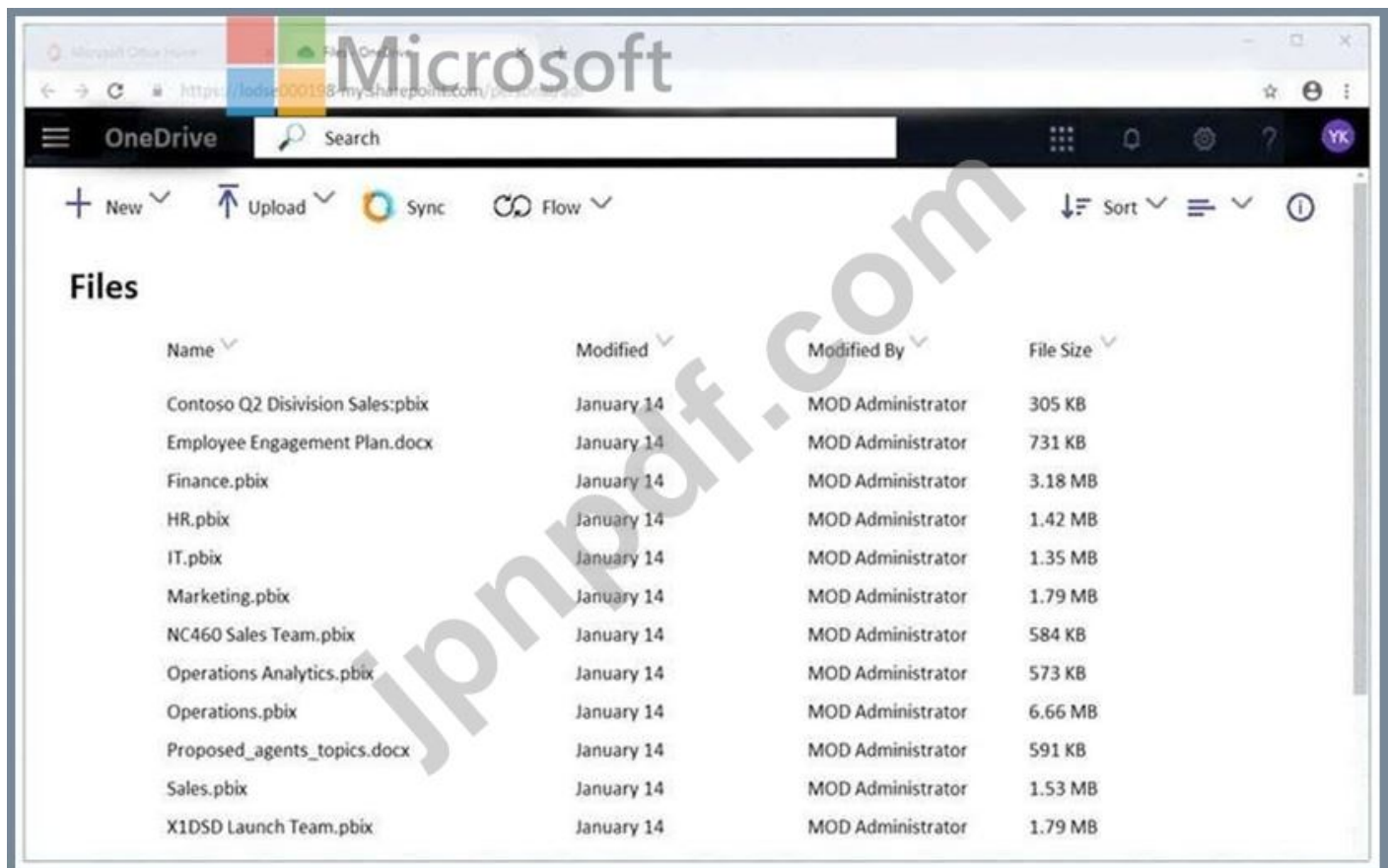
Contoso Landings

Contoso Web 3

Executive Corner



Microsoft



フィッシング攻撃から保護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。

* フィッシングメールメッセージがなりすましドメインから送信された場合、メッセージを隔離する必要があります。

* できるだけ多くのフィッシングメールメッセージを識別する必要があります。

この解決策は、現在の SMTP ドメイン名と後で追加されるドメイン名に適用する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

1. Microsoft 365 管理センターにサインインした後、[セキュリティ]、[脅威管理]、[ポリシー]、[ATP フィッシング対策] の順に選択します。
 2. [デフォルト ポリシー] を選択して調整します。
 3. [偽装] セクションで、[編集] を選択します。
 4. [保護するドメインの追加] に移動し、所有するドメインを自動的に含めるトグルを選択します。
 5. [アクション] に移動し、[電子メールが偽装ユーザーによって送信された場合] ドロップダウンを開き、[メッセージを隔離] アクションを選択します。
- [電子メールが偽装ドメインから送信された場合] ドロップダウンを開き、[メッセージを隔離] アクションを選択します。

6. [偽装に関する安全性のヒントをオンにする] を選択します。システムが偽装ユーザー、ドメイン、または異常な文字を検出したときに、ユーザーにヒントを提供するかどうかを選択します。選択する
7. [メールボックス インテリジェンス] を選択し、オンになっていることを確認します。これにより、使用パターンを学習してメールをより効率的に作成できます。
8. [信頼できる送信者とドメインを追加する] を選択します。ここでは、なりすましとして分類すべきでない電子メール アドレスまたはドメインを追加できます。
9. [設定を確認する] を選択し、すべてが正しいことを確認して、[閉じる] を選択します。

参照：

<https://support.office.com/en-us/article/protect-against-phishing-attempts-in-microsoft-365-86c425e1-1686-430a>

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view>

最新問題: 33

contoso.com という名前の Azure Active Directory (Azure AD) テナントを使用する Microsoft 365 サブスクリプションがあります。OneDrive には、外部ユーザーと共有されるファイルが保存されます。ファイルは次の表に示すように構成されています。

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

OneDrive アカウントに保存されているコンテンツに適用されるデータ損失防止 (DLP) ポリシーを作成します。ポリシーには次の 3 つのルールが含まれています。

* ルール:

* 条件: ラベル 1、組織外のユーザーと共有されているコンテンツを検出する

* アクション: 外部ユーザーのコンテンツへのアクセスを制限します。

* ユーザー通知: コンテンツを最後に変更したユーザーに通知します。

* ユーザーオーバーライド: オン

※優先度 :0

* ルール 2:

※条件 :ラベル1またはラベル2

* アクション: コンテンツへのアクセスを制限する

※優先度 :1

* ルール 3:

* 条件: ラベル 2、組織外のユーザーと共有されているコンテンツを検出する

* アクション: 外部ユーザーのコンテンツへのアクセスを制限します。

* ユーザー通知: コンテンツを最後に変更したユーザーに通知します。

* ユーザーオーバーライド: オン

※優先度 2

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ]を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ]を選択します。注: 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


Statements	Yes	No
External users can access File1.	<input type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input type="radio"/>
External users can access File3.	<input type="radio"/>	<input type="radio"/>



Answer:

Answer Area

Statements	Yes	No
External users can access File1.	<input checked="" type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input checked="" type="radio"/>
External users can access File3.	<input type="radio"/>	<input checked="" type="radio"/>



最新問題: 34

Microsoft 365 サブスクリプションをお持ちです。

ユーザーは、Microsoft OneDrive 内のいくつかのファイルに変更が加えられたと報告しました。ユーザーの OneDrive 内のどのユーザーがどのファイルを変更したかを特定する必要があります。

あなたは何をすべきか？

- A. Azure Active Directory 管理センターから、監査ログを開きます。
- B. OneDrive 管理センターから、[デバイス アクセス] を選択します。
- C. [セキュリティとコンプライアンス] から、電子情報開示検索を実行します。
- D. Microsoft Cloud App Security から、アクティビティ ログを開きます。

Answer: D ([メッセージを残す](#))

説明/参照:

<https://docs.microsoft.com/en-us/cloud-app-security/activity-filters>

最新問題: 35

監査のセキュリティ要件を満たすソリューションをユーザー管理者に推奨する必要があります。Azure Active Directory 管理センターからどのブレードを使用することをお勧めしますか?

- A. サインイン
- B. Azure AD ID 保護
- C. 認証方式
- D. アクセスレビュー

Answer: ([解答を表示する](#))

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

トピック 3、Contoso, Ltd

既存の環境

インフラストラクチャー

ネットワークには、Microsoft Azure Active Directory (Azure AD) テナントに同期されている contoso.com という名前の Active Directory ドメインが含まれています。パスワードライトバックが有効になっています。

ドメインには、Windows Server 2016 を実行するサーバーが含まれています。ドメインには、Windows 10 Enterprise を実行するラップトップおよびデスクトップコンピューターが含まれています。

各クライアント コンピュータには 1 つのボリュームがあります。

各オフィスは NAT デバイスを使用してインターネットに接続します。オフィスの IP アドレスは次の表に示されています。

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

名前付きロケーションは、次の表に示すように Azure AD で定義されます。

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

[多要素認証] ページから、198.35.3.0/24 のアドレス スペースが信頼できる IP リストに定義されます。

Azure Multi-Factor Authentication (MFA) は、財務部門のユーザーに対して有効になっています。

テナントには、次の表に示すユーザーが含まれます。

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

テナントには、次の表に示すグループが含まれています。

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

カスタマー ロックボックスは Microsoft 365 で有効になっています。

Microsoft Intune の構成

Intune に登録されているデバイスは、次の表に示すように構成されています。

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

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

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

デバイス コンプライアンス ポリシーには、次の表に示す割り当てがあります。

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

[コンプライアンス ポリシーが割り当てられていないデバイスをマークする] 設定が [準拠] に設定されます。

要件

技術的要件

Contoso は次の技術要件を特定します。

最小特権の原則を使用する

User1 がレポート閲覧者の役割をユーザーに割り当てられるようにする

User6 がカスタマー ロックボックスの要求をできるだけ早く承認するようにする User9 が

Azure AD Privileged Identity Management を実装できるようにする

最新問題: 36

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード

必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

Exchange Online の電子メール メッセージと SharePoint Online のドキュメントが 8 年間保持されるようにする必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

注意: 当社の目的上、保存期間は 8 年間となります。

Exchange Online で電子メール メッセージを保持するには:

ステップ 1: 保持タグを作成する

1. Exchange 管理センターに移動します。
2. コンプライアンス管理 + に移動します
3. 次のオプションのいずれかを選択します。

* メールボックス全体に自動的に適用 (デフォルト): デフォルトのポリシー タグ (DPT) を作成するには、このオプションを選択します。DPT を使用して、メールボックス内のすべてのアイテムに適用されるデフォルトの削除ポリシーとデフォルトのアーカイブ ポリシーを作成できます。

* 特定のフォルダーに自動的に適用: 受信トレイや削除済みアイテムなどの既定のフォルダーに保持ポリシー タグ (RPT) を作成するには、このオプションを選択します。

* ユーザーがアイテムとフォルダーに適用 (個人): 個人タグを作成するには、このオプションを選択します。これらのタグを使用すると、Outlook および Outlook on the web (以前の Outlook Web App) ユーザーは、親フォルダーまたはメールボックス全体に適用される設定とは異なるアーカイブまたは削除の設定をメッセージまたはフォルダーに適用できます。

4. [新しい保持タグ] ページのタイトルとオプションは、選択したタグの種類によって異なります。次のフィールドに入力します。

* 名前: 保持タグの名前を入力します。タグ名は表示目的であり、タグが適用されるフォルダーやアイテムには影響しません。ユーザーにプロビジョニングした個人タグは、Outlook および Web 上の Outlook で利用できることを考慮してください。

* このタグを次のデフォルト フォルダーに適用します: このオプションは、[特定のフォルダーに自動的に適用] を選択した場合にのみ使用できます。

* 保持アクション: アイテムが保持期間に達した後に実行されるアクションを次のいずれか選択します。

* 削除して回復を許可: アイテムを削除しますが、Outlook または Web 上の Outlook の [削除済みアイテムの回復] オプションを使用してユーザーがアイテムを回復できるようにするには、このアクションを選択します。アイテムは、メールボックス データベースまたはメールボックス ユーザーに対して構成された削除済みアイテムの保存期間に達するまで保持されます。

* 完全に削除: メールボックス データベースからアイテムを完全に削除するには、このオプションを選択します。

* アーカイブに移動: このアクションは、DPT または個人タグを作成している場合にのみ使用できます。アイテムをユーザーのインプレース アーカイブに移動するには、このアクションを選択します。

* 保存期間: 次のオプションのいずれかを選択します。

* 決してしない: アイテムを決して削除したり、アーカイブに移動したりしないことを指定するには、このオプションを選択します。

* アイテムが次の経過日数 (日数) に達した場合: このオプションを選択し、アイテムが移動または削除されるまでにアイテムを保持する日数を指定します。カレンダーとタスクを除くすべてのサ

ポートされているアイテムの保存期間は、アイテムが受信または作成された日から計算されません。カレンダーとタスクのアイテムの保存期間は終了日から計算されます。

* コメント: このオプションのフィールドを使用して、管理上のメモやコメントを入力します。このフィールドはユーザーには表示されません。

ステップ 2: 保持ポリシーを作成する

1. [コンプライアンス管理] に移動します [追加 +]

2. [新しい保持ポリシー] で、次のフィールドに入力します。

* 名前: 保持ポリシーの名前を入力します。

* 保持タグ: [追加 +] をクリックして、この保持ポリシーに追加するタグを選択します。

保持ポリシーには次のタグを含めることができます。

* アーカイブに移動アクションを持つ 1 つの DPT。

* 削除および回復の許可または完全に削除のアクションを持つ 1 つの DPT。

* 削除および回復の許可または完全に削除のアクションを含むボイス メール メッセージ用の 1 つの DPT。

* アイテムを削除するには、受信トレイなどのデフォルト フォルダーごとに 1 つの RPT が必要です。

* 任意の数の個人タグ。

ステップ 3: メールボックス ユーザーにアイテム保持ポリシーを適用する

アイテム保持ポリシーを作成したら、それをメールボックス ユーザーに適用する必要があります。異なるユーザーのセットに異なる保持ポリシーを適用できます。

* [受信者] > [メールボックス] に移動します。

* リスト ビューでは、Shift キーまたは Ctrl キーを使用して複数のメールボックスを選択します。

* 詳細ペインで、[その他のオプション] をクリックします。

* [保持ポリシー] で、[更新] をクリックします。

* [保持ポリシーの一括割り当て] で、メールボックスに適用する保持ポリシーを選択し、[保存] をクリックします。

SharePoint Online でドキュメントを保持する場合

セキュリティとコンプライアンス管理センターにアクセスする

1. Office 365 管理センターに移動します。

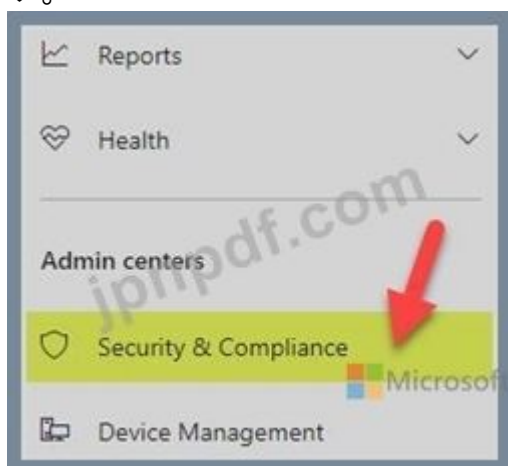


Office 365

Apps

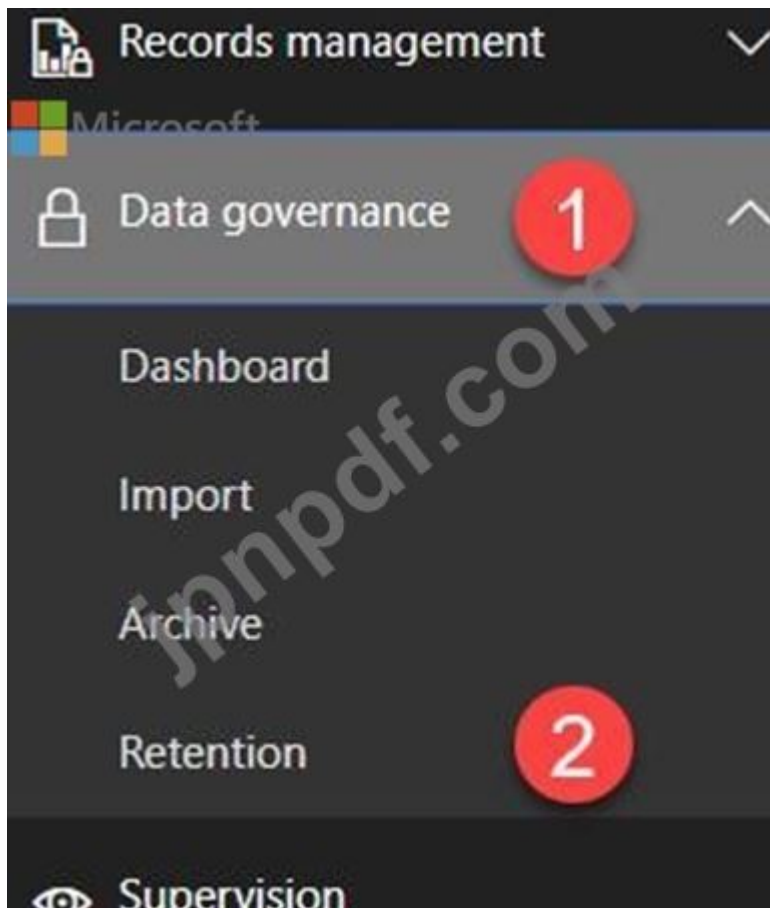


2. 利用可能な管理センターのリストから、「セキュリティとコンプライアンス」をクリックします。

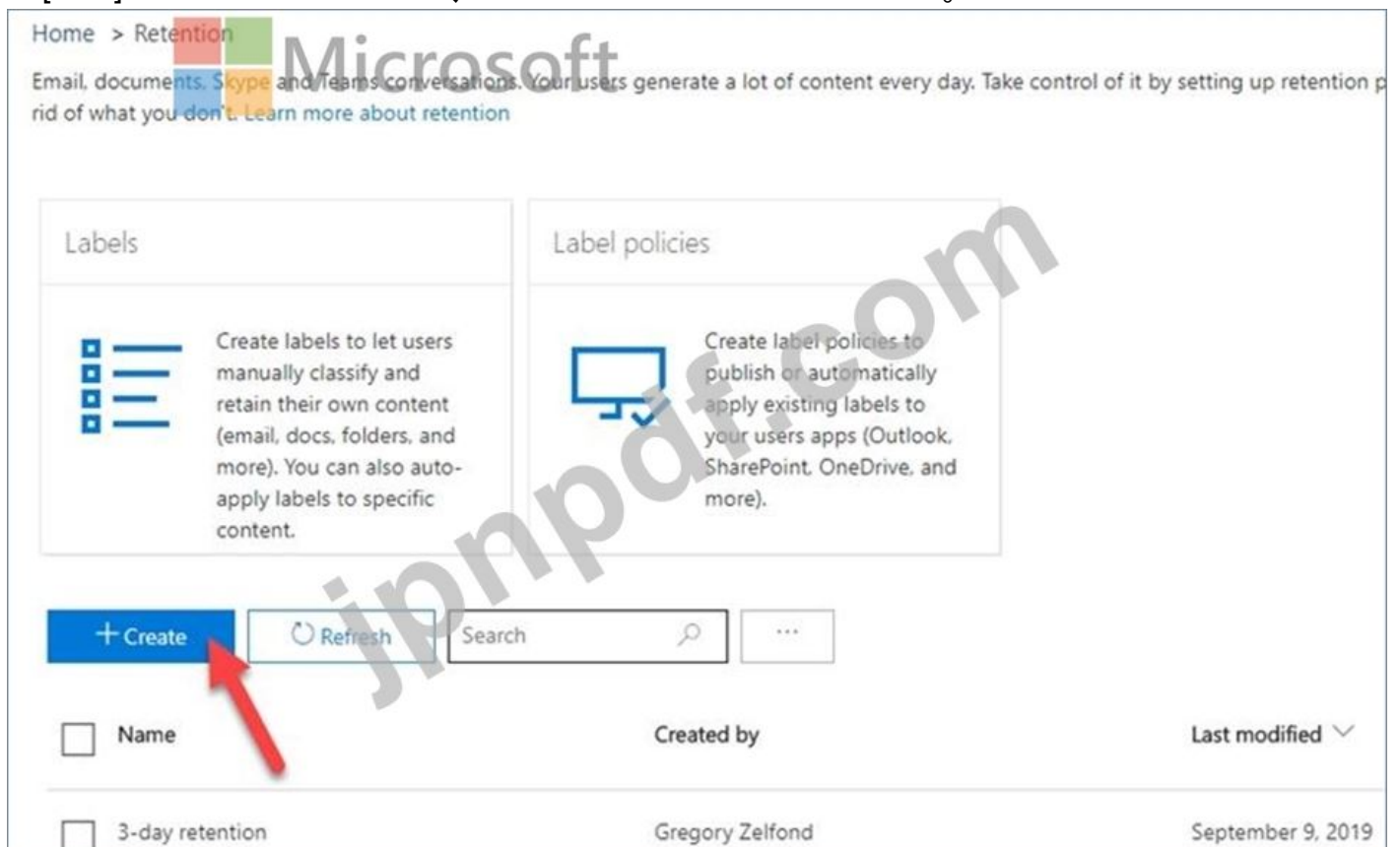


SharePoint サイトで保持ポリシーを作成して公開する方法

セキュリティとコンプライアンス管理センターに移動したので、SharePoint サイトで保持ポリシーを作成して公開する準備が整いました。



1. [作成] ボタンをクリックして、新しい保持ポリシーを作成します。



2. ポリシーに名前と説明を付けます。

Create a policy to retain what you want and get rid of what you don't.

- Name your policy
- Settings
- Choose locations
- Review your settings

Name your policy

Name * ⓘ

Retain for 2 days, then delete 1

Description ⓘ

This policy retains documents for 2 days after they were last modified and then deletes the 2

3

Next Cancel

3. 次の画面では、ロジックを設定します。コンテンツを保持する日数、月数、または年数を構成したり、計算 (保持期間) を作成日または最終変更日から計算するかどうかを指定したりできます。最後に、保存期間の終了後にコンテンツを保持するか削除するかを指定することもできます。次へ」をクリック

Create a policy to retain what you want and get rid of what you don't.

- Name your policy
- Settings
- Choose locations
- Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 2 days 1

Retain the content based on when it was last modified ⓘ 2

Do you want us to delete it after this time? ⓘ

Yes No 3

At this time, creating a policy to delete Teams content that's less than 30 days old is not supported. If you want this policy to apply to Teams content, specify a retention period that's equal to or more than 30 days.

No, just delete content that's older than ⓘ

1 years

Need more options?

Use advanced retention settings ⓘ

4

Back Next Cancel

4. 次の画面で、ポリシーを適用する場所を選択します。これは、電子メール (Exchange)、SharePoint サイト、OneDrive アカウント、および Office 365 グループに適用できます。



5. 私の場合、単一の Office 365 グループ サイトにポリシーを適用しました。



6. 最後の画面で、設定を確認して「このポリシーを作成」ボタンをクリックする必要があります。下部に表示されるメッセージに注意することが重要です。前の手順で設定したロジックに従ってポリシーが有効になるとすぐに、コンテンツが削除される可能性があることが警告されます。



Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name Edit

Retain for 2 days, then delete

Description Edit

This policy retains documents for 2 days after they were last modified and then deletes them

Applies to content in these locations Edit

SharePoint sites

Settings Edit

Retention period

Keep content, and delete it if it's older than 2 days

⚠ Content that's currently older than this will be deleted after you turn on the policy.

Back

Save for later

Create this policy

Cancel

参考文献:

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-re>

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-reten>

<https://sharepointmaven.com/how-to-set-a-retention-policy-on-a-sharepoint-site/>

最新問題: 37

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボセクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

Operations という名前のグループのメンバーが IPO という単語を含む電子メール メッセージを削除できないようにするケースを作成する必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

1. セキュリティ & コンプライアンス センターに移動します。
2. セキュリティ/コンプライアンス センターで、[電子情報開示] > [電子情報開示] をクリックし、[ケースの作成] をクリックします。
3. [新しいケース] ページで、ケースに名前を付け、必要に応じて説明を入力し、[保存] をクリックします。ケース名は組織内で一意である必要があります。



新しいケースは、電子情報開示ページのケースのリストに表示されます。

ケースを作成したら、次のステップはケースにメンバーを追加することです。ケースを作成した電子情報開示マネージャーは、メンバーとして自動的に追加されます。メンバーを追加した後にケースにアクセスできるように、メンバーには適切な電子情報開示権限が割り当てられている必要があります。

4. セキュリティ/コンプライアンス センターで、[電子情報開示] > [電子情報開示] をクリックして、組織内のケースのリストを表示します。
5. メンバーを追加するケースの名前をクリックします。
[このケースの管理] フライアウト ページが表示されます。

Manage this case



Manage members

+ Add

- Remove

Search



^ Users (1)

Company Admin

Manage role groups

+ Add

- Remove

Search



^ Role Groups (0)

Manage case status

Name *

New case1

Description

test

Created

2018-03-22 15:15:16

Status

Closing

Delete case

Reopen case





6. [メンバーの管理] で、[追加] をクリックしてメンバーをケースに追加します。役割グループをケースに追加することも選択できます。[役割グループの管理] で [追加] をクリックします。
7. ケースのメンバーとして追加できるユーザーまたは役割グループのリストで、追加するユーザーまたは役割グループの名前の横にあるチェック ボックスをオンにします。
8. グループのメンバーとして追加するユーザーまたは役割グループを選択した後、[追加] をクリックします。[このケースの管理] で [保存] をクリックして、ケース メンバーの新しいリストを保存します。
9. 保存] をクリックして、ケースメンバーの新しいリストを保存します。

電子情報開示ケースを使用して保留を作成し、ケースに関連する可能性のあるコンテンツを保存できます。ケースの管理者であるユーザーのメールボックスと OneDrive for Business サイトを保留することができます。Office 365 グループのグループ メールボックス、SharePoint サイト、および OneDrive for Business サイトに保留を設定することもできます。同様に、Microsoft Teams または Yammer グループに関連付けられているメールボックスとサイトを保留することができます。コンテンツの場所を保留にすると、コンテンツの場所から保留を解除するか、保留を削除するまで、コンテンツは保留されます。

電子情報開示ケースの保留を作成するには:

1. セキュリティ/コンプライアンス センターで、[電子情報開示] > [電子情報開示] をクリックして、組織内のケースのリストを表示します。
2. 保留を作成するケースの横にある [開く] をクリックします。
3. ケースのホームページで、保留] タブをクリックします。



4. [保留] ページで、[作成] をクリックします。
5. [保留に名前を付ける] ページで、保留に名前を付けます。保留の名前は組織内で一意である必要

があります。



The screenshot shows a web form titled "Name your hold". It contains two text input fields: "Name *" with a placeholder "Enter a friendly name" and "Description" with a placeholder "Enter a friendly description for your hold". At the bottom, there are two buttons: "Next" (highlighted in blue) and "Cancel". A faint watermark "ipnpdf.com" is visible across the form. The Microsoft logo is partially visible on the right side of the description field.

6. (オプション) [説明] ボックスに、保留の説明を追加します。

7. 次へ」をクリックします。

8. 保留するコンテンツの場所を選択します。メールボックス、サイト、パブリック フォルダーを保留にすることができます。

Choose locations

Location	Include
Exchange email	None
Office 365 group email	Choose users, groups, or teams A
Skype for Business	
Teams messages	Microsoft
To-Do	
Yammer conversations	
SharePoint sites	None
OneDrive accounts	Choose sites B
Office 365 group sites	
Teams sites	
Yammer networks	
Exchange public folders	None C

Back Next Cancel

- a. 電子メールの交換 - [ユーザー、グループ、またはチームの選択] をクリックし、もう一度 [ユーザー、グループ、またはチームの選択] をクリックします。
- 保留するメールボックスを指定します。検索ボックスを使用して、保留するユーザーのメールボックスと配布グループを検索します (グループメンバーのメールボックスを保留する場合)。Microsoft チーム、Yammer グループ、または Office 365 グループに関連付けられたメールボックスを保留することもできます。ユーザー、グループ、チームのチェックボックスをオンにし、[選択] をクリックして、[完了] をクリックします。



a. [キーワード] の下のボックスに検索クエリを入力すると、検索条件を満たすコンテンツのみが保留されます。キーワード、メッセージ プロパティ、またはファイル名などのドキュメント プロパティを指定できます。AND、OR、NOT などのブール演算子を使用する、より複雑なクエリを使用することもできます。キーワード ボックスを空のままにすると、指定したコンテンツの場所にあるすべてのコンテンツが保留されます。

b. [条件の追加] をクリックして 1 つ以上の条件を追加し、保留の検索クエリを絞り込みます。各条件は、ホールドの作成時に作成および実行される KQL 検索クエリに句を追加します。たとえば、日付範囲を指定して、その日付範囲内に作成された電子メールまたはサイト ドキュメントを保留にすることができます。条件は、AND 演算子によってキーワードクエリ (キーワード ボックスで指定) に論理的に接続されます。つまり、アイテムはキーワードクエリと保留状態の両方を満たす必要があります。

9. クエリベースの保持を設定したら、[次へ] をクリックします。

10. 設定を確認し、[この保留を作成] をクリックします。

参照：

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-cases?view=o365-worldwide>

最新問題: 38

どの財務部門のユーザーに Azure MFA 資格情報の入力を求めるかを評価しています。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input checked="" type="radio"/>	<input type="radio"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input checked="" type="radio"/>	<input type="radio"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 39

あなたの会社には、Microsoft 365 サブスクリプション、Microsoft Azure サブスクリプション、および contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。当社は、次の表に示す営業所を設置しております。

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

テナントには、次の表に示すユーザーが含まれます。

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

次の図に示す Microsoft Cloud App Security ポリシーを作成します。

Create filters for the policy

Act on:

Single activity:
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

In a single app

Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR

equals

From group equals

as

Alerts

Create alert Use your organization's default settings

Daily alert limit

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	<input type="radio"/>	<input type="radio"/>
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	<input type="radio"/>	<input type="radio"/>
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements

Yes

No

In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

最新問題: 40

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正解がある場合もありますが、他の質問セットには正解がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Microsoft 365 サブスクリプションをお持ちです。

User1 という名前のユーザーがいます。複数のユーザーが User1 のメールボックスへの完全なアクセス権を持っています。

User1 に送信された一部の電子メール メッセージは、ユーザーが閲覧する前に読まれ、削除されたようです。

User1 のメールボックスにサインインしたユーザーを特定するためにセキュリティとコンプライアンスで監査ログを検索すると、結果は空白になります。

User1 のメールボックスへの今後のサインインを表示できることを確認する必要があります。

Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner コマンドを実行します。

それは目標を達成していますか？

A. はい

B. いいえ

Answer: B (メッセージを残す)

参照 :

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

最新問題: 41

管理者が電子メール メッセージやドキュメントにフッターを追加するラベルを公開できるようにする必要があります。

このタスクを完了するには、Microsoft Office 365 ポータルにサインインします。

Answer:

以下の説明を参照してください。

説明

機密ラベルを設定する必要があります。

- * セキュリティとコンプライアンス管理センターに移動します。
 - * 分類 > に移動します
 - * 新しいラベルを作成するには、[+ ラベルの作成] をクリックします。
 - * ラベルに名前と説明を入力し、クリックします。
 - * 暗号化オプションはそのままにしておきます
 - * [コンテンツ マーキング] ページで、チェックボックスをオンにします
 - * [テキストのカスタマイズ] リンクをクリックしてフッター テキストを追加し、[保存] をクリックします (質問の場合、追加するテキストは関係ありません)。
 - * 次へ」をクリックします。
 - * Office アプリの自動ラベル付けをオフのままにして、次へ」をクリックします。
 - * [送信] ボタンをクリックして変更を保存します。
- ※ ラベルの発行準備が完了しました。完了」ボタンをクリックしてページを終了し、ラベルを作成します。

最新問題: 42

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は Microsoft 365 E5 ライセンスが割り当てられます。

監査データはどのくらいの期間保存されますか？

- A. 30日
- B. 90日
- C. 365日
- D. 5年

Answer: B (メッセージを残す)

参考文献:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

最新問題: 43

Microsoft 365 サブスクリプションをお持ちです。

Site2 という名前のサイトを含む SiteCollection1 という名前のサイト コレクションがありま

す。Site2 には、Customers という名前のドキュメント ライブラリが含まれています。

Customers には Litware.docx という名前のドキュメントが含まれています。Litware.docx を完全に削除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
From PowerShell, run Remove-SPOUserProfile	
Delete Litware.docx from the Recycle Bin of Site2.	
From PowerShell, run Set-SPOSite.	
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

Answer:

Actions	Answer Area
From PowerShell, run Remove-SPOUserProfile	Delete Litware.docx from Customers.
Delete Litware.docx from the Recycle Bin of Site2.	Delete Litware.docx from the Recycle Bin of Site2.
From PowerShell, run Set-SPOSite.	Delete Litware.docx from the Recycle Bin of SiteCollection1.
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

説明

Answer Area

Delete Litware.docx from Customers.

Delete Litware.docx from the Recycle Bin of Site2.

Delete Litware.docx from the Recycle Bin of SiteCollection1.

最新問題: 44

デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。次の図に示すように、Microsoft OneDrive で共有設定を構成します。

Links

Choose the kind of link that's selected by default when users share items.

Default link type

Shareable: Anyone with the link


Internal: Only people in your organization

Direct: Specific people



External sharing

Users can share with:



SharePoint OneDrive

Most permissive	Anyone	Users can create shareable links that don't require sign-in
	New and existing external users	External users must sign-in
	Existing external users	Only users already in your organization's directory
Least permissive	Only people in your organization	No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

Allow or block sharing with people on specific domains

Allow only these domains Contoso.com, Adatum.com [Add domains](#)

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

注: 正しく選択するたびに 1 ポイントの価値があります。

A user who has an email address of user1@fabrikam.com [answer choice]

 Microsoft	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

Answer:

A user who has an email address of user1@fabrikam.com [answer choice]

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

参照 :

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

最新問題: 45

ユーザーが Microsoft Office 365 ProPlus アプリケーションまたは Android デバイスからドキュメントまたは電子メール メッセージ内のリンクを選択するタイミングを管理するソリューション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す必要があります。

- * fabrikam.com という名前のドメインへのアクセスをブロックします。
 - * ユーザーが fabrikam.com へのリンクを選択したときに情報を保存します
- このタスクを完了するには、Microsoft 365 ポータルにサインインします。

Answer:

以下の説明を参照してください。

説明

安全なリンク ポリシーを構成する必要があります。

* Office 365 セキュリティとコンプライアンス管理センターに移動します。

* [脅威管理] > [ポリシー] > [安全なリンク] に移動します。

* [組織全体に適用するポリシー] で [デフォルト] を選択し、[編集] アイコンをクリックします。

* [次の URL をブロックする] セクションに 「f.fabrikam.com」と入力します。これは質問の最初の要件を満たしています。

* [電子メール以外のコンテンツに適用する設定] セクションで、[ユーザーが安全なリンクをクリックしたときは追跡しない] チェックボックスをオフにします。これは質問の 2 番目の要件を満たしています。

* [保存] をクリックして変更を保存します。

参照：

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view>

最新問題: 46

どのポリシーがどのデバイスに適用されますか? 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。

DevicePolicy1:	None
	Device1 only
	Device3 only
	Device2 and Device3 only
	Device1 and Device3 only
	Device1, Device2, and Device3

DevicePolicy2:	None
	Device4 only
	Device2 and Device4 only
	Device2, Device3, and Device 4 only

Microsoft

Answer:

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device4 only

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
 GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaihu.html> (**32930%OFF**問題集 溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 47

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Groups administrator
Admin2	User administrator

contoso.com のグループ名前付けポリシーに禁止単語として 「internal」を追加します。

contoso.com のグループ名前付けポリシーのプレフィックスとして Contoso- を追加します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input checked="" type="radio"/>	<input type="radio"/>

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide>

最新問題: 48

あなたの会社は、Microsoft 365 E5 サブスクリプションと contoso.com という名前のハイブリッド Azure Active Directory を持っています。
 Contoso.com には次のユーザーが含まれます。
 次の図に示すように、Contoso.com のパスワード保護を構成します。

Custom smart lockout

Lockout threshold ⓘ

 Microsoft
10 ✓

Lockout duration in seconds ⓘ

60 ✓

Custom banned passwords

Enforce custom list ⓘ

Yes No

Custom banned password list ⓘ

Contoso ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes No

Mode ⓘ

Enforced Audit

Answer Area

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change his password to CONTOSOCONTOSO.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can change his password to myCONTOSOcmp1exPWD.	<input checked="" type="radio"/>	<input type="radio"/>

Answer:

Answer Area



Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input checked="" type="checkbox"/>
User2 can change his password to CONTOSOCONTOSO.	<input type="radio"/>	<input checked="" type="checkbox"/>
User3 can change his password to myCONTOSOcmp1exPWD.	<input checked="" type="checkbox"/>	<input type="radio"/>

最新問題: 49

ユーザー管理者に対して、セキュリティ要件を満たすソリューションを推奨する必要があります。

監査。

Azure Active Directory 管理センターからどのブレードを使用することをお勧めしますか？

- A. サインイン
- B. Azure AD ID 保護
- C. 認証方式
- D. アクセスレビュー

Answer: ([解答を表示する](#))

説明/参照:

参考文献:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

テストレット 2

概要

Litware, Inc. は、シカゴの本社に 1,000 人のユーザーを擁し、別のオフィスに 100 人のユーザーを抱える金融会社です。

サンフランシスコ支社。

既存の環境

内部ネットワークインフラストラクチャ

ネットワークには単一のドメイン フォレストが含まれています。フォレストの機能レベルは Windows Server 2016 です。

ユーザーは、Active Directory で定義されているサインイン時間制限の対象となります。

ネットワークの IP アドレス範囲は次の表に示されています。

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

オフィスはマルチプロトコル ラベル スイッチング (MPLS) を使用して接続します。

ネットワークでは次のオペレーティング システムが使用されています。

Windowsサーバー2016

Windows 10 エンタープライズ

Windows 8.1 エンタープライズ

内部ネットワークには、次の表に示すシステムが含まれています。

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

Litware はサードパーティの電子メール システムを使用します。

クラウドインフラストラクチャ

Litware は最近、すべてのユーザーを対象とした Microsoft 365 サブスクリプション ライセンスを購入しました。

Microsoft Azure Active Directory (Azure AD) Connect がインストールされており、デフォルトの認証を使用します

設定。ユーザー アカウントはまだ Azure AD に同期されていません。

次の表に示す Microsoft 365 ユーザーとグループがあります。

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

計画された変更

Litware は次の変更を実装する予定です。

電子メール システムを Microsoft Exchange Online に移行する

Azure AD Privileged Identity Management を実装する

セキュリティ要件

Litware では、次のセキュリティ要件が特定されています。

すべての Azure AD ユーザー アカウントを含む Group2 という名前のグループを作成します。Group2 は次のことに慣れます。

Windows Analytics への制限付きアクセスを提供する

Azure Information Protection ポリシーをパイロットに適用するために使用される Group3 という名前のグループを作成します。

ユーザー。Group3 にはユーザー アカウントのみを含める必要があります

Azure Advanced Threat Protection (ATP) を使用して、フォレストを標的とするセキュリティの脅威を検出します。

Active Directory からロックアウトされたユーザーが Azure AD および Active Directory にサインインできないようにする

User1 に対するコンプライアンス管理者ロールの永続的適格割り当てを実装します。

ドメインに参加しているサーバー上で Windows Defender と Windows Defender ATP を統合する

デフォルトでゲスト ユーザー アカウントの Azure リソースへのアクセスを禁止する

ドメインに参加しているすべてのコンピューターが Azure AD に登録されていることを確認する

多要素認証 (MFA) の要件

Microsoft Office 365 と Azure のセキュリティ機能は、パイロット Azure ユーザー アカウントを使用してテストされます。

MFA をテストするための次の要件を特定します。

パイロット ユーザーは、シカゴ オフィスの内部ネットワークからサインインしない限り、MFA を使用する必要があります。

MFA はシカゴ オフィスの内部ネットワークでは使用しないでください。

認証試行が疑わしい場合は、ユーザーの場所に関係なく、MFA を使用する必要があります。

正当な認証試行の中断は最小限に抑える必要があります

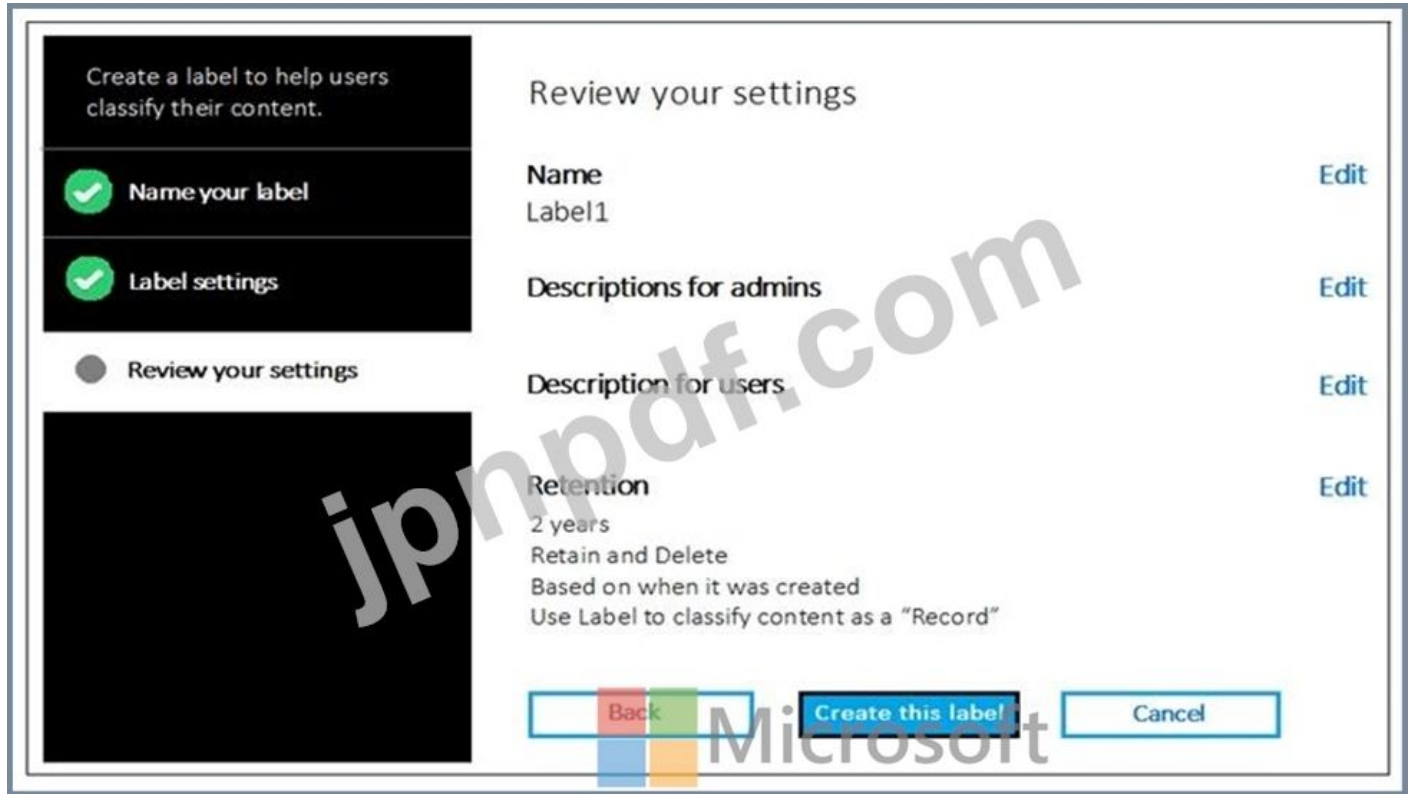
一般的な要件

Litware は、Active Directory フォレストへの追加のサーバーとサービスの展開を最小限に抑えたいと考えています。

最新問題: 50

Microsoft 365 サブスクリプションをお持ちです。

次の例に示すように、Label1 という名前の保持ラベルを作成します。



Label1 を SharePoint サイトに公開します。

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

注: 正しく選択するたびに 1 ポイントの価値があります。

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

	▼
never delete the file.	
delete the file before January 1, 2021.	
delete the file after January 1, 2021.	

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

	▼
always remain in the library.	
remain in the library until you delete the file.	
be deleted automatically on March 15, 2021.	

Answer:

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

Microsoft

never delete the file.
delete the file before January 1, 2021.
delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

Microsoft

always remain in the library.
remain in the library until you delete the file.
be deleted automatically on March 15, 2021.

説明

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

Microsoft

never delete the file.
delete the file before January 1, 2021.
delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

Microsoft

always remain in the library.
remain in the library until you delete the file.
be deleted automatically on March 15, 2021.

参考文献:

<https://docs.microsoft.com/en-us/office365/securitycompliance/labels>

最新問題: 51

contoso.com という名前の Microsoft Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

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

次の設定を持つ Azure AD Identity Protection ユーザー リスク ポリシーを作成して適用します。

- * 割り当て: グループ 1 を含む、グループ 2 を除く
- * 条件: サインインリスクが低以上
- * アクセス: アクセスを許可、パスワードの変更が必要

ポリシーが User1 と User2 にどのような影響を与えるかを特定する必要があります。
User1 と User2 が見慣れない場所からサインインするとどうなりますか? 回答するには、回答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。

Must change their password:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	

Prompted for MFA:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	

Answer:

Must change their password:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	

Prompted for MFA:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	

最新問題: 52

あなたの会社は、Microsoft 365 E5 サブスクリプションと contoso.com という名前のハイブリッド Azure Active Directory を持っています。

Contoso.com には次のユーザーが含まれます。

次の図に示すように、Contoso.com のパスワード保護を構成します。

Answer Area

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change his password to CONTOSOCONTOSO.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can change his password to myCONTOSOc0mp1exPWD.	<input checked="" type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change his password to CONTOSOCONTOSO.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can change his password to myCONTOSOc0mp1exPWD.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 53

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

Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を実装します。PIM から、アプリケーション管理者の役割を確認し、次の表に示すユーザーを検出します。

Name	Assignment type
UserA	Permanent
UserB	Eligible 
UserC	Eligible

アプリケーション管理者の役割は、PIM で次の設定を使用するように構成されています。

最大アクティベーション期間: 1 時間

通知: 無効にする

インシデント/リクエストチケット: 無効にする

多要素認証: 無効にする

承認が必要: 有効にする

選択した承認者: 結果はありません

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input checked="" type="radio"/>

説明

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input type="radio"/>

最新問題: 54

セキュリティ要件を満たす電子メール マルウェア ソリューションを推奨する必要があります。推奨事項には何を含めるべきですか? 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。

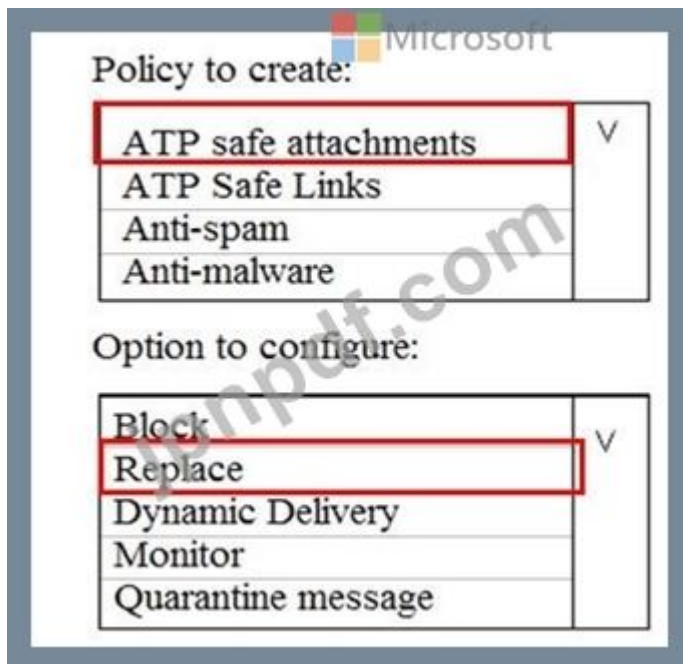
Policy to  create:


ATP safe attachments	V
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

Answer:



Policy to  create:

ATP safe attachments	V
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

最新問題: 55

どのデバイスが Intune に準拠しているかを評価しています。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input type="radio"/>
Device6 is compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Device2 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device6 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

説明

Statements	Yes	No
Device2 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device6 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 56

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー閲覧者の役割はどのユーザーにも割り当てられていません。

User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないようにする解決策を推奨する必要があります。

解決策: コンプライアンス マネージャーの閲覧者ロールを User5 に割り当てることをお勧めします。

これは目標を達成していますか?

A. はい

B. いいえ

Answer: [\(解答を表示する\)](#)

最新問題: 57

ハイブリッド Microsoft Exchange Server 組織があります。すべてのユーザーは Microsoft 365 E5 ライセンスを持っています。Advanced Threat Protection (ATP) フィッシング対策ポリシーを実装する予定です。すべてのユーザーに対してメールボックス インテリジェンスを有効にする必要があります。まず何をすべきでしょうか?

A. Microsoft Azure Active Directory Connect (Azure AD Connect) で属性フィルターを構成します。

B. ATP アドオンを購入します。

C. Microsoft Azure Active Directory Connect (Azure AD Connect) でディレクトリ拡張属性の同期を選択します。

D. オンプレミスのメールボックスを Exchange Online に移行します。

Answer: [D \(メッセージを残す\)](#)

説明

参考文献:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies>

最新問題: 58

Group1 および Group2 という名前の 2 つのグループと、次の表に示すユーザーを含む Microsoft

365 E5 サブスクリプションがあります。

Name	Role	Member of
Admin1	Global Administrator	None
User1	Global reader	Group1
User2	Global reader	Group2

次の図に示すように、特権アクセス設定が構成されています。



次の設定を持つ特権アクセス ポリシーがあります。

* ポリシー名: 新しいトランスポート ルール

* ポリシーの種類: タスク

* ポリシーの範囲 交換

※承認タイプ :マニュアル

※承認者グループ :グループ1

User1 は、新しいトランスポート ルール ポリシーへの 2 時間のアクセスを要求します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



最新問題: 59

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Azure Active Directory (Azure AD) から、Group1 という名前のセキュリティ グループ

を作成します。10人のユーザーを Group1 に追加します。

Group1 のメンバーが非標準デバイスから Microsoft Exchange Online に接続する場合は、場所に関係なく、アプリによる制限を適用する必要があります。

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。

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	▼
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	▼
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Answer:

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	▼
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	▼
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

最新問題: 60

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Azure Active Directory (Azure AD) から、Group1 という名前のセキュリティグループを作成します。10人のユーザーを Group1 に追加します。

Group1 のメンバーが非標準デバイスから Microsoft Exchange Online に接続する場合は、場所に関係なく、アプリによる制限を適用する必要があります。

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。

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	▼
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailboxPolicy and Set-OwaMailboxPolicy	▼
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Answer:

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	▼
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	


From an Exchange Online Remote PowerShell session, run:

New-OwaMailboxPolicy and Set-OwaMailboxPolicy	▼
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

最新問題: 61

ADGroup1 と ADGroup2 のメンバーはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

 Microsoft


ADGroup1:

None	▼
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

ADGroup2:

None	▼
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

Answer:

ADGroup1:  Microsoft

None	v
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

ADGroup2:

None	v
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 62

User1 と User2 という名前の 2 人のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

次の表に示す監査保持ポリシーを作成します。

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	None	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccessed	User1	9 Months
30	AuditRetention3	Sharepoint	None	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	None	10 Years

ユーザーは次のアクションを実行します。

User1 は Microsoft SharePoint Online サイトの名前を変更します。

User2 が電子メール メッセージを送信します。

各アクションの監査ログ レコードはどのくらいの期間保持されますか? 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。

User1 renames a SharePoint site:

90 days
6 months
9 months
1 year
10 years

User2 sends an email message:

90 days
6 months
9 months
1 year
10 years

Answer:

User1 renames a SharePoint site:

90 days
6 months
9 months
1 year
10 years

User2 sends an email message:

90 days
6 months
9 months
1 year
10 years

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide>

最新問題: 63

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	Microsoft Role
User1	Information Protection Administrator
User2	Information Protection Analyst
User3	Information Protection Investigator

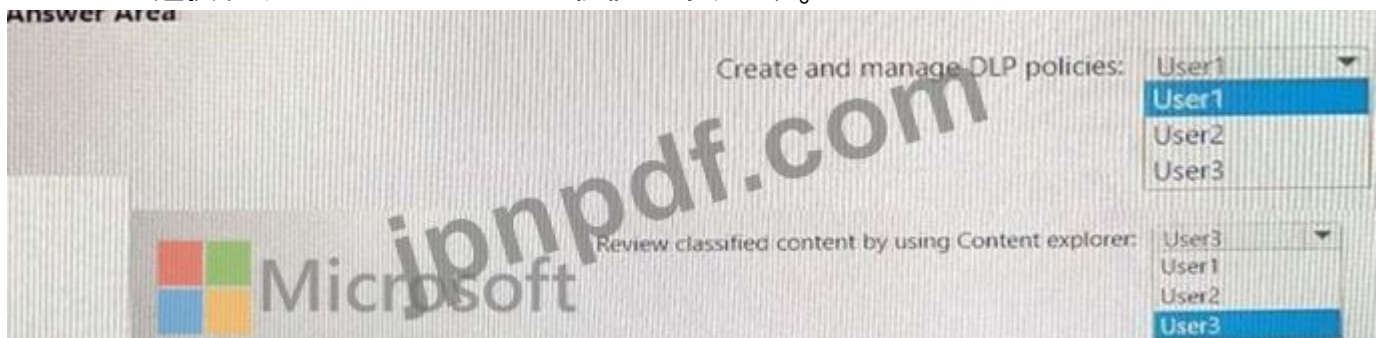
次のタスクを委任する必要があります。

データ損失防止 (DLP) ポリシーを作成および管理します。コンテンツ エクスプローラーを使用して、機密コンテンツを確認します。

ソリューションでは、最小特権の原則を使用する必要があります。

どのユーザーが各タスクを実行する必要がありますか? 回答するには、適切なユーザーを正しいタスクにドラッグします。各ユーザーは 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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



説明



最新問題: 64

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Microsoft 365 E5

サブスクリプションがあります。

contoso.com の Azure AD Identity Protection アラートは、次のように構成されています。

Alert on user risk level at or above

Low Medium High

Emails are sent to the following users. ⓘ

INCLUDED >

1 selected

Add additional emails to receive alert notifications (Preview). ⓘ

User1 という名前のユーザーは、Azure AD Identity Protection からアラートを受信するように構成されています。

次の表に示すように、contoso.com にユーザーを作成します。

Name	Role
User2	Security reader
User3	User administrator
User4	None
User5	None

ユーザーは、次の表に示すサインインを実行します。

Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>

参照 :

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

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

最新問題: 65

User1 という名前のユーザーと次の表に示すグループを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Type
Group1	Microsoft 365
Group2	Security

次の図に示すコンプライアンス マネージャーの改善アクションがあります。

Enable self-service password reset

Save Cancel

Overview

Details

Implementation Status: Not implemented

Test Status: Failed high risk

Points achieved: 0 / 27

Group: Default Group

Managed by: Your organization

Action scope: Tenant

Action type: Technical

Products: Microsoft 365

Documents: 0

Assigned to: None

Testing Source: Manual

Implementation Testing Standards and Regulations Documents

Implementation status: Not implemented

Implementation date: Not Available

Implementation notes: This action hasn't been implemented yet. Refer to the implementation instructions for this action.

Edit implementation details

How to implement

Microsoft recommends that your organization enable self-service password reset to allow users who have either forgotten their password or whose account has been locked out as a result of malicious attempts, using an alternate factor to reset their password without the assistance of the help desk.

How to Use Microsoft Solutions to Implement

Your organization can use Azure Active Directory (Azure AD) to give users the ability to change or reset their password with no administrator or help desk involvement. Select **Launch Now** to enable Self-Service Password Reset (SSPR) by selecting "All" or "Selected" on the "Properties" page to determine applicable users.

Launch Now

Learn More

Let users reset their own passwords in Office 365
How it works: Azure Active Directory self-service password reset

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

The Enable self-service password reset improvement action can be assigned to [answer choice].

Twenty-four hours after self-service password reset (SSPR) is enabled for all users. Points achieved will be [answer choice].

User1 only
User1 only
Group1 only
User1 and Group1 only
Group1 and Group2 only
User1, Group1, and Group2

27 / 27
0 / 27
1 / 27
2 / 27
5 / 27
27 / 27

Answer:
Microsoft 365

The Enable self-service password reset improvement action can be assigned to [answer choice].

Twenty-four hours after self-service password reset (SSPR) is enabled for all users. Points achieved will be [answer choice].

User1 only
User1 only
Group1 only
User1 and Group1 only
Group1 and Group2 only
User1, Group1, and Group2

27 / 27
0 / 27
1 / 27
2 / 27
5 / 27
27 / 27

説明

Answer Area

The Enable self-service password reset improvement action can be assigned to [answer choice]. User1 only

Twenty-four hours after self-service password reset (SSPR) is enabled for all users, Points achieved will be [answer choice]. 27 / 27

最新問題: 66

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Azure Active Directory (Azure AD) から、Group1 という名前のセキュリティ グループを作成します。10 人のユーザーを Group1 に追加します。

Group1 のメンバーが非準拠デバイスから Microsoft Exchange Online に接続する場合は、場所に関係なく、アプリによる制限を適用する必要があります。

あなたは何をすべきか？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。

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	v
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	v
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Answer:

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	v
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	v
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

説明

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	v
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailboxPolicy and Set-OwaMailboxPolicy	v
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

最新問題: 67

Microsoft 365 サブスクリプションをお持ちです。

セキュリティ マネージャーは、データ損失防止 (DLP) ポリシーの一致が発生するたびに電子メール メッセージを受信します。

アラート通知を実行可能な DLP イベントに制限する必要があります。

あなたは何をすべきか？

- A. セキュリティとコンプライアンス管理センターから、DLP ポリシーのポリシー ヒントを変更します。
- B. Cloud App Security 管理センターから、アラートにフィルターを適用します。
- C. セキュリティとコンプライアンス管理センターから、DLP ポリシーのユーザー オーバーライド設定を変更します。
- D. セキュリティとコンプライアンス管理センターから、アラート ポリシーの一致したアクティビティのしきい値を変更します。

Answer: D (メッセージを残す)

参照：

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

最新問題: 68

Microsoft 365 サブスクリプションをお持ちです。

サブスクリプションの監査を有効にします。

Auditor という名前のユーザーに監査ログをレビューする機能を提供する予定です。

監査人をグローバル管理者の役割グループに追加します。

数日後、Auditor が監査を無効にしていることがわかりました。

グローバル管理者役割グループから監査人を削除し、監査を有効にします。

監査を無効にできないようにする

最小特権の原則を使用する

監査ログを確認できる

どの役割グループに監査人を追加する必要がありますか？

A. コンプライアンス管理者

B. 警備員

C. セキュリティ管理者

D. セキュリティリーダー

Answer: B ([メッセージを残す](#))

最新問題: 69

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

ユーザーが Active Directory (AD) ドメインのメンバーであるコンピューターからドキュメント ライブラリとの同期関係を確立したときに、SharepointAdmins@contoso.com がアラートを受信するようにする必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

Answer:

1. セキュリティ & コンプライアンス センターの [アラートの管理] に移動します。
2. [アクティビティ アラート] ページで、[+ 新規] をクリックします。
アクティビティ アラートを作成するためのフライアウト ページが表示されます。

Name *:

A

Description

B

Alert type

Custom ▾

C

Send this alert when... *

D

Activities *:



Choose activities for alert ▾

Users:

Show results for all users

Send this alert to... *

E

Recipients *:

Show results for all users

3. 次のフィールドに入力してアクティビティアラートを作成します。

- a. 名前アラートの名前を入力します。アラート名は組織内で一意である必要があります。
- b. 説明 (オプション) - 追跡されるアクティビティやユーザー、電子メール通知の送信先ユーザーなど、アラートについて説明します。説明は、他の管理者にアラートの目的を説明するための迅速かつ簡単な方法を提供します。
- c. アラートの種類 - [カスタム] オプションが選択されていることを確認してください。
- d. このアラートを送信するタイミング - 「このアラートを送信するタイミング」をクリックし、次の2つのフィールドを構成します。
アクティビティ - ドロップダウン リストをクリックして、アラートを作成できるアクティビティ

を表示します。これは、Office 365 監査ログを検索するときに表示されるアクティビティ リストと同じです。1 つ以上の特定のアクティビティを選択することも、アクティビティ グループ名をクリックしてグループ内のすべてのアクティビティを選択することもできます。これらのアクティビティの説明については、「監査ログの検索」の「監査対象のアクティビティ」セクションを参照してください。アラートに追加したアクティビティをユーザーが実行すると、電子メール通知が送信されます。

ユーザー - このボックスをクリックして、1 人以上のユーザーを選択します。このボックス内のユーザーが、[アクティビティ] ボックスに追加したアクティビティを実行すると、アラートが送信されます。組織内のユーザーがアラートで指定されたアクティビティを実行したときにアラートを送信するには、[ユーザー] ボックスを空白のままにします。

e. このアラートの送信先 - [このアラートを送信] をクリックし、[受信者] ボックスをクリックして名前を入力し、ユーザー ([ユーザー] ボックスで指定) がアクティビティ ([アクティビティ] ボックスで指定) を実行したときに電子メール通知を受信するユーザーを追加します。)。デフォルトで受信者のリストに追加されることに注意してください。このリストから自分の名前を削除できます。

4. 「保存」をクリックしてアラートを作成します。

新しいアラートが [アクティビティ アラート] ページのリストに表示されます。

Name	Recipients	Status ▲	Date modified
Executive mailbox alert	compliance@contoso.com	On	2016-06-08 14:42:02
SharePoint upload alert	admin@contoso.com	Off	2016-06-08 14:23:39
External sharing alert	admin@contoso.com	Off	2016-06-08 14:24:08

アラートのステータスはオンに設定されます。アラートの送信時に電子メール通知を受信する受信者もリストされることに注意してください。

参照：

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-activity-alerts?view=o365-worldwide>

最新問題: 70

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

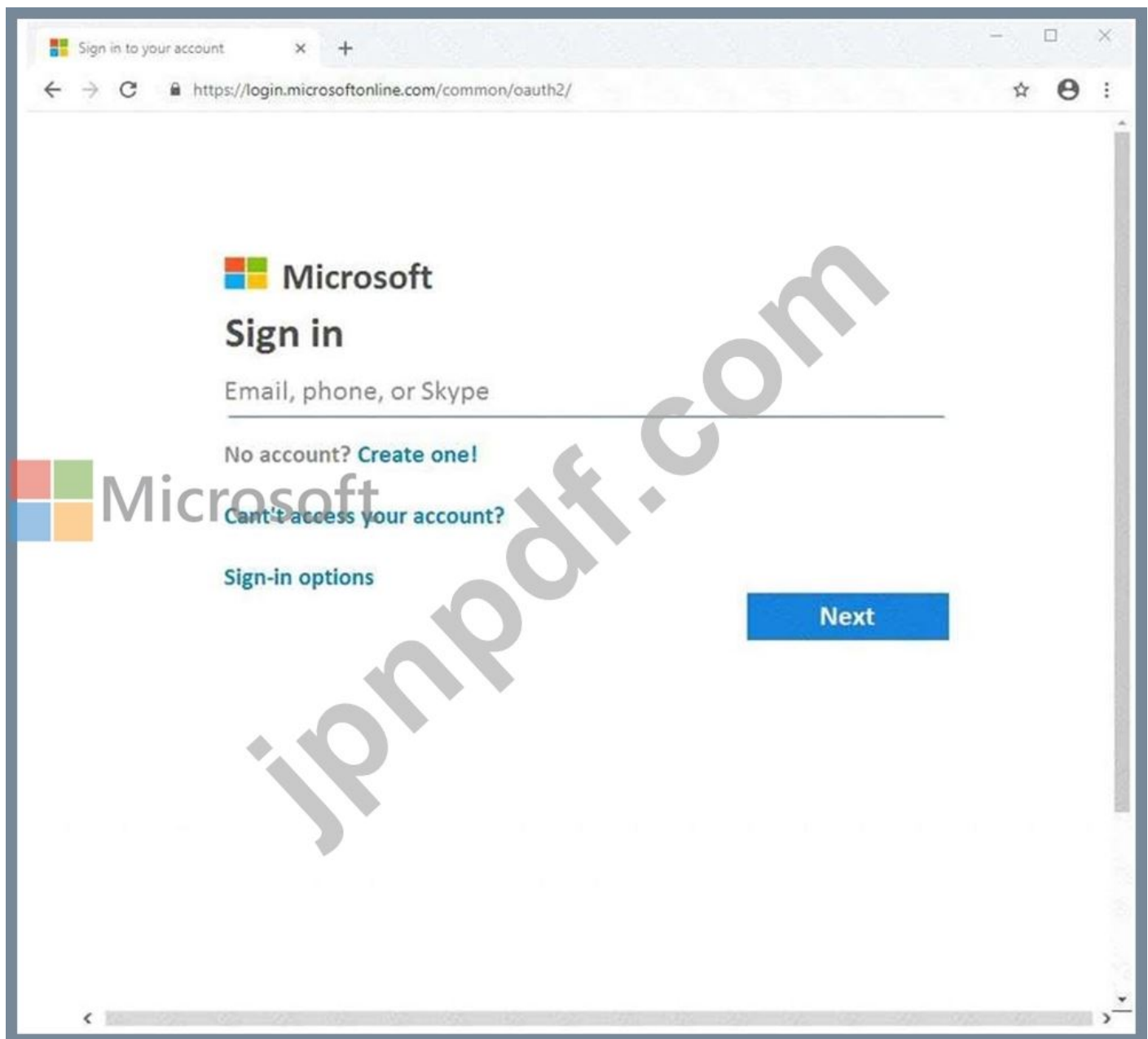
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいただけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

パスワードを入力するには、「パスワードの入力」ボックスにカーソルを置き、下のパスワードを

クリックします。

Microsoft 365 ユーザー名:

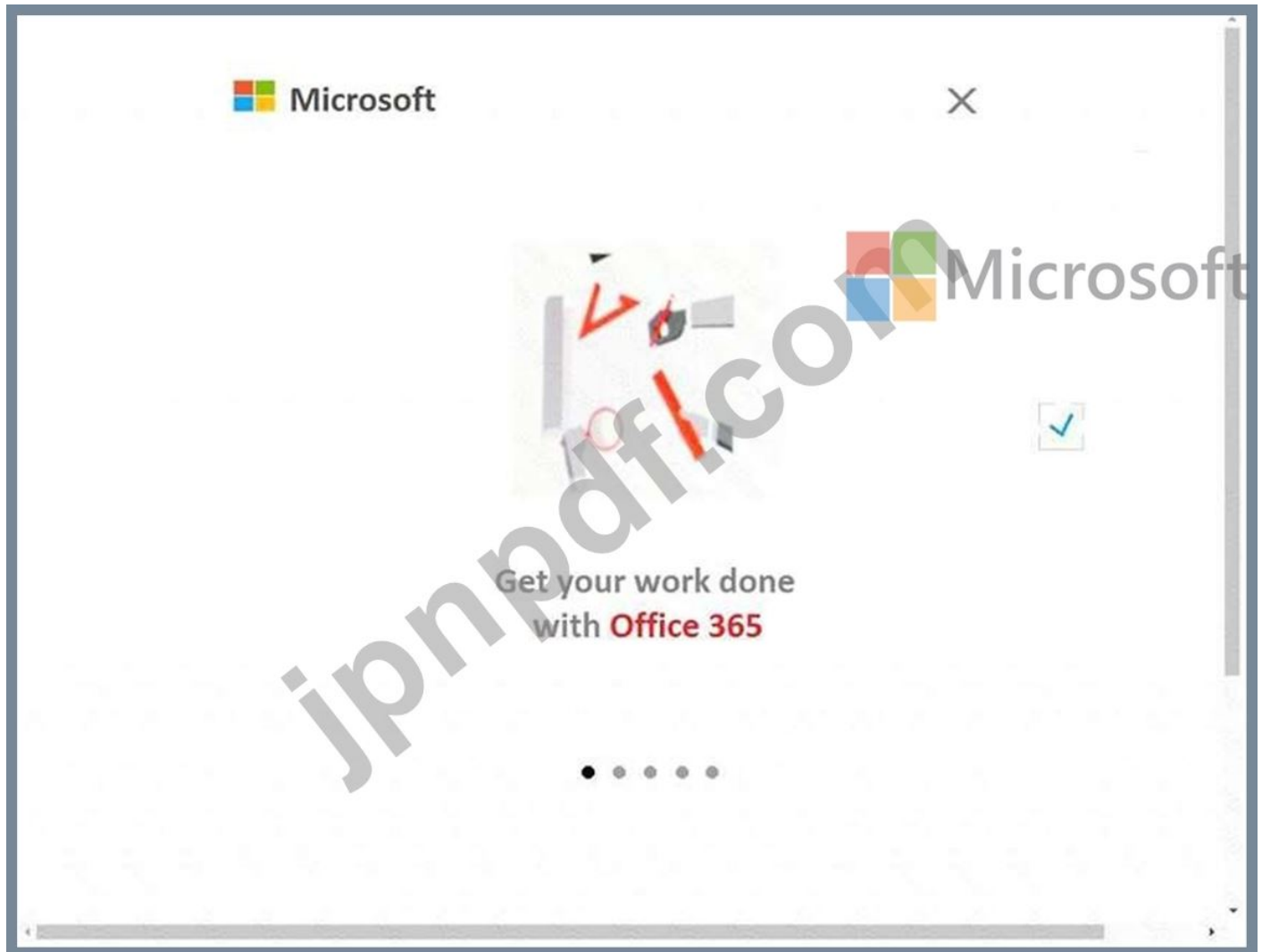
admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308



Microsoft



Microsoft

Brainstorm
together in **Word**



Microsoft



Microsoft

Stay on top of what matters with **Outlook**





Access Office 365 apps and documents in one place with **Office.com**



Microsoft Office Home x +

office.com/auth=2

Contoso electronics Office 365

Good morning Install Office

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Integrated Team Sales Process

You edited this Jan 15

You edited this Jan 15

Sales Results Overview
lodse000198.sharepoint.co...

Sales Process
lodse000198.sharepoint.co...

Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

AD Slogans



AD Slogans

lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



Microsoft



Microsoft

No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

Upload and open...

New

Go to OneDrive →

OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →

SharePoint

Frequent sites

Following



Sales and Marketing



Retail



Communication Site

SharePoint

Frequent sites

Following



Contoso Landings



Contoso Web 3



Executive Corner

Go to SharePoint →



Microsoft

Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

Allan Deyoung という名前のユーザーのメールボックスを保留する電子情報開示ケースを作成する必要があります。保留には、件名に「merger」または「Contoso」という単語が含まれる電子メールメッセージを保持する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

1. セキュリティ & コンプライアンス センターの [電子情報開示] に移動し、[ケースの作成] をクリックします。
2. [新しいケース] ページで、ケースに名前を付け、必要に応じて説明を入力し、[保存] をクリックします。ケース名は組織内で一意である必要があります。

New case

Enter a name and description
Give this case a friendly name so you can easily find it again later.

*Case name

Description

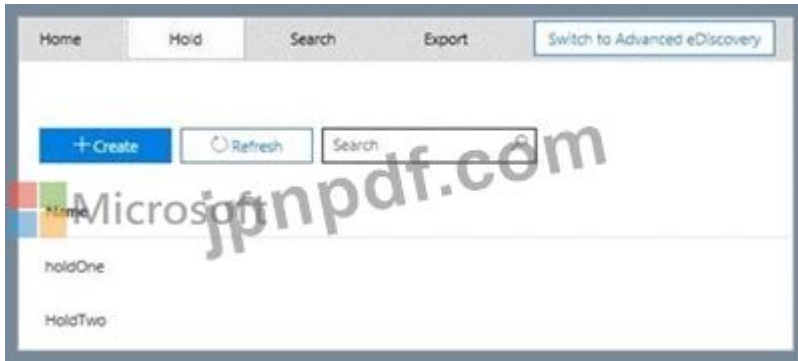
Save Cancel Microsoft

新しいケースがページ上のケースのリストに表示されます。ケース名の上にカーソルを置くと、

ケースのステータス (アクティブまたはクローズ)、ケースの説明 (前のステップで作成されたもの)、ケースが最後に変更された日時など、ケースに関する情報が表示されます。そしてそれを変えたのは誰なのか。

電子情報開示ケースの保留を作成するには:

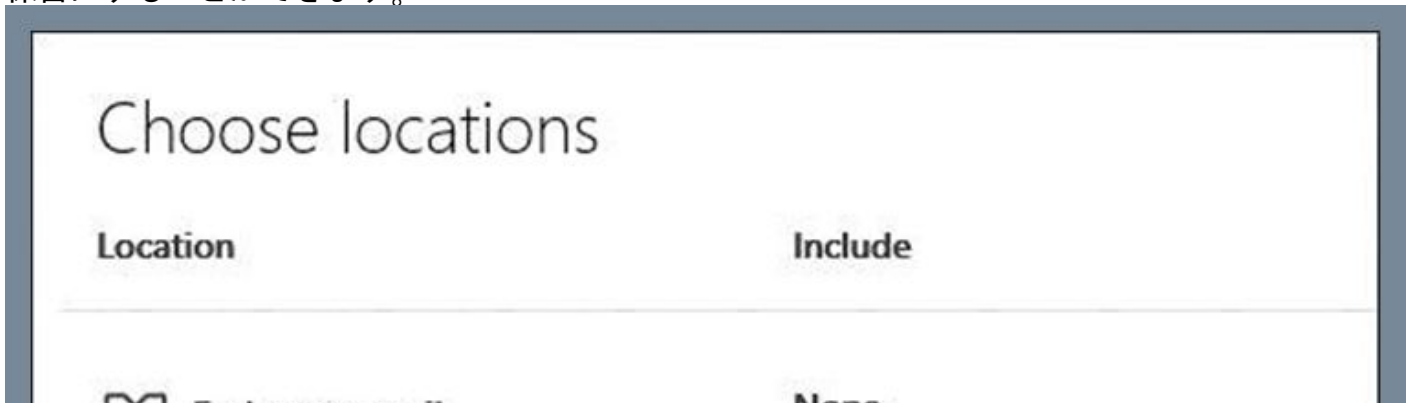
1. セキュリティ/コンプライアンス センターで、をクリックして組織内のケースのリストを表示します。
2. 保留を作成するケースの横にある [開く] をクリックします。
3. ケースのホームページで、保留] タブをクリックします。



4. [保留] ページで、[作成] をクリックします。
5. [保留に名前を付ける] ページで、保留に名前を付けます。保留の名前は組織内で一意である必要があります。



6. (オプション) [説明] ボックスに、保留の説明を追加します。
7. 次へ] をクリックします。
8. 保留するコンテンツの場所を選択します。メールボックス、サイト、パブリック フォルダーを保留にすることができます。



-  Exchange email
-  Office 365 group email
-  Skype for Business
-  Teams messages
-  To-Do
-  Yammer conversations


None
Choose users, groups, or teams



-  SharePoint sites
-  OneDrive accounts
-  Office 365 group sites
-  Teams sites
-  Yammer networks

None
Choose sites



-  Exchange public folders

None



* 電子メールの交換 - [ユーザー、グループ、またはチームの選択] をクリックし、次に [ユーザー、

グループ、またはチームの選択] をクリックします。

*再びチーム。保留するメールボックスを指定します。検索ボックスを使用して、保留するユーザーのメールボックスと配布グループを検索します (グループ メンバーのメールボックスを保留する場合)。Microsoft チーム、Yammer グループ、または Office 365 グループに関連付けられたメールボックスを保留することもできます。

ユーザー、グループ、チームのチェック ボックスをオンにし、[選択] をクリックして、[完了] をクリックします。

ノート

[ユーザー、グループ、またはチームの選択] をクリックして保留にするメールボックスを指定すると、表示されるメールボックス ピッカーは空になります。これはパフォーマンスを向上させるための設計によるものです。このリストにユーザーを追加するには、検索ボックスに名前 (最低 3 文字) を入力します。

9. クエリベースの保持を設定した後、

10. 設定を確認し、クリックします。

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-cases?view=o365-worldwide#step-4-pla>

最新問題: 71

カスタム ネットワーク インジケータがオンになっている Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) 展開があります。Microsoft Defender ATP は、Windows を実行する 2 台のコンピューターを保護します

以下の表に示すように、10。

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender ATP には、次の表に示すマシン グループがあります。

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp
Last	Ungrouped machines (default)	None

Microsoft Defender セキュリティ センターから、次の表に示す URL/ドメイン インジケータを作成します。

URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	<input type="radio"/>	<input type="radio"/>
From a web browser on Computer1,you can open http://www.litwareinc.com/public.	<input type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
From a web browser on Computer1,you can open http://www.litwareinc.com/public.	<input checked="" type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input type="radio"/>	<input checked="" type="radio"/>

説明

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
From a web browser on Computer1,you can open http://www.litwareinc.com/public.	<input checked="" type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 72

Microsoft 365 サブスクリプションの数人のユーザーが、添付ファイルのない電子メールメッセージを受信したと報告しています。

メッセージから削除された添付ファイルを確認する必要があります。

どの 2 つのツールを使用できますか? それぞれの正解は完全な解決策を示します。

注: 正しく選択するたびに 1 ポイントの価値があります。

- A. Exchange 管理センター
- B. Azure ATP 管理センター
- C. Web 上の Outlook
- D. セキュリティとコンプライアンスの管理センター
- E. Microsoft Azure セキュリティ センター

Answer: [\(解答を表示する\)](#)

説明/参照:

参考文献:

<https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files>

最新問題: 73

MFA 構成にどの IP アドレス空間を含める必要がありますか?

- A. 131.107.83.0/28

B. 192.168.16.0/20

C. 172.16.0.0/24

D. 192.168.0.0/20

Answer: B ([メッセージを残す](#))

トピック 2、Contoso, Ltd

概要

Contoso, Ltd. は、モントリオールに本社を置き、シアトルとニューヨークに 3 つの支社を構えるコンサルティング会社です。

当社は、次の表に示す営業所を設置しております。

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

Contoso には、IT、人事 (HR)、法務、マーケティング、財務の部門があります。Contoso は Microsoft を使用しています

365。

既存の環境

インフラストラクチャー

ネットワークには、Microsoft Azure Active Directory (Azure AD) テナントに同期されている contoso.com という名前の Active Directory ドメインが含まれています。パスワードライトバックが有効になっています。

ドメインには、Windows Server 2016 を実行するサーバーが含まれています。ドメインには、Windows 10 Enterprise を実行するラップトップおよびデスクトップコンピューターが含まれています。

各クライアントコンピュータには 1 つのボリュームがあります。

各オフィスは NAT デバイスを使用してインターネットに接続します。オフィスの IP アドレスは次の表に示されています。

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

名前付きロケーションは、次の表に示すように Azure AD で定義されます。

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

[多要素認証] ページから、198.35.3.0/24 のアドレススペースが信頼できる IP リストに定義されます。

Azure Multi-Factor Authentication (MFA) は、財務部門のユーザーに対して有効になっています。

テナントには、次の表に示すユーザーが含まれます。

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

テナントには、次の表に示すグループが含まれています。

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

カスタマー ロックボックスは Microsoft 365 で有効になっています。

Microsoft Intune の構成

Intune に登録されているデバイスは、次の表に示すように構成されています。

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

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

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

デバイス コンプライアンス ポリシーには、次の表に示す割り当てがあります。

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

[コンプライアンス ポリシーが割り当てられていないデバイスをマークする] 設定が [準拠] に設定されます。

要件

技術的要件

Contoso は次の技術要件を特定します。

- * 最小特権の原則を使用する
- * User1 がレポート閲覧者の役割をユーザーに割り当てられるようにします
- * User6 がカスタマー ロックボックスのリクエストをできるだけ早く承認するようにします。
- * User9 が Azure AD Privileged Identity Management を実装できることを確認する

最新問題: 74

次の図に示すように、コンプライアンス マネージャーが表示されます。



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

注: 正しく選択するたびに 1 ポイントの価値があります。

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	<input checked="" type="checkbox"/>
review actions	<input type="checkbox"/>
perform an assessment	<input type="checkbox"/>
create a service request with Microsoft	<input type="checkbox"/>

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	<input checked="" type="checkbox"/>
proves that the organization is compliant	<input type="checkbox"/>
shows that actions are required to evaluate compliance	<input type="checkbox"/>

Answer:

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	<input checked="" type="checkbox"/>
review actions	<input type="checkbox"/>
perform an assessment	<input type="checkbox"/>
create a service request with Microsoft	<input type="checkbox"/>

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	<input checked="" type="checkbox"/>
proves that the organization is compliant	<input type="checkbox"/>
shows that actions are required to evaluate compliance	<input type="checkbox"/>

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-m>

最新問題: 75

ワークロード管理者のセキュリティ要件を満たすようにアクセス レビューを構成する予定です。アクセス レビュー ポリシーを作成し、スコープとグループを指定します。他にどのような設定を構成する必要がありますか? 回答するには、回答領域で適切な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。

Set the frequency to:

One time	<input checked="" type="checkbox"/>
Weekly	<input type="checkbox"/>
Monthly	<input type="checkbox"/>

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	<input checked="" type="checkbox"/>
Advanced settings	<input type="checkbox"/>
Programs	<input type="checkbox"/>
Reviewers	<input type="checkbox"/>

Answer:

set the frequency to.

One time	<input checked="" type="checkbox"/>
Weekly	<input type="checkbox"/>
Monthly	<input type="checkbox"/>

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	<input checked="" type="checkbox"/>
Advanced settings	<input type="checkbox"/>
Programs	<input type="checkbox"/>
Reviewers	<input type="checkbox"/>

最新問題: 76

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー 閲覧者の役割はどのユーザーにも割り当てられていません。

User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないようにする解決策を推奨する必要があります。

解決策: User5 に割り当てられたライセンスを変更することをお勧めします。

これは目標を達成していますか?

A. いいえ

B. はい

Answer: [\(解答を表示する\)](#)

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%**w特別割引コード: **Freepdfdumps**)

最新問題: 77

Microsoft 365 サブスクリプションでいくつかの Advanced Threat Protection (ATP) ポリシーを構成します。

User1 という名前のユーザーが脅威管理ダッシュボードで ATP レポートを表示できるようにする必要があります。

User1 に必要なロール権限を提供するのはどのロールですか？

- A. セキュリティ管理者
- B. Exchange 管理者
- C. コンプライアンス管理者
- D. メッセージ センター リーダー

Answer: A ([メッセージを残す](#))

説明/参照:

<https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are-need-to-view-the-atp-reports>

最新問題: 78

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	Group2
User3	Group1, Group2

次の設定を持つ Azure Active Directory (Azure AD) Identity Protection サインイン リスク ポリシーを作成して適用します。

割り当て: グループ 1 を含む、グループ 2 を除外

条件 :ユーザーのリスクレベルが中以上

アクセス: アクセスを許可、パスワードの変更が必要

ユーザーはサインインを試行します。各ユーザーのリスク レベルを次の表に示します。

User	User risk level
User1	High
User2	Medium
User3	High

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ]を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 must change his password.	<input type="radio"/>	<input type="radio"/>
User2 must change his password.	<input type="radio"/>	<input type="radio"/>
User3 must change his password.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 must change his password.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must change his password.	<input type="radio"/>	<input checked="" type="radio"/>
User3 must change his password.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 79

Microsoft 365 サブスクリプションをお持ちです。監査が有効になっています。

User1 という名前のユーザーは、Group1 という名前の動的セキュリティグループのメンバーです。

User1 が Group1 のメンバーではなくなっていることがわかります。

User1 が Group1 から削除された理由を特定するには、監査ログを検索する必要があります。

検索ではどの 2 つのアクションを使用する必要がありますか? 回答するには、回答領域で適切なアクティビティを選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Search
Results

Clear


Activities

Show results for all activities

Clear all to show results for all activities

Search

Date ▼	IP address	User	Activity	Item
User administration activities				
Added user	Deleted user		Set license properties	
Reset user password	Changed user password		Changed user license	
Updated user	Set property that forces user to change password			
Azure AD group administration activities				
Added group	Updated group		Deleted group	
Added member to group	Removed member from group			
Application administration activities				
Added service principal	Removed a service principal from the directory		Set delegation entry	
Removed credentials from a service principal	Added delegation entity		Added credentials to a service principal	


Microsoft

Answer:

Search

Clear

Results

Activities

Date	IP address	User	Activity	Item
<input type="text" value="Show results for all activities"/>				

× Clear all to show results for all activities

Search

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

最新問題: 80

20 のデータ損失防止 (DLP) ポリシーを含む Microsoft 365 サブスクリプションがあります。次のことを特定する必要があります。

- * ポリシー アラートをトリガーせずに適用されるルール
- * DLP ポリシーに一致した上位 10 個のファイル
- * 誤って分類されたアラート

各要件に対してどのレポートを使用する必要がありますか? 回答するには、適切なレポートを正しい要件にドラッグします。各レポートは 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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

<input type="text" value="DLP policy matches"/>	<input type="text" value="Rules that are applied without triggering a policy alert:"/>
<input type="text" value="False positive and override"/>	<input type="text" value="The top 10 files that have matched DLP policies:"/>
<input type="text" value="Incident reports"/>	<input type="text" value="Alerts that are miscategorized:"/>

Answer:



最新問題: 81

Azure Active Directory (Azure AD) コネクタと Microsoft Office 365 コネクタを備えた Azure Sentinel ワークスペースがあります。

次のタスクを実行するには、組み込みのロールベースのアクセス制御 (RBAC) ロールを割り当てる必要があります。

* プレイブックを作成して実行します。

* インシデントを管理します。

ソリューションでは、最小特権の原則を使用する必要があります。

どの2つの役割を割り当てるべきですか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに1ポイントの価値があります。

- A. オートメーションオペレーター
- B. Azure Sentinel レスポンダー
- C. Automation Runbook オペレーター
- D. Azure Sentinel の貢献者
- E. ロジック アプリのコントリビューター

Answer: ([解答を表示する](#))

説明/参照:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

最新問題: 82

Microsoft 365 サブスクリプションをお持ちです。

次の例に示すように、Label1 という名前の保持ラベルを作成します。

Create a label to help users classify their content.

- Name your label
- Label settings
- Review your settings

Review your settings

Name Edit
Label1

Descriptions for admins Edit

Description for users Edit

Retention Edit

2 years
Retain and Delete
Based on when it was created
Use Label to classify content as a "Record"



[Back](#) [Create this label](#) [Cancel](#)

Label1 を SharePoint サイトに公開します。

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

注: 正しく選択するたびに 1 ポイントの価値があります。

<p>If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].</p>	<table border="1"> <tr> <td style="text-align: right;">▼</td> </tr> <tr> <td>never delete the file.</td> </tr> <tr> <td>delete the file before January 1, 2021.</td> </tr> <tr> <td>delete the file after January 1, 2021.</td> </tr> </table>	▼	never delete the file.	delete the file before January 1, 2021.	delete the file after January 1, 2021.
▼					
never delete the file.					
delete the file before January 1, 2021.					
delete the file after January 1, 2021.					
<p>If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].</p>	<table border="1"> <tr> <td style="text-align: right;">▼</td> </tr> <tr> <td>always remain in the library.</td> </tr> <tr> <td>remain in the library until you delete the file.</td> </tr> <tr> <td>be deleted automatically on March 15, 2021.</td> </tr> </table>	▼	always remain in the library.	remain in the library until you delete the file.	be deleted automatically on March 15, 2021.
▼					
always remain in the library.					
remain in the library until you delete the file.					
be deleted automatically on March 15, 2021.					

Answer:

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

Microsoft	▼
never delete the file.	
delete the file before January 1, 2021.	
delete the file after January 1, 2021.	

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

	▼
always remain in the library.	
remain in the library until you delete the file.	
be deleted automatically on March 15, 2021.	

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/labels>

最新問題: 83

どのポリシーがどのデバイスに適用されますか? 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。

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

Answer:

DevicePolicy1:

- None
- Device1 only
- Device3 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device3

DevicePolicy2:

- None
- Device4 only
- Device2 and Device4 only
- Device2, Device3, and Device 4 only

最新問題: 84

contoso.com という名前の Microsoft Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

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

次の設定を持つ Azure AD Identity Protection ユーザー リスク ポリシーを作成して適用します。

割り当て: グループ 1 を含む、グループ 2 を除外

条件: サインインリスクが低以上

アクセス: アクセスを許可、パスワードの変更が必要

ポリシーが User1 と User2 にどのような影響を与えるかを特定する必要があります。

User1 と User2 が見慣れない場所からサインインするとどうなりますか? 回答するには、回答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。


Must change their password:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	

Prompted for MFA:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	

Answer:

Must change their password:		▼
	User1 only	
User2 only		
Both User1 and User2		
Neither User1 not User2		
Prompted for MFA:		▼
	User1 only	
User2 only		
Both User1 and User2		
Neither User1 not User2		

最新問題: 85

次のものを含むオンプレミスの Hyper-V インフラストラクチャがあります。

Active Directory ドメイン

Server1 という名前のドメイン コントローラー

Server2 という名前のメンバー サーバー

セキュリティ ポリシーでは、Server1 がインターネットに接続できないように指定されています。Server2 はインターネットに接続できます。

ドメインのセキュリティを監視するには、Azure Advanced Threat Protection (ATP) を実装する必

要があります。

各サーバーで何を構成する必要がありますか? 答えるには、適切なコンポーネントを正しいサーバーにドラッグします。各コンポーネントは1回だけ使用することも、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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに1ポイントの価値があります。

Components

- An Azure ATP sensor
- An Azure ATP standalone sensor
- An event subscription
- A port mirroring source

Answer Area

Server1: Component

Server2: Component

Component

Answer:

Components

- An Azure ATP sensor
- An Azure ATP standalone sensor
- An event subscription
- A port mirroring source

Answer Area

Server1: An Azure ATP standalone sensor

Server2: A port mirroring source

An event subscription

最新問題: 86

管理者が電子メール メッセージやドキュメントにフッターを追加するラベルを公開できるようにする必要があります。

このタスクを完了するには、Microsoft Office 365 ポータルにサインインします。

Answer:

機密ラベルを設定する必要があります。

セキュリティとコンプライアンス管理センターに移動します。

[分類] > [機密ラベル] に移動します。

[+ ラベルの作成] をクリックして新しいラベルを作成します。

ラベルに名前と説明を入力し、[次へ] をクリックします。

[暗号化] オプションを [なし] のままにして、[次へ] をクリックします。

[コンテンツ マーキング] ページで、[フッターを追加] チェックボックスをオンにします。

[テキストのカスタマイズ] リンクをクリックしてフッター テキストを追加し、[保存] をクリックします (質問の場合、追加するテキストは関係ありません)。

次へ」をクリックします。

[Office アプリの自動ラベル付け] をオフのままにして、[次へ] をクリックします。

送信」ボタンをクリックして変更を保存します。

これでラベルを公開する準備が整いました。完了」ボタンをクリックしてページを終了し、ラベルを作成します。

最新問題: 87

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正解がある場合もありますが、他の質問セットには正解がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー閲覧者の役割はどのユーザーにも割り当てられていません。

User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないようにする解決策を推奨する必要があります。

解決策: User1 をコンプライアンス マネージャー共同作成者ロールから削除することをお勧めします。

それは目標を達成していますか？

A. はい

B. いいえ

Answer: B (メッセージを残す)

説明

参考文献:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

最新問題: 88

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 サブスクリプションがあります。Site1 には、次の表に示すフォルダーが含まれています。

Name	File in folder
Folder1	File1
Folder2	File2

09:00 に、次の図に示すように、Policy1 という名前の Microsoft Cloud App Security ポリシーを作成します。

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

× App equals Microsoft SharePoint...

+

Apply to:
selected folders Currently supports Box, SharePoint, Dropbox, OneDrive.

Folder1 (Microsoft SharePoint Online) ×

[Add more folder\(s\)](#)

Apply to:
all file owners

Inspection method
None Alerts

Create an alert for each matching file [Restore default settings](#)

Daily alert limit 5

Send alert as email ⓘ

Send alert as text message ⓘ

[Save as default settings](#)

Send alerts to Flow [Create a playbook in Flow](#)

Policy1 を作成した後、次の表に示すようにファイルを Site1 にアップロードします。

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
File1 triggers an alert from Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>

参照 :

<https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

最新問題: 89

ネットワークにはオンプレミスの Active Directory ドメインが含まれています。ドメインには、Windows Server を実行し、高度な監査が有効になっているサーバーが含まれています。サーバーのセキュリティ ログは、サードパーティの SIEM ソリューションを使用して収集されません。

Microsoft 365 サブスクリプションを購入し、スタンドアロン センサーを使用して Azure Advanced Threat Protection (ATP) を展開することを計画しています。

機密性の高いグループが変更されたときと、悪意のあるサービスが作成されたときを確実に検出できるようにする必要があります。

あなたは何をすべきか？

- A. Office 365 セキュリティ & コンプライアンス センターで監査を構成します。
- B. Azure ATP センサーの遅延更新をオフにします。
- C. SIEM と Azure ATP を統合します。
- D. Azure ATP センサーでドメイン シンクロナイザー候補の設定を変更します。

Answer: D ([メッセージを残す](#))

最新問題: 90

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザーとデバイス オブジェクトは毎日追加および削除されます。営業部門のユーザーは頻繁にデバイスを変更します。

次の 3 つのグループを作成する必要があります。

Group	Requirement
1	All the devices of users where the Department attributes is set to Sales
2	All the devices where the Department attribute is set to Sales
3	All the devices where the deviceOwnership attribute is set to Company

ソリューションでは、管理労力を最小限に抑える必要があります。

メンバーシップの種類ごとに作成するグループ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。

Groups that have assigned membership:

0
1
2
3

Groups that have dynamic membership:

0
1
2
3


Answer:

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	




説明

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	



参考文献:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dyn>

最新問題: 91

カスタム ネットワーク インジケーターがオンになっている Microsoft Defender for Endpoint 展開があります。

次の表に示すように、Microsoft Defender for Endpoint は、Windows 10 を実行する 2 台のコンピューターを保護します。

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender のエンドポイントには、次の表に示すデバイス グループがあります。

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp

Answer Area



Statements

From a web browser on Computer1, you can open http://www.contoso.com.	Yes	No
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	<input type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area



Statements

From a web browser on Computer1, you can open http://www.contoso.com.	Yes	No
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	<input type="radio"/>	<input checked="" type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com.	<input checked="" type="radio"/>	<input type="radio"/>

説明

Answer Area



Statements

From a web browser on Computer1, you can open http://www.contoso.com.	Yes	No
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	<input checked="" type="radio"/>	<input type="radio"/>
From a web browser on Computer2, you can open http://www.litwareinc.com	<input type="radio"/>	<input checked="" type="radio"/>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
 GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **92**

Azure Sentinel ワークスペースがあります。

Azure Active Directory (Azure AD) Identity Protection が危険なサインインを検出したときに Azure Sentinel アラートを生成するルールを構成します。ユーザーに連絡し、報告された危険なサインインが正当なものかどうかを確認するための Azure Logic Apps ソリューションを開発します。

次の要件を満たすようにワークスペースを構成する必要があります。

* 危険なサインインに対してアラートがトリガーされた場合は、Azure ロジック アプリを呼び出します。

* Azure Sentinel ポータルに、検出および解決された危険なサインインの統計を表示するカスタムダッシュボードを追加します。

各要件を満たすには、Azure Sentinel で何を構成する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

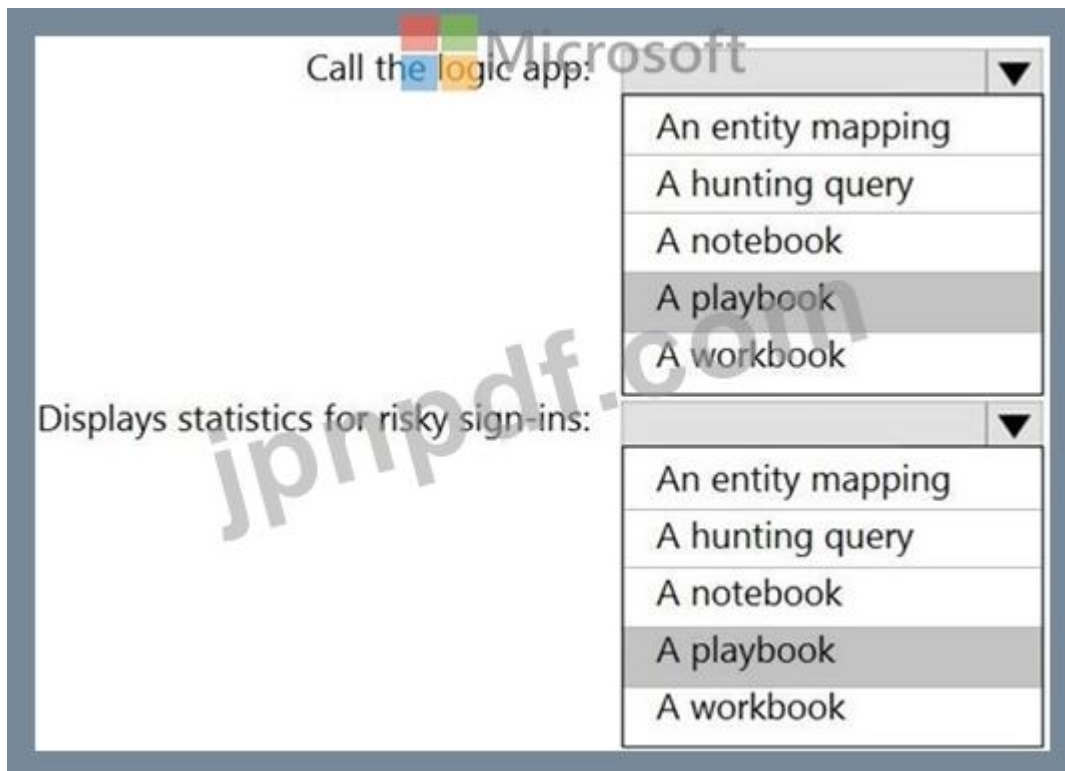
Call the logic app:

▼
An entity mapping
A hunting query
A notebook
A playbook
A workbook
▼
An entity mapping
A hunting query
A notebook
A playbook
A workbook

 Microsoft
displays statistics for risky sign-ins:

Answer:

テーブルの説明が自動的に生成される



参照：

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

最新問題: 93

次の図に示すように、コンプライアンス マネージャーが表示されます。



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

注: 正しく選択するたびに 1 ポイントの価値があります。

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	V
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	V
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

Answer:

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	V
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	V
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

説明

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	V
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	V
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-m>

最新問題: 94

Admin1 と Admin2 のサインインを保護するソリューションを推奨する必要があります。
推奨事項には何を含めるべきですか?

- A. デバイスのコンプライアンス ポリシー
- B. アクセスレビュー
- C. ユーザーリスクポリシー
- D. サインイン リスク ポリシー

Answer: C ([メッセージを残す](#))

説明

参考文献:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy>
トピック 1、Litware, Inc

概要

Litware, Inc. は、シカゴの本社に 1,000 人のユーザー、サンフランシスコの支社に 100 人のユーザーを抱える金融会社です。

既存の環境

内部ネットワークインフラストラクチャ

ネットワークには単一のドメイン フォレストが含まれています。フォレストの機能レベルは Windows Server 2016 です。

ユーザーは、Active Directory で定義されているサインイン時間制限の対象となります。

ネットワークの IP アドレス範囲は次の表に示されています。

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

オフィスはマルチプロトコル ラベル スイッチング (MPLS) を使用して接続します。

ネットワークでは次のオペレーティング システムが使用されています。

- * Windows Server 2016
- * Windows 10 エンタープライズ
- * Windows 8.1 エンタープライズ

内部ネットワークには、次の表に示すシステムが含まれています。

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

Litware はサードパーティの電子メール システムを使用します。

クラウドインフラストラクチャ

Litware は最近、すべてのユーザーを対象とした Microsoft 365 サブスクリプション ライセンスを

購入しました。

Microsoft Azure Active Directory (Azure AD) Connect がインストールされており、デフォルトの認証設定を使用します。

ユーザー アカウントはまだ Azure AD に同期されていません。

次の表に示す Microsoft 365 ユーザーとグループがあります。

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

計画された変更

Litware は次の変更を実装する予定です。

* 電子メール システムを Microsoft Exchange Online に移行する

* Azure AD Privileged Identity Management を実装する

セキュリティ要件

Litware では、次のセキュリティ要件が特定されています。

* すべての Azure AD ユーザー アカウントを含む Group2 という名前のグループを作成します。Group2 は、Windows Analytics への制限付きアクセスを提供するために使用されます。

* Azure Information Protection ポリシーをパイロット ユーザーに適用するために使用される Group3 という名前のグループを作成します。Group3 にはユーザー アカウントのみを含める必要があります

* Azure Advanced Threat Protection (ATP) を使用して、フォレストを標的とするセキュリティの脅威を検出します。

* Active Directory からロックアウトされたユーザーが Azure AD および Active Directory にサインインできないようにします

* User1 に対するコンプライアンス管理者ロールの永続的適格割り当てを実装します。

* ドメインに参加しているサーバー上で Windows Defender と Windows Defender ATP を統合します。

* ゲスト ユーザー アカウントの Azure リソースへのアクセスをデフォルトで禁止します

* ドメインに参加しているすべてのコンピューターが Azure AD に登録されていることを確認してください

多要素認証 (MFA) の要件

Microsoft Office 365 と Azure のセキュリティ機能は、パイロット Azure ユーザー アカウントを使用してテストされます。

MFA をテストするための次の要件を特定します。

* パイロット ユーザーは、シカゴ オフィスの内部ネットワークからサインインしない限り、MFA を使用する必要があります。

MFA はシカゴ オフィスの内部ネットワークでは使用しないでください。

* 認証試行が疑わしい場合は、ユーザーの場所に関係なく、MFA を使用する必要があります。

* 正当な認証試行の中断は最小限に抑える必要があります。一般要件 Litware は、Active Directory フォレスト内での追加のサーバーとサービスの展開を最小限に抑えたいと考えています。

最新問題: 95

あなたの会社には、次の表に示すユーザーが含まれる Microsoft 365 サブスクリプションがあります。

Name	Member of
User1	Group1
User2	Group2
User3	Group3

同社は Windows Defender Advanced Threat Protection (Windows Defender ATP) を実装しています。Windows Defender ATP には、次の表に示す役割が含まれています。

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP には、次の表に示すマシン グループが含まれています。

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

最新問題: 96

Microsoft 365 E5 サブスクリプションと Sentinel1 という名前の Sentinel ワークスペースがあります。

Sentinel でガイド付き調査 - プロセス アラート ノートブック= を開始する必要があります。

最初に何を作成する必要がありますか？

- A. Azure ロジック アプリ
- B. Azure Machine Learning ワークスペース
- C. Kusto クエリ
- D. Log Analytic ワークスペース

Answer: D ([メッセージを残す](#))

最新問題: 97

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Groups administrator
Admin2	User administrator

contoso.com のグループ名前付けポリシーに禁止単語として「Internal」を追加します。

contoso.com のグループ名前付けポリシーのプレフィックスとして Contoso- を追加します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input checked="" type="radio"/>	<input type="radio"/>

参照：

<https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide>

最新問題: 98

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー 閲覧者の役割はどのユーザーにも割り当てられていません。

User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないようにする解決策を推奨する必要があります。

解決策: User1 をコンプライアンス マネージャー共同作成者ロールから削除することをお勧めします。

これは目標を達成していますか?

A. はい

B. いいえ

Answer: (解答を表示する)

説明/参照:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

最新問題: 99

Microsoft エンドポイント マネージャーを使用する Microsoft 365 E5 サブスクリプションを持っています。

コンプライアンス ポリシー設定は、次の図に示すように構成されています。

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.



2020 年 2 月 25 日に、次の表に示すデバイス コンプライアンス ポリシーを作成します。

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

2020 年 3 月 1 日、ユーザーは次の表に示すように Windows 10 デバイスを Microsoft エンドポイント マネージャーに登録します。

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On March 6, 2020, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On March 12, 2020, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
On March 6, 2020, Device1 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
On March 12, 2020, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 100

Azure サブスクリプションと Microsoft 365 サブスクリプションをお持ちです。

次のアクションを実行する必要があります。

Azure Sentinel をデプロイします。

Azure Sentinel を使用して Microsoft 365 アクティビティ ログを収集します。

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** 

- Turn on Microsoft Graph data connect.
- Add Azure Sentinel.
- Create a SQL pool in Azure Synapse Analytics.
- Connect a data connector.
- Create an Azure Log Analytics workspace.
- Create an Azure Data Lake Analytics account.

Answer:





Actions **Answer Area**

- Turn on Microsoft Graph data connect.
- Add Azure Sentinel.
- Create a SQL pool in Azure Synapse Analytics.
- Connect a data connector.
- Create an Azure Log Analytics workspace.
- Create an Azure Data Lake Analytics account.

Create an Azure Log Analytics workspace.

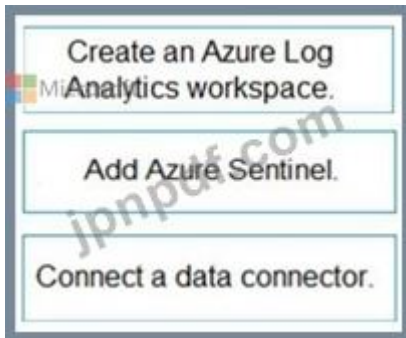
Add Azure Sentinel.

Connect a data connector.

説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーション、チャットまたはテキストメッセージ 説明が自動的に生成



参照 :

<https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard>

<https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365>

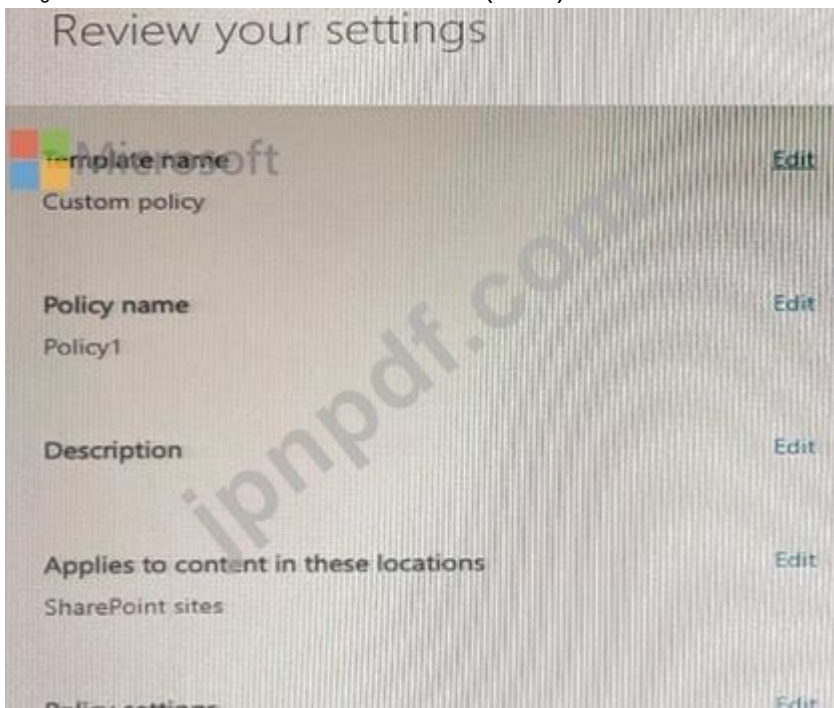
最新問題: 101

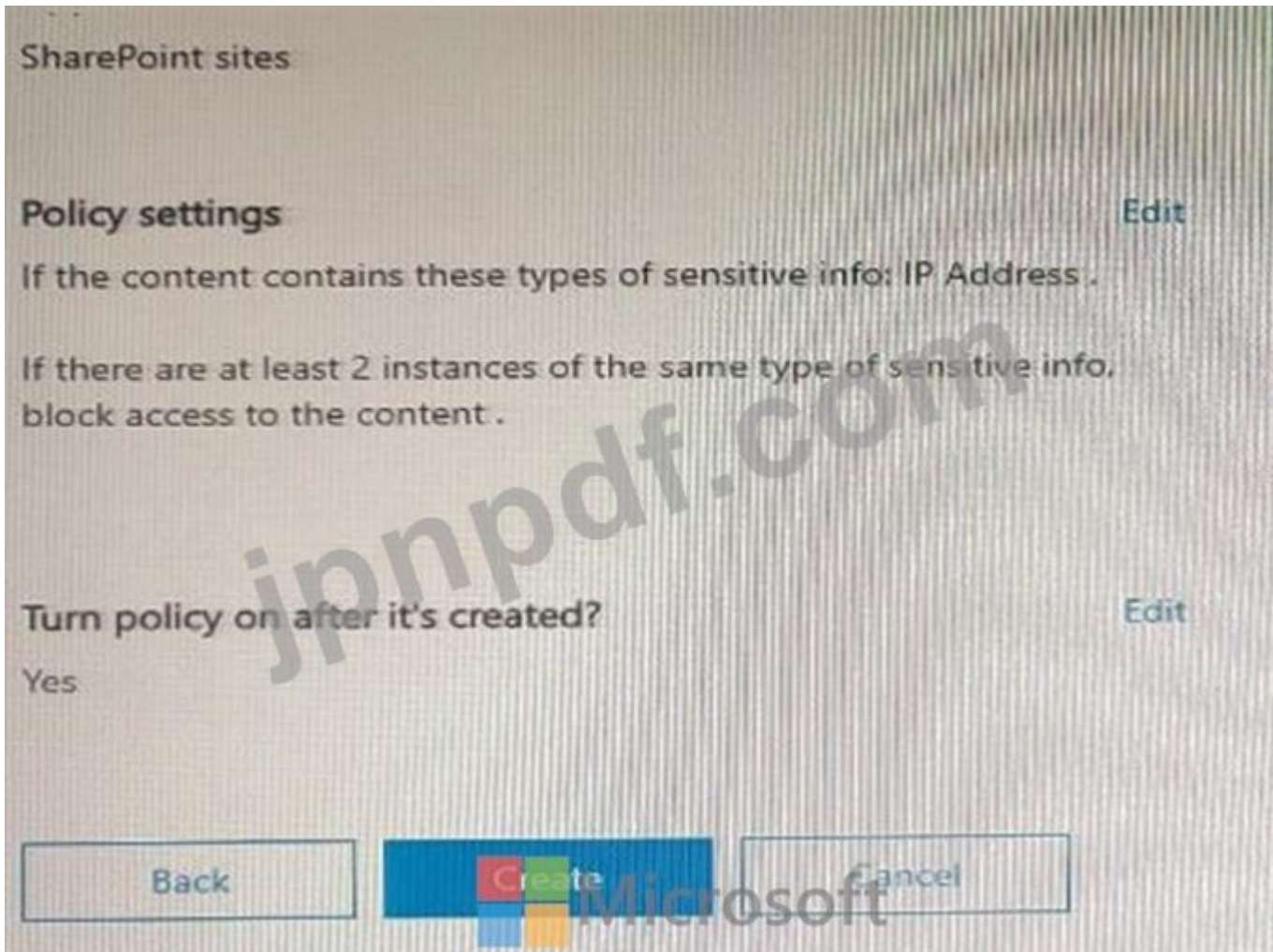
User 1 と User2 という名前の 2 人のユーザーを含む Microsoft E5 サブスクリプションがあります。

Site1 という名前の Microsoft SharePoint サイトがあります。Site1 には、次の表に示すように IP アドレスを含むファイルが保存されます。

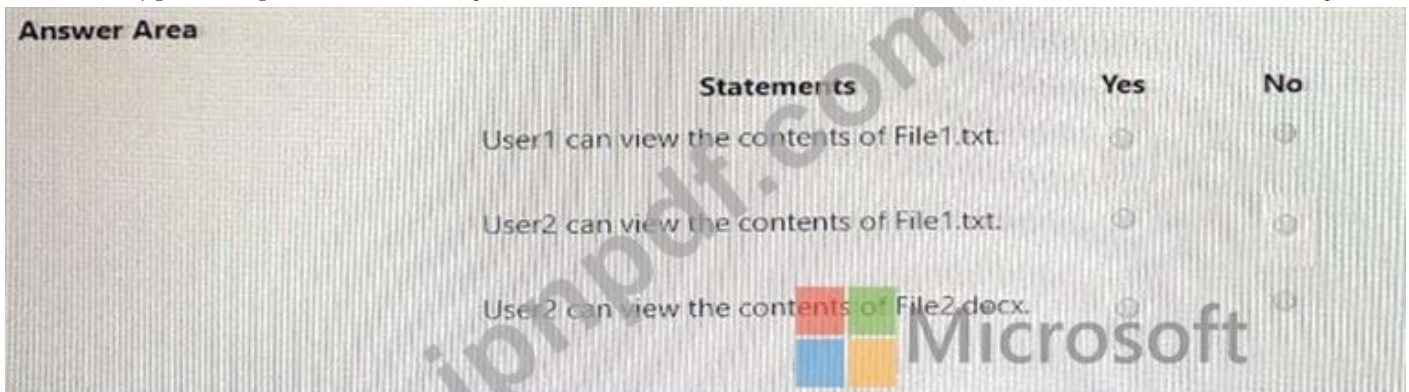
Name	Number of IP addresses
File1.txt	3
File2.docx	1

User1 には、Site1 の SharePoint 管理者ロールが割り当てられます。User2 は Site1 のメンバーです。次の図に示すデータ損失防止 (DLP)1 ポリシーを作成します。

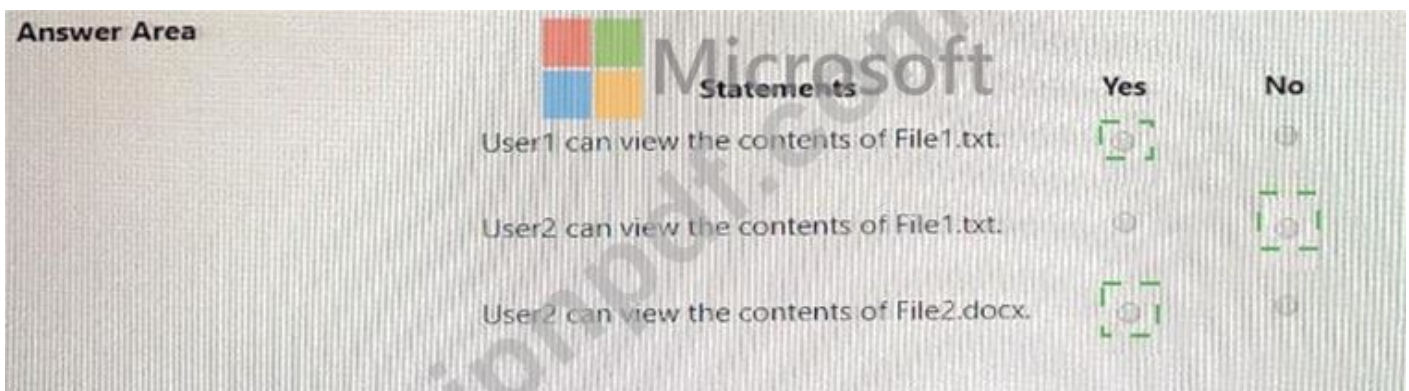




次の各ステートメントについて、ステートメントが正しい場合は [はい] を選択します。そうでない場合は、[いいえ] を選択します。注: 正しい選択肢はそれぞれ 1 ポイントの価値があります。



Answer:



説明

Answer Area

Microsoft

Statements	Yes	No
User1 can view the contents of File1.txt.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can view the contents of File1.txt.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can view the contents of File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 102

User1、User2、User3 という 3 人のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

次の表に示すロール アクティベーション設定を持つ Azure AD ロールがあります。

Name	Require justification on activation	Require approval to activate	Approver
Role1	No	Yes	User1
Role2	Yes	No	Not applicable

次の表に示すロール割り当て設定を持つ Azure AD ロールがあります。

Name	Allow permanent eligible assignment	Allow permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

Azure AD ロールには、次の表に示すように適格なユーザーが割り当てられています。

Name	Eligible assignment
Role1	User1, User2
Role2	User3

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 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

Microsoft

Statements	Yes	No
User1 can approve his own Role1 assignment request.	<input type="radio"/>	<input type="radio"/>
User1 can approve the Role2 assignment request of User3.	<input type="radio"/>	<input type="radio"/>
User1 must provide a justification to approve the Role1 assignment request of User2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area	Statements	Yes	No
	User1 can approve his own Role1 assignment request.	<input checked="" type="radio"/>	<input type="radio"/>
	User1 can approve the Role2 assignment request of User3.	<input type="radio"/>	<input checked="" type="radio"/>
	User1 must provide a justification to approve the Role1 assignment request of User2.	<input checked="" type="radio"/>	<input type="radio"/>

説明

Answer Area	Statements	Yes	No
	User1 can approve his own Role1 assignment request.	<input checked="" type="radio"/>	<input type="radio"/>
	User1 can approve the Role2 assignment request of User3.	<input type="radio"/>	<input checked="" type="radio"/>
	User1 must provide a justification to approve the Role1 assignment request of User2.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 103

Microsoft 365 テナントがあります。

次の図に示すように、アプリケーション制御プロファイルを使用する攻撃対象領域削減ポリシーを作成します。

The screenshot shows the 'Create profile' page for Application Control in the Microsoft Endpoint Manager Admin Center. The page is divided into four sections: Basics, Configuration settings, Scope tags, and Assignments. The 'Review + create' button is highlighted with a red box.

Section	Property	Value
Basics	Name	ApplicationControlPolicy1
	Description	...
	Platform	Windows 10 and later
Configuration settings	App locker application control	Enforce Components, Store Apps, and Smartlocker
	Turn on Windows SmartScreen	Yes
Scope tags	...	
Assignments	Included groups	Group1
	Excluded groups	Group2

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

注: 正しく選択するたびに 1 ポイントの価値があります。

When only a member of Group1 connects to a site that is identified as dangerous by application control, [answer choice]

▼
the site will open without warning
the site will be blocked from opening
the member will receive a security warning

When only a member of Group2 connects to a site that is identified as dangerous by application control, [answer choice]

▼
the site will open without warning
the site will be blocked from opening
the member will receive a security warning

Answer:

When only a member of Group1 connects to a site that is identified as dangerous by application control, [answer choice]	▼
	the site will open without warning
	the site will be blocked from opening
	the member will receive a security warning
When only a member of Group2 connects to a site that is identified as dangerous by application control, [answer choice]	▼
	the site will open without warning
	the site will be blocked from opening
	the member will receive a security warning

説明

When only a member of Group1 connects to a site that is identified as dangerous by application control, [answer choice]	▼
	the site will open without warning
	the site will be blocked from opening
	the member will receive a security warning
When only a member of Group2 connects to a site that is identified as dangerous by application control, [answer choice]	▼
	the site will open without warning
	the site will be blocked from opening
	the member will receive a security warning

ボックス 1: メンバーはセキュリティ警告を受け取ります。

Group1 はポリシーに含まれているため、SmartScreen が有効になります。SmartScreen は警告を表示します。

ボックス 2: サイトは警告なしにオープンします。

Group2 はポリシーから除外されているため、SmartScreen は有効になりません。したがって、警告は表示されません。

最新問題: 104

Active Directory の脅威検出を構成する必要があります。ソリューションはセキュリティ要件を満たしている必要があります。

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

- Configure the Directory services setting in Azure ATP
- Download and install the ATA Gateway on DC1, DC2, and DC3
- Download and install the Azure ATP sensor package on DC1, DC2, and DC3
- Configure a site-to-site VPN
- Create a workspace in Azure ATP
- Download and install the ATA Center on Server1

-
-
-

Answer:

Actions

Answer Area

- Configure the Directory services setting in Azure ATP
- Download and install the ATA Gateway on DC1, DC2, and DC3
- Download and install the Azure ATP sensor package on DC1, DC2, and DC3
- Configure a site-to-site VPN
- Create a workspace in Azure ATP
- Download and install the ATA Center on Server1

- Create a workspace in Azure ATP
- Download and install the Azure ATP sensor package on DC1, DC2, and DC3
- Configure the Directory services setting in Azure ATP



最新問題: 105

Microsoft 365 サブスクリプションをお持ちです。

Case1 という名前のデータ主体要求 (DSR) ケースがあります。

Case1 には、データ主体によって Microsoft Exchange Online パブリック フォルダーに投稿されたすべての電子メールが含まれていることを確認する必要があります。

コンテンツ検索クエリにどの追加プロパティを含める必要がありますか？

A. 種類: 外部データ

B. アイテムクラス: ipm.externaldata

C. アイテムクラス:ipm.post

D. 種類: メールアドレス

Answer: C (メッセージを残す)

説明/参照:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?view=o365-worldwide>

最新問題: 106

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

各ユーザーが最大 5 台のデバイスを Azure Active Directory (Azure AD) に参加できるようにする必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

* Microsoft 365 管理センターにサインインした後、> Azure Active Directory > デバイス。

* デバイス設定に移動します。

* ユーザーがデバイスを Azure AD に参加できるように設定します

- * [Azure AD 参加デバイスの追加のローカル管理者] 設定を [なし] に設定します。
 - * ユーザーが自分のデバイスを A に登録できるように設定します
 - * [デバイスに参加するには多要素認証が必要] 設定はデフォルト設定のままにしておきます。
 - * デバイスの最大数を設定します
 - * ユーザーはデバイス間で設定とアプリ データを同期できるようにすべてを設定します。
- ※画面左上の「保存」ボタンをクリックしてください。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>
<https://docs.microsoft.com/en-us/microsoft-365/compliance/use-your-free-azure-ad-subscription-in-office-365?v>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
 GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら：<https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 107

ワークロード管理者のセキュリティ要件を満たすようにアクセス レビューを構成する予定です。アクセス レビュー ポリシーを作成し、スコープとグループを指定します。他にどのような設定を構成する必要がありますか？ 回答するには、回答領域で適切な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。

Set the frequency to:

One time	▼
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	▼
Advanced settings	
Programs	
Reviewers	

Answer:

set the frequency to.

One time	v
Weekly	
Monthly	



To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

最新問題: 108

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

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

次の図に示すように、Azure AD Privileged Identity Management (PIM) でセキュリティ オペレーター ロールを構成します。



次の表に示すように、セキュリティ オペレーター ロールに割り当てを追加します。

Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

どのユーザーがセキュリティ オペレーター ロールをアクティブ化できますか？

- A. ユーザー 1、ユーザー 2、およびユーザー 3
- B. User2 と User3 のみ
- C. User2 のみ
- D. 使用され、User2 のみ
- E. User3 のみ

Answer: ([解答を表示する](#))

最新問題: 109

Azure Sentinel ワークスペースがあります。

Azure Active Directory (Azure AD) Identity Protection が危険なサインインを検出したときに Azure Sentinel アラートを生成するルールを構成します。ユーザーに連絡し、報告された危険なサインインが正当なものかどうかを確認するための Azure Logic Apps ソリューションを開発します。

次の要件を満たすようにワークスペースを構成する必要があります。

* 危険なサインインに対してアラートがトリガーされた場合は、Azure ロジック アプリを呼び出します。

* Azure Sentinel ポータルに、検出および解決された危険なサインインの統計を表示するカスタムダッシュボードを追加します。

各要件を満たすには、Azure Sentinel で何を構成する必要がありますか？ 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Call the logic app:

▼
An entity mapping
A hunting query
A notebook
A playbook
A workbook

Displays statistics for risky sign-ins:

▼
An entity mapping
A hunting query
A notebook
A playbook
A workbook

Answer:

Call the logic app:

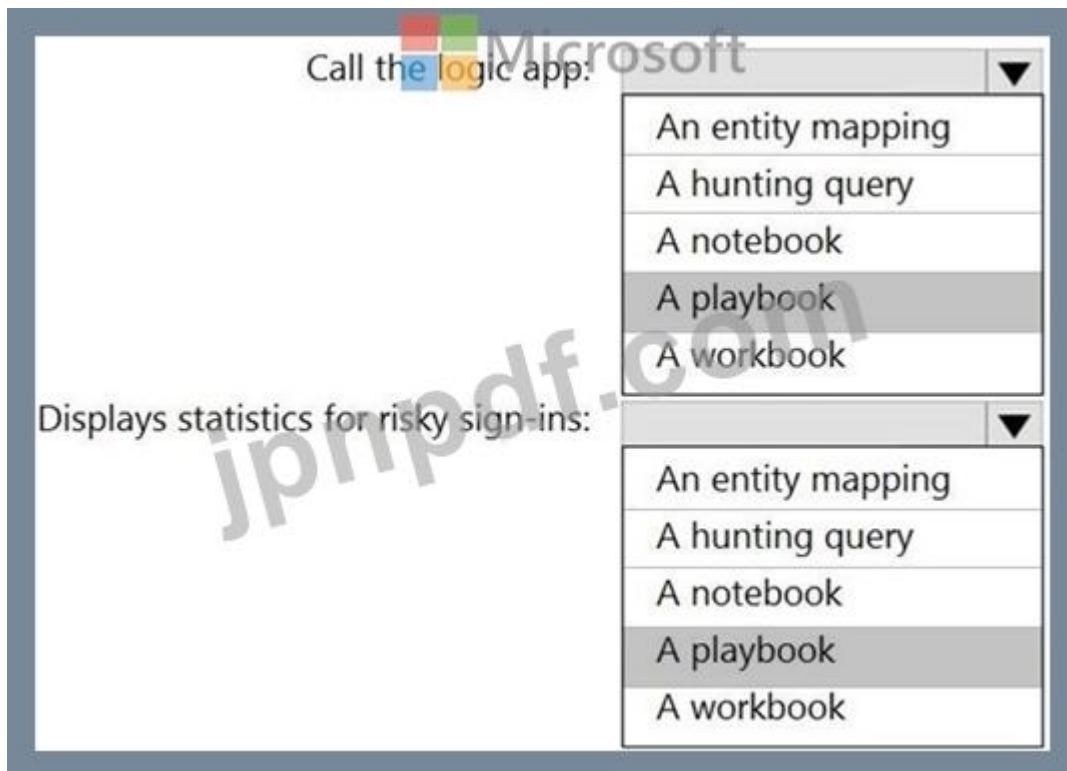
▼
An entity mapping
A hunting query
A notebook
A playbook
A workbook

Displays statistics for risky sign-ins:

▼
An entity mapping
A hunting query
A notebook
A playbook
A workbook

説明

テーブルの説明が自動的に生成される



参照 :

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

最新問題: 110

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	Group2
User3	Group1, Group2

次の設定を持つ Azure Active Directory (Azure AD) Identity Protection サインイン リスク ポリシーを作成して適用します。

割り当て: グループ 1 を含む、グループ 2 を除外

条件 :ユーザーのリスクレベルが中以上

アクセス: アクセスを許可、パスワードの変更が必要

ユーザーはサインインを試行します。各ユーザーのリスク レベルを次の表に示します。

User	User risk level
User1	High
User2	Medium
User3	High

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 must change his password.	<input type="radio"/>	<input type="radio"/>
User2 must change his password.	<input type="radio"/>	<input type="radio"/>
User3 must change his password.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 must change his password.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must change his password.	<input type="radio"/>	<input checked="" type="radio"/>
User3 must change his password.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 111

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー閲覧者の役割はどのユーザーにも割り当てられていません。User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないようにする解決策を推奨する必要があります。

解決策: User5 に割り当てられたライセンスを変更することをお勧めします。

これは目標を達成していますか?

A. はい

B. いいえ

Answer: ([解答を表示する](#))

説明/参照:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

最新問題: 112

次の図に示すように、管理者はAzure AD特権ID管理を構成します。

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

セキュリティ要件を満たすためにあなたは何をすべきですか？

A. Admin2 の割り当ての種類を固定に変更します。

B. Azure Active Directory 管理センターから、Exchange 管理者の役割を Admin2 に割り当てます。

C. Azure Active Directory 管理センターから、Exchange 管理者の役割を Admin1 に削除します。

D. Admin1 の割り当ての種類を[適格]に変更します。

Answer: ([解答を表示する](#))

テストレット1

概要

Fabrikam、Inc.は、パートナー小売店お子様製品を販売する製造会社です。

ヨーロッパ全域のオフィスには5,000人の従業員がいます。

どこの環境

ネットワークインフラ

ネットワークにはfabrikam.comという名前のActive Directoryフォレストが含まれています。

FabrikamはハイブリッドMicrosoftを持っています。

Azure Active Directory (Azure AD) 環境

マイクロソフトは特定のアプリケーションにいくつかのオンプレミスサーバーを維持していますが、ほとんどのエンドユーザーは

アプリケーションは、Microsoft 365 E5サブスクリプションによって提供されます。

問題ステートメント

Fabrikam は以下のことを指摘しています。

シアトルの金曜日以来、ITチームは「Unhealthy」を含む自動電子メールメッセージを受信していません。

・
ファイル名「ID同期通知」を参照してください。

・
マルウェアを含む電子メールの添付ファイルを最近開いたユーザーが何人かありました。

・
マルウェアは時間がかかりました。

必要条件

計画された変更

Fabrikam は以下の変更を実装する予定です。

・
Fabrikam は、Active Directory への疑わしいサインインを監視および調査する計画です。

・
Fabrikam は、パートナーに Microsoft 365 に保存されている一部のデータへのアクセスを提供する計画です。

・
アプリケーション管理

Fabrikam は、ワークロード アプリケーションを管理するための以下のアプリケーション権利を認定しています。

・
ユーザー管理者は様々な国から働きます

・
ユーザー管理者はAzure Active Directory管理センターを使用します

・
Admin1とAdmin2という2人の新しい管理者がMicrosoftの管理を担当します。

・
Exchange Onlineのみ

セキュリティ要件

Fabrikam は、以下のセキュリティ要件を確認しています。

・
ユーザー管理者によるAzure Active Directory管理センターへのアクセスは、毎回確認する必要があります。

・
管理者が3日以内にアクセス要求に応答しない場合、アクセス権は削除されました

・
Microsoft 365のワークロードを管理するユーザーは、

・
グローバル管理者はこの要件から承認する必要があります。

・
ユーザーが会社のデータを表示するために外部ユーザーを招待できないようにする必要があります。グローバル管理者のみ

・
User1というユーザーは招待状を送信する必要があります

・
Azure Advanced Threat Protection (ATP)は、機密性を高めるためにセキュリティグループの変更

をキャプチャする必要があります。

Active Directoryのドメイン管理者などのグループ

ワークロード管理者は、ワークロード管理者からサインインする場合は多要素認証 (MFA) を使用する必要があります。

匿名またはなじみのない場所

管理者が Azure に認証される時はユーザー管理者の場所を監査する必要があります。

広告

マルウェアを含む添付ファイルを含む電子メールメッセージは、マルウェアなしで配信する必要があります。

愛着

可能な限り最低限の特権を原則として使用する必要があります

最新問題: 113

Microsoft 365 サブスクリプションをお持ちです。

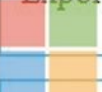
顧客は、彼女の名前が記載されているすべての文書を提供するように要求しています。

コンテンツのコピーを顧客に提供する必要があります。


どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、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


Close the case.
Regenerate a report.
View the results.
Export the results.
 Microsoft
Create a Data Subject Request (DSR) case.
Save the search.
Download the results.

Answer:

- Close the case.
- Regenerate a report.
- View the results.
-  Export the results.
- Create a Data Subject Request (DSR) case.
- Save the search.
- Download the results.

- Create a Data Subject Request (DSR) case.
- View the results.
- Save the search.
- Export the results.

説明

- Create a Data Subject Request (DSR) case.
-  View the results.
- Save the search.
- Export the results.

参照 :

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

最新問題: 114

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	Department
User1	Finance
User2	Research
User3	Finance

財務部門のユーザーが研究部門のユーザーとファイルを共有できないように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？

- A. 通信コンプライアンス
- B. 条件付きアクセス
- C. インサイダーリスク管理
- D. 情報バリア

Answer: B ([メッセージを残す](#))

最新問題: 115

Microsoft 365 サブスクリプションと Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) サブスクリプションを持っています。

次の表に示すように、Microsoft エンドポイント マネージャーにデバイスが登録されています。

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

Microsoft Defender ATP と Endpoint Manager を統合します。

デバイスの Microsoft Defender ATP リスク レベルを評価する予定です。

どのデバイスを評価できるかを特定する必要があります。

どのデバイスを識別する必要がありますか？

- A. デバイス 1 とデバイス 2 のみ
- B. デバイス1のみ
- C. デバイス 1 とデバイス 3 のみ
- D. デバイス 2 とデバイス 3 のみ

Answer: (解答を表示する)

説明

Microsoft Defender ATP は、Windows 10、Windows Server、macOSX、Linux をサポートしていません。

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/evaluation-lab>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/minimumrequireme>

最新問題: 116

どのポリシーがどのデバイスに適用されますか？ 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。

DevicePolicy1:	<input type="checkbox"/> None
	<input type="checkbox"/> Device1 only
	<input type="checkbox"/> Device3 only
	<input type="checkbox"/> Device2 and Device3 only
	<input type="checkbox"/> Device1 and Device3 only
	<input type="checkbox"/> Device1, Device2, and Device3
DevicePolicy2:	<input type="checkbox"/> None
	<input type="checkbox"/> Device4 only
	<input type="checkbox"/> Device2 and Device4 only
	<input type="checkbox"/> Device2, Device3, and Device 4 only

Answer:

DevicePolicy1:	<input checked="" type="checkbox"/> None
	<input type="checkbox"/> Device1 only
	<input type="checkbox"/> Device3 only
	<input type="checkbox"/> Device2 and Device3 only
	<input type="checkbox"/> Device1 and Device3 only
	<input type="checkbox"/> Device1, Device2, and Device3
DevicePolicy2:	<input checked="" type="checkbox"/> None
	<input type="checkbox"/> Device4 only
	<input type="checkbox"/> Device2 and Device4 only
	<input type="checkbox"/> Device2, Device3, and Device 4 only

説明

DevicePolicy1:	<input type="checkbox"/> None
	<input type="checkbox"/> Device1 only
	<input type="checkbox"/> Device3 only
	<input type="checkbox"/> Device2 and Device3 only
	<input checked="" type="checkbox"/> Device1 and Device3 only
	<input type="checkbox"/> Device1, Device2, and Device3
DevicePolicy2:	<input type="checkbox"/> None
	<input checked="" type="checkbox"/> Device4 only
	<input type="checkbox"/> Device2 and Device4 only
	<input type="checkbox"/> Device2, Device3, and Device 4 only

最新問題: 117

ADGroup1 と ADGroup2 のメンバーはどのユーザーですか? 回答するには、回答領域で適切なオ

プシオ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。

ADGroup1:


None	v
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

ADGroup2:

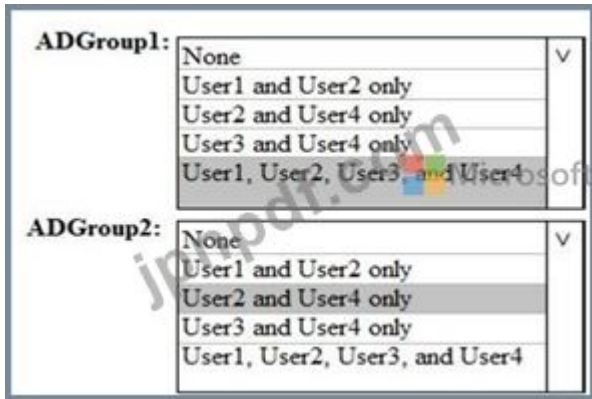
None	v
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

Answer:

Actions	Answer Area
Close the case.	Create a Data Subject Request (DSR) case.
Regenerate a report.	View the results.
View the results.	Save the search.
Export the results.	Export the results.
Create a Data Subject Request (DSR) case.	
Save the search.	
Download the results.	



説明



参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#support>

最新問題: 118

Microsoft 365 サブスクリプションをお持ちです。

次の図に示すように、Retention1 という名前の保持ポリシーを作成しています。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 2 years ▾

Retain the content based on when it was last modified ▾ ⓘ

Do you want us to delete it after this time? ⓘ

Yes No

No, just delete content that's older than ⓘ

1 years ▾

Need more options?

Use advanced retention settings ⓘ

Back

Next

Cancel

Retention1 を SharePoint サイトと OneDrive アカウントに適用します。

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

注: 正しく選択するたびに 1 ポイントの価値があります。

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained	▼
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	▼
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

Answer:

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained	▼
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	▼
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

最新問題: 119

User1 と User2 という名前の 2 人のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

1 月 1 日に、次の表に示す機密ラベルを作成します。

Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

1 月 2 日に、ラベルを User1 に公開します。

1 月 3 日。ユーザー 1 は、Doc1 という名前の Microsoft Word 文書を作成し、その文書にラベルを適用します。

1月4日、User2がDoc1を編集します。

1月15日に、ラベルのコンテンツの有効期限を28日に延長します。

User2のDoc1へのアクセスはいつ期限切れになりますか？

A. 1月23日

B. 1月31日

C. 1月25日

D. 1月24日

Answer: C ([メッセージを残す](#))

最新問題: 120

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

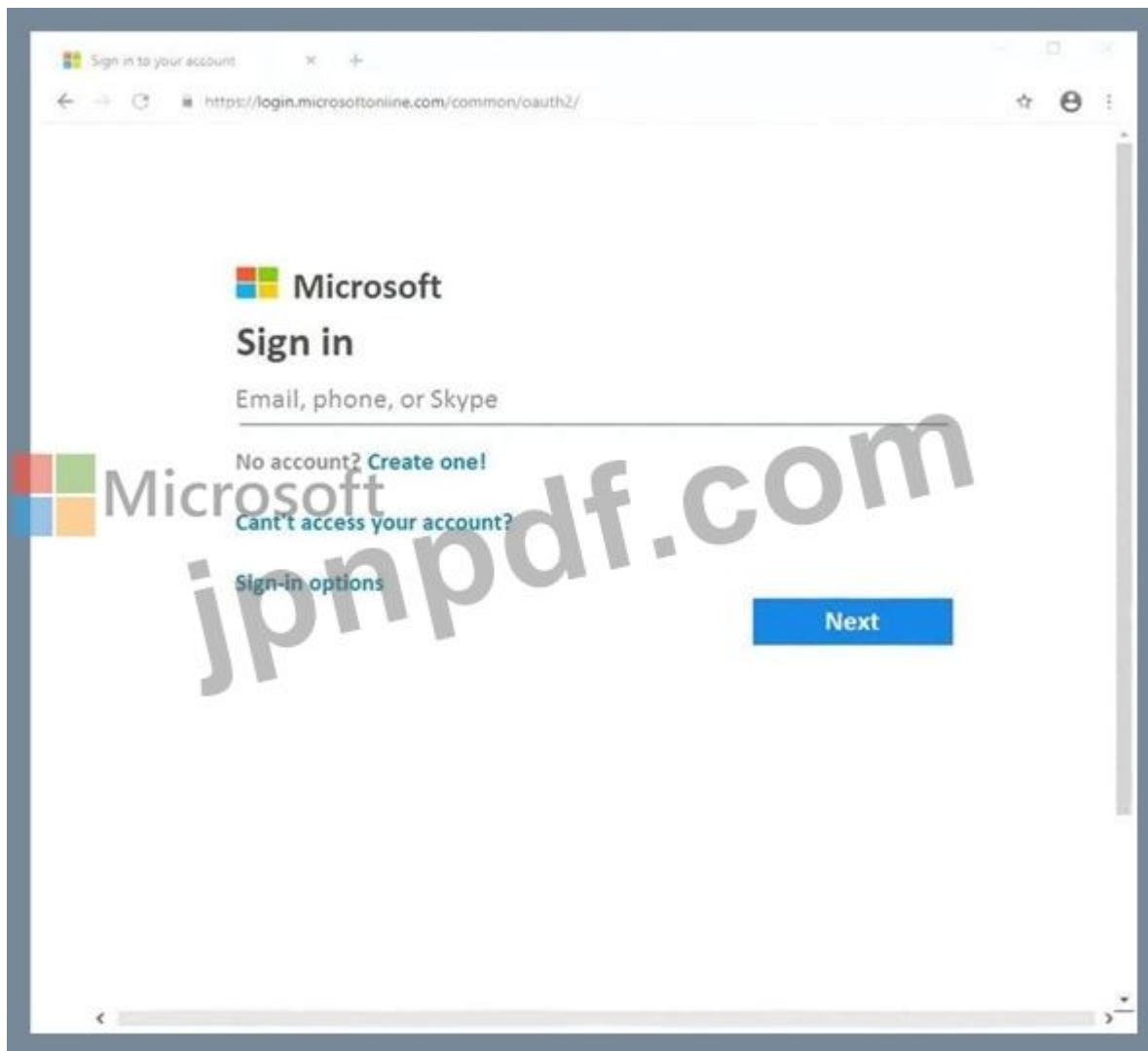
[次へ] ボタンが使用可能になったら、それをクリックしてラボセクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能(コピーアンドペースト、外部Webサイトに移動する機能など)は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308

Microsoft



jpnpdf.com



Get your work done
with Office 365

Microsoft





jpnpdf.com

Brainstorm
together in **Word**





Stay on top of what matters with Outlook



Microsoft



Microsoft



Access Office 365 apps and documents in one place with

Office.com



Microsoft Office Home | Microsoft

Contoso electronics | Office 365

Good morning Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint

OneNote | Skype | Calendar | People | All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recommended

You edited this
Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

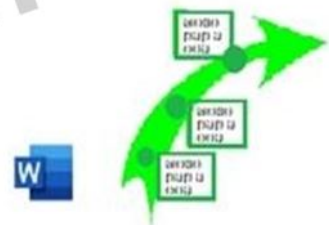
You edited this
Jan 15



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this
Jan 15



AD Slogans

lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



Recent

Pinned

Shared with me

Discover



Microsoft



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

Upload and open...

New

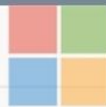
Go to OneDrive →

Recent

Pinned

Shared with me

Discover



Microsoft



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →

SharePoint

Frequent sites

Following

SM

Sales and Marketing

R

Retail

Cs

Communication Site

SharePoint

Frequent sites

Following

CL

Contoso Landings

CW

Contoso Web 3

EC

Executive Corner

Go to SharePoint →

Name	Modified	Modified By	File Size
Contoso Q2 Division Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

データラベルを含む保持ポリシーを作成する必要があります。ポリシーではすべての Microsoft Office を削除する必要があります

6 か月以上前の 365 コンテンツ。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

Office 365 ラベルの作成は 2 段階のプロセスです。最初のステップは、名前、説明、保持ポリシー、およびコンテンツのレコードとしての分類を含む実際のラベルを作成することです。これが完了したら、2 番目のステップでは、公開する特定の場所を指定するラベル付けポリシーを使用してラベルを展開し、ラベルを自動的に適用する必要があります。

Office 365 ラベルを作成するには、次の手順に従います。

1. セキュリティおよびコンプライアンス センターを開く。
2. 「分類」をクリックします。
3. 「ラベル」をクリックします。
4. ラベルには次のような構成が必要です。ラベルに名前を付け (名前)、管理者用の説明を追加 (管理者用の説明)、ユーザー用の説明を追加 (ユーザー用の説明)。
5. 構成が完了したら、「次へ」をクリックします。
6. 左側のメニューで「ラベル設定」をクリックします。
7. ラベル設定を構成する必要があります。この画面では、保持スイッチを次のいずれかに切り替えることができます。

「オン」または「オフ」。「オン」を選択すると、「このラベルがコンテンツに適用される時」という質問に 2 つのオプションのいずれかで答えることができます。最初のオプションは「すべて」です。選択

ボックスから、保持期間と保持期間の終了時に実行されるアクションを選択できます。3つのアクションは、データを削除するか、レビューのための承認フローをトリガーするか、何もアクションを起こさないかです。2番目のオプションは、指定した時間が経過した後、またはデータの古さに基づいてデータを保持しないことです。と

8. これでラベルが作成されました。

ラベルポリシーを作成するには、次の手順に従います。

1. セキュリティおよびコンプライアンスセンターを開く

2. 「データガバナンス」、保持」をクリックします。

3. 画面上部の [ラベルポリシー] ボックスを選択します。と

4. 現在、2つのオプションがあります。1つ目は、です。組織がエンドユーザーにラベルを手動で適用させたい場合は、これが選択するオプションです。これは場所に基づいていることに注意してください。2番目のオプションは、ラベルを自動適用することです。自動適用を使用すると、指定した基準を満たしたときにラベルを自動的に適用できます。

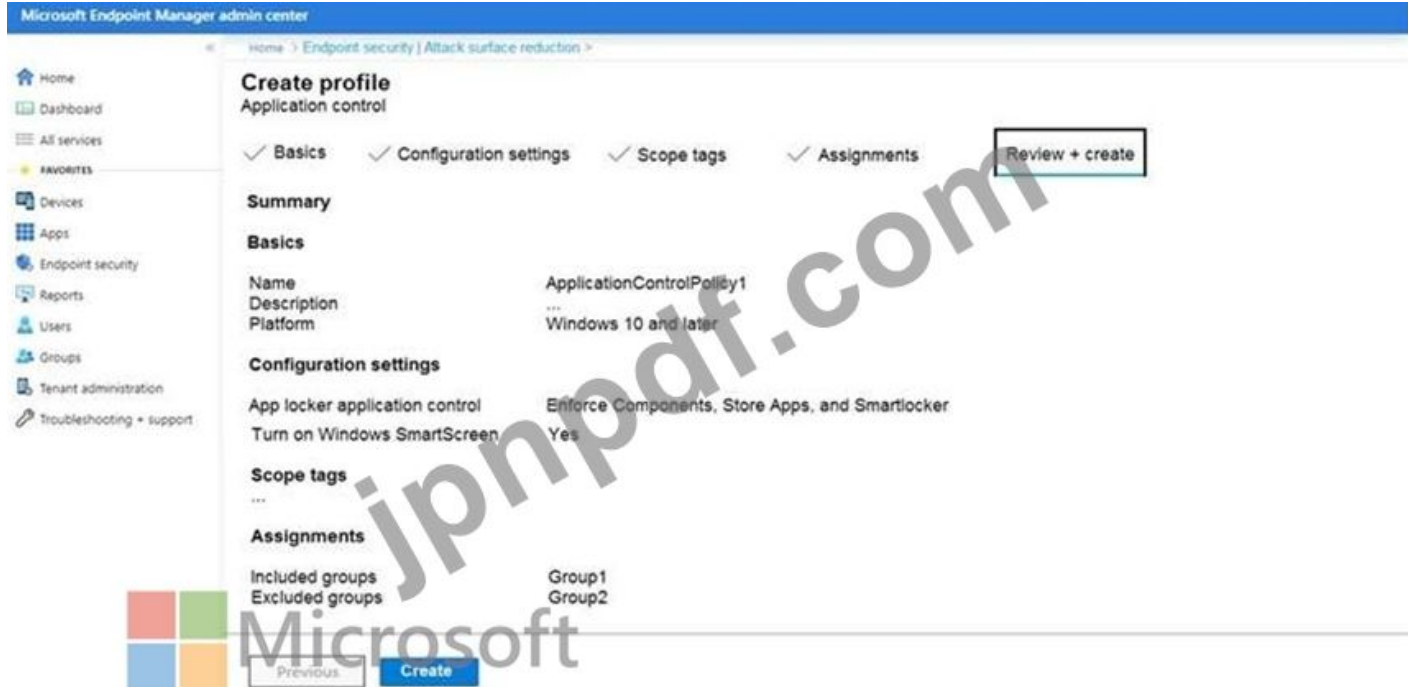
参考文献:

<https://www.maadarani.com/office-365-classification-and-retention-labels/>

最新問題: 121

Microsoft 365 テナントがあります。

次の図に示すように、アプリケーション制御プロファイルを使用する攻撃対象領域削減ポリシーを作成します。



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

注: 正しく選択するたびに1ポイントの価値があります。

When only a member of Group1 connects to a site that is identified as dangerous by application control, [answer choice]

the site will open without warning
the site will be blocked from opening
the member will receive a security warning

When only a member of Group2 connects to a site that is identified as dangerous by application control, [answer choice]

the site will open without warning
the site will be blocked from opening
the member will receive a security warning

Answer:

When only a member of Group1 connects to a site that is identified as dangerous by application control, [answer choice]

the site will open without warning
the site will be blocked from opening
the member will receive a security warning

When only a member of Group2 connects to a site that is identified as dangerous by application control, [answer choice]

the site will open without warning
the site will be blocked from opening
the member will receive a security warning

有効な MS-500 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！ GoShiken.com が最新の MS-500 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (32930%OFF問題集 溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 122

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

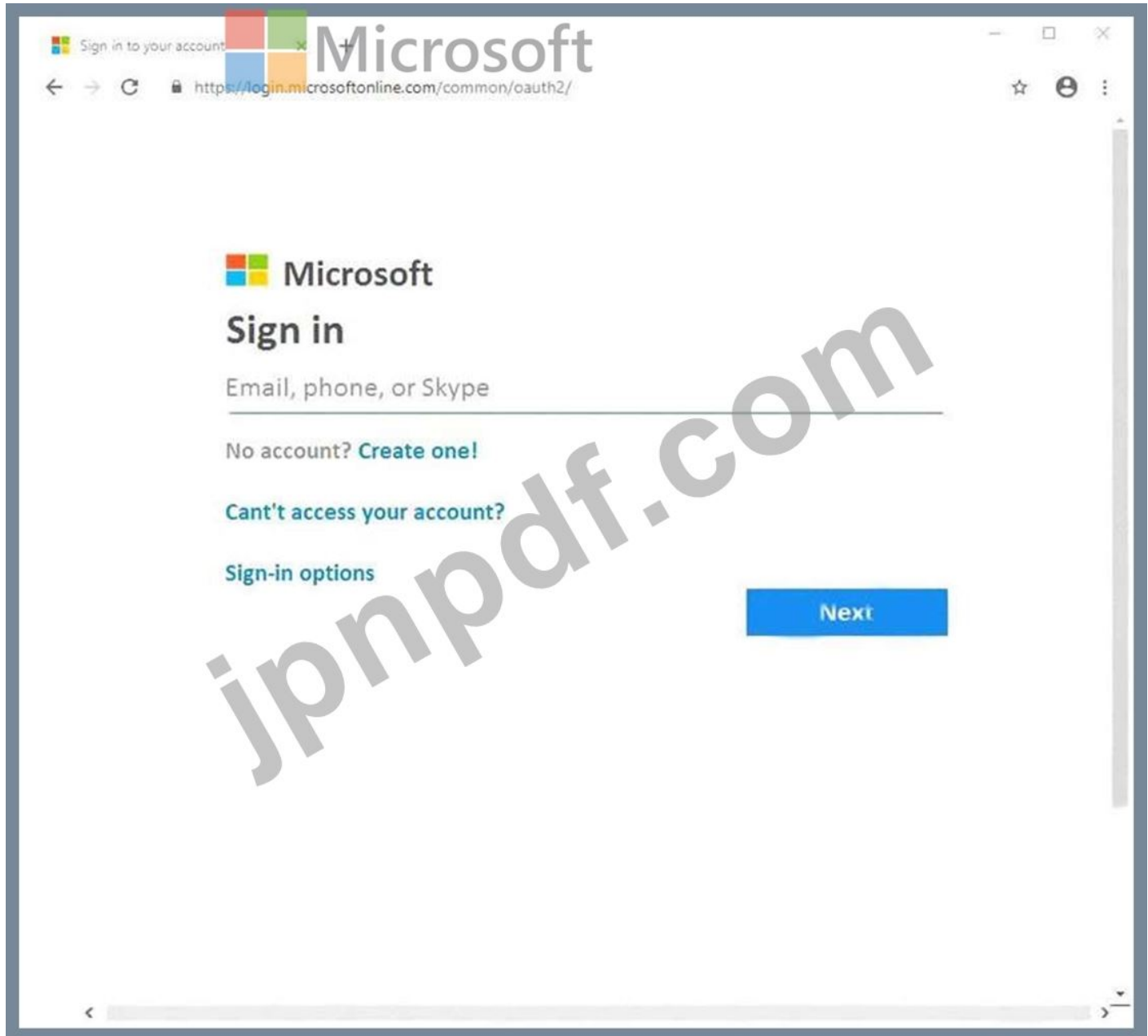
スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のす

すべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

Microsoft 365 ポータルがブラウザーに正常に読み込まれない場合は、Ctrl-K キーを押して、新し

いブラウザ タブにポータルを再読み込みします。
次の情報はテクニカル サポート専用です。
ラボ インスタンス: 11122308





Brainstorm together in **Word**



Stay on top of what matters with **Outlook**





Microsoft



Access Office 365 apps and documents in one place with **Office.com**



Microsoft Office Home | office.com/?auth=2

Contoso electronics | Office 365

Good morning Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint

OneNote | Skype | Calendar | People | All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Excel

Integrated Team Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recommended

You edited this Jan 15

Excel

P and L Summary
lodse000198.sharepoint.co...

You edited this Jan 15

Word

Contoso Electronics Outdoor...
lodse000198.sharepoint.co...

You edited this Jan 15

Word

Ad Slogans
lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

Upload and open... **New**

[Go to OneDrive](#) →



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

[Go to OneDrive](#) →

SharePoint

Frequent sites

Following

- Sales and Marketing
- Retail
- Communication Site

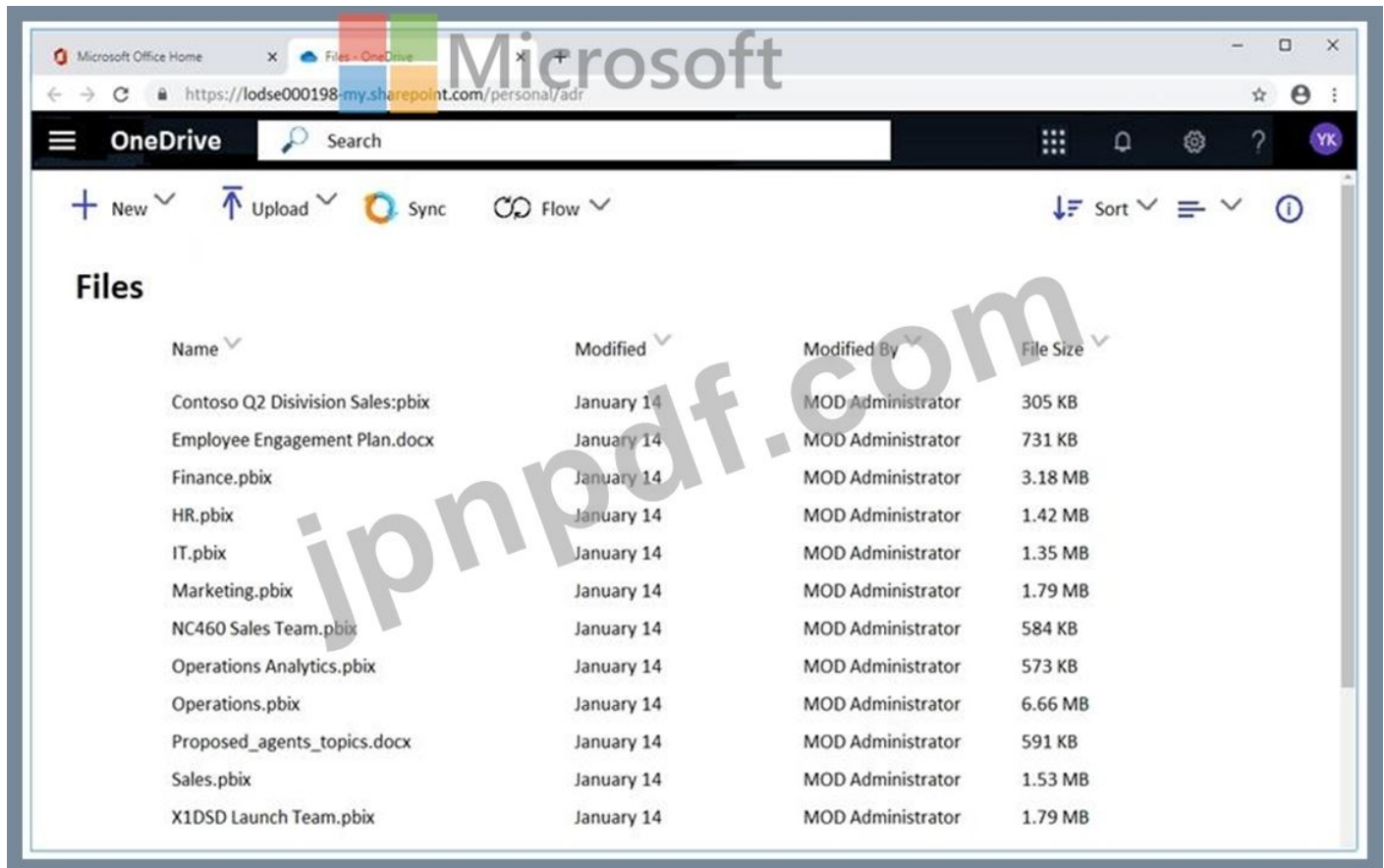
[Go to SharePoint](#) →

SharePoint

Frequent sites

Following

- Contoso Landings
- Contoso Web 3
- Executive Corner



ユーザーのメールボックス検索を自動化するスクリプトを作成する予定です。スクリプトは、Allan Deyoung という名前のユーザーのメールボックスで、差し止めという単語を含むメッセージを検索します。

スクリプトに含まれる検索を作成する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

ステップ 1: 実行する検索に関する情報を含む CSV ファイルを作成する このステップで作成するカンマ区切り値 (CSV) ファイルには、検索する各ユーザーの行が含まれています。ユーザーの Exchange Online メールボックス (有効な場合はアーカイブ メールボックスを含む) と OneDrive for Business サイトを検索できます。または、メールボックスまたは OneDrive for Business サイトのみを検索することもできます。SharePoint Online 組織内の任意のサイトを検索することもできます。ステップ 3 で実行するスクリプトは、CSV ファイル内の行ごとに個別の検索を作成します。

1. メモ帳を使用して、次のテキストをコピーして .txt ファイルに貼り付けます。このファイルをローカル コンピューター上のフォルダーに保存します。他のスクリプトもこのフォルダーに保存します。

ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate
sarad@contoso.onmicrosoft.com、https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、1/1/2000、12/31/2005 sarad @contoso.onmicrosoft.com、https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2006/1/1、2010/12/31 sarad@contoso.onmicrosoft.com、https://contoso-

my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2011/1/1、2016/3/21

、https://contoso.sharepoint.com/sites/contoso、2016年3月21日

、https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com、2015年1月1日、

、https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com、1/1/2015、ファイルの最初の行、つまりヘッダ行には、New-ComplianceSearch コマンドレットで使用されるパラメーターがリストされています。新しいコンテンツ検索。各パラメータ名はカンマで区切られます。ヘッダ行にスペースが含まれていないことを確認してください。ヘッダ行の下の各行は、各検索のパラメーター値を表します。CSV ファイル内のプレースホルダー データを実際のデータに置き換えてください。

2. Excel で .txt ファイルを開き、次の表の情報を使用して、各検索の情報を含むファイルを編集します。

Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see Keyword queries and search conditions for Content Search .
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

3. Excel ファイルを CSV ファイルとしてローカル コンピューター上のフォルダーに保存します。ステップ 3 で作成したスクリプトは、この CSV ファイル内の情報を使用して検索を作成します。

参照：

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-searches> コンテンツ検索のキーワード クエリと検索条件

<https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365>

最新問題: 123

Microsoft Defender for Endpoint を使用し、Device1 という名前の 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。

script1 という名前の PowerShell スクリプトがあります。このスクリプトはフォレンジック データを収集し、その結果をスクリプトの実行元のデバイスにファイルとして保存します。

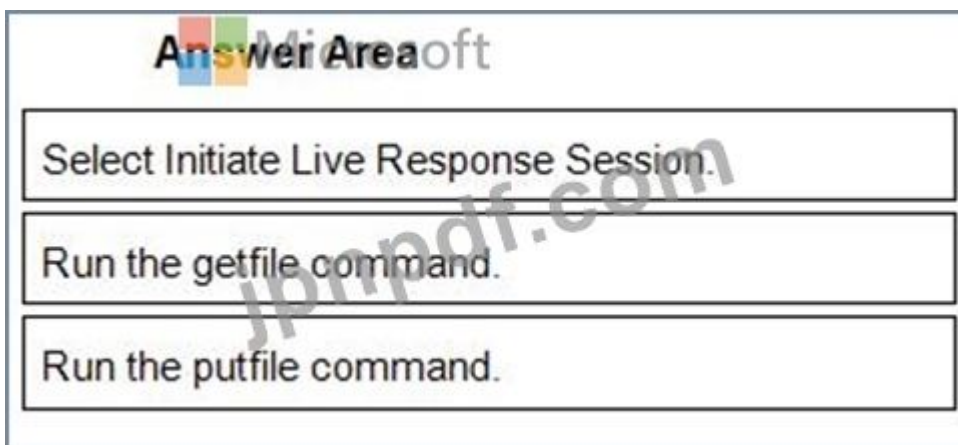
Device1 での不審なアクティビティに関する Microsoft Defender for Endpoint アラートを受け取ります。

Device1 で script1 を実行し、スクリプトの出力ファイルを取得する必要があります。

Microsoft 365 Defender ポータルで順番に実行する必要がある 4 つのアクションはどれですか？ 回答するには、アクション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。



Answer:



1 - [ライブ応答セッションの開始] を選択します。

2 - getfile コマンドを実行します。

3 - putfile コマンドを実行します。

最新問題: 124

次の図に示すように、コンプライアンス マネージャーが表示されます。



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

注: 正しく選択するたびに 1 ポイントの価値があります。

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	▼
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	▼
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

Answer:

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	▼
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

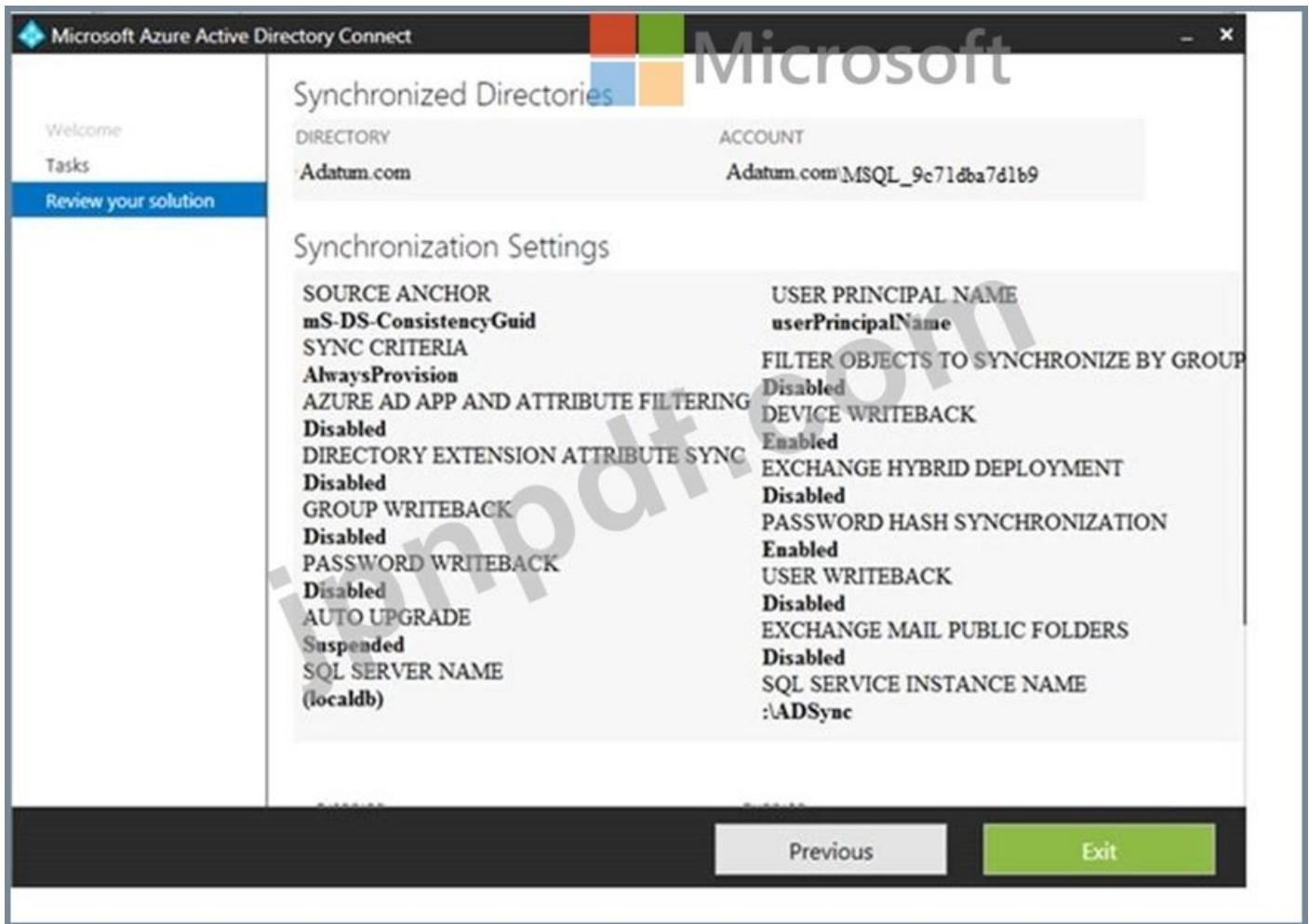
proves that the organization is non-compliant	▼
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud>

最新問題: 125

次の図に示すように、Microsoft Azure Active Directory (Azure AD) Connect を構成します。



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

注: 正しく選択するたびに1ポイントの価値があります。

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

最新問題: 126

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

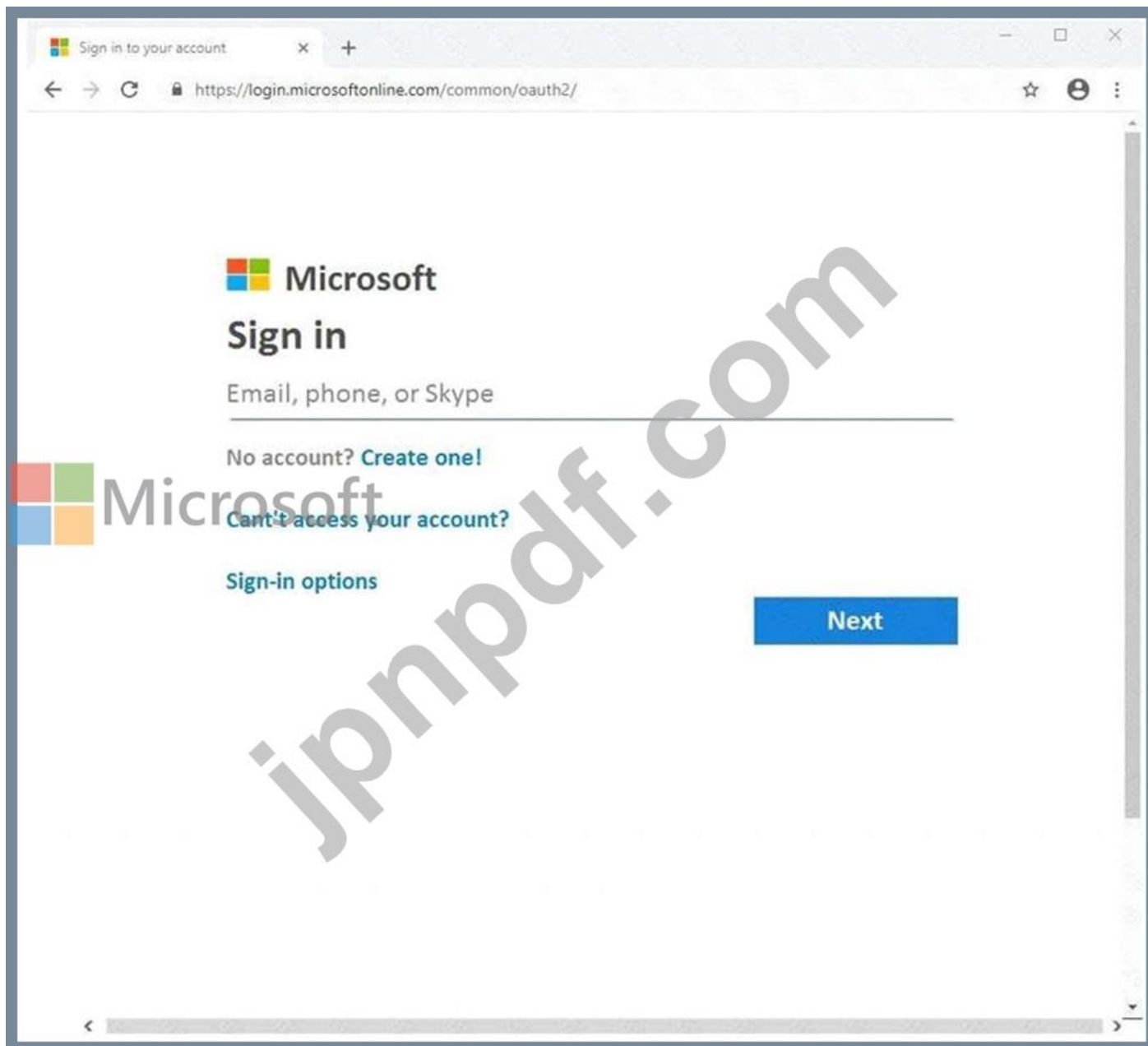
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308

Microsoft



Microsoft



Get your work done
with **Office 365**



jpnpdf.com

Microsoft



Microsoft

Brainstorm
together in **Word**



Microsoft



Microsoft

Stay on top of what matters with Outlook





Access Office 365 apps and documents in one place with **Office.com**



Microsoft Office Home x +

office.com/?auth=2

Contoso electronics Office 365

Good morning Install Office

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Excel

Integrated Team Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

Microsoft

You edited this Jan 15

Excel

P and L Summary
lodse000198.sharepoint.co...

You edited this Jan 15

Word

Contoso Electronics Outdoor...
lodse000198.sharepoint.co...

You edited this Jan 15

Word

AD Slogans
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

Upload and open...

New

Go to OneDrive



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive

SharePoint

Frequent sites Following

SM Sales and Marketing

R Retail

C Communication Site

Go to SharePoint

SharePoint

Frequent sites Following

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner



Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

ユーザーのメールボックス検索を自動化するスクリプトを作成する予定です。スクリプトは、Allan Deyoung という名前のユーザーのメールボックスで、差し止めという単語を含むメッセージを検索します。

スクリプトに含まれる検索を作成する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

ステップ 1: 実行する検索に関する情報を含む CSV ファイルを作成する このステップで作成するカンマ区切り値 (CSV) ファイルには、検索する各ユーザーの行が含まれています。ユーザーの Exchange Online メールボックス (有効な場合はアーカイブ メールボックスを含む) と OneDrive for Business サイトを検索できます。または、メールボックスまたは OneDrive for Business サイトのみを検索することもできます。SharePoint Online 組織内の任意のサイトを検索することもできます。ステップ 3 で実行するスクリプトは、CSV ファイル内の行ごとに個別の検索を作成します。

1. メモ帳を使用して、次のテキストをコピーして .txt ファイルに貼り付けます。このファイルをローカル コンピューター上のフォルダーに保存します。他のスクリプトもこのフォルダーに保存します。

ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate
 sarad@contoso.onmicrosoft.com、https://contoso-
 my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法
 的)、1/1/2000、12/31/2005 sarad @contoso.onmicrosoft.com、https://contoso-

my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2006/1/1、2010/12/31 sarad@contoso.onmicrosoft.com、https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2011/1/1、2016/3/21

、https://contoso.sharepoint.com/sites/contoso、2016年3月21日

、https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com、2015年1月1日、

、https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com、1/1/2015、ファイルの最初の行、つまりヘッダ行には、New-ComplianceSearch コマンドレットで使用されるパラメーターがリストされています。新しいコンテンツ検索。各パラメータ名はカンマで区切られます。ヘッダ行にスペースが含まれていないことを確認してください。ヘッダ行の下の各行は、各検索のパラメーター値を表します。CSV ファイル内のプレースホルダー データを実際のデータに置き換えてください。

2. Excel で .txt ファイルを開き、次の表の情報を使用して、各検索の情報を含むファイルを編集します。

Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see Keyword queries and search conditions for Content Search .
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

3. Excel ファイルを CSV ファイルとしてローカル コンピューター上のフォルダーに保存します。ステップ 3 で作成したスクリプトは、この CSV ファイル内の情報を使用して検索を作成します。

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-search> コンテンツ検索のキーワード クエリと検索条件

<https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search>

conditions?view=o365

最新問題: 127

次の図に示すように、ネットワークには、Azure Active Directory (Azure AD) と同期するオンプレミスの Active Directory ドメインが含まれています。

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	4.00 hours ago
Password Hash Sync	Enabled

USER SIGN-IN



Federation

Disabled

0 domains

Seamless single sign-on

Disabled

0 domains

Pass-through authentication

Enabled

1 agent

同期スケジュールは次のように構成されています。

```
Administrator: Windows PowerShell
PS C:\> get-ADSyncScheduler

AllowedSyncCycleInterval      : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 00:30:00
CustomizedSyncCycleInterval   :
NextSyncCyclePolicyType       : Delta
NextSyncCycleStartTimeInUTC    : 1/28/2020 3:47:41 PM
LargerRunHistoryInterval      : 7:00:00:00
SyncCycleEnabled              : True
MaintenanceEnabled            : True
StagingModeEnabled            : False
SchedulerSuspended            : False
SyncCycleInProgress           : False
```

ドロップダウンメニューを使用して、図に示されている情報に基づいて各質問に答える回答の選択肢を選択します。

注:正しく選択するたびに 1 ポイントの価値があります。

Which employees can authenticate by using Azure AD?

- Only employees who have an Azure AD user account
- Employees who have an Azure AD user account and a synced on-premises account
- Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

- Fix the synchronization server and install Azure AD Connect in staging mode
- Fix the synchronization server and install an additional authentication agent
- Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
- Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

Answer:

Which employees can authenticate by using Azure AD?

- Only employees who have an Azure AD user account
- Employees who have an Azure AD user account and a synced on-premises account
- Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

- Fix the synchronization server and install Azure AD Connect in staging mode
- Fix the synchronization server and install an additional authentication agent
- Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
- Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

説明

Which employees can authenticate by using Azure AD?

- Only employees who have an Azure AD user account
- Employees who have an Azure AD user account and a synced on-premises account
- Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

- Fix the synchronization server and install Azure AD Connect in staging mode
- Fix the synchronization server and install an additional authentication agent
- Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
- Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

最新問題: 128

User1 と User2 という名前の 2 人のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

1 月 1 日に、次の表に示す機密ラベルを作成します。

Name	Value
Assign permissions now or let users decide?	Label1
User access to content expires	Assign permissions now
Assign permissions to specific users and groups	After 21 days
	Co-Author: User1 and User2

1 月 2 日に、ラベルを User1 に公開します。

1 月 3 日。ユーザー 1 は、Doc1 という名前の Microsoft Word 文書を作成し、その文書にラベルを適用します。

1 月 4 日。User2 が Doc1 を編集します。

1 月 15 日に、ラベルのコンテンツの有効期限を 28 日に延長します。

User2 の Doc1 へのアクセスはいつ期限切れになりますか？

- A. 1月31日
- B. 1月24日
- C. 1月23日
- D. 1月25日

Answer: D (メッセージを残す)

最新問題: 129

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があ

ります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Microsoft 365 テナントがあります。Microsoft Azure Information Protection で CompanyConfidential という名前のラベルを作成します。CompanyConfidential をグローバル ポリシーに追加します。

ユーザーは CompanyConfidential を使用して電子メール メッセージを保護し、ラベルを複数の外部受信者に送信します。外部受信者は、電子メール メッセージを開けないと報告しています。外部の受信者が、自分に送信された保護された電子メール メッセージを開けられるようにする必要があります。

解決策: ラベルの暗号化設定を変更します。

これは目標を達成していますか?

A. いいえ

B. はい

Answer: A ([メッセージを残す](#))

最新問題: 130

ADGroup1 と ADGroup2 のメンバーはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

The screenshot shows a Microsoft exam question interface. At the top, there is a Microsoft logo. Below it, there are two dropdown menus labeled ADGroup1 and ADGroup2. Each dropdown menu has five options: None, User1 and User2 only, User2 and User4 only, User3 and User4 only, and User1, User2, User3, and User4. The dropdown menus are currently set to 'None'.

ADGroup1:	Options	Dropdown Arrow
	None	▼
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

ADGroup2:	Options	Dropdown Arrow
	None	▼
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

Answer:

ADGroup1:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	
ADGroup2:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values>

最新問題: 131

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Group	Role
User1	Microsoft Defender for Identity Contoso Users	None
User2	Microsoft Defender for Identity Contoso Viewers	None
User3	Not applicable	Security administrator
User4	Not applicable	Security operator

Microsoft Defender for Identity ポータルからいくつかのセキュリティ アラートが表示されることわかります。

contoso.com 内のどのユーザーがセキュリティ アラートを閉じることができるかを特定する必要があります。

どのユーザーを特定する必要がありますか？

- A. User3 のみ
- B. User1 と User2 のみ
- C. User3 と User4 のみ
- D. User1 と User3 のみ
- E. User1 のみ

Answer: (解答を表示する)

参照 :

<https://docs.microsoft.com/en-us/defender-for-identity/role-groups>

最新問題: 132

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Groups administrator
Admin2	User administrator

contoso.com のグループ名前付けポリシーに禁止単語として 「internal」を追加します。

contoso.com のグループ名前付けポリシーのプレフィックスとして Contoso- を追加します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ]を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input checked="" type="radio"/>	<input type="radio"/>

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide>

最新問題: 133

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正解がある場合もありますが、他の質問セットには正解がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー 閲覧者の役割はどのユーザーにも割り当てられていません。User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないようにする解決策を推奨する必要があります。

解決策: User1 をコンプライアンス マネージャー 共同作成者ロールから削除することをお勧めします。

それは目標を達成していますか？

A. はい

B. いいえ

Answer: B (メッセージを残す)

説明

参考文献:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

最新問題: 134

Microsoft 365 サブスクリプションをお持ちです。

Site1 という名前の Microsoft SharePoint Online サイトがあります。

Site1 を検索する Case1 という名前のデータ主体要求 (DSR) ケースがあります。

新しい機密情報の種類を作成します。

Case1 が新しい種類の機密情報を含むすべてのドキュメントを返す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. セキュリティとコンプライアンス管理センターから、新しい ID による検索リストを作成します。

B. Site1 から、検索辞書を変更します。

C. セキュリティとコンプライアンス管理センターから、新しいガイド付き検索を作成します。

D. Site1 から、Site1 の再インデックス作成を開始します。

Answer: (解答を表示する)

最新問題: 135

Microsoft 365 サブスクリプションをお持ちです。

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

隔離内の添付ファイルの保存期間を構成する必要があります。

どのタイプの脅威管理ポリシーを作成する必要がありますか？

A. ATP フィッシング対策

B. DKIM

C. スпам対策

D. マルウェア対策

Answer: C ([メッセージを残す](#))

説明/参照:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files#BKMK_ModQuarantineTime 情報保護の実装と管理 テストレット 1 これは ケース スタディです。ケーススタディは個別に時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了できるように時間を管理する必要があります。

ケーススタディに含まれる質問に答えるには、ケーススタディで提供される情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれる場合があります。このケーススタディでは、各質問は他の質問から独立しています。

このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認し、変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。

ケーススタディを開始するには

このケーススタディの最初の質問を表示するには、**次へ** ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用してケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに [すべての情報] タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたなら、**質問** ボタンをクリックして質問に戻ります。

概要

Fabrikam, Inc. は、パートナーの小売店を通じて製品を販売する製造会社です。Fabrikam には、ヨーロッパ全土のオフィスに 5,000 人の従業員がいます。

既存の環境

ネットワークインフラストラクチャ

ネットワークには、fabrikam.com という名前の Active Directory フォレストが含まれていません。Fabrikam には、ハイブリッド Microsoft Azure Active Directory (Azure AD) 環境があります。同社は特定のアプリケーション用にいくつかのオンプレミス サーバーを維持していますが、ほとんどのエンドユーザー アプリケーションは Microsoft 365 E5 サブスクリプションによって提供されています。

問題の声明

Fabrikam は次の問題を特定しています。

* 先週の金曜日以来、IT チームは件名に **異常な ID 同期通知** を含む自動電子メール メッセージを受信しています。

* 最近、数人のユーザーがマルウェアを含む電子メールの添付ファイルを開いてしまいました。マ

ルウェアを削除するプロセスには時間がかかりました。

要件

計画された変更

Fabrikam は次の変更を実装する予定です。

- * Fabrikam は、Active Directory への不審なサインインを監視および調査する予定です
- * Fabrikam は、パートナーが Microsoft 365 アプリケーション管理に保存されているデータの一部にアクセスできるようにする予定です。Fabrikam は、ワークロード アプリケーションを管理するための次のアプリケーション要件を特定します。
- * ユーザー管理者はさまざまな国から勤務します
- * ユーザー管理者は Azure Active Directory 管理センターを使用します。
- * Admin1 と Admin2 という名前の 2 人の新しい管理者は、Microsoft Exchange Online のみの管理を担当します。セキュリティ要件 Fabrikam は、次のセキュリティ要件を特定します。
- * ユーザー管理者による Azure Active Directory 管理センターへのアクセスは 7 日ごとに確認する必要があります。管理者が 3 日以内にアクセス要求に応答しなかった場合は、アクセスを削除する必要があります
- * Microsoft 365 ワークロードを管理するユーザーは、一度に最大 3 時間の管理タスクのみを実行できます。グローバル管理者はこの要件を免除される必要があります
- * ユーザーは、会社データを表示するために外部ユーザーを招待できないようにする必要があります。グローバル管理者と User1 という名前のユーザーのみが招待を送信する必要があります
- * Azure Advanced Threat Protection (ATP) は、Active Directory のドメイン管理者などの機密性の高いグループのセキュリティ グループの変更をキャプチャする必要があります。
- * ワークロード管理者は、匿名または見知らぬ場所からサインインする場合、多要素認証 (MFA) を使用する必要があります。
- * ユーザー管理者の場所は、管理者が Azure AD に認証するときに監査する必要があります
- * マルウェアを含む添付ファイルを含む電子メール メッセージは、添付ファイルなしで配信する必要があります
- * 可能な限り最小特権の原則を使用する必要があります

最新問題: 136

contoso.com という名前の Microsoft Azure Active Directory (Azure AD) テナントがあります。

次の表に示すように、4 つの Windows 10 デバイスがテナントに参加しています。

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

どのデバイスで BitLocker To Go を使用でき、どのデバイスで自動ロック解除をオンにできます

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: 正しく選択するたびに 1 ポイントの価値があります。

BitLocker To Go:	Device3 only
	Device1 and Device2 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4
Auto-unlock:	Device1 and Device2 only
	Device1 and Device3 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4

Answer:

BitLocker To Go:	Device3 only
	Device1 and Device2 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4
Auto-unlock:	Device1 and Device2 only
	Device1 and Device3 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4

説明

BitLocker To Go:	Device3 only
	Device1 and Device2 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4
Auto-unlock:	Device1 and Device2 only
	Device1 and Device3 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする

人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (32930%OFF問題集
溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 137

デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。
次の図に示すように、Microsoft OneDrive で共有設定を構成します。

Links

Choose the kind of link that's selected by default when users share items.

Default link type

- Shareable: Anyone with the link
- Internal: Only people in your organization
- Direct: Specific people

External sharing

Users can share with:

SharePoint **OneDrive**

Anyone
Users can create shareable links that don't require sign-in

New and existing external users
External users must sign-in

Existing external users
Only users already in your organization's directory

Only people in your organization
No external sharing allowed.

Most permissive

Least permissive

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

Allow or block sharing with people on specific domains

Allow only these domains: Contoso.com, Adatum.com

[Add domains](#)

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

注: 正しく選択するたびに 1 ポイントの価値があります。

A user who has an email address of user1@fabrikam.com [answer choice]

 Microsoft ▼
cannot access OneDrive content
can access OneDrive content after a link is created
must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

▼
the user cannot access OneDrive content
the user can access OneDrive content after a link is created
must be added to a group before the user can access shared files

Answer:

A user who has an email address of user1@fabrikam.com [answer choice]

 Microsoft ▼
cannot access OneDrive content
can access OneDrive content after a link is created
must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

▼
the user cannot access OneDrive content
the user can access OneDrive content after a link is created
must be added to a group before the user can access shared files

Explanation:

参考文献:

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

最新問題: 138

Microsoft 365 サブスクリプションをお持ちです。

顧客は、彼女の名前が記載されているすべての文書を提供するように要求しています。

コンテンツのコピーを顧客に提供する必要があります。

どの4つのアクションを順番に実行する必要がありますか? 回答するには、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

- Close the case.
- Regenerate a report.
- View the results.
- Export the results.
- Create a Data Subject Request (DSR) case.
- Save the search.
- Download the results.

Answer Area

Empty answer area boxes.

jpnpdf.com



Answer:

Actions

- Close the case.
- Regenerate a report.
- View the results.
- Export the results.
- Create a Data Subject Request (DSR) case.
- Save the search.
- Download the results.

Answer Area

Create a Data Subject Request (DSR) case.

View the results.

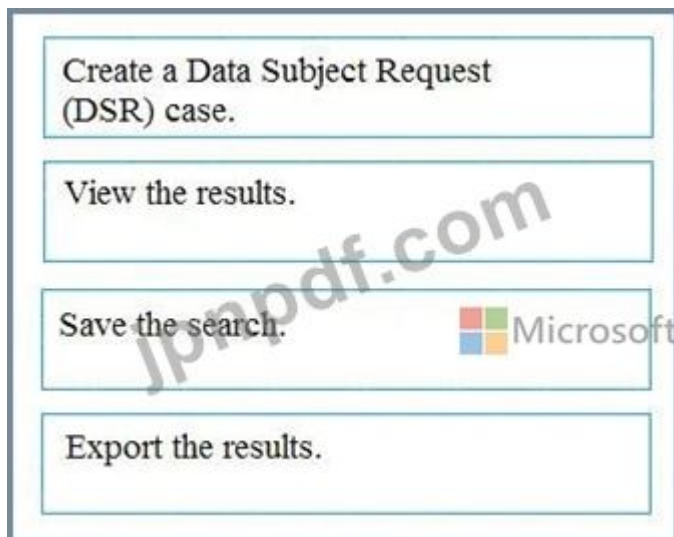
Save the search.

Export the results.

jpnpdf.com



説明



参照：

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

最新問題: 139

ネットワークにはオンプレミスの Active Directory ドメインが含まれています。ドメインには、次の表に示すサーバーが含まれています。

Name	Configuration
DC1	Domain controller
Server1	Member server

ドメインに Azure Advanced Threat Protection (ATP) を実装する予定です。

Azure ATP スタンドアロン センサーを Server1 にインストールします。

Azure ATP を使用してドメインを監視する必要があります。

- A. DO のポートミラーリングを設定します。
- B. サーバー 1 のポートミラーリングを設定します。
- C. Microsoft Monitoring Agent をサーバーにインストールします。
- D. Microsoft Monitoring Agent を DC1 にインストールします。

Answer: D (メッセージを残す)

タスク 1

管理者が電子メール メッセージやドキュメントにフッターを追加するラベルを公開できるようにする必要があります。

タスク 2

Microsoft OneDrive にドキュメントを 2 年間保持し、その後ドキュメントを自動的に削除するラベルを発行する予定です。

ラベルを作成する必要があります。

タスク 3

<https://LODSe44454.sharepoint.com/sites/leadership> で、ユーザー名 Irvin Sayers が Budget という単語を含むドキュメントを完全に削除できないようにする必要があります。

タスク 4

ConfidentialHR.docx という名前のファイルを Microsoft SharePoint ライブラリに追加する予定で

す。

別のユーザーが ConfidentialHR.xlsx にアクセスしたときに、Megan Bowen という名前のユーザーに通知が届くようにする必要があります。

タスク5

クレジットカード番号を含む Microsoft OneDrive 内のコンテンツを識別するポリシーを作成する必要があります。

タスク6

Microsoft SharePoint コンテンツが複数のドメインのユーザーと共有されていることがわかりました。

Contoso.com という名前の電子メール ドメイン内のユーザーにのみ共有招待を送信できるようにする必要があります。

タスク7

あなたの会社は別の会社と合併する予定です。

Debra Berger という名前のユーザーはあなたの会社の幹部です。

Debra Berger に、「merger」という単語を含む Alex Wiber という名前のユーザーのすべての電子メール コンテンツを提供する必要があります。

タスク8

Exchange Online に接続しようとするときに、管理対象外のモバイル デバイスが隔離されていることを確認する必要があります。

タスク9

ユーザーが Microsoft Office 365 proPlus アプリケーションまたは Android デバイスからドキュメントまたは電子メール メッセージ内のリンクを選択するタイミングを管理するソリューションを実装する必要があります。ソリューション。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。

* fabrikam.com という名前のドメインへのアクセスをブロックします。

* ユーザーが fabrikam.com へのリンクを選択したときに情報を保存します

タスク 10

すべてのフィッシングメール メッセージを自動的に隔離するように組織を構成する必要があります。

タスク 11

すべてのユーザーが 100 日ごとにパスワードを変更する必要があることを確認する必要があります。

タスク 12

Grady Archie という名前のユーザーが Microsoft 365 テナントのサービスの正常性を監視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、最小特権の原則を使用する必要があります。

最新問題: 140

ワークロード管理者のセキュリティ要件を満たすようにアクセス レビューを構成する予定です。アクセス レビュー ポリシーを作成し、スコープとグループを指定します。

他にどのような設定を構成する必要がありますか？ 回答するには、回答領域で適切な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。

Set the frequency to:

One time	▼
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	▼
Advanced settings	
Programs	
Reviewers	

Answer:

Set the frequency to:

One time	▼
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	▼
Advanced settings	
Programs	
Reviewers	

最新問題: 141

contoso.com の既定のドメイン名を使用する Microsoft 365 サブスクリプションがあります。多要素認証 (MFA) サービスの設定は、図に示すように構成されています。(「展示」タブをクロックします。)

multi-factor authentication
users service settings

app passwords [\(earn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(earn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets

verification options [\(earn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication [\(earn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60)



contoso.com で、次の表に示すユーザーを作成します。

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

構成の効果は何ですか？ 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。

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

Answer:

User1:



Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

最新問題: 142

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

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

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

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

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

Policy1 を適用する必要があります。

どのグループに Policy1 を適用できますか? 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: 正しく選択するたびに 1 ポイントの価値があります。

On-premises Active Directory groups:

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

Azure AD groups:

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

Answer:

On-premises Active Directory groups:

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

Azure AD groups:

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

説明

On-premises Active Directory groups:

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

Azure AD groups:

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

参照 :

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

最新問題: 143

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正解がある場合もありますが、他の質問セットには正解がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

contoso.com という名前のオンプレミスの Active Directory ドメインがあります。

Windows Server を実行する Server1 という名前のサーバーに Azure AD Connect をインストールして実行します。

Azure AD Connect イベントを表示する必要があります。

Server1 のセキュリティ イベント ログを使用します。

それは目標を達成していますか？

A. はい

B. いいえ

Answer: B (メッセージを残す)

説明

参考文献:

<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

最新問題: 144

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

<input type="checkbox"/>	Name	Group type	Membership type	Email	Security enable
<input type="checkbox"/>	 Group1	Microsoft 365	Assigned	Group1@sk220130.onmicrosoft.com	No
<input type="checkbox"/>	 Group2	Microsoft 365	Assigned	Group2@sk220130.onmicrosoft.com	Yes
<input type="checkbox"/>	 Group3	Distribution	Assigned	Group3@sk220130.onmicrosoft.com	No
<input type="checkbox"/>	 Group4	Mail enabled security	Assigned	Group4@sk220130.onmicrosoft.com	Yes
<input type="checkbox"/>	 Group5	Security	Assigned		Yes

ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。注: 正しい選択肢はそれぞれ 1 ポイントの価値があります。

Answer Area

[Answer choice] can be assigned to receive noncompliance notifications generated by device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

[Answer choice] can be assigned device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

Answer:

Answer Area

[Answer choice] can be assigned to receive noncompliance notifications generated by device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

[Answer choice] can be assigned device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

説明

Answer Area

[Answer choice] can be assigned to receive noncompliance notifications generated by device compliance policies. Group1, Group2, Group3, Group4, and Group5

[Answer choice] can be assigned device compliance policies. Group1, Group2, Group3, and Group4 only

最新問題: 145

Microsoft 365 E5 サブスクリプションをお持ちです。

すべてのコンピューターは Windows 10 を実行し、Windows Defender Advanced Threat Protection (Windows Defender ATP) にオンボードされています。

MachineGroup1 という名前の Windows Defender マシングループを作成します。

MachineGroup1 のコンピューターのセキュリティ設定の委任を有効に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

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Azure portal, create an RBAC role.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Azure Cloud Shell, run the Add-InfoRoleMember cmdlet.

Answer Area

Answer:

Microsoft
Answer Area

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

1 - Microsoft Azure ポータルから、Azure Active Directory (Azure AD) グループを作成します。

2 - Windows Defender セキュリティ センターから、ロールを作成します。

3 - Windows Defender セキュリティ センターから、MachineGroup1 のアクセス許可を構成します。

最新問題: 146

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

多要素認証 (MFA) サービスの設定は、図に示すように構成されています。(「展示」タブをクロックします。)

multi-factor authentication

users service settings



app passwords [\(earn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(earn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets

verification options [\(earn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication [\(earn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust


Days before a device must re-authenticate (1-60)

contoso.com で、次の表に示すユーザーを作成します。

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

構成の効果は何ですか? 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。

User1:  Microsoft	
Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	
User2:	
Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

Answer:

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	



User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

説明

User1:  Microsoft

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

Microsoft 365 サブスクリプションをよろしく申し上げます。

どのコンテンツがデータ投げ防止 (DIP) ポリシーの対象となるかをユーザーが手動で指定できるようにする必要がありますか？

最初に何を作成する必要がありますか？

- A. 保持ラベル
- B. 安全な添付ファイル ポリシー
- C. カスタム機密情報タイプ
- D. データ主体リクエスト (OSR)

Answer: D ([メッセージを残す](#))

最新問題: 148

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

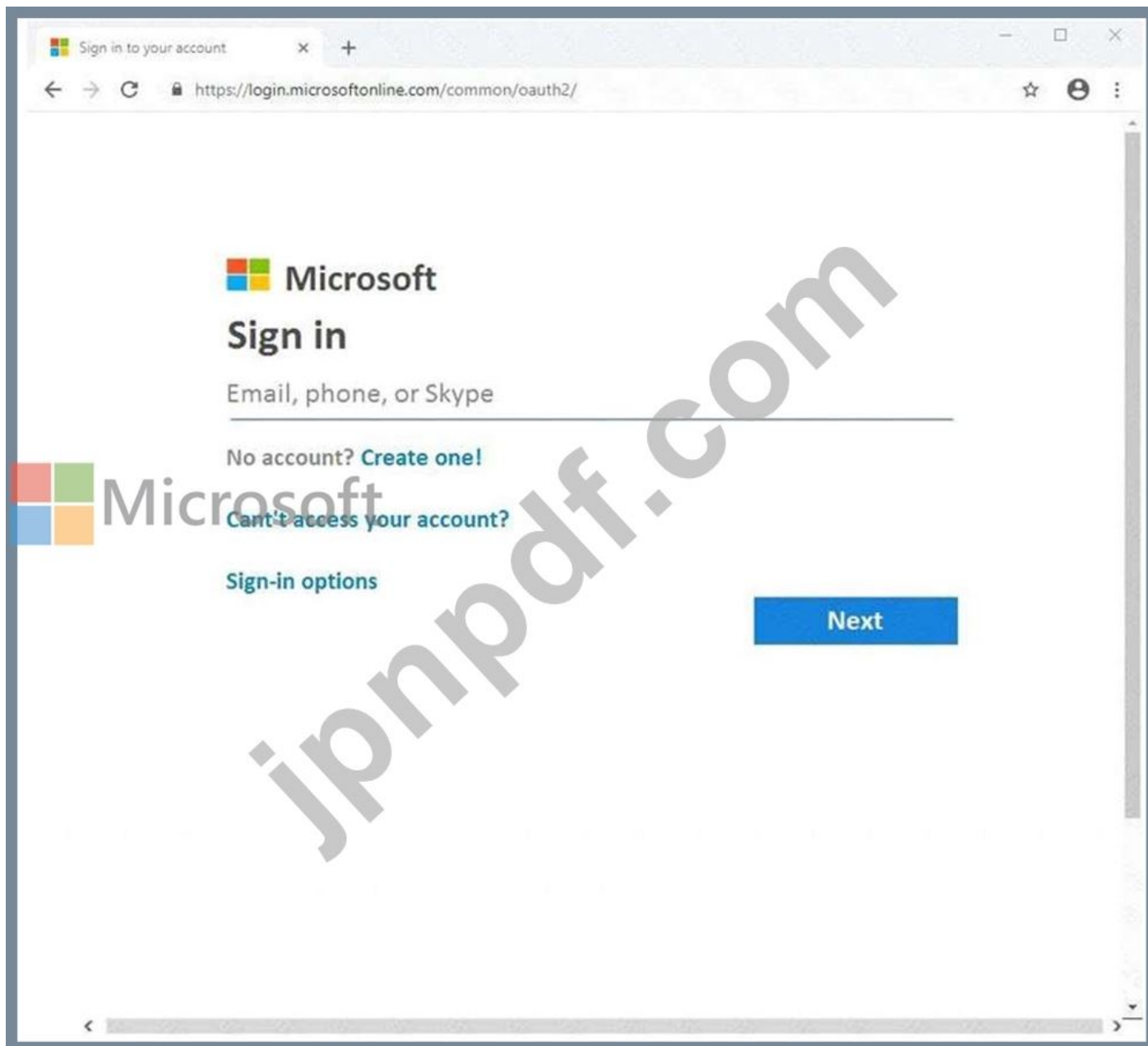
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308

Microsoft



Microsoft



Get your work done
with **Office 365**



jpnpdf.com

Microsoft



Microsoft

Brainstorm
together in **Word**



Microsoft



Microsoft

Stay on top of what matters with **Outlook**





Access Office 365 apps and documents in one place with **Office.com**



Microsoft Office Home x +

office.com/?auth=2

Contoso electronics Office 365

Good morning Install Office

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15 **Excel**
Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15 **Excel**
Integrated Team Sales Process
Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15 **Org Chart**
Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15 **Excel**
P and L Summary
lodse000198.sharepoint.co...

You edited this Jan 15 **Word**
Contoso Electronics Outdoor...
lodse000198.sharepoint.co...

You edited this Jan 15 **Word**
AD Slogans
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

Upload and open...

New

Go to OneDrive



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive

SharePoint

Frequent sites

Following

SM Sales and Marketing

R Retail

Cs Communication Site

SharePoint

Frequent sites

Following

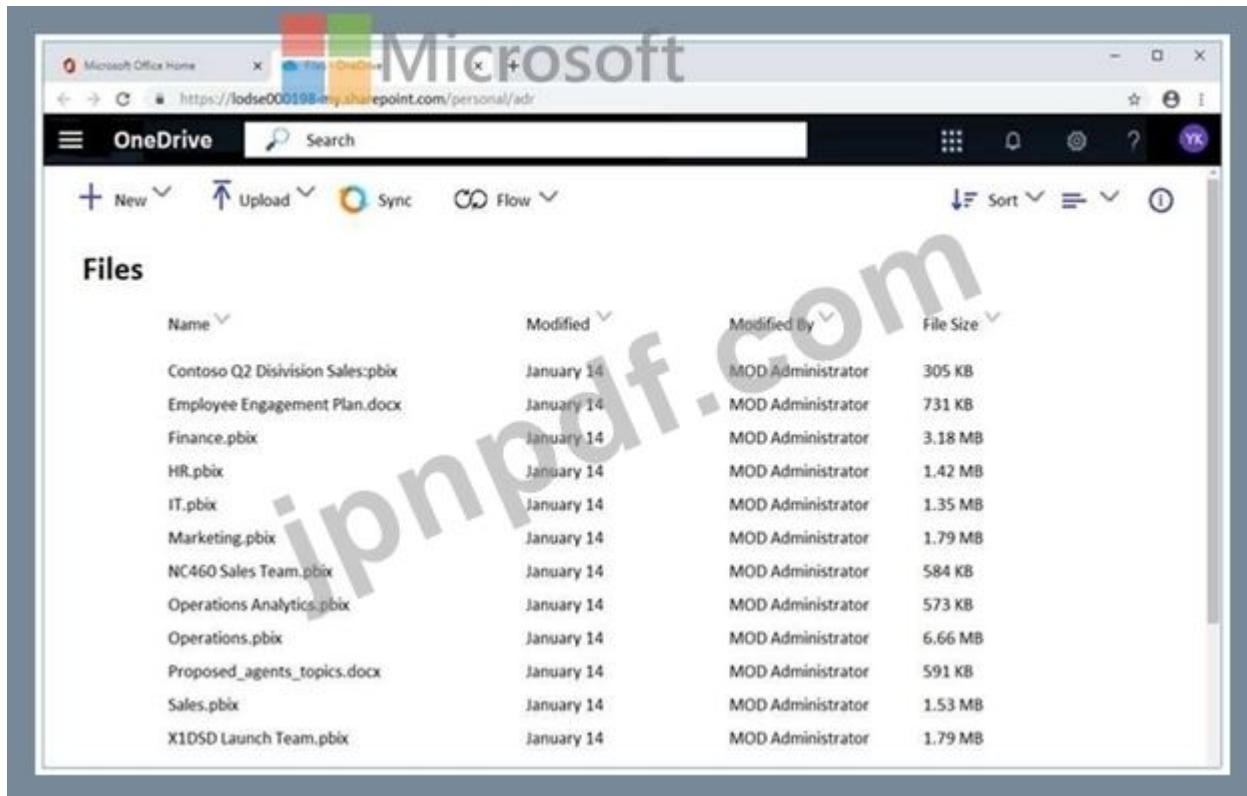
CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

Go to SharePoint





Allan Deyoung という名前のユーザーが検索を実行し、メールボックス、SharePoint Online サイト、および OneDrive for Business の場所で保留を実行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、最小特権の原則を使用する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

* Microsoft 365 管理センターにサインインした後、セキュリティ & コンプライアンス センターに移動します。

* セキュリティおよびコンプライアンス センターの左側のペインで、[アクセス許可] を選択し、電子情報開示マネージャーの横にあるチェックボックスをオンにします。

* [電子情報開示マネージャー] フライアウト ページで、割り当てる電子情報開示アクセス許可に基づいて次のいずれかを実行します。

ユーザーを電子情報開示マネージャーにするには: [電子情報開示マネージャー] の横にある [編集] を選択します。[電子情報開示マネージャーの選択] セクションで、[電子情報開示マネージャーの選択] ハイパーリンクを選択し、[+ 追加] を選択します。

電子情報開示マネージャーとして追加するユーザー (複数可) を選択し、[追加] を選択します。

ユーザーの追加が完了したら、[完了] を選択します。次に、[編集] [電子情報開示マネージャーの選択] フライアウト ページで、[保存] を選択して、電子情報開示マネージャーのメンバーシップへの変更を保存します。

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwi>

最新問題: 149

ネットワークには contoso.com という名前の Active Directory ドメインが含まれています。ドメインには、Windows Server 2016 を実行し、リモート アクセス サーバーの役割がインストールされている VPN1 という名前の VPN サーバーが含まれています。

Microsoft Azure サブスクリプションをお持ちです。

Azure Advanced Threat Protection (ATP) をデプロイしています。

Windows Server 2016 を実行する Server1 という名前のサーバーに Azure ATP スタンドアロンセンサーをインストールします。

VPN と Azure ATP を統合する必要があります。

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。

On VPN1:	Configure an authentication provider.	v
	Configure an accounting provider.	
	Create a connection request policy.	
	Create a RADIUS client.	

On Server1, enable the following inbound port:

443	v
1723	
1813	
8080	
8531	

Answer:

On VPN1:

Configure an authentication provider.	v
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:


443	v
1723	
1813	
8080	
8531	

On VPN1:

Configure an authentication provider.	V
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	V
1723	
1813	
8080	
8531	



参照 :

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn>

最新問題: 150

ユーザーは次のファイルを Microsoft OneDrive に保存します。

ファイル.docx

重要ファイル.docx

ファイル_重要.docx

次の例に示すフィルターを持つ Microsoft Cloud App Security ファイル ポリシー Policy1 を作成します。

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

X File name contains words File

Apply to: all files

Apply to: all file owners



Policy1 はどのファイルに適用されますか?

- A. ファイル_重要.docx のみ
- B. ファイル.docx、重要ファイル.docx、およびファイル_重要.docx
- C. ファイル.docx のみ
- D. 重要ファイル.docx のみ
- E. File.docx および File_Minimum.docx のみ

Answer: ([解答を表示する](#))

参照：

<https://docs.microsoft.com/en-us/cloud-app-security/file-filters>

最新問題: 151

Microsoft 365 サブスクリプションを持つ Azure Active Directory (Azure AD) テナントがある。最近、危険なサインインに対して多要素認証 (MFA) を要求するようにテナントを構成した。MFA を必要としたユーザーを確認する必要がある。

あなたは何をすべきか？

- A. Microsoft 365 管理センターから、セキュリティとコンプライアンスのレポートを確認します。
- B. Microsoft 365 コンプライアンス管理センターから監査ログ検索を実行し、結果を CSV ファイルにダウンロードします。
- C. Azure Active Directory 管理センターから、認証方法のアクティビティを確認します。
- D. Azure Active Directory 管理センターから、sign-ms を CSV ファイルにダウンロードします。

Answer: ([解答を表示する](#))

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 152

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

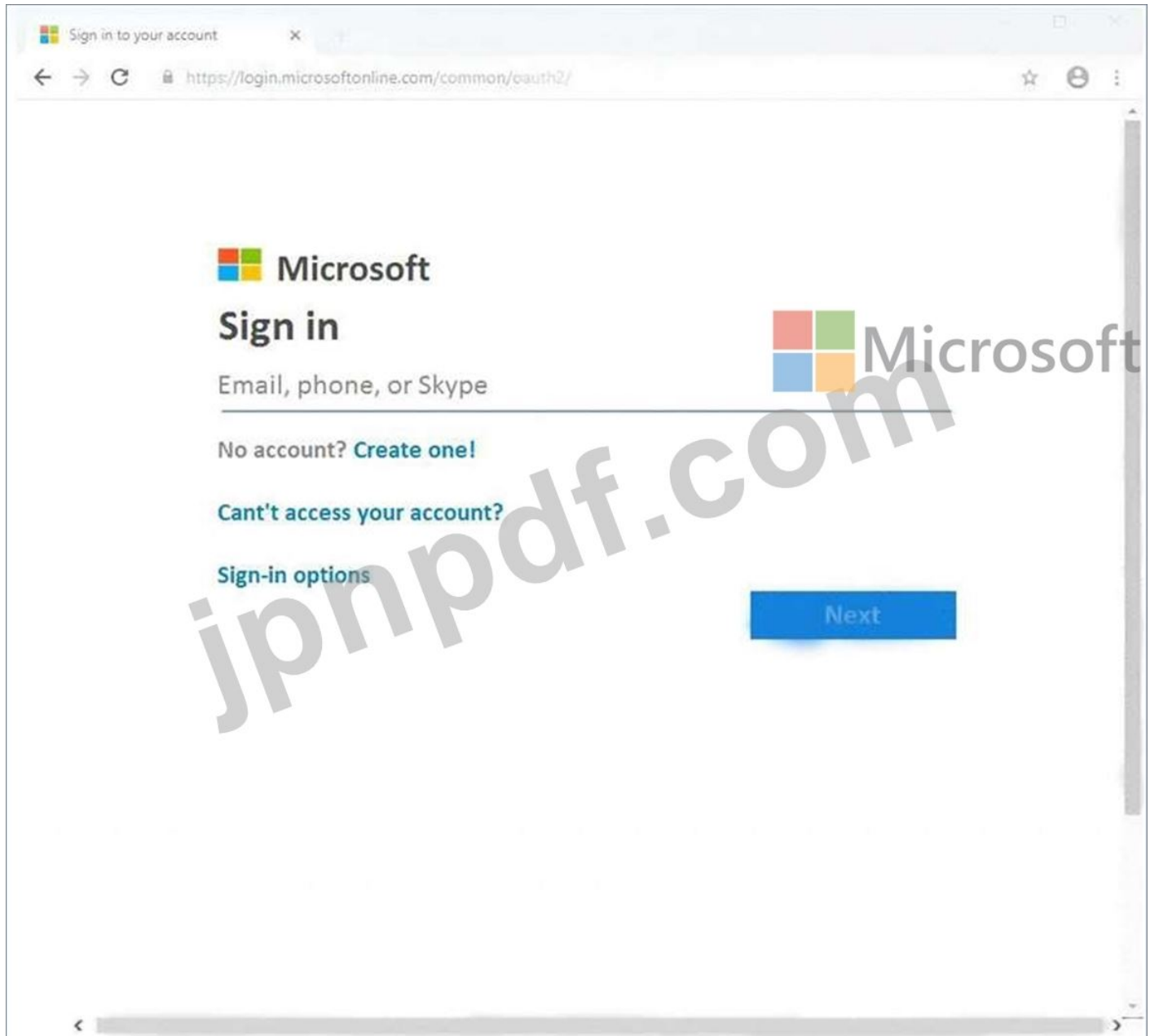
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308

 Microsoft



jpnpdf.com

Get your work done
with **Office 365**



 Microsoft

Microsoft

Microsoft ✕



jpnpdf.com

Brainstorm
together in Word



Microsoft



Stay on top of what matters with Outlook



Microsoft

Microsoft



Microsoft



Access Office 365 apps and documents in one place with

Office.com



jpnpdf.com

Microsoft Office Home x + Microsoft

office.com/?auth=2

Contoso electronics Office 365

Good morning Install Office

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Integrated Team Sales Process

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

Sales Process
lodse000198.sharepoint.co...

Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended Microsoft

You edited this Jan 15

Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15

Word

Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

AD Slogans

AD Slogans
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

↑ Upload and open...

New ▾

Go to OneDrive →



Microsoft

Recent Pinned Shared with me Discover

Microsoft

↑

OneDrive

No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →

SharePoint

Frequent sites

Following

SM Sales and Marketing

R Retail

Cs Communication Site

Go to SharePoint →

SharePoint

Frequent sites

Following

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

次の要件を満たすために Azure Information Protection ラベルを作成する必要があります。

* コンテンツは 21 日後に期限切れになる必要があります。

※ オフラインアクセスは 21 日間のみ許可する必要があります。

※ ドキュメントはクラウドキーを使用して保護する必要があります。

※ 認証されたユーザーはコンテンツの閲覧のみが可能である必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

1. まだ行っていない場合は、新しいブラウザ ウィンドウを開いて Azure portal にサインインします。次に、[Azure Information Protection] ウィンドウに移動します。

たとえば、リソース、サービス、ドキュメントの検索ボックスに「情報」と入力し、[Azure Information Protection] を選択します。

2. [分類] > [ラベル] メニュー オプションから: [Azure Information Protection - ラベル] ペインで、変更するラベルを選択します。

[ラベル] ウィンドウで、[このラベルを含むドキュメントと電子メールに対するアクセス許可を設定する] を見つけて、[保護] を選択します。

3. 「保護」を選択します。

4. [保護] ペインで、[Azure (クラウド キー)] を選択します。

5. [アクセス許可の設定] を選択して、このポータルで新しい保護設定を定義します。

6. [Azure のアクセス許可の設定 (クラウド キー)] を選択した場合、このオプションでユーザーと使用権限を選択できます。

保護されたドキュメントや電子メールを開けられるようにするユーザーを指定するには、[アクセ

ス許可の追加] を選択します。

次に、[アクセス許可の追加] ペインで、選択したラベルによって保護されるコンテンツを使用する権限を持つユーザーとグループの最初のセットを選択します。

* リストから [選択] を選択し、[追加] を選択して組織からすべてのユーザーを追加できます。

<組織名> - すべてのメンバー。この設定ではゲスト アカウントが除外されます。または、**「認証されたユーザーを追加」**を選択するか、ディレクトリを参照することもできます。

すべてのメンバーを選択するか、ディレクトリを参照する場合、ユーザーまたはグループには電子メールアドレスが必要です。運用環境では、ユーザーとグループはほぼ常に電子メールアドレスを持っていますが、単純なテスト環境では、ユーザー アカウントまたはグループに電子メールアドレスを追加する必要がある場合があります。

* ファイル コンテンツの有効期限設定を 21 日に変更します。

* オフライン アクセスを許可する設定を 21 日に変更します。

権限と設定の構成が完了したら、**「OK」**をクリックします。

この設定のグループ化により、Azure Rights Management サービスのカスタム テンプレートが作成されます。これらのテンプレートは、Azure Rights Management と統合されるアプリケーションおよびサービスで使用できます。

7. **「OK」** をクリックして **「保護」** ペインを閉じると、**「ラベル」** ペインの **「保護」** オプションとしてユーザー定義または選択したテンプレートが表示されます。

8. **「ラベル」** ペインで、**「保存」** をクリックします。

9. **「Azure Information Protection」** ペインの **「保護」** 列を使用して、ラベルに必要な保護設定が表示されていることを確認します。

* 保護を設定している場合はチェックマークが付きます。

※ 保護を解除するラベルを設定している場合は、×印が解除されます。

※ プロテクトが設定されていない場合は空白となります。

「保存」 をクリックすると、変更内容がユーザーとサービスに自動的に適用されます。個別の公開オプションはなくなりました。

参照：

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection>

最新問題: 153

Microsoft 365 E5 サブスクリプションをお持ちです。

すべてのコンピューターは Windows 10 を実行し、Windows Defender Advanced Threat Protection (Windows Defender ATP) にオンボードされています。

MachineGroup1 という名前の Windows Defender マシン グループを作成します。

MachineGroup1 のコンピューターのセキュリティ設定の委任を有効に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

- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.
- From the Azure portal, create an RBAC role.
- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Azure Cloud Shell, run the Add-Hso1RoleMember cmdlet.

Answer Area



Answer:

Actions

- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.
- From the Azure portal, create an RBAC role.
- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Azure Cloud Shell, run the Add-Hso1RoleMember cmdlet.

Answer Area

- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.

説明

Answer Area

- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Windows Defender Security Center, create a role.
- From Windows Defender Security Center, configure the permissions for MachineGroup1.

最新問題: 154

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
User1	Global administrator
User2	Compliance administrator
User3	Security administrator
User4	Security operator

Azure Active Directory (Azure AD) Identity Protection を実装する予定です。
どのユーザーが次のアクションを実行できるかを特定する必要があります。

- * ユーザーリスクポリシーを設定します。
- * 危険なユーザーのレポートを表示します。

どのユーザー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。

Configure a user risk policy:

▼

User1 only
User1 and User3 only
User3 and User4 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

▼

User1 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4


Microsoft

Answer:

Configure a user risk policy:

	▼
User1 only	
User1 and User3 only	
User3 and User4 only	
User1, User3, and User4 only	
User1, User2, User3, and User4	

View the risky users report:

	▼
User1 only	
User3 and User4 only	
User1, User2, and User3 only	
User1, User3, and User4 only	
User1, User2, User3, and User4	

参照 :

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

最新問題: 155

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Groups administrator
Admin2	User administrator

contoso.com のグループ名前付けポリシーに禁止単語として「Internal」を追加します。

contoso.com のグループ名前付けポリシーのプレフィックスとして Contoso- を追加します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input checked="" type="radio"/>	<input type="radio"/>

ユーザー管理者とグローバル管理者は、グループパスワードポリシーから除外されます。

参照：

<https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide>

最新問題: 156

デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。

次の図に示すように、Microsoft OneDrive で共有設定を構成します。

Links


Choose the kind of link that's selected by default when users share items.

Default link type

Shareable: Anyone with the link

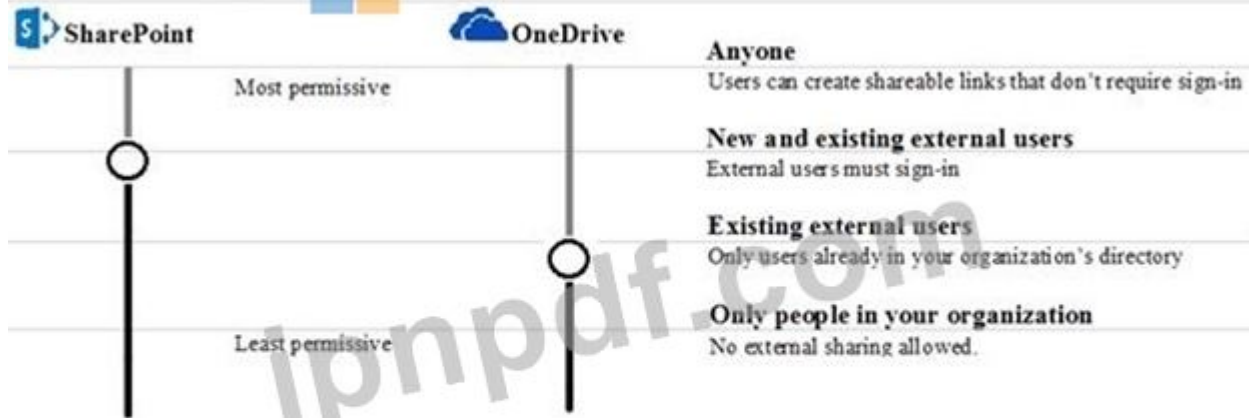
Internal: Only people in your organization

Direct: Specific people



External sharing

Users can share with:



Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

Allow or block sharing with people on specific domains
Allow only these domains: Contoso.com, Adatum.com

[Add domains](#)

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

注: 正しく選択するたびに 1 ポイントの価値があります。

A user who has an email address of user1@fabrikam.com [answer choice]

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

Answer:

A user who has an email address of user1@fabrikam.com [answer choice]

cannot access OneDrive content
 can access OneDrive content after a link is created
 must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

the user cannot access OneDrive content
 the user can access OneDrive content after a link is created
 must be added to a group before the user can access shared files

参照 :

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

最新問題: 157

Microsoft 365 サブスクリプションをお持ちです。

サイトに保存されている機密データを検索するには、Microsoft SharePoint Online でデータ損失防止 (DLP) クエリを作成する必要があります。

どの種類のサイト コレクションを最初に作成する必要がありますか？

- A. レコードセンター
- B. コンプライアンス ポリシー センター
- C. 電子情報開示センター
- D. エンタープライズ検索センター
- E. ドキュメントセンター

Answer: ([解答を表示する](#))

参照 :

<https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bbb>

最新問題: 158

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

多要素認証 (MFA) サービスの設定は、図に示すように構成されています。(「展示」タブをクリックします。)

multi-factor authentication

users service settings



app passwords [\(earn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(earn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets

verification options [\(earn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication [\(earn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60)

contoso.com で、次の表に示すユーザーを作成します。

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

構成の効果は何ですか? 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。

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

Answer:

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

最新問題: 159

Microsoft 365 E5 サブスクリプションをお持ちです。

一部のユーザーは、Microsoft SharePoint Online にアクセスするために認証アプリを使用する必要があります。

SharePoint Online にアクセスするために認証アプリを使用したユーザーを表示する必要があります。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。

あなたは何をするべきか？

A. Azure Active Directory 管理センターから、サインインを表示します。

- B. セキュリティとコンプライアンス管理センターからレポートをダウンロードします。
- C. Azure Active Directory 管理センターのエンタープライズ アプリケーション ブレードから、監査ログを表示します。
- D. Azure Active Directory 管理センターから、監査ログを表示します。

Answer: A ([メッセージを残す](#))

説明/参照:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

最新問題: 160

ネットワークにはオンプレミスの Active Directory ドメインが含まれています。ドメインには、Windows Server を実行し、高度な監査が有効になっているサーバーが含まれています。サーバーのセキュリティ ログは、サードパーティの SIEM ソリューションを使用して収集されません。

Microsoft 365 サブスクリプションを購入し、スタンドアロン センサーを使用して Azure Advanced Threat Protection (ATP) を展開することを計画しています。

機密性の高いグループが変更されたときと、悪意のあるサービスが作成されたときを確実に検出できるようにする必要があります。

あなたは何をすべきか？

- A. Office 365 セキュリティ & コンプライアンス センターで監査を構成します。
- B. Azure ATP センサーの遅延更新をオフにします。
- C. Azure ATP センサーでドメイン シンクロナイザー候補の設定を変更します。
- D. SIEM と Azure ATP を統合します。

Answer: (解答を表示する)

説明

参考文献:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>

最新問題: 161

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

Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を実装します。

PIM から、アプリケーション管理者の役割を確認し、次の表に示すユーザーを検出します。

Name	Assignment type
UserA	Permanent
UserB	Eligible
UserC	Eligible

アプリケーション管理者の役割は、PIM で次の設定を使用するように構成されています。

最大アクティベーション期間: 1 時間

通知: 無効にする

インシデント/リクエストチケット: 無効にする

多要素認証: 無効にする

承認が必要: 有効にする

選択した承認者: 結果はありません

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input type="radio"/>

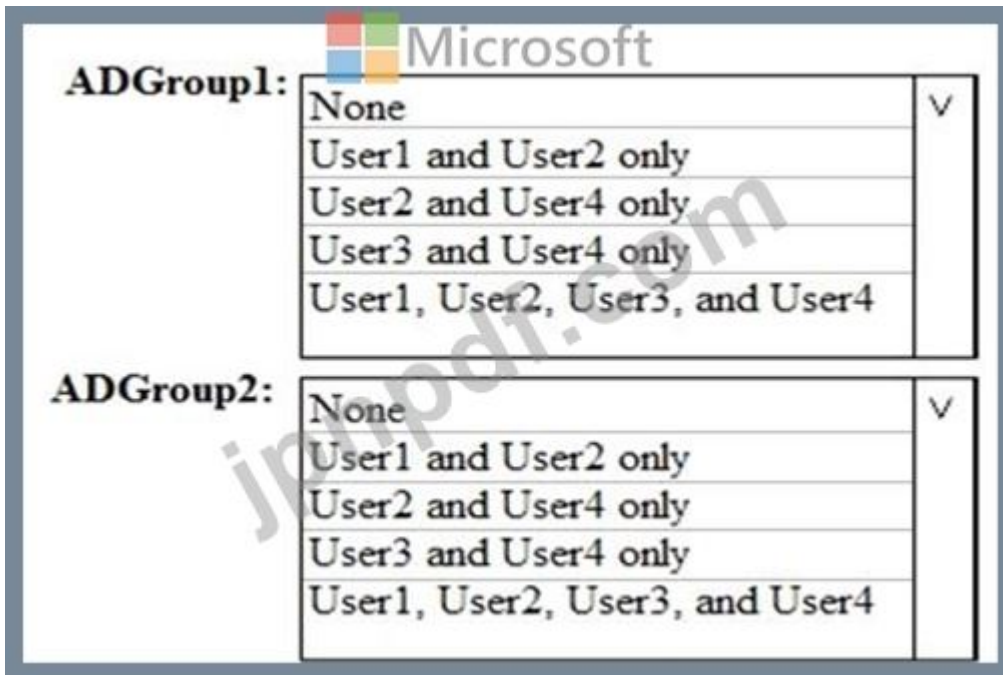
Answer:

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input checked="" type="radio"/>

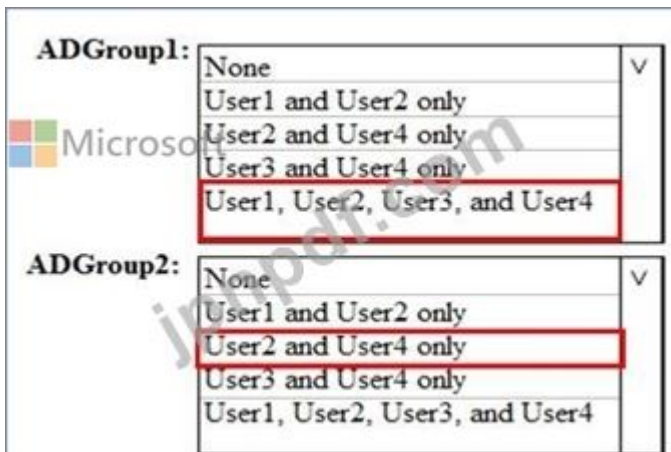
最新問題: 162

ADGroup1 と ADGroup2 のメンバーはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values>

最新問題: 163


User 1 と User2 という名前の 2 人のユーザーを含む Microsoft E5 サブスクリプションがあります。

Site1 という名前の Microsoft SharePoint サイトがあります。Site1 には、次の表に示すように IP アドレスを含むファイルが保存されます。

Name	Number of IP addresses
File1.txt	3
File2.docx	1

User1 には、Site1 の SharePoint 管理者ロールが割り当てられます。User2 は Site1 のメンバーです。次の図に示すデータ損失防止 (DLP)1 ポリシーを作成します。

Review your settings

 **Template name** Edit
Custom policy

Policy name Edit
Policy1

Description Edit

Applies to content in these locations Edit
SharePoint sites

Policy settings Edit

SharePoint sites

Policy settings Edit

If the content contains these types of sensitive info: IP Address .

If there are at least 2 instances of the same type of sensitive info, block access to the content .

Turn policy on after it's created? Edit

Yes

Back

Create

Cancel

次の各ステートメントについて、ステートメントが正しい場合は [はい] を選択します。そうでない場合は、[いいえ] を選択します。注: 正しい選択肢はそれぞれ 1 ポイントの価値があります。



Answer:



説明




最新問題: 164

User1、User2、User3 という 3 人のユーザーが含まれる Microsoft 365 E5 テナントがあります。次の表に示すように、ユーザーに役割または役割グループを割り当てる必要があります。

User	Role or role group
User1	SharePoint admin
User2	Data Investigator
User3	User admin

各ユーザーに役割または役割グループを割り当てるには何を使用する必要がありますか？ 回答するには、適切なツールを正しい役割または役割グループにドラッグします。各ツールは 1 回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

Tools	Answer Area
Azure Defender for Servers	User1: Tool
Compliance Manager	User2: Tool
Microsoft 365 admin center	User3:  Tool
Security & Compliance admin center	
Trust Center	

Answer:

Tools	Answer Area 
Azure Defender for Servers	User1: Microsoft 365 admin center
Compliance Manager	User2: Security & Compliance admin center
Microsoft 365 admin center	User3: Microsoft 365 admin center
Security & Compliance admin center	
Trust Center	

参照：

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide>

最新問題: 165

セキュリティ要件を満たす電子メール マルウェア ソリューションを推奨する必要があります。推奨事項には何を含めるべきですか? 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。

Policy to create soft

ATP safe attachments	v
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	v
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

Answer:

Actions

- From PowerShell, run Remove-SPOUserProfile
- Delete Litware.docx from the Recycle Bin of Site2.
- From PowerShell, run Set-SPOSite.
- Delete Litware.docx from the Recycle Bin of SiteCollection1.
- From Powershell, run Remove-SPOUserInfo
- Delete Litware.docx from Customers.

Answer Area

- Delete Litware.docx from Customers.
- Delete Litware.docx from the Recycle Bin of Site2.
- Delete Litware.docx from the Recycle Bin of SiteCollection1.

説明

Policy to create:

ATP safe attachments	v
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	v
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

最新問題: 166

次の表に示すユーザーを含むハイブリッド Microsoft 365 展開があります。

Name	Mailbox	Cloud license
User1	On-premises Microsoft Exchange Server	Microsoft Teams
User2	On-premises Microsoft Exchange Server	Microsoft Exchange Online Plan 2
User3	On-premises Microsoft Exchange Server	Microsoft Teams, Exchange Online Plan 2
User4	Microsoft Exchange Online	Microsoft Teams, Exchange Online Plan 2

電子情報開示コンテンツ検索を実行する必要があります。

コンテンツ検索にはどのユーザー データを含めることができますか? 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: 正しく選択するたびに 1 ポイントの価値があります。



Answer:
ANSWER AREA



説明
Answer Area



有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 167

contoso.com の既定のドメイン名を使用する Microsoft 365 サブスクリプションがあります。多要素認証 (MFA) サービスの設定は、図に示すように構成されています。(「展示」タブをクロックします。)

multi-factor authentication
users service settings

app passwords (earn more)
 Allow users to create app passwords to sign in to non-browser apps
 Do not allow users to create app passwords to sign in to non-browser apps

trusted ips(earn more)
 Skip multi-factor authentication for requests from federated users on my intranet
 Skip multi-factor authentication for requests from following range of IP address subnets

verification options (earn more)
 Methods available to users:
 Call to phone
 Text message to phone
 Notification through mobile app
 Verification code from mobile app or hardware token

remember multi-factor authentication (earn more)
 Allow users to remember multi-factor authentication on devices they trust
 Days before a device must re-authenticate (1-60)

contoso.com で、次の表に示すユーザーを作成します。

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

構成の効果は何ですか？ 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。

User1:

Can sign in to the My Apps portal without using MFA	<input type="checkbox"/>
Completed the MFA registration	<input checked="" type="checkbox"/>
Must complete the MFA registration at the next sign-in	<input type="checkbox"/>

User2:

Can sign in to the My Apps portal without using MFA	<input checked="" type="checkbox"/>
Must use app passwords for legacy apps	<input type="checkbox"/>
Must use an app password to sign in to the My-Apps portal	<input type="checkbox"/>

Answer:

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

説明

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	



User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

最新問題: 168

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
User1	Information Protection Administrator
User2	Information Protection Analyst
User3	Information Protection Investigator

次のタスクを委任する必要があります。

データ損失防止 (DLP) ポリシーを作成および管理します。コンテンツ エクスプローラーを使用して、機密コンテンツを確認します。

ソリューションでは、最小特権の原則を使用する必要があります。

どのユーザーが各タスクを実行する必要がありますか? 回答するには、適切なユーザーを正しいタスクにドラッグします。各ユーザーは 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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



:

最新問題: 169

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Microsoft 365 サブスクリプションがあります。

次の要件を満たす Azure AD Privileged Identity Management (PIM) ソリューションを推奨する必要があります。

* セキュリティ管理者ロールがアクティブ化されると、管理者に通知する必要があります。

* セキュリティ管理者ロールを割り当てられたユーザーは、30 日間サインインしない場合、そのロールから自動的に削除される必要があります。

各要件に対してどの Azure AD PIM 設定を構成することを推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Administrators must be notified when the Security administrator role is activated:

	▼
Alerts	
Roles	
Access reviews	

Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days:

	▼
Alerts	
Roles	
Access reviews	

Answer:

Administrators must be notified when the Security administrator role is activated:

	▼
Alerts	
Roles	
Access reviews	

Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days:



	▼
Alerts	
Roles	
Access reviews	

説明

Administrators must be notified when the Security administrator role is activated:

	▼
Alerts	
Roles	
Access reviews	

Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days:



	▼
Alerts	
Roles	
Access reviews	

参照 :

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-config>

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-change>

最新問題: 170

出品物を参照してください。

Name	In device group
Device1	Group1
Device2	Group2
Device3	Group3

Microsoft Defender for Endpoint には、次の表に示すインシデントが含まれています。

Name	Device	File evidence	File verdict
Case1	Device1	C:\Temp\File1.exe	Suspicious
Case2	Device2	C:\Temp\File2.exe	Malicious
Case3	Device3	C:\Temp\File3.exe	Malicious

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。さもないと、[いいえ] を選択します。

Statements

	Yes	No
C:\Temp\File1.exe will be remediated automatically.	<input checked="" type="radio"/>	<input type="radio"/>
C:\Temp\File2.exe will be remediated automatically.	<input checked="" type="radio"/>	<input type="radio"/>
C:\Temp\File3.exe will be remediated automatically.	<input checked="" type="radio"/>	<input type="radio"/>

Answer:

Statements

	Yes	No
C:\Temp\File1.exe will be remediated automatically.	<input type="radio"/>	<input checked="" type="radio"/>
C:\Temp\File2.exe will be remediated automatically.	<input type="radio"/>	<input checked="" type="radio"/>
C:\Temp\File3.exe will be remediated automatically.	<input type="radio"/>	<input checked="" type="radio"/>

説明

グラフィカル ユーザー インターフェイス、アプリケーションの説明が自動的に生成される

Statements

	Yes	No
C:\Temp\File1.exe will be remediated automatically.	<input type="radio"/>	<input checked="" type="radio"/>
C:\Temp\File2.exe will be remediated automatically.	<input checked="" type="radio"/>	<input type="radio"/>
C:\Temp\File3.exe will be remediated automatically.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 171

Group1 と Group2 という名前の 2 つのグループを含む Microsoft 365 サブスクリプションがあります。

次の表に示すコンプライアンス評価があります。

Name	Group
Ca1	Group1
Ca2	Group1
Ca3	Group2

You have the improvement actions shown in the following table.

Action	Compliance assessment	Improvement action	Points	Action type
Action1	Ca1	Create and publish a retention label	5	Technical
Action2	Ca2	Create and publish a retention label	5	Technical
Action3	Ca3	Enable Windows 10 Security baseline	5	Technical
Action4	Ca1	Restrict access to privileged accounts	10	Operational

Statements	Yes	No
The compliance score for Ca1 will increase by 15 points.	<input type="radio"/>	<input type="radio"/>
The compliance score for Ca2 will increase by 15 points.	<input type="radio"/>	<input type="radio"/>
The compliance score for Ca3 will increase by 10 points.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
The compliance score for Ca1 will increase by 15 points.	<input checked="" type="radio"/>	<input type="radio"/>
The compliance score for Ca2 will increase by 15 points.	<input type="radio"/>	<input checked="" type="radio"/>
The compliance score for Ca3 will increase by 10 points.	<input checked="" type="radio"/>	<input type="radio"/>

説明

はい いいえ はい

最新問題: 172

Microsoft 365 サブスクリプションをお持ちです。

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

隔離内の添付ファイルの保存期間を構成する必要があります。

どのタイプの脅威管理ポリシーを作成する必要がありますか？

- A. ATP フィッシング対策
- B. DKIM
- C. スпам対策
- D. マルウェア対策

Answer: C ([メッセージを残す](#))

説明/参照:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined->

最新問題: 173

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 サブスクリプションがあります。Site1 には、次の表に示すフォルダーが含まれています。

Name	File in folder
Folder1	File1
Folder2	File2

09:00 に、次の図に示すように、Policy1 という名前の Microsoft Cloud App Security ポリシーを作成します。

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

× App equals Microsoft SharePoint...

+ (Add filter)

Apply to:

selected folders Currently supports Box, SharePoint, Dropbox, OneDrive.

Folder1 (Microsoft SharePoint Online) ×

[Add more folder\(s\)](#)

Apply to:

all file owners

Microsoft

Inspection method

None

Alerts

Create an alert for each matching file [Restore default settings](#)

Daily alert limit 5

Send alert as email ⓘ

Send alert as text message ⓘ

[Save as default settings](#)

Send alerts to Flow

[Create a playbook in Flow](#)

Policy1 を作成した後、次の表に示すようにファイルを Site1 にアップロードします。

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>

説明

Statements

Yes

No

File1 triggers an alert from Policy1.

File3 triggers an alert from Policy1.



Microsoft

File9 triggers an alert from Policy1.

参照 :

<https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

最新問題: 174

Microsoft 365 サブスクリプションをお持ちです。

Site2 という名前のサイトを含む SiteCollection1 という名前のサイトコレクションがあります。Site2 には、Customers という名前のドキュメント ライブラリが含まれています。

Customers には Litware.docx という名前のドキュメントが含まれています。Litware.docx を完全に削除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
From PowerShell, run Remove-SPOUserProfile	<input type="text"/>
Delete Litware.docx from the Recycle Bin of Site2.	<input type="text"/>
From PowerShell, run Set-SPOSite.	<input type="text"/>
Delete Litware.docx from the Recycle Bin of SiteCollection1.	<input type="text"/>
From Powershell, run Remove-SPOUserInfo	<input type="text"/>
Delete Litware.docx from Customers.	<input type="text"/>

Answer:

Actions	Answer Area
From PowerShell, run Remove-SPOUserProfile	Delete Litware.docx from Customers.
Delete Litware.docx from the Recycle Bin of Site2.	Delete Litware.docx from the Recycle Bin of Site2.
From PowerShell, run Set-SPOSite.	Delete Litware.docx from the Recycle Bin of SiteCollection1.
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

最新問題: 175

Microsoft 365 テナントがあります。

顧客の詳細を保存するデータベースがあります。各顧客は、数字と文字の固定パターンで構成される一意の 13 桁の ID を持っています。

次の要件を満たすデータ損失防止 (DLP) ソリューションを実装する必要があります。

単一の顧客 ID を含む電子メール メッセージを社外に送信できます。

2 つ以上の顧客 ID を含む電子メール メッセージは、会社のデータ プライバシー チームによって承認される必要があります。

ソリューションに含めるべき 2 つのコンポーネントはどれですか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 1 ポイントの価値があります。

- A. 機密情報の種類
- B. 機密ラベル
- C. 保持ラベル
- D. DLP ポリシー
- E. メール フロー ルール

Answer: A,D (メッセージを残す)

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-entity-settings?view=o365-worldwide>

最新問題: 176

Microsoft 365 サブスクリプションをお持ちです。

管理者が電子情報開示検索を開始するたびに、電子メールで通知を受ける必要があります。セキュリティとコンプライアンス管理センターから何をすべきですか？

- A. [検索と調査] から、ガイド付き検索を作成します。
- B. イベントからイベントを作成します。
- C. [アラート] から、アラート ポリシーを作成します。
- D. 検索と調査から、電子情報開示ケースを作成します。

Answer: C ([メッセージを残す](#))

説明/参照:

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

最新問題: 177

あなたの会社には、Microsoft 365 サブスクリプション、Microsoft Azure サブスクリプション、および contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。

当社は、次の表に示す営業所を設置しております。

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

テナントには、次の表に示すユーザーが含まれます。

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

次の図に示す Microsoft Cloud App Security ポリシーを作成します。

Create filters for the policy

Act on:

Single activity:
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

In a single app

Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR

equals

From group equals

as

Alerts

Create alert Use your organization's default settings

Daily alert limit

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements

	Yes	No
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	<input type="radio"/>	<input type="radio"/>
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	<input type="radio"/>	<input type="radio"/>
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements

In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

Yes

No

In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

最新問題: 178

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

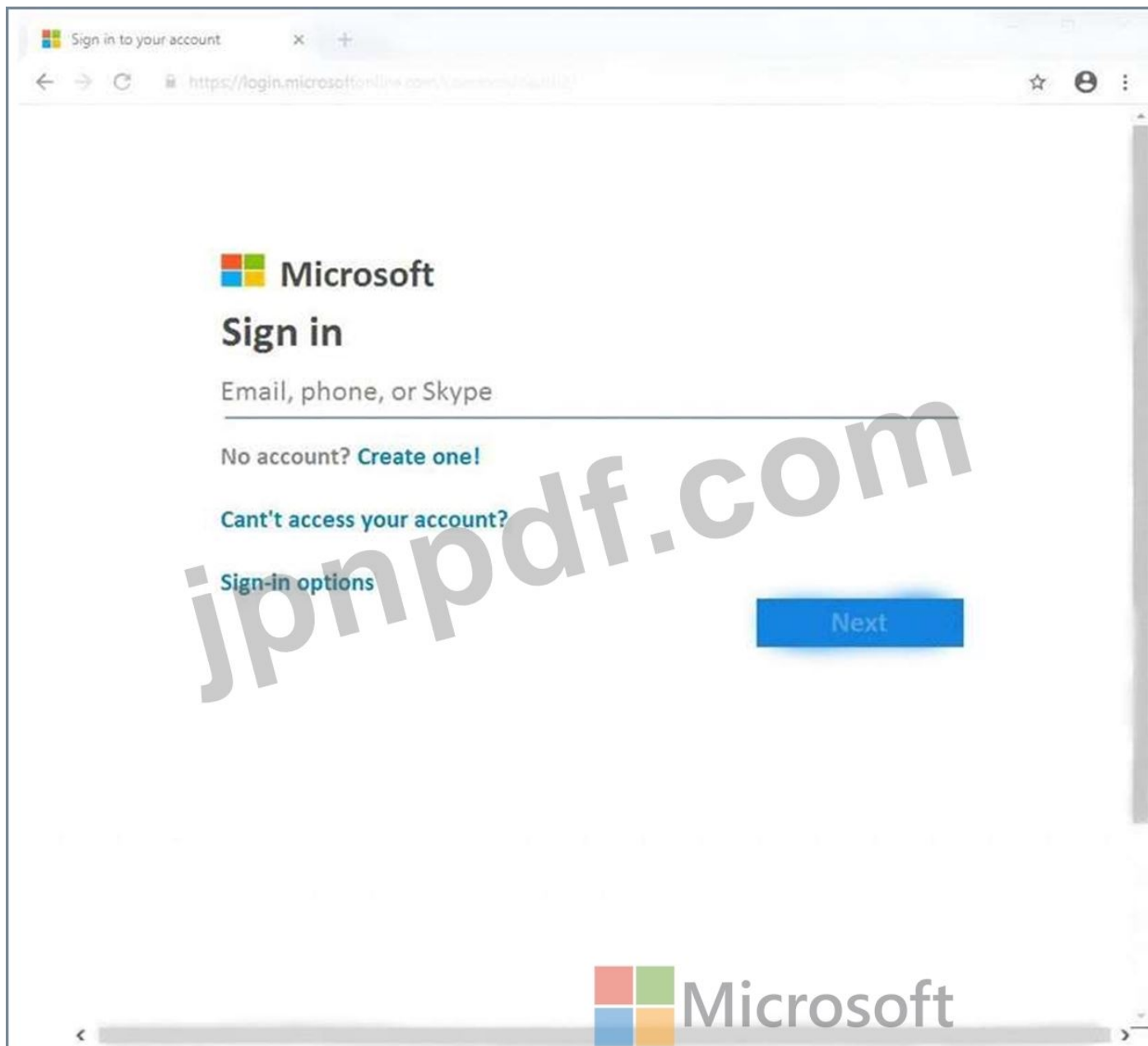
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308

 Microsoft



jpnpdf.com

Get your work done
with **Office 365**



 Microsoft



jpnpdf.com

Brainstorm
together in Word





Stay on top of what matters with Outlook



Microsoft



Microsoft



Access Office 365 apps and documents in one place with

[Office.com](https://office.com)



Microsoft Office Home | office.com/1a1b1c2

Contoso electronics | Office 365

Good morning Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint

OneNote | Skype | Calendar | People | All apps

Recommended

You edited this Jan 15

Excel

Integrated Team Sales Process

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Excel

Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Word

Org Chart

Org Chart
lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover **Microsoft**

Recommended **Microsoft**

You edited this Jan 15

Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15

Word

Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Word

AD Slogans

AD Slogans
lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover



No recent online documents
share and collaborate with others. To get started, create a new document
or drag it here to upload and open.

Upload and open... **New** ▾

Go to OneDrive →



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →



SharePoint

Frequent sites Following

- SM** Sales and Marketing
- R** Retail
- Cs** Communication Site

Go to SharePoint →

SharePoint

Frequent sites **Following**

- CL** Contoso Landings
- CW** Contoso Web 3
- EC** Executive Corner

Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

ユーザーのメールボックス検索を自動化するスクリプトを作成する予定です。スクリプトは、Allan Deyoung という名前のユーザーのメールボックスで、差し止めという単語を含むメッセージを検索します。

スクリプトに含まれる検索を作成する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

ステップ 1: 実行する検索に関する情報を含む CSV ファイルを作成する このステップで作成するカンマ区切り値 (CSV) ファイルには、検索する各ユーザーの行が含まれています。ユーザーの Exchange Online メールボックス (有効な場合はアーカイブ メールボックスを含む) と OneDrive for Business サイトを検索できます。または、メールボックスまたは OneDrive for Business サイトのみを検索することもできます。SharePoint Online 組織内の任意のサイトを検索することもできます。ステップ 3 で実行するスクリプトは、CSV ファイル内の行ごとに個別の検索を作成します。

1. メモ帳を使用して、次のテキストをコピーして .txt ファイルに貼り付けます。このファイルをローカル コンピューター上のフォルダーに保存します。他のスクリプトもこのフォルダーに保存します。

ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate
 sarad@contoso.onmicrosoft.com、https://contoso-
 my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的
 的)、1/1/2000、12/31/2005 sarad @contoso.onmicrosoft.com、https://contoso-

my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2006/1/1、2010/12/31 sarad@contoso.onmicrosoft.com、https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2011/1/1、2016/3/21

、https://contoso.sharepoint.com/sites/contoso、2016年3月21日

、https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com、2015年1月1日、

、https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com、1/1/2015、ファイルの最初の行、つまりヘッダ行には、New-ComplianceSearch コマンドレットで使用されるパラメーターがリストされています。新しいコンテンツ検索。各パラメータ名はカンマで区切られます。ヘッダ行にスペースが含まれていないことを確認してください。ヘッダ行の下の各行は、各検索のパラメーター値を表します。CSV ファイル内のプレースホルダー データを実際のデータに置き換えてください。

2. Excel で .txt ファイルを開き、次の表の情報を使用して、各検索の情報を含むファイルを編集します。

Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see Keyword queries and search conditions for Content Search .
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

3. Excel ファイルを CSV ファイルとしてローカル コンピューター上のフォルダーに保存します。ステップ 3 で作成したスクリプトは、この CSV ファイル内の情報を使用して検索を作成します。

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-search> コンテンツ検索のキーワード クエリと検索条件

<https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search>

最新問題: 179

contoso.com という名前の Azure Active Directory (Azure AD) テナントを使用する Microsoft 365 サブスクリプションがあります。テナント内のすべてのデバイスは、Microsoft Intune を使用して管理されます。

セッション制御をサポートする App1 という名前のクラウドアプリを購入します。

アプリへのアクセスをリアルタイムで確認できるように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

- From the Azure Active Directory admin center, register App1.
- From the Cloud App Security admin center, create an access policy.
- From the Cloud App Security admin center, create an app discovery policy.
- From the Device Management admin center, create an app configuration policy.
- From the Azure Active Directory admin center, create a conditional access policy.
- From the Device Management admin center, add an App1.

Answer Area

Three empty boxes for the answer.

Answer:

Actions

- From the Azure Active Directory admin center, register App1.
- From the Cloud App Security admin center, create an access policy.
- From the Cloud App Security admin center, create an app discovery policy.
- From the Device Management admin center, create an app configuration policy.
- From the Azure Active Directory admin center, create a conditional access policy.
- From the Device Management admin center, add an App1.

Answer Area

- From the Azure Active Directory admin center, register App1.
- From the Azure Active Directory admin center, create a conditional access policy.
- From the Cloud App Security admin center, create an access policy.

説明

From the Azure Active Directory admin center, register App1.

From the Azure Active Directory admin center, create a conditional access policy.

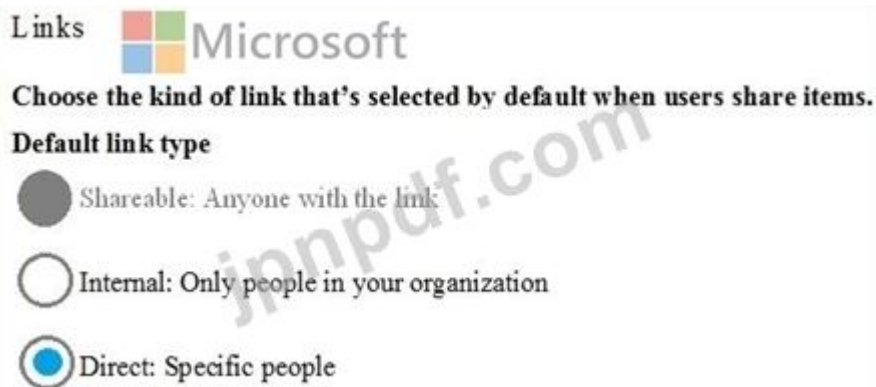
From the Cloud App Security admin center, create an access policy.

参考文献:

<https://docs.microsoft.com/en-us/cloud-app-security/access-policy-aad>


最新問題: 180


デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。次の図に示すように、Microsoft OneDrive で共有設定を構成します。




External sharing

Users can share with:



 **SharePoint**

 **OneDrive**

	Most permissive	
○		Anyone Users can create shareable links that don't require sign-in
		New and existing external users External users must sign-in
		Existing external users Only users already in your organization's directory
○	Least permissive	Only people in your organization No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

Allow or block sharing with people on specific domains

Allow only these domains Contoso.com, Adatum.com [Add domains](#)

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

注: 正しく選択するたびに 1 ポイントの価値があります。

A user who has an email address of user1@fabrikam.com [answer choice]


▼

- cannot access OneDrive content
- can access OneDrive content after a link is created
- must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

▼

- the user cannot access OneDrive content
- the user can access OneDrive content after a link is created
- must be added to a group before the user can access shared files



Answer:

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	



説明

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

参考文献:

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

最新問題: 181

Microsoft 365 サブスクリプションをお持ちです。すべてのユーザーは Microsoft Exchange Online を使用します。

Microsoft 365 は、カスタム ルールなしで既定のポリシー設定を使用するように構成されています。

メッセージの衛生状態を管理します。

不審な電子メールメッセージはデフォルトでどこに配置されますか? 回答するには、適切な場所を正しいメッセージタイプにドラッグします。各場所は1回だけ使用することも、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、ペイン間で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。

The screenshot shows the Microsoft Exchange interface. On the left, under 'Locations', there are three boxes: 'ATP quarantine', 'The Junk Email folder of a user's mailbox', and 'The Chutter folder a user's mailbox'. In the center, there are two categories: 'Messages that contain word-filtered content' and 'Messages that are classified as phishing:'. On the right, under 'Answer Area', there are two empty boxes labeled 'Location'.

Answer:

The screenshot shows the same Microsoft Exchange interface as above, but with the correct answer highlighted. The 'Locations' section has three boxes, all of which are highlighted with a green border. The 'Answer Area' has two boxes, both of which are highlighted with a red border and contain the text 'The Junk Email folder of a user's mailbox'.

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！ GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 182

あなたの会社には、次の表に示すユーザーが含まれる Microsoft 365 サブスクリプションがあります。

Name	Member of
User1	Group1
User2	Group2
User3	Group3

同社は Windows Defender Advanced Threat Protection (Windows Defender ATP) を実装しています。Windows Defender ATP には、次の表に示す役割が含まれています。

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP には、次の表に示すマシン グループが含まれています。

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 183

あなたの会社には、Microsoft 365 サブスクリプション、Microsoft Azure サブスクリプション、および contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。

当社は、次の表に示す営業所を設置しております。

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

テナントには、次の表に示すユーザーが含まれます。

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

次の図に示す Microsoft Cloud App Security ポリシーを作成します。

Create filters for the policy

Act on:

Single activity:
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

In a single app

Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR


equals

From group equals

as

Alerts

Create alert Use your organization's default settings
Daily alert limit 5



次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements

Yes No

In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

Answer:

Statements	Yes	No
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	<input checked="" type="radio"/>	<input type="radio"/>
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	<input checked="" type="radio"/>	<input type="radio"/>
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 184

Microsoft 365 テナントがあります。

顧客の詳細を保存するデータベースがあります。各顧客は、数字と文字の固定パターンで構成される一意の 13 桁の ID を持っています。

次の要件を満たすデータ損失防止 (DLP) ソリューションを実装する必要があります。

* 単一の顧客 ID を含む電子メール メッセージは社外に送信できます。

* 2 つ以上の顧客 ID を含む電子メール メッセージは、会社のデータ プライバシー チームの承認が必要です。

ソリューションに含めるべき 2 つのコンポーネントはどれですか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 1 ポイントの価値があります。

A. 機密情報の種類

B. 機密ラベル

C. 保持ラベル

D. DLP ポリシー

E. メール フロー ルール

Answer: A,D ([メッセージを残す](#))

説明/参照:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-entity-settings?>

view=o365-ワールドワイド

Microsoft 365 のガバナンスとコンプライアンス機能を管理する

テストレット 1

これはケーススタディです。ケーススタディは個別に時間が設定されるわけではありません。各ケースを完了したいだけ試験時間を費やすことができます。ただし、この試験には追加のケーススタディやセクションが存在する場合があります。この試験に含まれるすべての質問を指定された時間内に完了できるように時間を管理する必要があります。

ケーススタディに含まれる質問に答えるには、ケーススタディで提供される情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれる場合があります。このケーススタディでは、各質問は他の質問から独立しています。

このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認し、変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。

ケーススタディを開始するには

このケーススタディの最初の質問を表示するには、「次へ」ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用してケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに [すべての情報] タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたなら、「質問」ボタンをクリックして質問に戻ります。

概要

Contoso, Ltd. は、モントリオールに本社を置き、シアトルとニューヨークに 2 つの支社を構えるコンサルティング会社です。

当社は、次の表に示す営業所を設置しております。

Location	Employees	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

Contoso には、IT、人事 (HR)、法務、マーケティング、財務の部門があります。Contoso は Microsoft を使用しています

365。

既存の環境

インフラストラクチャー

ネットワークには、Microsoft Azure Active Directory (Azure AD) テナントに同期されている contoso.com という名前の Active Directory ドメインが含まれています。パスワードライトバックが有効になっています。

ドメインには、Windows Server 2016 を実行するサーバーが含まれています。ドメインには、Windows 10 Enterprise を実行するラップトップおよびデスクトップコンピューターが含まれています。

各クライアント コンピュータには 1 つのボリュームがあります。

各オフィスは NAT デバイスを使用してインターネットに接続します。オフィスの IP アドレスは次の表に示されています。

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

名前付きロケーションは、次の表に示すように Azure AD で定義されます。

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

[多要素認証] ページから、198.35.3.0/24 のアドレス スペースが信頼できる IP リストに定義されます。

Azure Multi-Factor Authentication (MFA) は、財務部門のユーザーに対して有効になっています。テナントには、次の表に示すユーザーが含まれます。

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

テナントには、次の表に示すグループが含まれています。

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

カスタマー ロックボックスは Microsoft 365 で有効になっています。

Microsoft エンドポイント マネージャーの構成

Microsoft エンドポイント マネージャーに登録されているデバイスは、次の表に示すように構成されています。

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

Microsoft エンドポイント マネージャーのデバイス コンプライアンス ポリシーは、次の表に示すように構成されています。

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

デバイス コンプライアンス ポリシーには、次の表に示す割り当てがあります。

Name	Include	Exclude
DevicePolicy1	GroupC	<i>None</i>
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	<i>None</i>

[コンプライアンス ポリシーが割り当てられていないデバイスをマークする] 設定が [準拠] に設定されます。

要件

技術的要件

Contoso は次の技術要件を特定します。

- * 最小特権の原則を使用する
- * User1 がレポート閲覧者の役割をユーザーに割り当てられるようにします
- * User6 がカスタマー ロックボックスのリクエストをできるだけ早く承認するようにします。
- * User9 が Azure AD Privileged Identity Management を有効にして構成できることを確認します

最新問題: 185

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Azure Active Directory (Azure AD) から、Group1 という名前のセキュリティ グループを作成します。10 人のユーザーを Group1 に追加します。

Group1 のメンバーが非準拠デバイスから Microsoft Exchange Online に接続する場合は、場所に関係なく、アプリによる制限を適用する必要があります。

あなたは何をすべきか？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。
 From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	▼
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	▼
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Answer:

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	▼
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

最新問題: 186

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group2

次の表に示すように、contoso.com にデバイスを登録します。

Name	Platform	Member of	Microsoft Intune managed
Device1	Windows 10	GroupA	Yes
Device2	iOS	GroupB	No

次の表に示すように、Intune でアプリ保護ポリシーを作成します。

Name	Platform	Management state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	With enrollment	Group2
Policy3	iOS	Apps on Intune managed devices	GroupA
Policy4	iOS	Apps on Intune managed devices	GroupB

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	<input type="radio"/>	<input type="radio"/>
When User2 uses Device1, Policy2 applies.	<input type="radio"/>	<input type="radio"/>
When User2 uses Device2, Policy4 applies.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	<input type="radio"/>	<input checked="" type="radio"/>
When User2 uses Device1, Policy2 applies.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 uses Device2, Policy4 applies.	<input type="radio"/>	<input checked="" type="radio"/>

説明

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	<input type="radio"/>	<input checked="" type="radio"/>
When User2 uses Device1, Policy2 applies.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 uses Device2, Policy4 applies.	<input type="radio"/>	<input checked="" type="radio"/>

参考文献:

最新問題: 187

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

ユーザーがドキュメントを機密扱いとしてタグ付けする場合、機密扱いのウォーターマークがドキュメントに適用されるようにする必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

Answer:

1. 管理センターで、コンプライアンス管理センターを選択します。
2. [分類] > [機密ラベル] を選択します。
3. [ラベルの作成] を選択し、警告が表示されたら、[はい] を選択します。
4. ラベル名、ツールチップ、および説明を入力します。次へ」を選択します。
5. 暗号化をオンにします。アクセス許可をいつ割り当てるか、ユーザーのコンテンツへのアクセスを期限切れにするかどうか、オフライン アクセスを許可するかどうかを選択します。
6. [アクセス許可の割り当て] > [これらの電子メール アドレスまたはドメインを追加] を選択します。
7. 電子メール アドレスまたはドメイン名 (Contoso.org など) を入力します。[追加] を選択し、追加する電子メール アドレスまたはドメインごとに繰り返します。
8. [プリセットまたはカスタムから権限を選択] を選択します。
9. ドロップダウン リストを使用して、レビュー担当者や閲覧者などの事前設定された権限を選択するか、カスタム権限を選択します。[カスタム] を選択した場合は、リストから権限を選択します。[保存] > [保存] > [次へ] を選択します。
10. [コンテンツ マーキング] をオンにし、使用するマーキングを選択します。
11. 選択したマーキングごとに、「テキストのカスタマイズ」を選択します。文書上に表示するテキストを入力し、フォントとレイアウトのオプションを設定します。[保存] を選択し、追加のマーキングについて繰り返します。次へ」を選択します。
12. 必要に応じて、エンドポイントのデータ損失防止をオンにします。次へ」を選択します。
13. 必要に応じて、自動ラベル付けをオンにします。条件を追加します。たとえば、[次の内容を含むコンテンツを検出する] で、[条件を追加する] を選択します。条件を入力します。たとえば、パスワード、社会保障、またはその他の機密情報が検出された場合にラベルが追加されるという条件を追加します。次へ」を選択します。

14. 設定を確認し、[作成] を選択します。ラベルが作成されました。追加のラベルが必要な場合は、このプロセスを繰り返します。
15. デフォルトでは、ラベルは機密、内部、公開の順序で Office アプリに表示されます。順序を変更するには、ラベルごとに [その他のアクション] (省略記号) を選択し、ラベルを上下に移動します。通常、権限は、最低レベルから最高レベルの権限の順にリストされます。
16. ラベルにサブラベルを追加するには、「その他のアクション」、サブレベルの追加」の順に選択します。
17. 完了したら、[ラベルの発行] > [発行するラベルの選択] > [追加] を選択します。公開するラベルを選択し、[追加] > [完了] > [次へ] を選択します。
18. デフォルトでは、新しいラベル ポリシーは全員に適用されます。ポリシーを適用するユーザーを制限する場合は、[ユーザーまたはグループの選択] > [追加] を選択します。ポリシーを適用するユーザーを選択し、[追加] > [完了] > [次へ] を選択します。
19. ドキュメントと電子メールにデフォルトのラベルが必要な場合は、ドロップダウン リストから希望のラベルを選択します。残りの設定を確認し、必要に応じて調整し、[次へ] を選択します。
20. ポリシーの名前と説明を入力します。次へ」を選択します。
21. 設定を確認し、[公開] を選択します。

参照：

<https://support.office.com/en-us/article/create-and-manage-sensitivity-labels-2fb96b54-7dd2-4f0c-ac8d-170790d4b8b9>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

最新問題: 188

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー 閲覧者の役割はどのユーザーにも割り当てられていません。

User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないよ

うにする解決策を推奨する必要があります。

解決策: コンプライアンス マネージャーの閲覧者ロールを User5 に割り当てることをお勧めします。

これは目標を達成していますか?

- A. はい
- B. いいえ

Answer: B (メッセージを残す)

最新問題: 189

Microsoft Privacy のプライバシー リスク管理を使用する Microsoft 365 E5 サブスクリプションを持っています。

サブスクリプションで検出された個人データ タイプのインスタンスを確認する必要があります。

Microsoft Purview コンプライアンス ポータルでは何を使用する必要がありますか?

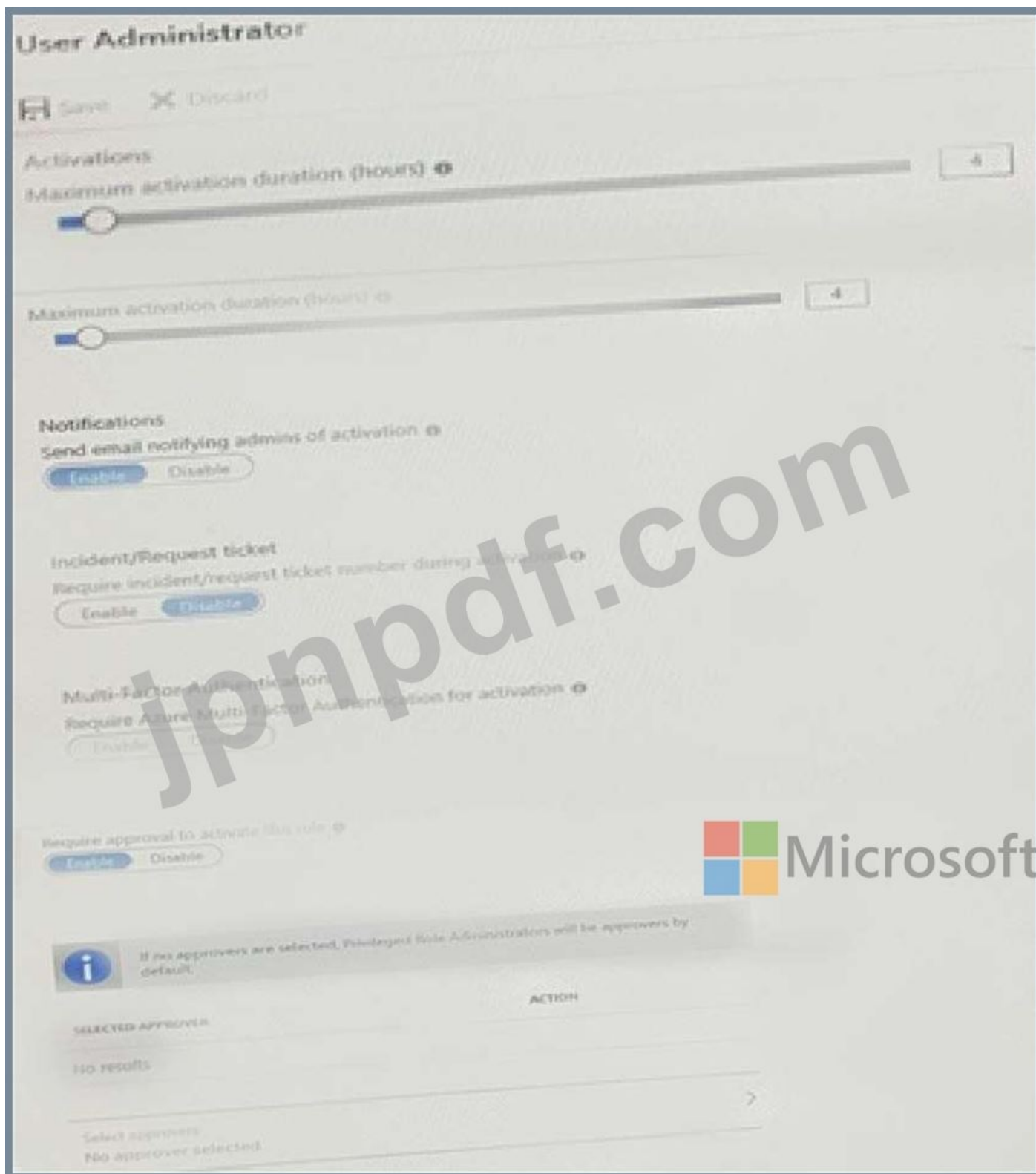
- A. ユーザーデータ消去
- B. コンテンツエクスペローラー
- C. コンテンツ検索
- D. 電子情報開示ケース

Answer: B (メッセージを残す)

最新問題: 190

Contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

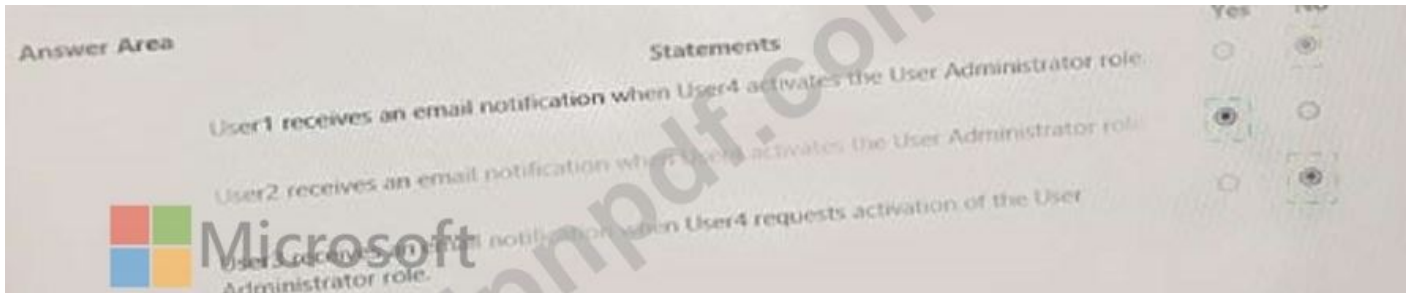
ユーザー管理者ロールは、次の図に示すように、Azure AD Privileged Identity Management (PIM) で構成されます。



User4 にユーザー管理者ロールの資格を与えます。
次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択してください。/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:



最新問題: 191

次の表に示すユーザーを含む Microsoft 365 サブスクリプションを所有しています。

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

User1、User2、および User3 がセルフサービス パスワード リセット (SSPR) を使用できることを確認する必要があります。この解決策はユーザー 4 に影響を与えてはなりません。
 解決策: Group3 に対して SSPR を有効にします。

これは目標を達成していますか?

- A. はい
- B. いいえ

Answer: B (メッセージを残す)

既定では、セルフサービス パスワード リセットはディレクトリ作成者とセキュリティ管理者に対して有効になっていますが、Azure Information Protection 管理者とクラウドアプリケーション管理者に対しては有効ではありません。したがって、User4 が Group3 に属しているため、User3 の SSPR を Group3 ではなく Group2 に適用して、User3 の SSPR を有効にする必要があります。したがって、Group3 で User4 を有効にすると、User4 が影響を受けることになります。

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

最新問題: 192

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

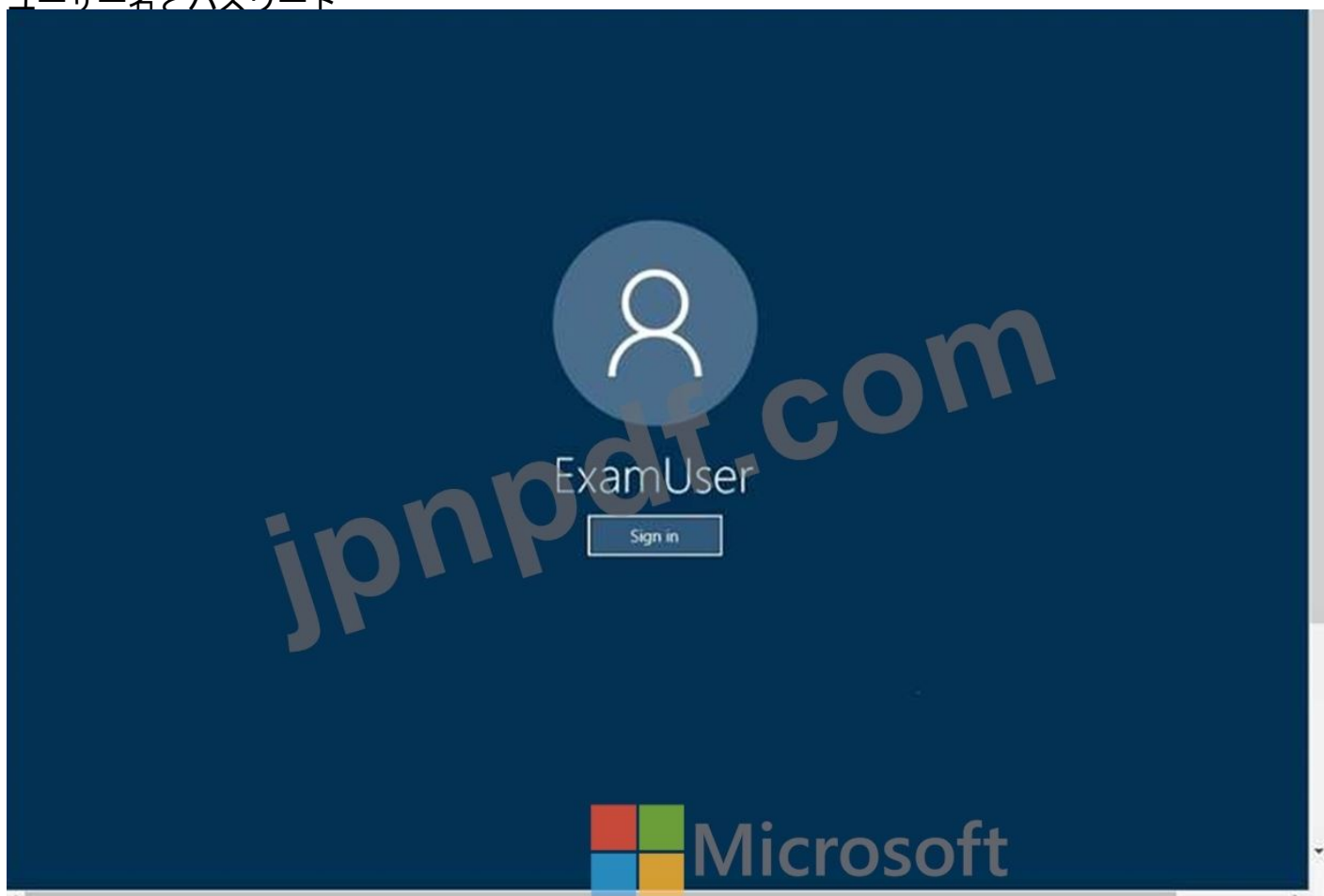
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

ユーザーがドキュメントを機密扱いとしてタグ付けする場合、機密扱いのウォーターマークがドキュメントに適用されるようにする必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

Answer:

1. 管理センターで、コンプライアンス管理センターを選択します。
2. [分類] > [機密ラベル] を選択します。
3. [ラベルの作成] を選択し、警告が表示されたら、[はい] を選択します。
4. ラベル名、ツールチップ、および説明を入力します。次へ」を選択します。
5. 暗号化をオンにします。アクセス許可をいつ割り当てるか、ユーザーのコンテンツへのアクセスを期限切れにするかどうか、オフライン アクセスを許可するかどうかを選択します。
6. [アクセス許可の割り当て] > [これらの電子メール アドレスまたはドメインを追加] を選択します。
7. 電子メール アドレスまたはドメイン名 (Contoso.org など) を入力します。[追加] を選択し、追加する電子メール アドレスまたはドメインごとに繰り返します。
8. [プリセットまたはカスタムから権限を選択] を選択します。
9. ドロップダウン リストを使用して、レビュー担当者や閲覧者などの事前設定された権限を選択するか、カスタム権限を選択します。[カスタム] を選択した場合は、リストから権限を選択します。[保存] > [保存] > [次へ] を選択します。
10. [コンテンツ マーキング] をオンにし、使用するマーキングを選択します。
11. 選択したマーキングごとに、「テキストのカスタマイズ」を選択します。文書上に表示するテキストを入力し、フォントとレイアウトのオプションを設定します。[保存] を選択し、追加のマーキングについて繰り返します。次へ」を選択します。
12. 必要に応じて、エンドポイントのデータ損失防止をオンにします。次へ」を選択します。
13. 必要に応じて、自動ラベル付けをオンにします。条件を追加します。たとえば、「次の内容を含むコンテンツを検出する」で、「条件を追加する」を選択します。条件を入力します。たとえば、パスワード、社会保障、またはその他の機密情報が検出された場合にラベルが追加されるという条件を追加します。次へ」を選択します。
14. 設定を確認し、[作成] を選択します。ラベルが作成されました。追加のラベルが必要な場合は、このプロセスを繰り返します。
15. デフォルトでは、ラベルは機密、内部、公開の順序で Office アプリに表示されます。順序を変

更するには、ラベルごとに [その他のアクション] (省略記号) を選択し、ラベルを上下に移動します。通常、権限は、最低レベルから最高レベルの権限の順にリストされます。

16. ラベルにサブラベルを追加するには、「その他のアクション」、「サブレベルの追加」の順に選択します。

17. 完了したら、[ラベルの発行] > [発行するラベルの選択] > [追加] を選択します。公開するラベルを選択し、[追加] > [完了] > [次へ] を選択します。

18. デフォルトでは、新しいラベル ポリシーは全員に適用されます。ポリシーを適用するユーザーを制限する場合は、[ユーザーまたはグループの選択] > [追加] を選択します。ポリシーを適用するユーザーを選択し、[追加] > [完了] > [次へ] を選択します。

19. ドキュメントと電子メールにデフォルトのラベルが必要な場合は、ドロップダウン リストから希望のラベルを選択します。残りの設定を確認し、必要に応じて調整し、[次へ] を選択します。

20. ポリシーの名前と説明を入力します。次へ」を選択します。

21. 設定を確認し、[公開] を選択します。

参照：

<https://support.office.com/en-us/article/create-and-manage-sensitivity-labels-2fb96b54-7dd2-4f0c-ac8d-170790d4b8b9>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

最新問題: 193

contoso.com という名前の Azure Active Directory (Azure AD) テナントを使用する Microsoft 365 サブスクリプションがあります。OneDrive には、外部ユーザーと共有されるファイルが保存されます。ファイルは次の表に示すように構成されています。

Name	Applic label soft
File1	Label1 om
File2 ipri	Label1, Label2
File3	Label2

OneDrive アカウントに保存されているコンテンツに適用されるデータ損失防止 (DLP) ポリシーを作成します。ポリシーには次の 3 つのルールが含まれています。

* ルール:

* 条件: ラベル 1、組織外のユーザーと共有されているコンテンツを検出する

* アクション: 外部ユーザーのコンテンツへのアクセスを制限します。

* ユーザー通知: コンテンツを最後に変更したユーザーに通知します。

* ユーザーオーバーライド: オン

※優先度 :0

* ルール 2:

※条件 :ラベル1またはラベル2

* アクション: コンテンツへのアクセスを制限する

※優先度 :1

* ルール 3:

* 条件: ラベル 2、組織外のユーザーと共有されているコンテンツを検出する

* アクション: 外部ユーザーのコンテンツへのアクセスを制限します。

* ユーザー通知: コンテンツを最後に変更したユーザーに通知します。

* ユーザーオーバーライド: オン

※ 優先度 2

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。注: 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

Statements	Yes	No
External users can access File1.	<input type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input type="radio"/>
External users can access File3.	<input type="radio"/>	<input type="radio"/>



Answer:

Answer Area

Statements	Yes	No
External users can access File1.	<input checked="" type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input checked="" type="radio"/>
External users can access File3.	<input type="radio"/>	<input checked="" type="radio"/>



説明

Statements

Yes

No

External users can access File1

The users in contoso.com can access File2

External users can access File3 Microsoft

最新問題: 194

Microsoft 365 サブスクリプションをお持ちです。すべてのユーザーは Microsoft Exchange Online を使用します。

Microsoft 365 は、カスタム ルールなしで既定のポリシー設定を使用するように構成されています。

メッセージの衛生状態を管理します。

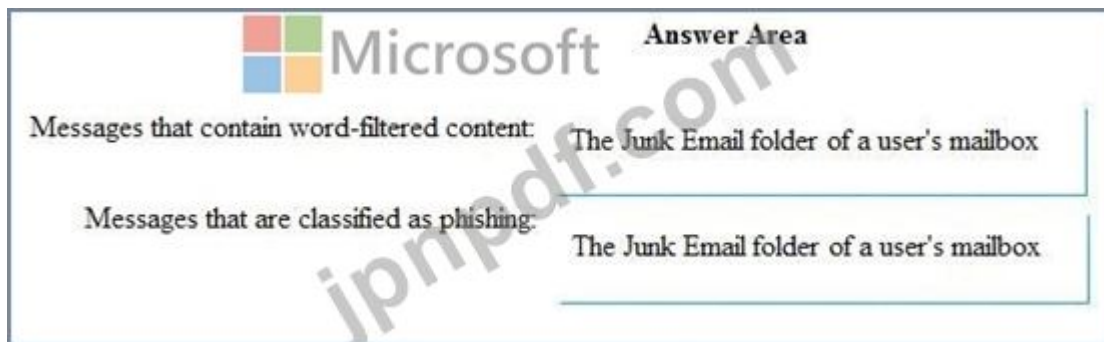
不審な電子メール メッセージはデフォルトでどこに配置されますか? 回答するには、適切な場所を正しいメッセージ タイプにドラッグします。各場所は 1 回だけ使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

The screenshot shows the Microsoft 365 message hygiene interface. On the left, under 'Locations', there are three boxes: 'ATP quarantine', 'The Junk Email folder of a user's mailbox', and 'The Chutter folder a user's mailbox'. In the center, there are two categories of messages: 'Messages that contain word-filtered content' and 'Messages that are classified as phishing'. On the right, under 'Answer Area', there are two empty boxes labeled 'Location'. A Microsoft logo is visible at the bottom center.

Answer:

The screenshot shows the same Microsoft 365 message hygiene interface as above, but with the answer applied. The 'Locations' boxes are now dashed. In the 'Answer Area', the two 'Location' boxes now contain 'The Junk Email folder of a user's mailbox' for both 'Messages that contain word-filtered content' and 'Messages that are classified as phishing'. A Microsoft logo is visible at the bottom center.

説明



最新問題: 195

すべてのフィッシングメールメッセージを自動的に隔離するように組織を構成する必要があります。

このタスクを完了するには、Microsoft 365 ポータルにサインインします。

Answer:

以下の説明を参照してください。

説明

フィッシング対策ポリシーを編集する必要があります。

* Office 365 セキュリティとコンプライアンス管理センターに移動します。

* 脅威管理に移動します

* [デフォルト ポリシー] をクリックします。

* [偽装] セクションで、をクリックします。

* [アクション] セクションに進みます。

* [偽装ユーザーから電子メールが送信された場合:] ボックスで、ドロップダウン リストから [メッセージを隔離する] を選択します。

* [偽装ドメインから電子メールが送信された場合:] ボックスで、ドロップダウン リストから [メッセージを隔離する] を選択します。

* [保存] をクリックして変更を保存します。

* [閉じる] をクリックして、フィッシング対策ポリシー ウィンドウを閉じます。

最新問題: 196

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザーとデバイス オブジェクトは毎日追加および削除されます。営業部門のユーザーは頻繁にデバイスを変更します。

次の 3 つのグループを作成する必要があります。

Group	Requirement
1	All the devices of users where the Department attributes is set to Sales
2	All the devices where the Department attribute is set to Sales
3	All the devices where the deviceOwnership attribute is set to Company

ソリューションでは、管理労力を最小限に抑える必要があります。

メンバーシップの種類ごとに作成するグループ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。

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

Answer:

Groups that have assigned membership:

Microsoft

▼
0
1
2
3

Groups that have dynamic membership:

▼
0
1
2
3

説明

Groups that have assigned membership:

Microsoft

▼
0
1
2
3

Groups that have dynamic membership:

▼
0
1
2
3

参考文献:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dyn>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
 GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe244001@onmicrosoft.com

Microsoft 365 パスワード: &=Q8v@2qGzYz

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11032396

グループ所有者が Office 365 グループを 180 日ごとに更新するようにする必要があります。

このタスクを完了するには、Microsoft Office 365 管理センターにサインインします。

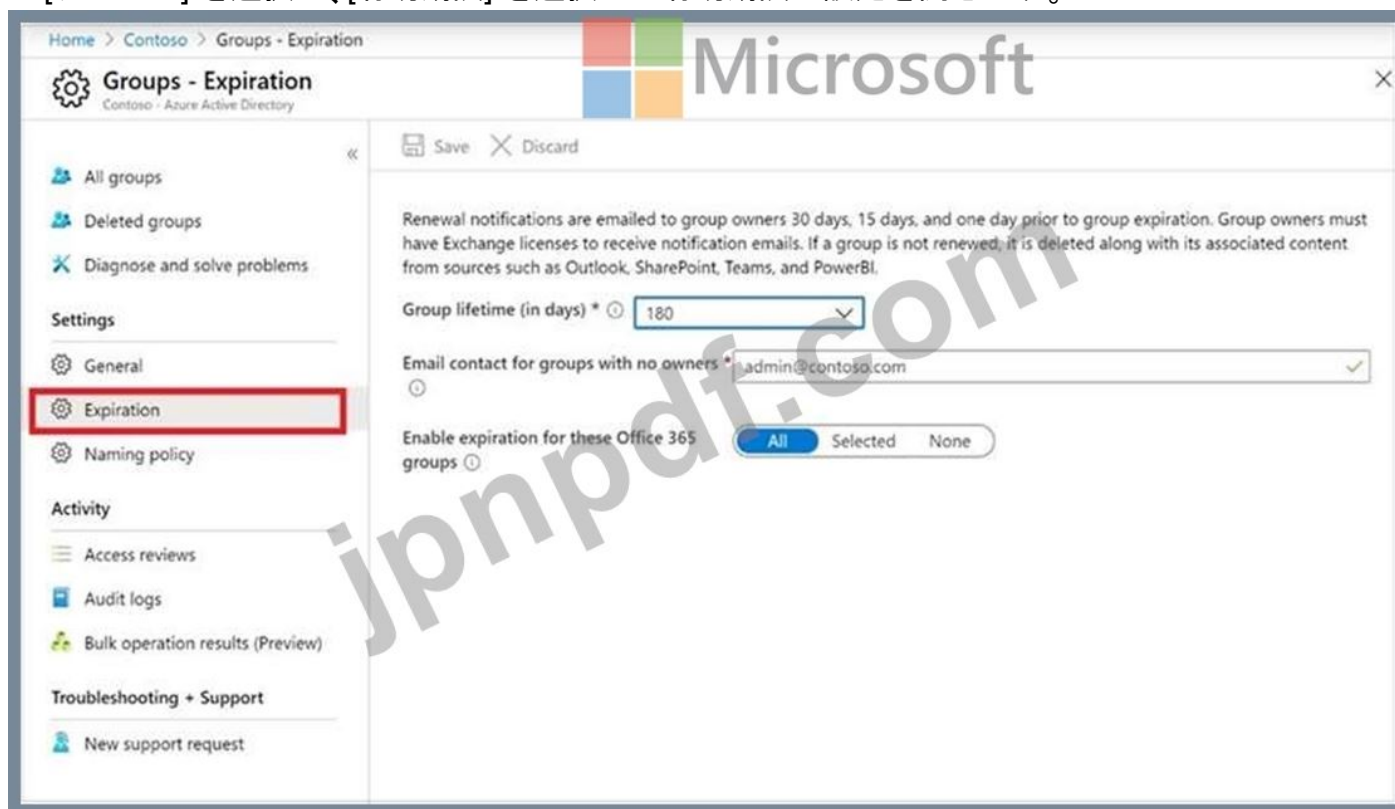
Answer:

以下の説明を参照してください。

説明

グループの有効期限を設定する

1. Azure AD 組織のグローバル管理者であるアカウントを使用して、Azure AD 管理センターを開きます。
2. [グループ] を選択し、[有効期限] を選択して有効期限の設定を開きます。



3. [有効期限] ページでは、次のことができます。

- * グループの有効期間を日数で設定します。プリセット値の 1 つを選択することも、カスタム値を選択することもできます (31 日以上)。
- * グループに所有者がない場合に更新および有効期限の通知を送信する電子メール アドレスを指定します。
- * 有効期限が切れる Office 365 グループを選択します。以下の有効期限を設定できます。
- * すべての Office 365 グループ

- * 選択された Office 365 グループのリスト
 - * すべてのグループの有効期限を制限する場合はなし
- 完了したら、[保存] を選択して設定を保存します。
参照：

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-lifecycle>

最新問題: 198

20 のデータ損失防止 (DLP) ポリシーを含む Microsoft 365 サブスクリプションがあります。
次のことを特定する必要があります。

- * ポリシー アラートをトリガーせずに適用されるルール
- * DLP ポリシーに一致した上位 10 個のファイル
- * 誤って分類されたアラート

各要件に対してどのレポートを使用する必要がありますか？ 回答するには、適切なレポートを正しい要件にドラッグします。各レポートは 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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



説明



最新問題: 199

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

contoso.com という名前の Microsoft Azure Active Directory (Azure AD) テナントに関連付けられた Microsoft 365 E5 サブスクリプションがあります。

Active Directory フェデレーション サービス (AD FS) を使用して、オンプレミスの Active Directory とテナントをフェデレーションします。

Azure AD Connect には次の設定があります。

- * ソースアンカー: objectGUID
- * パスワードハッシュ同期: 無効
- * パスワードライトバック: 無効
- * ディレクトリ拡張属性の同期: 無効
- * Azure AD アプリと属性フィルタリング: 無効
- * Exchange ハイブリッド展開: 無効
- * ユーザー書き戻し: 無効

Azure AD Identity Protection で漏洩した資格情報の検出を使用できることを確認する必要があります。

解決策: パスワードハッシュ同期設定を変更します。

それは目標を達成していますか？

A. はい

B. いいえ

Answer: A ([メッセージを残す](#))

説明/参照:

参考文献:

<https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps>

最新問題: 200

Group1 および Group2 という名前の 2 つのグループと、次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Role	Member of
Admin1	Global Administrator	None
User1	Global reader	Group1
User2	Global reader	Group2

次の図に示すように、特権アクセス設定が構成されています。

Privileged Access

Privileged access provides a way for people in your organization to perform tasks that would otherwise require a higher level of permission or an admin role. When someone submits a request to access a privileged task, the default approval group you choose can approve or deny it.

After you choose the approval group, create policies to define the types of privileged tasks people can request access to.

Create policies and manage requests

Learn more about privileged access

Allow privileged access requests and choose a default approval group

次の設定を持つ特権アクセス ポリシーがあります。

* ポリシー名: 新しいトランスポート ルール

* ポリシーの種類: タスク

* ポリシーの範囲: 交換

※承認タイプ: マニュアル

※承認者グループ: グループ1

User1 は、新しいトランスポート ルール ポリシーへの 2 時間のアクセスを要求します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 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

Statements	Yes	No
Admin1 can approve the request.	<input type="radio"/>	<input type="radio"/>
User1 can approve the request.	<input type="radio"/>	<input type="radio"/>
User2 can approve the request.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can approve the request.	<input type="checkbox"/>	<input type="checkbox"/>
User1 can approve the request.	<input type="checkbox"/>	<input type="checkbox"/>
User2 can approve the request.	<input type="checkbox"/>	<input type="checkbox"/>

説明

Answer Area



Statements	Yes	No
Admin1 can approve the request.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User1 can approve the request.	<input type="checkbox"/>	<input type="checkbox"/>
User2 can approve the request.	<input type="checkbox"/>	<input type="checkbox"/>

最新問題: 201

Microsoft 365 サブスクリプションでいくつかの Advanced Threat Protection (ATP) ポリシーを構成します。

User1 という名前のユーザーが脅威管理ダッシュボードで ATP レポートを表示できるようにする必要があります。

User1 に必要なロール権限を提供するのはどのロールですか？

- A. セキュリティリーダー
- B. メッセージセンター リーダー
- C. コンプライアンス管理者
- D. 情報保護管理者

Answer: A ([メッセージを残す](#))

説明/参照:

参照:

<https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are->

atpレポートの表示に必要な

最新問題: 202

Site1 という名前の Microsoft SharePoint Online サイトがあります。次の表に示すユーザーがいます。

Name	Role
User1	Owner
User2	Member

次の表に示す保持ラベルを作成します。

Name	Retention period	Retention action	Based on
Retention1	4 years	Retain only	When a file was labeled
Retention2	2 years	Retain and delete	When a file was labeled

Answer Area

Statements	Yes	No
User1 can delete File1 on March 10, 2021.	<input type="radio"/>	<input type="radio"/>
User2 can delete File1 on March 10, 2025.	<input type="radio"/>	<input type="radio"/>
User2 can edit File2 on March 15, 2023.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can delete File1 on March 10, 2021.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete File1 on March 10, 2025.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can edit File2 on March 15, 2023.	<input checked="" type="radio"/>	<input type="radio"/>

説明

Answer Area

Statements	Yes	No
User1 can delete File1 on March 10, 2021.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete File1 on March 10, 2025.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can edit File2 on March 15, 2023.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 203

Microsoft 365 サブスクリプションでいくつかの Advanced Threat Protection (ATP) ポリシーを構成します。

User1 という名前のユーザーが脅威管理ダッシュボードで ATP レポートを表示できるようにする必要があります。

User1 に必要なロール権限を提供するのはどのロールですか？

- A. セキュリティリーダー
- B. レポートリーダー
- C. 情報保護管理者
- D. Exchange 管理者

Answer: A (メッセージを残す)

説明/参照:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-atp?view=o365-worldly#what-permissions-are-needed-to-> ATP レポートの表示

最新問題: 204

デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。
次の図に示すように、Microsoft OneDrive で共有設定を構成します。

The image shows two screenshots of Microsoft 365 sharing settings. The top screenshot is titled "Links" and asks to choose the default link type. The bottom screenshot is titled "External sharing" and shows settings for SharePoint and OneDrive, including a permission scale and advanced settings for external sharing.

Links

Choose the kind of link that's selected by default when users share items.

Default link type

- Shareable: Anyone with the link
- Internal: Only people in your organization
- Direct: Specific people

External sharing

Users can share with:

SharePoint	OneDrive	Permission Level	Description
<input type="checkbox"/>	<input type="checkbox"/>	Most permissive	Anyone Users can create shareable links that don't require sign-in
<input type="checkbox"/>	<input type="checkbox"/>		New and existing external users External users must sign-in
<input type="checkbox"/>	<input type="checkbox"/>		Existing external users Only users already in your organization's directory
<input type="checkbox"/>	<input type="checkbox"/>	Least permissive	Only people in your organization No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing


- Allow or block sharing with people on specific domains

Allow only these domains: Contoso.com, Adatum.com

Add domains

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

注:正しく選択するたびに 1 ポイントの価値があります。

	A user who has an email address of user1@fabrikam.com [answer choice]	<input type="text"/> <input type="text"/> cannot access OneDrive content <input type="text"/> can access OneDrive content after a link is created <input type="text"/> must be added to be a group before the user can access shared files
	If a new guest user is created for user2@contoso.com [answer choice]	<input type="text"/> <input type="text"/> the user cannot access OneDrive content <input type="text"/> the user can access OneDrive content after a link is created <input type="text"/> must be added to a group before the user can access shared files

Answer:

A user who has an email address of user1@fabrikam.com [answer choice]	<input type="text"/> <input type="text"/> cannot access OneDrive content ! <input type="text"/> can access OneDrive content after a link is created <input type="text"/> must be added to be a group before the user can access shared files
If a new guest user is created for user2@contoso.com [answer choice]	<input type="text"/> <input type="text"/> the user cannot access OneDrive content <input type="text"/> the user can access OneDrive content after a link is created <input type="text"/> must be added to a group before the user can access shared files

説明

A user who has an email address of user1@fabrikam.com [answer choice]

Microsoft

cannot access OneDrive content
can access OneDrive content after a link is created
must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

the user cannot access OneDrive content
the user can access OneDrive content after a link is created
must be added to a group before the user can access shared files

参考文献:

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

最新問題: 205

ユーザーは次のファイルを Microsoft OneDrive に保存します。

- * ファイル.docx
- * 重要ファイル.docx
- * ファイル_重要.docx

次の例に示すフィルターを持つ Microsoft Cloud App Security ファイル ポリシー Policy1 を作成します。

Create a filter for the files this policy will act on

Microsoft

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

File name contains words File

Apply to: all files

Apply to: all file owners

Policy1 はどのファイルに適用されますか?

- A. ファイル_重要.docx のみ
- B. ファイル.docx、重要ファイル.docx、およびファイル_重要.docx
- C. ファイル.docx のみ
- D. 重要ファイル.docx のみ
- E. File.docx および File_Minimum.docx のみ

Answer: B ([メッセージを残す](#))

参照 :

<https://docs.microsoft.com/en-us/cloud-app-security/file-filters>

最新問題: 206

contoso.com という名前の Microsoft Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

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

次の設定を持つ Azure AD Identity Protection サインイン リスク ポリシーを作成して適用します。

* 割り当て: グループ 1 を含む、グループ 2 を除く


※条件 :サインインリスクが低以上

* アクセス: アクセスを許可、パスワード多要素認証が必要


ポリシーが User1 と User2 にどのような影響を与えるかを特定する必要があります。

各ユーザーが匿名 IP アドレスからサインインするとどうなりますか? 回答するには、回答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。

User1:		▼
Blocked		
Can sign in without MFA		
Prompted for MFA		
User2:		▼
		
Blocked		
Can sign in without MFA		
Prompted for MFA		

Answer:

User1:		▼
Blocked		
Can sign in without MFA		
Prompted for MFA		
	User2:	▼
Blocked		
Can sign in without MFA		
Prompted for MFA		

説明

User1: ▼

Blocked
Can sign in without MFA
Prompted for MFA

User2: ▼

Blocked
Can sign in without MFA
Prompted for MFA



最新問題: 207

Group3を作成する必要があります。

グループを作成するには2つの方法がありますか？

- A. Microsoft 365 管理センターの Office 365 グループ
- B. Microsoft 365 管理センターのメールが有効なセキュリティ グループ
- C. Microsoft 365 管理センターのセキュリティ グループ
- D. Microsoft 365 管理センターの配布リスト
- E. Azure AD 管理センターのセキュリティ グループ

Answer: A,D (メッセージを残す)

トピック 2、Fabrikam inc. 概要

既存の環境

ネットワークインフラストラクチャ

ネットワークには、fabrikam.com という名前の Active Directory フォレストが含まれています。Fabrikam には、ハイブリッド Microsoft Azure Active Directory (Azure AD) 環境があります。同社は特定のアプリケーション用にいくつかのオンプレミス サーバーを維持していますが、ほとんどのエンドユーザー アプリケーションは Microsoft 365 E5 サブスクリプションによって提供されています。

問題の声明

Fabrikam は次の問題を特定しています。

先週の金曜日以来、IT チームは件名に「異常な ID 同期通知」を含む自動電子メール メッセージを受信しています。

最近、数人のユーザーがマルウェアを含む電子メールの添付ファイルを開いてしまいました。マルウェアを削除するプロセスには時間がかかりました。

要件

計画された変更

Fabrikam は次の変更を実装する予定です。

Fabrikam は、Active Directory への不審なサインインを監視および調査する予定です Fabrikam は、Microsoft 365 アプリケーション管理に保存されているデータの一部へのアクセスをパートナーに提供する予定です Fabrikam は、ワークロード アプリケーションを管理するための次のアプリケーション要件を特定します。

ユーザー管理者はさまざまな国から勤務します

ユーザー管理者は Azure Active Directory 管理センターを使用します。

Admin1 と Admin2 という 2 人の新しい管理者は、Microsoft Exchange Online のみの管理を担当します。セキュリティ要件 Fabrikam は、次のセキュリティ要件を特定します。

ユーザー管理者による Azure Active Directory 管理センターへのアクセスは、7 日ごとに確認する必要があります。管理者が 3 日以内にアクセス要求に応答しなかった場合は、アクセスを削除する必要があります。Microsoft 365 ワークロードを管理するユーザーは、一度に最大 3 時間の管理タスクのみを実行できます。グローバル管理者は、この要件を免除する必要があります。ユーザーは、会社データを表示するために外部ユーザーを招待できないようにする必要があります。グローバル管理者と User1 という名前のユーザーのみが招待を送信する必要があります。Azure Advanced Threat Protection (ATP) は機密グループのセキュリティ グループの変更をキャプチャする必要があります。

最新問題: 208

contoso.com という名前の Azure Active Directory (Azure AD) テナントを含む Microsoft 365 E5 サブスクリプションがあります。

contoso.com の Azure AD Identity Protection アラートは、次のように構成されています。

Save Discard Download

Alert on user risk level at or above

Low Medium High

Emails are sent to the following users. ⓘ

INCLUDED

1 selected

Add additional emails to receive alert notifications (Preview). ⓘ

User1 という名前のユーザーは、Azure AD Identity Protection からアラートを受信するように構成されています。

次の表に示すように、contoso.com にユーザーを作成します。

Name	Role
User2	Security reader
User3	User administrator
User4	None
User5	None

ユーザーは、次の表に示すサインインを実行します。

Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>

説明

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input checked="" type="radio"/>

ボックス 1: いいえ

User1 は、中以上に分類される 2 つのアラートを受信します。

感染したデバイスからのサインインは低として分類されます。このリスク検出では、ユーザーのデバイスではなく、IP アドレスが識別されます。

複数のデバイスが 1 つの IP アドレスの背後にあり、その一部のみがボット ネットワークによって制御されている場合、他のデバイスからのサインインによってこのイベントが不必要にトリガーされる可能性があるため、このリスク検出は「低」に分類されます。

ボックス 2: いいえ

User2 は、中以上に分類される 2 つのアラートを受信します。

電子メール アラートは、すべてのグローバル管理者、セキュリティ管理者、およびセキュリティ閲覧者に送信されます。感染したデバイスからのサインインは低として分類されます。このリスク検出では、ユーザーのデバイスではなく、IP アドレスが識別されます。

複数のデバイスが 1 つの IP アドレスの背後にあり、その一部のみがボット ネットワークによっ

て制御されている場合、他のデバイスからのサインインによってこのイベントが不必要にトリガーされる可能性があるため、このリスク検出は「低」に分類されます。

ボックス 3: いいえ

User3 は変更を受け取りません。

電子メール アラートは、すべてのグローバル管理者、セキュリティ管理者、およびセキュリティ閲覧者に送信されます。

参照：

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

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-r>

最新問題: 209

あなたの会社は、Microsoft 365 E5 サブスクリプションと contoso.com という名前のハイブリッド Azure Active Directory を持っています。

Contoso.com には次のユーザーが含まれます。

次の図に示すように、Contoso.com のパスワード保護を構成します。

Custom smart lockout

Lockout threshold

Lockout duration in seconds

Custom banned passwords

Enforce custom list Yes No

Custom banned password list Contoso

Microsoft

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input type="radio"/>
User2 can change his password to CONTOSO\$0CONT0\$0.	<input type="radio"/>	<input type="radio"/>
User3 can change his password to myCONTOSO0mp1exPWD.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change his password to CONTOSO\$0CONT0\$0.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can change his password to myCONTOSO0mp1exPWD.	<input checked="" type="radio"/>	<input type="radio"/>

説明

Answer Area

Microsoft

Statements

User1 must change his password next time he authenticates to Azure Active Directory. Yes No

User2 can change his password to CONTOSOCONTOSO. Yes No

User3 can change his password to myCONTOSOcomp1exPWD. Yes No

最新問題: 210

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

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

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

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

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

Policy1 を適用する必要があります。

どのグループに Policy1 を適用できますか? 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: 正しく選択するたびに 1 ポイントの価値があります。

On-premises Active Directory groups:

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

Azure AD groups:



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

Answer:

On-premises Active Directory groups:

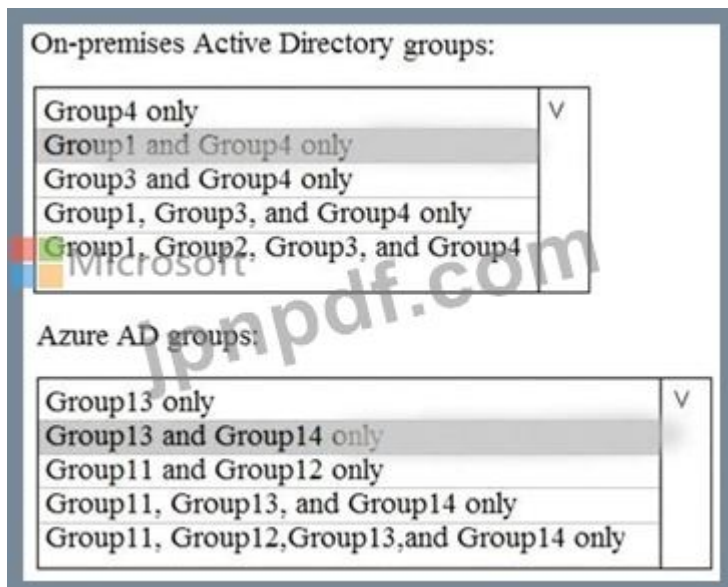
Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:



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

説明



参照 :

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

最新問題: 211

ネットワークにはオンプレミスの Active Directory ドメインが含まれています。ドメインには、Windows Server を実行し、高度な監査が有効になっているサーバーが含まれています。サーバーのセキュリティ ログは、サードパーティの SIEM ソリューションを使用して収集されません。

Microsoft 365 サブスクリプションを購入し、スタンドアロン センサーを使用して Azure Advanced Threat Protection (ATP) を展開することを計画しています。

機密性の高いグループが変更されたときと、悪意のあるサービスが作成されたときを確実に検出できるようにする必要があります。

あなたは何をするべきか？

- A. Azure ATP センサーの遅延更新をオフにします。
- B. Office 365 セキュリティ & コンプライアンス センターで監査を構成します。
- C. Azure ATP センサーの遅延更新をオンにします。
- D. SIEM と Azure ATP を統合します。

Answer: D (メッセージを残す)

ノート :

試験ではこの問題にはいくつかのバージョンがあります。試験の問題には 2 つの異なる正解があります。

1. SIEM と Azure ATP を統合します。
2. ドメイン コントローラーでイベント転送を構成する

試験で表示される可能性のあるその他の不正解の選択肢には次のものがあります。

1. Azure ATP 通知を構成する
2. Azure ATP センサーのドメイン シンクロナイザー候補設定を変更します。
3. サーバーの「アカウント管理の監査」グループ ポリシー設定を有効にします。

参照 :

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%**w 特別割引コード: **Freepdfdumps**)

最新問題: 212

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Groups administrator
Admin2	User administrator

contoso.com のグループ名前付けポリシーに禁止単語として「internal」を追加します。

contoso.com のグループ名前付けポリシーのプレフィックスとして Contoso- を追加します。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can create a security group named Contoso-internal.	<input checked="" type="radio"/>	<input type="radio"/>

参照 :

<https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide>

最新問題: 213

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

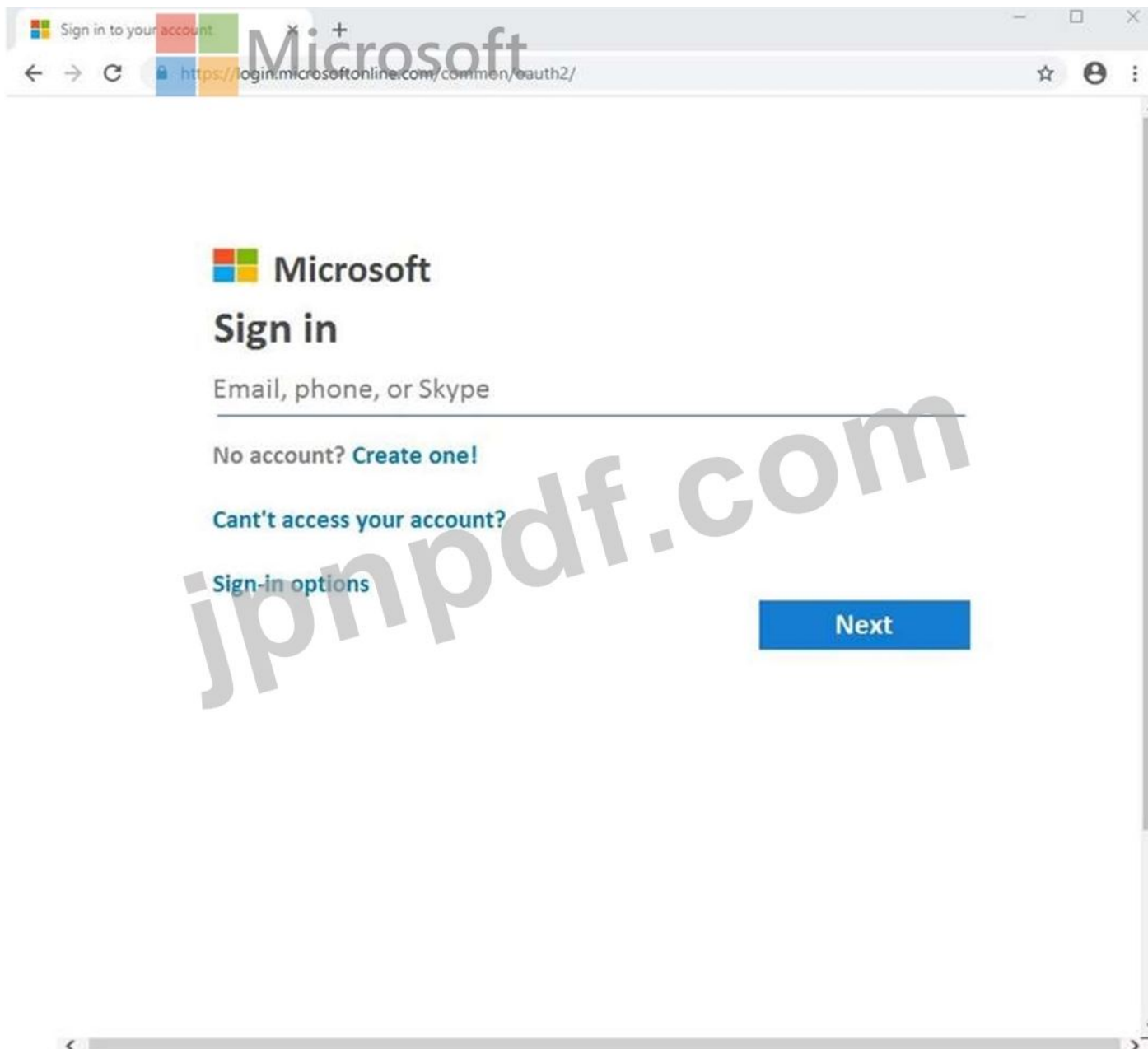
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で 「次へ」 ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308

Microsoft



Get your work done
with **Office 365**

jpnpdf.com



Microsoft



Microsoft



jpnpdf.com

Brainstorm
together in **Word**



Microsoft



Stay on top of what matters with Outlook



Microsoft

Microsoft



Microsoft



Access Office 365 apps and documents in one place with

Office.com



jpnpdf.com

Microsoft Office Home | Contoso electronics | Office 365

Good morning Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint

OneNote | Skype | Calendar | People | All apps

Recommended

You edited this Jan 15

Excel

Integrated Train Sales Process

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Excel

Sales Process

lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Microsoft

recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15



AD Slogans

lodse000198.sharepoint.co...

Ad Slogans



Recent | Pinned | Shared with me | Discover

Recent

Pinned

Shared with me

Discover



Microsoft



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

↑ Upload and open...

New ▾

Go to OneDrive →

Recent

Pinned

Shared with me

Discover



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →



Microsoft

SharePoint

Frequent sites

Following



Sales and Marketing



Retail



Communication Site

SharePoint

Frequent sites

Following



Contoso Landings



Contoso Web 3



Executive Corner

Go to SharePoint →

Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

フィッシング攻撃から保護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。

フィッシングメールメッセージがなりすましドメインから送信された場合、メッセージを隔離する必要があります。

できるだけ多くのフィッシング電子メールメッセージを識別する必要があります。

この解決策は、現在の SMTP ドメイン名と後で追加されるドメイン名に適用する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

1. Microsoft 365 管理センターにサインインした後、[セキュリティ]、[脅威管理]、[ポリシー]、[ATP フィッシング対策] の順に選択します。
2. [デフォルト ポリシー] を選択して調整します。
3. [偽装] セクションで、[編集] を選択します。
4. [保護するドメインの追加] に移動し、所有するドメインを自動的に含めるトグルを選択します。
5. [アクション] に移動し、[電子メールが偽装ユーザーによって送信された場合] ドロップダウンを開き、[メッセージを隔離] アクションを選択します。
[電子メールが偽装ドメインから送信された場合] ドロップダウンを開き、[メッセージを隔離] アクションを選択します。
6. [偽装に関する安全性のヒントをオンにする] を選択します。システムが偽装ユーザー、ドメイン、または異常な文字を検出したときに、ユーザーにヒントを提供するかどうかを選択します。
[保存] を選択します。
7. [メールボックス インテリジェンス] を選択し、オンになっていることを確認します。これによ

り、使用パターンを学習してメールをより効率的に作成できます。

8. [信頼できる送信者とドメインを追加する] を選択します。ここでは、なりすましとして分類すべきでない電子メールアドレスまたはドメインを追加できます。

9. [設定の確認] を選択し、すべてが正しいことを確認して、[保存]、[閉じる] の順に選択します。

参照：

https://support.office.com/en-us/article/protect-against-phishing-attempts-in-microsoft-365-86c425e1-1686-430a-9151-f7176cce4f2c#ID0EAABAAA=Try_it!


<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#example-anti-phishing-policy-ユーザーとドメインを保護する>

最新問題: 214

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザーとデバイス オブジェクトは毎日追加および削除されます。営業部門のユーザーは頻繁にデバイスを変更します。

次の 3 つのグループを作成する必要があります。

 Group	Requirement
1	All the devices of users where the Department attributes is set to Sales
2	All the devices where the Department attribute is set to Sales
3	All the devices where the deviceOwnership attribute is set to Company

ソリューションでは、管理労力を最小限に抑える必要があります。

メンバーシップの種類ごとに作成するグループ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。



Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

Answer:



Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

説明

Groups that have assigned membership:

Microsoft

Groups that have dynamic membership:

参考文献:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dyn>

最新問題: 215

出品物を参照してください。

Name	In device group
Device1	Group1
Device2	Group2
Device3	Group3

Microsoft Defender for Endpoint には、次の表に示すインシデントが含まれています。

Name	Device	File evidence	File verdict
Case1	Device1	C:\Temp\File1.exe	Suspicious
Case2	Device2	C:\Temp\File2.exe	Malicious
Case3	Device3	C:\Temp\File3.exe	Malicious

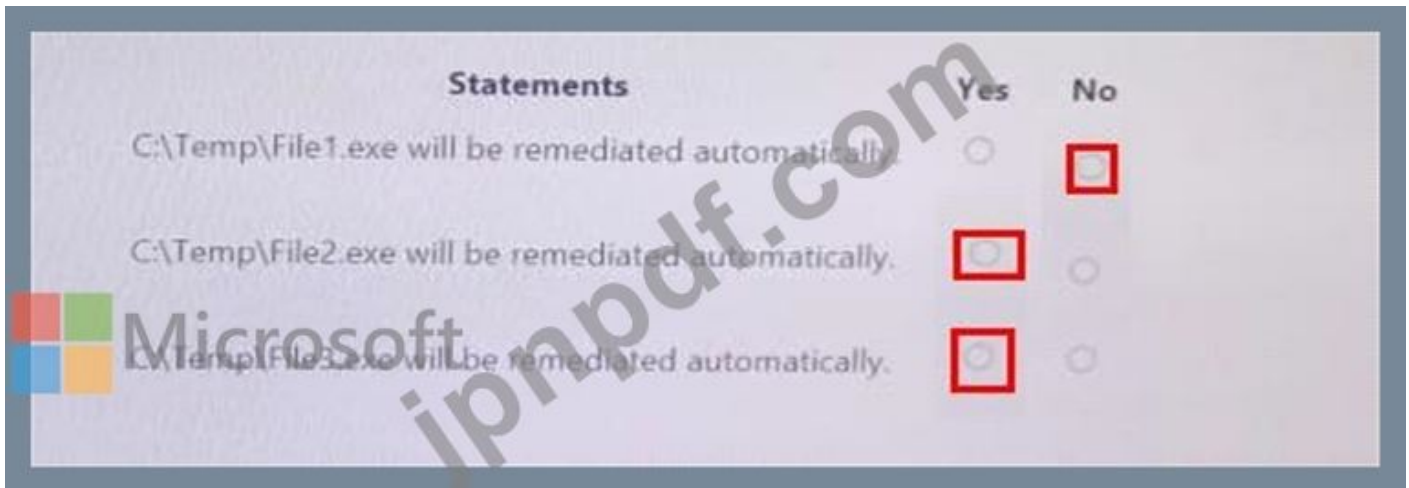
次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。さもないと、[いいえ] を選択します。

Statements

	Yes	No
C:\Temp\File1.exe will be remediated automatically.	<input type="radio"/>	<input type="radio"/>
C:\Temp\File2.exe will be remediated automatically.	<input type="radio"/>	<input type="radio"/>
C:\Temp\File3.exe will be remediated automatically.	<input type="radio"/>	<input type="radio"/>

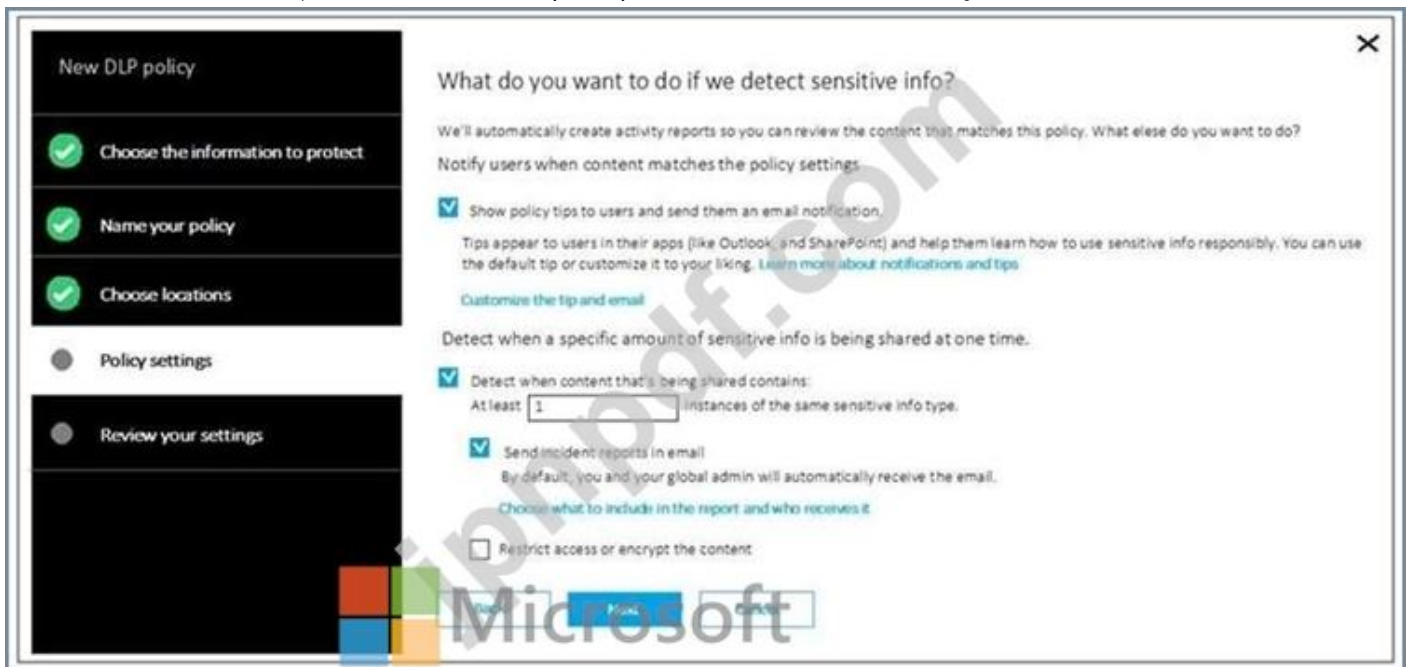
Microsoft

Answer:



最新問題: 216

次の図に示すように、データ損失防止 (DLP) ポリシーを作成します。



ユーザーが機密情報を含む電子メール メッセージを送信しようとした場合、ポリシーはどのような影響を及ぼしますか？

- A. ユーザーは通知を受け取り、電子メール メッセージを送信できます。
- B. ユーザーは通知を受け取りますが、電子メール メッセージを送信できません
- C. 通知なしでメールが送信されます。
- D. 電子メール メッセージはサイレントにブロックされます。

Answer: A (メッセージを残す)

説明/参照:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

最新問題: 217

Microsoft 365 サブスクリプションをお持ちです。セキュリティとコンプライアンス管理センターから、次の表に示す保持ポリシーを作成します。

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

次の図に示すように構成されている場合の Policy1。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 1 years ▾

No, just delete content that's older than ⓘ

1 years ▾

Delete the content based on when it was created ▾ ⓘ

Need more options?

Use advanced retention settings ⓘ

Back Next Cancel

Microsoft

Policy2 は次のように構成されています。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 3 years ▾

Retain the content based on when it was created ▾ ⓘ

Do you want us to delete it after this time?


Yes No

No, just delete content that's older than ⓘ

1 years ▾

Need more options?

Use advanced retention settings ⓘ



Back Next Cancel

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

Answer Area

	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

説明

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

参照：

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen->

最新問題: 218

次の表に示すユーザーを含む Microsoft 365 サブスクリプションを所有しています。

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

User1、User2、および User3 がセルフサービス パスワード リセット (SSPR) を使用できることを確認する必要があります。この解決策はユーザー 4 に影響を与えてはなりません。

解決策: Group2 に対して SSPR を有効にします。

これは目標を達成していますか?

- A. はい
- B. いいえ

Answer: A (メッセージを残す)

既定では、セルフサービス パスワード リセットはディレクトリ作成者とセキュリティ管理者に対

して有効になっていますが、Azure Information Protection 管理者とクラウド アプリケーション管理
者に対しては有効ではありません。

参照：

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

最新問題: 219

Azure ATP センサーをドメイン コントローラーにインストールします。

Domain Admins グループにメンバーを追加します。Azure ATP のタイムラインを表示すると、メ
ンバーシップの変更に関する情報が欠落していることがわかります。

Azure ATP レポートのセキュリティ要件を満たす必要があります。

何を設定すればよいでしょうか? 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。

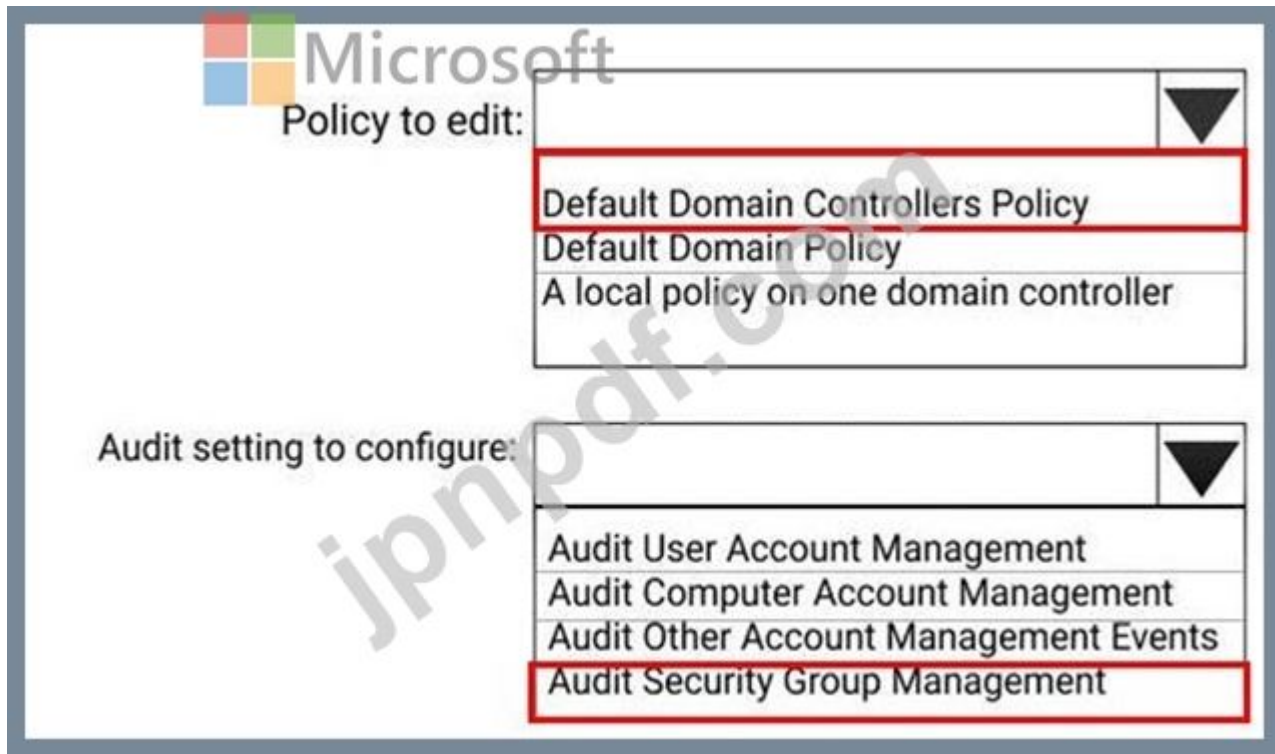
Policy to edit:

	▼
Default Domain Controllers Policy	
Default Domain Policy	
A local policy on one domain controller	

Audit setting to configure:

	▼
Audit User Account Management	
Audit Computer Account Management	
Audit Other Account Management Events	
Audit Security Group Management	

Answer:



参照 :

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy>

最新問題: 220

Microsoft 365 E5 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 Advanced Threat Protection (ATP) の安全な添付ファイル ポリシーを実装します。

添付ファイルを含む電子メール メッセージの受信に予想よりも時間がかかるとユーザーから報告があります。

添付ファイルを含む電子メール メッセージの受信にかかる時間を短縮する必要があります。のソリューションでは、すべての添付ファイルでマルウェアがスキャンされていることを確認する必要があります。マルウェアが含まれる添付ファイルは、ブロックされる。

ATPから何をすべきでしょうか？

- A. アクションをブロックに設定します。
- B. 例外を追加します。
- C. 条件を追加します。
- D. アクションを動的配信に設定します。

Answer: D (メッセージを残す)

説明/参照:

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing>

最新問題: 221

Microsoft 365 サブスクリプションをお持ちです。

セキュリティ マネージャーは、データ損失防止 (DLP) ポリシーの一致が発生するたびに電子メール メッセージを受信します。

アラート通知を実行可能な DLP イベントに制限する必要があります。

あなたは何をすべきか？

- A. セキュリティとコンプライアンス管理センターから、DLP ポリシーのポリシー ヒントを変更します。
- B. Cloud App Security 管理センターから、アラートにフィルターを適用します。
- C. セキュリティとコンプライアンス管理センターから、DLP ポリシーのユーザー オーバーライド設定を変更します。
- D. セキュリティとコンプライアンス管理センターから、アラート ポリシーの一致したアクティビティのしきい値を変更します。

Answer: D ([メッセージを残す](#))

参考文献:

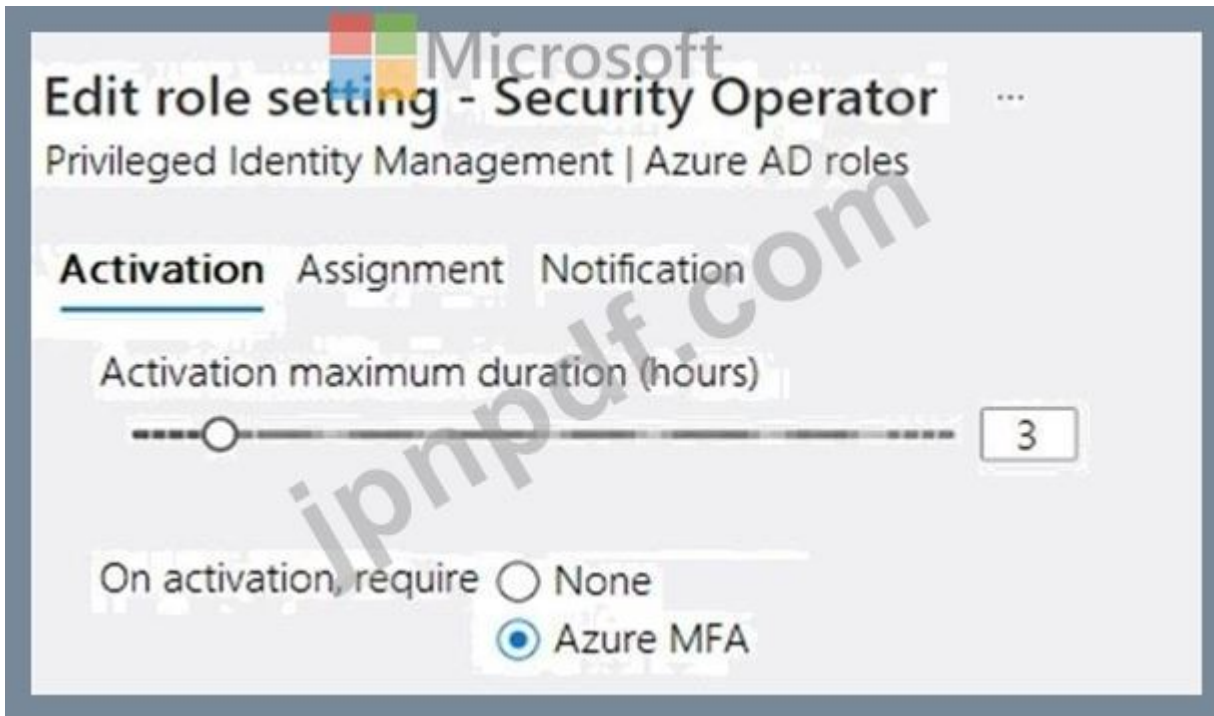
<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

最新問題: 222

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

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

次の図に示すように、Azure AD Privileged Identity Management (PIM) でセキュリティ オペレーター ロールを構成します。



次の表に示すように、セキュリティオペレーターロールに割り当てを追加します。

Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

どのユーザーがセキュリティオペレーターロールをアクティブ化できますか？

- A. User2 のみ
- B. User2 と User3 のみ
- C. User3 のみ
- D. 使用済みおよび User2 のみ
- E. ユーザー 1、ユーザー 2、およびユーザー 3

Answer: B ([メッセージを残す](#))

最新問題: 223

contoso.com という名前の AzureActive Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group2

次の表に示すように、contoso.com にデバイスを登録します。

Name	Platform	Member of	Microsoft Intune managed
Device1	Windows 10	GroupA	Yes
Device2	iOS	GroupB	No

次の表に示すように、Intune でアプリ保護ポリシーを作成します。

Name	Platform	Management state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	With enrollment	Group2
Policy3	iOS	Apps on Intune managed devices	GroupA
Policy4	iOS	Apps on Intune managed devices	GroupB

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注:正しく選択するたびに 1 ポイントの価値があります。



Statements

Yes

No

When User1 uses Device1, Policy3 applies.

When User2 uses Device1, Policy2 applies.

When User2 uses Device2, Policy4 applies.

Answer:

Statements

Yes

No

When User1 uses Device1, Policy3 applies.

When User2 uses Device1, Policy2 applies.

When User2 uses Device2, Policy4 applies.

説明

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	<input type="radio"/>	<input type="radio"/>
When User2 uses Device1, Policy2 applies.	<input type="radio"/>	<input type="radio"/>
When User2 uses Device2, Policy4 applies.	<input type="radio"/>	<input type="radio"/>

参考文献:

<https://docs.microsoft.com/en-us/intune/apps/app-protection-policy>

最新問題: 224

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザーとデバイス オブジェクトは毎日追加および削除されます。営業部門のユーザーは頻繁にデバイスを変更します。

次の 3 つのグループを作成する必要があります。

Group	Requirement
1	All the devices of users where the Department attribute is set to Sales
2	All the devices where the Department attribute is set to Sales
3	All the devices where the deviceOwnership attribute is set to Company

ソリューションでは、管理労力を最小限に抑える必要があります。

メンバーシップの種類ごとに作成するグループ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。

Microsoft

Groups that have assigned membership:

▼
0
1
2
3

Groups that have dynamic membership:

▼
0
1
2
3

Answer:

Groups that have assigned membership:

▼
0
1
2
3

Groups that have dynamic membership:

▼
0
1
2
3

Microsoft

参照：

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md>

最新問題: 225

Group3 をどのように構成すればよいでしょうか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Group type:

Microsoft
▼

An Office 365 group in the Microsoft 365 admin center

A security group in Active Directory Users and Computers

A security group in the Azure Active Directory admin center

Group membership criteria:

▼

A dynamic distribution list

A dynamic membership rule with an Advanced rule set to All users

A dynamic membership rule with a Simple rule set to userType Equals User

Answer:

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input type="checkbox"/>	<input type="checkbox"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input type="checkbox"/>	<input type="checkbox"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

説明

Group type:

Microsoft
▼

An Office 365 group in the Microsoft 365 admin center

A security group in Active Directory Users and Computers

A security group in the Azure Active Directory admin center

Group membership criteria:

▼

A dynamic distribution list

A dynamic membership rule with an Advanced rule set to All users

A dynamic membership rule with a Simple rule set to userType Equals User

最新問題: 226

ADGroup1 と ADGroup2 のメンバーはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。

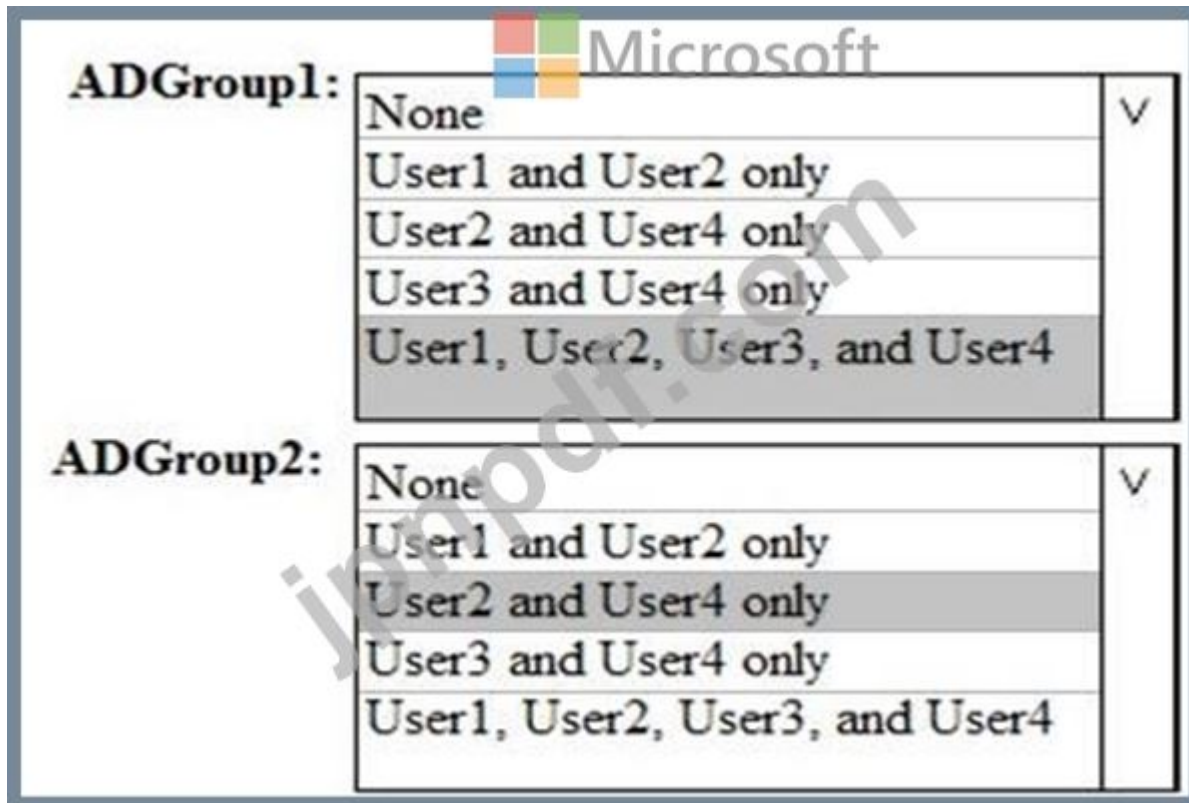
注: 正しく選択するたびに 1 ポイントの価値があります。

ADGroup1:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	
ADGroup2:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

Answer:

ADGroup1:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	
ADGroup2:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

説明



参照：

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#suppor>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら：<https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 227

どのデバイスが Intune に準拠しているかを評価しています。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input type="radio"/>
Device6 is compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	 Microsoft	Yes	No
Device2 is compliant.		<input checked="" type="radio"/>	<input type="radio"/>
Device5 is compliant.		<input type="radio"/>	<input checked="" type="radio"/>
Device6 is compliant.		<input checked="" type="radio"/>	<input type="radio"/>


最新問題: 228

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

File1.docx という名前のファイルが Microsoft OneDrive に保存されています。自動プロセスにより、File1.docx が 1 分ごとに更新されます。

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

Policy1

 Edit policy

 Delete policy

Status On

Description Policy1 description

Severity Low

[Edit](#)

Category Threat management

Conditions Activity is Copied file and File name is Like any of File1.docx

Aggregation Aggregated

Threshold 10 activities

Window 60 minutes

Scope All users

[Edit](#)

Email recipients prvi@sk180920.onmicrosoft.com

Daily notifications  limit Do not send email notifications

[Edit](#)

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

注: 正しく選択するたびに1ポイントの価値があります。

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].



	▼
Policy1 will not be triggered	
Policy1 will be triggered after 45 minutes	
Policy1 will be triggered after 60 minutes	

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

	▼
Policy1 will not be triggered	
Policy1 will be triggered within 20 minutes	
Policy1 will be triggered within 45 minutes	
Policy1 will be triggered after 60 minutes	

Answer:

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

参照 :


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

最新問題: 229

fabrikam.com の既定のドメイン名を使用する Microsoft 365 サブスクリプションがあります。次の図に示すように、安全なリンク ポリシーを作成します。

Safe links policy for your organization

Settings that apply to content across Office 365
 When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.
 Block the following URLs:

 -

Enter a valid URL

.phishing.
 malware.*com
 *.contoso.com

Settings that apply to content except email
 These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

Office 365 ProPlus, Office for iOS and Android
 Office Online of above applications

For the locations selected above:

Do not track when users click safe links:
 Do not let users click through safe links to original URL:

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

- A. fabrikam.phishing.fabrikam.com
- B. malware.fabrikam.com
- C. fabrikam.contoso.com
- D. www.malware.fabrikam.com

Answer: D ([メッセージを残す](#))

説明/参照:

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

最新問題: 230

Microsoft 365 サブスクリプションをお持ちです。

Site2 という名前のサイトを含む SiteCollection1 という名前のサイト コレクションがありません。Site2 には、Customers という名前のドキュメント ライブラリが含まれています。

Customers には Litware.docx という名前のドキュメントが含まれています。Litware.docx を完全に削除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
From PowerShell, run Remove-SPOUserProfile	
Delete Litware.docx from the Recycle Bin of Site2.	
From PowerShell, run Set-SPOSite.	
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

Answer:

Actions	Answer Area
From PowerShell, run Remove-SPOUserProfile	Delete Litware.docx from Customers.
Delete Litware.docx from the Recycle Bin of Site2.	Delete Litware.docx from the Recycle Bin of Site2.
From PowerShell, run Set-SPOSite.	Delete Litware.docx from the Recycle Bin of SiteCollection1.
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

最新問題: 231

セキュリティ要件を満たすには、Windows Defender ATP を実装する必要があります。あなたは何をするべきか？

- A. ForceDefenderPassiveMode レジストリ設定を作成します。
- B. Microsoft Monitoring Agent をダウンロードしてインストールします。
- C. ポートミラーリングの設定
- D. WindowsDefenderATPOnboardingScript.cmd を実行します。

Answer: ([解答を表示する](#))

最新問題: 232

ConfidentialHR.docx という名前のファイルを Microsoft SharePoint ライブラリに追加する予定です。

別のユーザーが ConfidentialHR.xlsx にアクセスしたときに、Megan Bowen という名前のユー

ザーに通知が届くようにする必要があります。

このタスクを完了するには、Microsoft 365 ポータルにサインインします。

Answer:

以下の説明を参照してください。

説明

アラート ポリシーを構成する必要があります。

* セキュリティとコンプライアンス管理センターに移動します。

* [アラート] > [アラート ポリシー] に移動します。

* 新しいポリシーを作成するには、[+ 新しいアラート ポリシー] をクリックします。

* ポリシーに名前を付け、重大度レベルを選択します。例: 中。

* [カテゴリ] セクションで、[情報ガバナンス] を選択し、[次へ] をクリックします。

* [アクティビティの選択] セクションで、[任意のファイルまたはフォルダーのアクティビティ] を選択します。

* [条件の追加] をクリックし、[ファイル名] を選択します。

* ファイル名 ConfidentialHR.xlsx」を入力し、次へ」をクリックします。

* 電子メール受信者セクションで、Megan Bowen を追加し、

* [完了] をクリックしてアラート ポリシーを作成します。

最新問題: 233

監査のセキュリティ要件を満たすソリューションをユーザー管理者に推奨する必要があります。Azure Active Directory 管理センターからどのブレードを使用することをお勧めしますか？

A. サインイン

B. Azure AD ID 保護

C. 認証方式

D. アクセスレビュー

Answer: ([解答を表示する](#))

参考文献:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

最新問題: 234

仮想マシンがロードされるまでお待ちください。ロードしたら、ラボセクションに進むことができます。これには数分かかる場合がありますが、待ち時間は全体のテスト時間から差し引かれません。

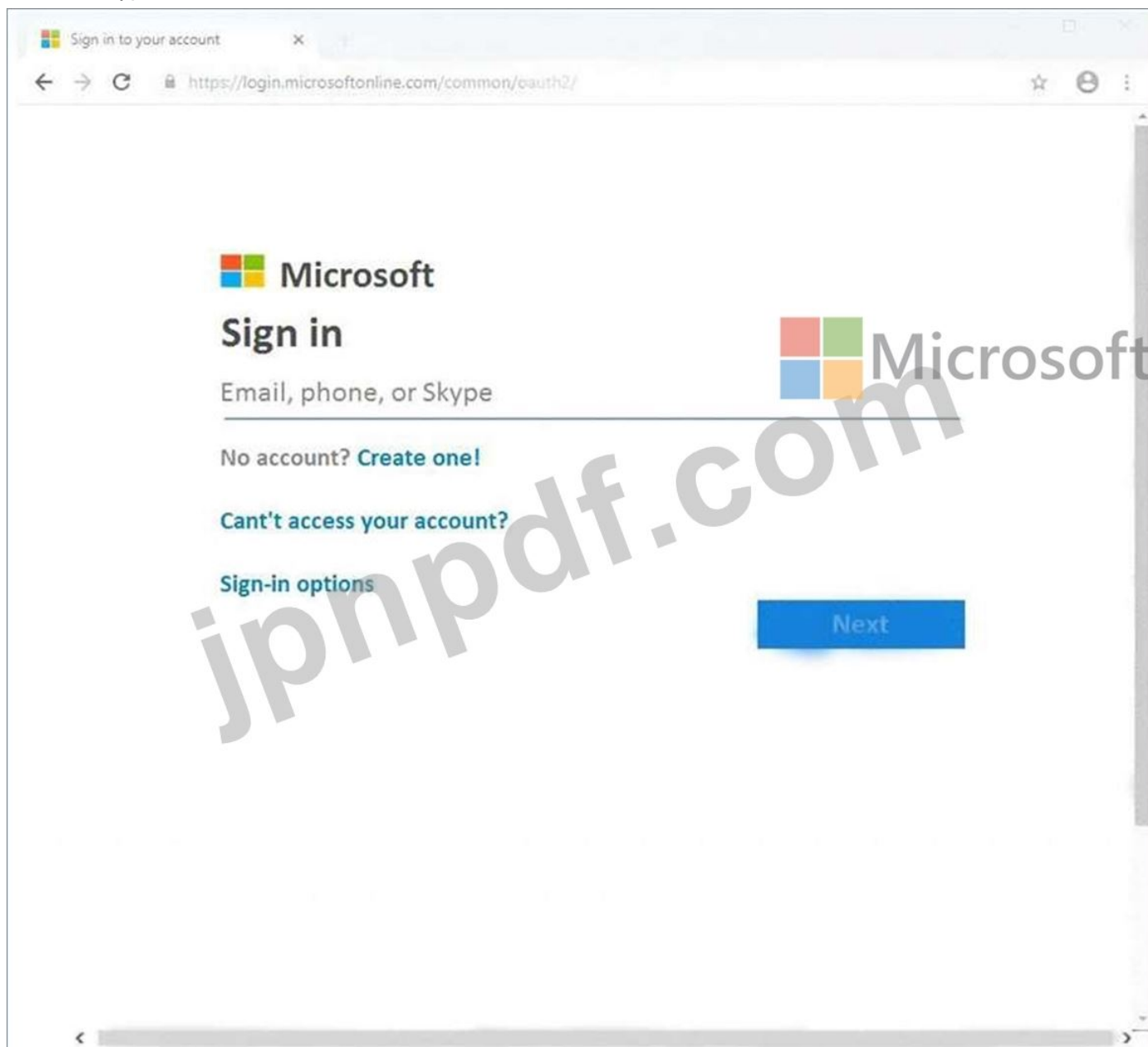
[次へ] ボタンが使用可能になったら、それをクリックしてラボ セクションにアクセスします。このセクションでは、実際の環境で一連のタスクを実行します。ほとんどの機能は実際の環境と同じように利用できますが、一部の機能 (コピー アンド ペースト、外部 Web サイトに移動する機能など) は設計上不可能です。

スコアは、ラボに記載されているタスクの実行結果に基づいています。言い換えれば、タスクをどのように達成するかは問題ではありません。タスクを正常に実行できれば、そのタスクの功績が得られます。

ラボは個別に時間が設定されていないため、この試験では複数のラボを完了する必要がある場合があります。各ラボを完了したいだけ時間を費やすことができます。ただし、ラボや試験の他のすべてのセクションを指定された時間内に完了できるように、時間を適切に管理する必要があります。

ラボ内で「次へ」ボタンをクリックして作業を送信すると、ラボに戻ることはできなくなりますのでご注意ください。

ユーザー名とパスワード



必要に応じて、次のログイン資格情報を使用します。

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

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

Microsoft 365 ユーザー名:

admin@LODSe00019@onmicrosoft.com

Microsoft 365 パスワード: #HSP.ug?\$p6un

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

次の情報はテクニカル サポート専用です。

ラボ インスタンス: 11122308



Microsoft

Microsoft ✕



jpnpdf.com

Brainstorm
together in Word



Microsoft



Stay on top of what matters with Outlook



Microsoft

Microsoft



Microsoft



Access Office 365 apps and documents in one place with

Office.com



Microsoft Office Home

office.com/?auth=2

Contoso electronics Office 365

Good morning Install Office

Start new

Outlook

OneDrive

Word

Excel

PowerPoint

OneNote

Skype

Calendar

People

All apps

Recommended

You edited this Jan 15

Integrated Team Sales Process

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15

Excel

P and L Summary
lodse000198.sharepoint.co...

You edited this Jan 15

Contoso Electronics Outdoor...

Contoso Electronics Outdoor...
lodse000198.sharepoint.co...

You edited this Jan 15

AD Slogans

AD Slogans
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

Upload and open...

New

Go to OneDrive →



OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →



SharePoint

Frequent sites

Following

SM Sales and Marketing

R Retail

Cs Communication Site

SharePoint

Frequent sites

Following

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

Go to SharePoint →

Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

ユーザーのメールボックス検索を自動化するスクリプトを作成する予定です。スクリプトは、Allan Deyoung という名前のユーザーのメールボックスで、差し止めという単語を含むメッセージを検索します。

スクリプトに含まれる検索を作成する必要があります。

このタスクを完了するには、Microsoft 365 管理センターにサインインします。

Answer:

以下の説明を参照してください。

説明

ステップ 1: 実行する検索に関する情報を含む CSV ファイルを作成する このステップで作成するカンマ区切り値 (CSV) ファイルには、検索する各ユーザーの行が含まれています。ユーザーの Exchange Online メールボックス (有効な場合はアーカイブ メールボックスを含む) と OneDrive for Business サイトを検索できます。または、メールボックスまたは OneDrive for Business サイトのみを検索することもできます。SharePoint Online 組織内の任意のサイトを検索することもできます。ステップ 3 で実行するスクリプトは、CSV ファイル内の行ごとに個別の検索を作成します。

1. メモ帳を使用して、次のテキストをコピーして .txt ファイルに貼り付けます。このファイルをローカル コンピューター上のフォルダーに保存します。他のスクリプトもこのフォルダーに保存します。

ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate
 sarad@contoso.onmicrosoft.com、https://contoso-
 my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的
 的)、1/1/2000、12/31/2005 sarad @contoso.onmicrosoft.com、https://contoso-

my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2006/1/1、2010/12/31 sarad@contoso.onmicrosoft.com、https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com、(または法的)、2011/1/1、2016/3/21

、https://contoso.sharepoint.com/sites/contoso、2016年3月21日

、https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com、2015年1月1日、

、https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com、1/1/2015、ファイルの最初の行、つまりヘッダ行には、New-ComplianceSearch コマンドレットで使用されるパラメーターがリストされています。新しいコンテンツ検索。各パラメータ名はカンマで区切られます。ヘッダ行にスペースが含まれていないことを確認してください。ヘッダ行の下の各行は、各検索のパラメーター値を表します。CSV ファイル内のプレースホルダー データを実際のデータに置き換えてください。

2. Excel で .txt ファイルを開き、次の表の情報を使用して、各検索の情報を含むファイルを編集します。

Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see Keyword queries and search conditions for Content Search .
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

3. Excel ファイルを CSV ファイルとしてローカル コンピューター上のフォルダーに保存します。ステップ 3 で作成したスクリプトは、この CSV ファイル内の情報を使用して検索を作成します。

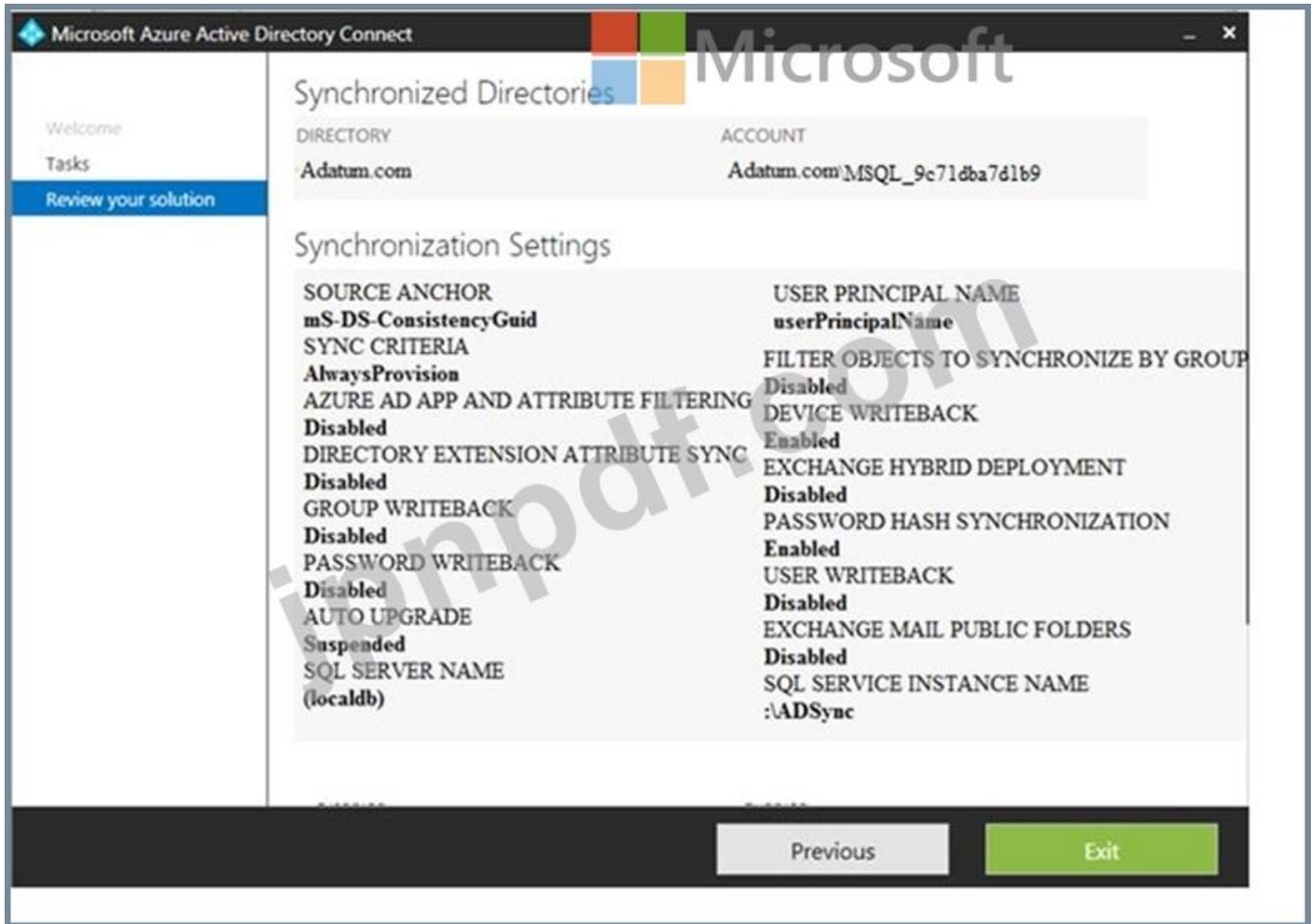
参照：

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-searches> コンテンツ検索のキーワード クエリと検索条件

<https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365>

最新問題: 235

次の図に示すように、Microsoft Azure Active Directory (Azure AD) Connect を構成します。



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

注: 正しく選択するたびに1ポイントの価値があります。

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

Answer:



参照：

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

最新問題: 236

次の表に示す Microsoft の条件があります。

Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

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

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

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

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	<i>None</i>
Policy1	User1	Label1	<i>None</i>
Policy2	User2	Label2	<i>None</i>

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

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

Answer:

Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input type="radio"/>	<input checked="" type="radio"/>

最新問題: 237

ネットワークには contoso.com という名前の Active Directory ドメインが含まれています。ドメインには、Windows Server 2016 を実行し、リモート アクセス サーバーの役割がインストールされている VPN1 という名前の VPN サーバーが含まれています。

Microsoft Azure サブスクリプションをお持ちです。

Azure Advanced Threat Protection (ATP) をデプロイしています。

Windows Server 2016 を実行する Server1 という名前のサーバーに Azure ATP スタンドアロンセンサーをインストールします。

VPN と Azure ATP を統合する必要があります。

あなたは何をすべきか？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。

On VPN1:

Configure an authentication provider.	v
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	v
1723	
1813	
8080	
8531	


Answer:

On VPN1:

Configure an authentication provider.	✓
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	✓
1723	
1813	
8080	
8531	



参照 :

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn>

最新問題: 238

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は Microsoft 365 E5 ライセンスが割り当てられます。

監査データはどのくらいの期間保存されますか？

- A. 30日
- B. 90日
- C. 365日
- D. 5年

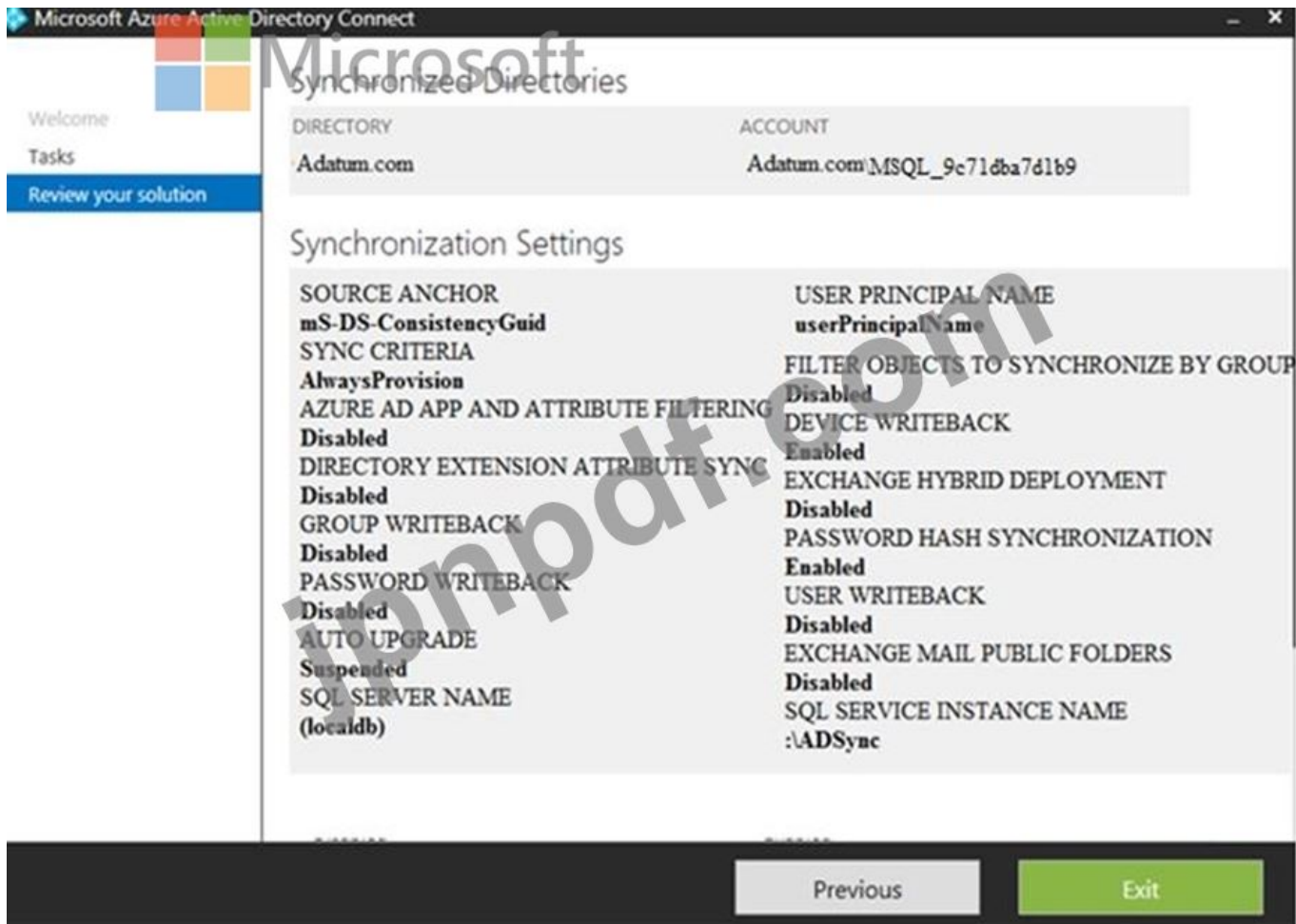
Answer: B ([メッセージを残す](#))

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

最新問題: 239

次の図に示すように、Microsoft Azure Active Directory (Azure AD) Connect を構成します。



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

注: 正しく選択するたびに1ポイントの価値があります。

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	V
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	V
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

Answer:

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

説明

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>


最新問題: 240

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

File1.docx という名前のファイルが Microsoft OneDrive に保存されています。自動プロセスにより、File1.docx が 1 分ごとに更新されます。

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

Policy1

 Edit policy

 Delete policy

Status On

Description Policy1 description

Severity Low

[Edit](#)

Category Threat management

Conditions Activity is Copied file and File name is Like any of File1.docx

Aggregation Aggregated

Threshold 10 activities

Window 60 minutes

Scope All users

[Edit](#)

Email recipients prvi@sk180920.onmicrosoft.com

Daily notifications  limit Do not send email notifications

[Edit](#)

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

注: 正しく選択するたびに1ポイントの価値があります。

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

Microsoft	▼
Policy1 will not be triggered	
Policy1 will be triggered after 45 minutes	
Policy1 will be triggered after 60 minutes	

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

	▼
Policy1 will not be triggered	
Policy1 will be triggered within 20 minutes	
Policy1 will be triggered within 45 minutes	
Policy1 will be triggered after 60 minutes	

Answer:

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

Microsoft	▼
Policy1 will not be triggered	
Policy1 will be triggered after 45 minutes	
Policy1 will be triggered after 60 minutes	

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].


	▼
Policy1 will not be triggered	
Policy1 will be triggered within 20 minutes	
Policy1 will be triggered within 45 minutes	
Policy1 will be triggered after 60 minutes	

参照 :

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

最新問題: 241

デフォルト名 litwareinc.com を使用する Microsoft 365 サブスクリプションがあります。次の図に示すように、Microsoft OneDrive で共有設定を構成します。

Links 

Choose the kind of link that's selected by default when users share items.

Default link type

Shareable: Anyone with the link

Internal: Only people in your organization

Direct: Specific people

External sharing

Users can share with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can create shareable links that don't require sign-in

New and existing external users
External users must sign-in

Existing external users
Only users already in your organization's directory

Only people in your organization
No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

Allow or block sharing with people on specific domains

Allow only these domains Contoso.com, Adatum.com [Add domains](#)

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

注: 正しく選択するたびに 1 ポイントの価値があります。

A user who has an email address of user1@fabrikam.com [answer choice]

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	



Answer:

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

説明

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to be a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice]

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

参考文献:

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする

人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (32930%OFF問題集
溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 242

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

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

どのデバイスで BitLocker To Go を使用でき、どのデバイスで自動ロック解除をオンにできますか? 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: 正しく選択するたびに 1 ポイントの価値があります。

BitLocker To Go:	<input type="checkbox"/> Device3 only <input type="checkbox"/> Device1 and Device2 only <input type="checkbox"/> Device1, Device2, and Device3 only <input type="checkbox"/> Device1, Device2, Device3, and Device4
Auto-unlock:	<input type="checkbox"/> Device1 and Device2 only <input type="checkbox"/> Device1 and Device3 only <input type="checkbox"/> Device1, Device2, and Device3 only <input type="checkbox"/> Device1, Device2, Device3, and Device4

Answer:

BitLocker To Go:	<input checked="" type="checkbox"/> Device3 only <input type="checkbox"/> Device1 and Device2 only <input type="checkbox"/> Device1, Device2, and Device3 only <input type="checkbox"/> Device1, Device2, Device3, and Device4
Auto-unlock:	<input type="checkbox"/> Device1 and Device2 only <input checked="" type="checkbox"/> Device1 and Device3 only <input type="checkbox"/> Device1, Device2, and Device3 only <input type="checkbox"/> Device1, Device2, Device3, and Device4

説明

BitLocker To Go:	Device3 only
	Device1 and Device2 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4
Auto-unlock:	Device1 and Device2 only
	Device1 and Device3 only
	Device1, Device2, and Device3 only
	Device1, Device2, Device3, and Device4

最新問題: 243

どのデバイスが Intune に準拠しているかを評価しています。
 次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input type="radio"/>
Device6 is compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Device2 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device6 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 244

あなたの会社は Microsoft 365 サブスクリプションを持っています。
 同社は、ユーザーが個人のデバイスをモバイル デバイス管理 (MDM) に登録することを禁止しています。

営業部門のユーザーは個人用の iOS デバイスを持っています。

営業部門のユーザーが iOS デバイスから Microsoft Power BI アプリを使用してテナント内の Power BI データにアクセスできることを確認する必要があります。

ユーザーがアプリのデータを iCloud にバックアップできないようにする必要があります。

何を作成する必要がありますか？

- A. Microsoft Intune のデバイス コンプライアンス ポリシー
- B. クライアント アプリ条件を持つ Microsoft Azure Active Directory (Azure AD) の条件付きアクセス ポリシー
- C. Microsoft Intune のアプリ保護ポリシー
- D. デバイスの状態条件がある Microsoft Azure Active Directory (Azure AD) の条件付きアクセス ポリシー

Answer: C ([メッセージを残す](#))

最新問題: 245

Used という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

ユーザーを確認する必要があります。Microsoft 365 コンプライアンス センターを使用して監査ログを検索し、Microsoft 365 役割グループに追加されたユーザーを特定できます。ソリューションでは、最小特権の原則を使用する必要があります。

User1 をどの役割グループに追加する必要がありますか？

- A. コンプライアンス管理
- B. セキュリティリーダー
- C. 組織管理
- D. 閲覧専用の組織管理

Answer: C ([メッセージを残す](#))

最新問題: 246

Microsoft 365 サブスクリプションをお持ちです。セキュリティとコンプライアンス管理センターから、次の表に示す保持ポリシーを作成します。

Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

次の図に示すように構成されている場合の Policy1。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 1 years ▾

No, just delete content that's older than ⓘ

1 years ▾

Delete the content based on when it was created ▾ ⓘ

Need more options?

Use advanced retention settings ⓘ

Back

Next

Cancel

Policy2 は次のように構成されています。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 3 years ▾

Retain the content based on when it was created ▾ ⓘ

Do you want us to delete it after this time?

Yes No

No, just delete content that's older than ⓘ

1 years ▾

Need more options?

Microsoft

Use advanced retention settings ⓘ

Back

Next

Cancel

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

Answer Area

Yes

No

If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019

If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019

If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022

Answer:

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

参照：

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the>

-保持の原則または優先するもの

最新問題: 247

Azure Active Directory (Azure AD) コネクタと Office 365 コネクタを備えた Microsoft Sentinel ワークスペースがあります。

ワークスペースから、カスタム クエリに基づいてセキュリティ プレイを実行する分析ルールを作成する予定です。

セキュリティ プレイブックとカスタム クエリをルールに追加できることを確認する必要があります。

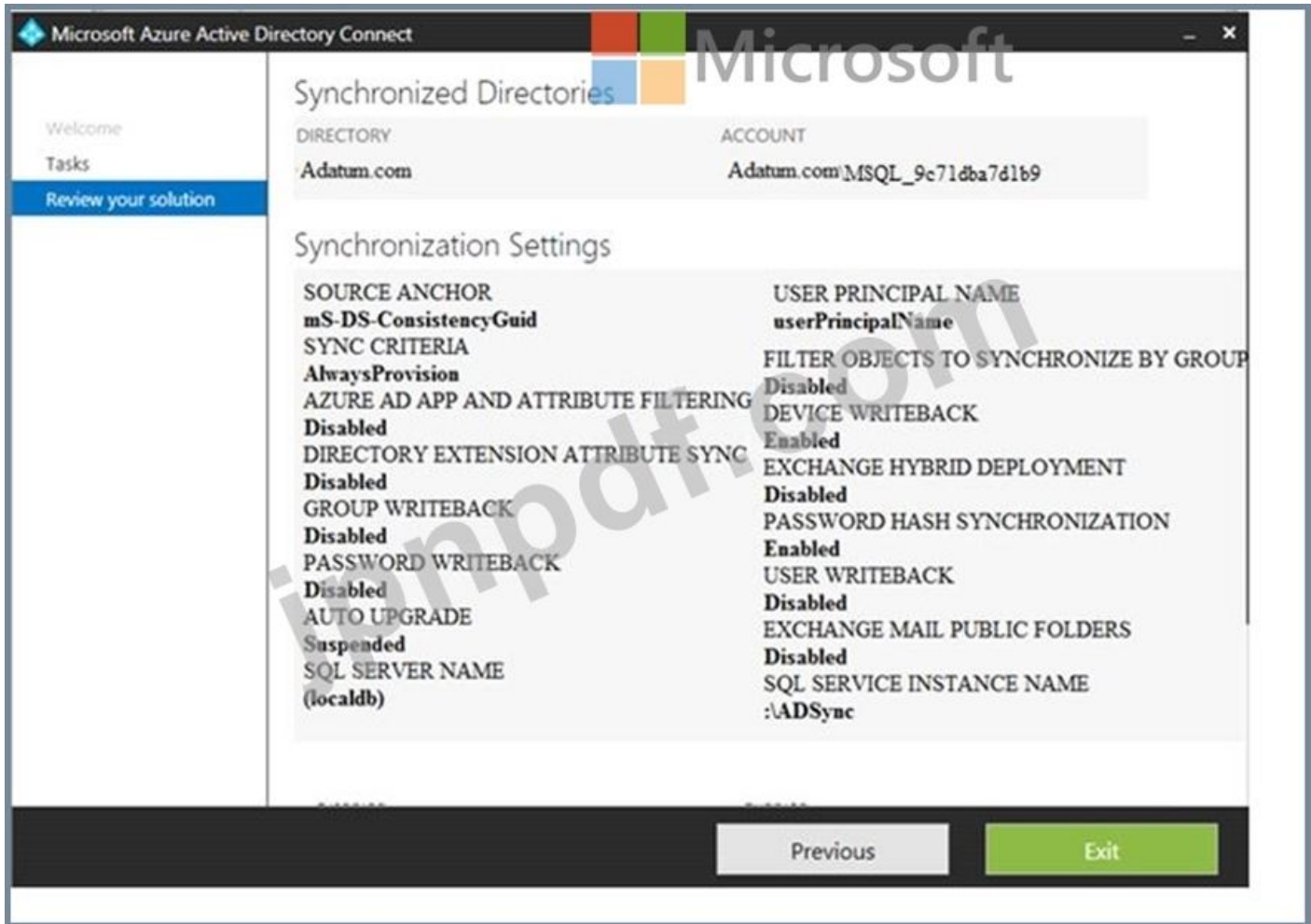
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択してください。

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:

最新問題: 248

次の図に示すように、Microsoft Azure Active Directory (Azure AD) Connect を構成します。



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

注: 正しく選択するたびに1ポイントの価値があります。

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

Answer:

When you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

When you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

参照 :

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

最新問題: 249

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	Department	Microsoft 365 role
Admin1	IT	Groups admin
Admin2	IT	User admin
Admin3	Research	User admin
Admin4	Finance	Groups admin

contoso.com の場合、次の構成を持つグループ名前付けポリシーを作成します。

<部署> - <グループ名>

次の表に示すグループを作成する予定です。

Name	Type
IT-Group1	Microsoft 365
Finance-Group2	Security

各グループの作成にはどのユーザーを使用できますか? 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: 正しく選択するたびに 1 ポイントの価値があります。

IT-Group1:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin4 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Finance-Group2:

- Admin4 only
- Admin1 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Answer:

IT-Group1:

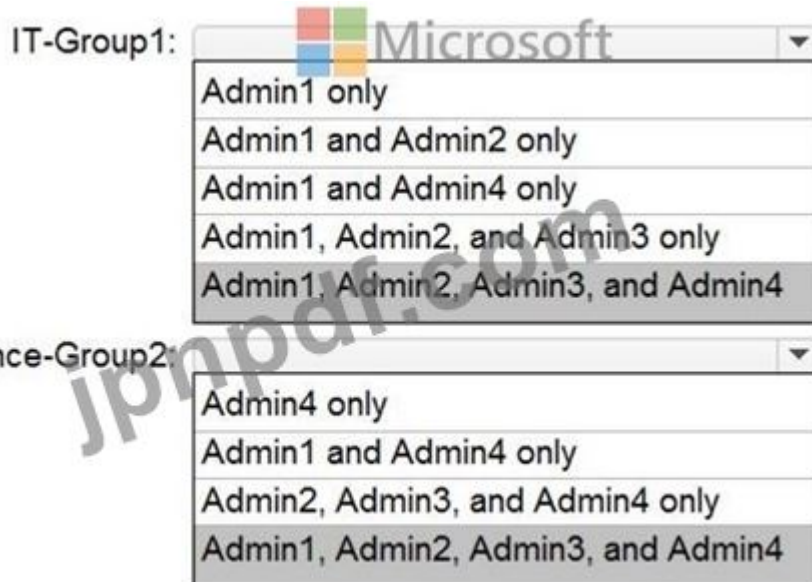
- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin4 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Finance-Group2:

- Admin4 only
- Admin1 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーションの説明が自動生成される



参照 :

<https://office365itpros.com/2020/01/22/using-groups-admin-role/>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

最新問題: 250

Microsoft 365 サブスクリプションをお持ちです。すべてのユーザーは Microsoft Exchange Online を使用します。

Microsoft 365 は、カスタム ルールなしで既定のポリシー設定を使用するように構成されています。

メッセージの衛生状態を管理します。

不審な電子メール メッセージはデフォルトでどこに配置されますか? 回答するには、適切な場所を正しいメッセージ タイプにドラッグします。各場所は 1 回だけ使用することも、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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。



Answer:



説明

Answer Area

Messages that contain word-filtered content: The Junk Email folder of a user's mailbox

Messages that are classified as phishing: The Junk Email folder of a user's mailbox



最新問題: 251

contoso.com の既定のドメイン名を使用する Microsoft 365 サブスクリプションがあります。多要素認証 (MFA) サービスの設定は、図に示すように構成されています。(「展示」タブをクロックします。)

multi-factor authentication
users service settings

app passwords (earn more)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips(earn more)

- Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

verification options (earn more)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication (earn more)

- Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60) [14]

Microsoft

contoso.com で、次の表に示すユーザーを作成します。

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

構成の効果は何ですか? 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。

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

Answer:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

最新問題: 252

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Azure Active Directory (Azure AD) から、Group1 という名前のセキュリティ グループを作成します。10 人のユーザーを Group1 に追加します。

Group1 のメンバーが非準拠デバイスから Microsoft Exchange Online に接続する場合は、場所に関係なく、アプリによる制限を適用する必要があります。

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。

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	v
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	v
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Answer:

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	v
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	v
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

説明

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	v
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	v
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

最新問題: 253

電子メールデータを暗号化するラベルを作成します

a. ユーザーは、送信する電子メールメッセージを保護するために Web 上の Outlook でラベルを使用できないと報告しています。

ユーザーが新しいラベルを使用して電子メールを保護できることを確認する必要があります。

あなたは何をするべきか？

- A. 6 時間待つ、ユーザーに再試行するよう依頼します。
- B. ラベルポリシーの優先順位を変更します。
- C. ラベルポリシーを作成する
- D. 新しい機密情報の種類を作成します

Answer: A ([メッセージを残す](#))

最新問題: 254

どのポリシーがどのデバイスに適用されますか? 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。

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

Answer:

DevicePolicy1:	<table border="1"> <tr><td>None</td></tr> <tr><td>Device1 only</td></tr> <tr><td>Device3 only</td></tr> <tr><td>Device2 and Device3 only</td></tr> <tr><td>Device1 and Device3 only</td></tr> <tr><td>Device1, Device2, and Device3</td></tr> </table>	None	Device1 only	Device3 only	Device2 and Device3 only	Device1 and Device3 only	Device1, Device2, and Device3
None							
Device1 only							
Device3 only							
Device2 and Device3 only							
Device1 and Device3 only							
Device1, Device2, and Device3							
DevicePolicy2:	<table border="1"> <tr><td>None</td></tr> <tr><td>Device4 only</td></tr> <tr><td>Device2 and Device4 only</td></tr> <tr><td>Device2, Device3, and Device 4 only</td></tr> </table>	None	Device4 only	Device2 and Device4 only	Device2, Device3, and Device 4 only		
None							
Device4 only							
Device2 and Device4 only							
Device2, Device3, and Device 4 only							

説明

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

最新問題: 255

Microsoft 365 サブスクリプションをお持ちです。

顧客は、彼女の名前が記載されているすべての文書を提供するように要求しています。

コンテンツのコピーを顧客に提供する必要があります。

どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、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

Close the case.
Regenerate a report.
View the results.
Export the results.
Create a Data Subject Request (DSR) case.
Save the search.
Download the results.

Answer:

Actions	Answer Area
Close the case.	Create a Data Subject Request (DSR) case.
Regenerate a report.	View the results.
View the results.	Save the search.
Export the results.	Export the results.
Create a Data Subject Request (DSR) case.	
Save the search.	
Download the results.	

参照 :

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

最新問題: 256

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) を使用する Microsoft 365 E5 サブスクリプションがあります。User という名前のユーザーです! ユーザー アカウント管理者の役割を担う資格があります。ユーザーが必要です!

ユーザー アカウント管理者ロールのアクティブ化を要求します。User1 はロールのアクティブ化をどこから要求すればよいですか?

- A. Microsoft 365 Defender ポータル
- B. マイ アクセス ポータル
- C. Azure Active Directory 管理センター
- D. Microsoft 365 管理センター

Answer: A ([メッセージを残す](#))

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集! GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 257

どのポリシーがどのデバイスに適用されますか? 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。

DevicePolicy1:	None
	Device1 only
	Device3 only
	Device2 and Device3 only
	Device1 and Device3 only
	Device1, Device2, and Device3

DevicePolicy2:	None
	Device4 only
	Device2 and Device4 only
	Device2, Device3, and Device 4 only

Answer:

DevicePolicy1:	None
	Device1 only
	Device3 only
	Device2 and Device3 only
	Device1 and Device3 only
	Device1, Device2, and Device3

DevicePolicy2:	None
	Device4 only
	Device2 and Device4 only
	Device2, Device3, and Device 4 only

最新問題: 258

あなたの会社は Microsoft 365 サブスクリプションを持っています。

同社は、ユーザーが個人のデバイスをモバイル デバイス管理 (MDM) に登録することを禁止しています。

営業部門のユーザーは個人用の iOS デバイスを持っています。

営業部門のユーザーが iOS デバイスから Microsoft Power BI アプリを使用してテナント内の Power BI データにアクセスできることを確認する必要があります。

ユーザーがアプリのデータを iCloud にバックアップできないようにする必要があります。

何を作成する必要がありますか？

A. デバイスの状態条件がある Microsoft Azure Active Directory (Azure AD) の条件付きアクセスポリシー

B. Microsoft Intune のアプリ保護ポリシー

C. クライアント アプリ条件を持つ Microsoft Azure Active Directory (Azure AD) の条件付きアクセスポリシー

D. Microsoft Intune のデバイス コンプライアンス ポリシー

Answer: B ([メッセージを残す](#))

説明/参照:

テストレット 1

概要

Fabrikam, Inc. は、パートナーの小売店を通じて製品を販売する製造会社です。ファブリカムは 5,000 人の従業員がヨーロッパ全土のオフィスに拠点を置いています。

既存の環境

ネットワークインフラストラクチャ

ネットワークには、fabrikam.com という名前の Active Directory フォレストが含まれていません。Fabrikam には、ハイブリッド Microsoft Azure Active Directory (Azure AD) 環境があります。同社は特定のアプリケーション用にいくつかのオンプレミス サーバーを維持していますが、ほとんどのエンドユーザー アプリケーションは Microsoft 365 E5 サブスクリプションによって提供されています。

問題の声明

Fabrikam は次の問題を特定しています。

先週の金曜日以来、IT チームは「不健康」という内容の自動電子メール メッセージを受信しています。

件名に「ID 同期通知」と入力します。

最近、数人のユーザーがマルウェアを含む電子メールの添付ファイルを開いてしまいました。を削除するプロセスは、

マルウェアには時間がかかりました。

要件

計画された変更

Fabrikam は次の変更を実装する予定です。

Fabrikam は、Active Directory への不審なサインインを監視し、調査することを計画しています

Fabrikam は、パートナーが Microsoft 365 に保存されているデータの一部にアクセスできるようにする予定です。

アプリケーション管理

Fabrikam は、ワークロード アプリケーションを管理するための次のアプリケーション要件を特定します。

ユーザー管理者はさまざまな国から勤務します

ユーザー管理者は Azure Active Directory 管理センターを使用します。

Admin1 と Admin2 という名前の 2 人の新しい管理者が Microsoft の管理を担当します。

Exchange Online のみ

セキュリティ要件

Fabrikam は次のセキュリティ要件を特定します。

ユーザー管理者による Azure Active Directory 管理センターへのアクセスは、毎回確認する必要があります

七日間。管理者が 3 日以内にアクセス要求に応答しなかった場合は、アクセスを削除する必要があります。Microsoft 365 ワークロードを管理するユーザーには、次の管理タスクの実行のみを許可する必要があります。

一度に最大3時間まで。グローバル管理者は、この要件を免除する必要があります。ユーザーは、会社データを表示するために外部ユーザーを招待できないようにする必要があります。グローバル管理者のみ

User1 という名前のユーザーは招待状を送信する必要があります

Azure Advanced Threat Protection (ATP) は、機密性の高いセキュリティ グループの変更をキャプチャする必要があります。

Active Directory のドメイン管理者などのグループ

ワークロード管理者は、サーバーからサインインするときに多要素認証 (MFA) を使用する必要があります。

匿名または見知らぬ場所

ユーザー管理者の場所は、管理者が Azure に認証するときに監査する必要があります

広告

マルウェアを含む添付ファイルを含む電子メール メッセージは、

アタッチメント

可能な限り最小特権の原則を使用する必要がある

テストレット 2

概要

Litware, Inc. は、シカゴの本社に 1,000 人のユーザー、サンフランシスコの支社に 100 人のユーザーを抱える金融会社です。

既存の環境

内部ネットワークインフラストラクチャ

ネットワークには単一のドメイン フォレストが含まれています。フォレストの機能レベルは Windows Server 2016 です。

ユーザーは、Active Directory で定義されているサインイン時間制限の対象となります。

ネットワークの IP アドレス範囲は次の表に示されています。

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

オフィスはマルチプロトコル ラベル スイッチング (MPLS) を使用して接続します。
ネットワークでは次のオペレーティング システムが使用されています。

Windowsサーバー2016

Windows 10 エンタープライズ

Windows 8.1 エンタープライズ

内部ネットワークには、次の表に示すシステムが含まれています。

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

Litware はサードパーティの電子メール システムを使用します。

クラウドインフラストラクチャ

Litware は最近、すべてのユーザーを対象とした Microsoft 365 サブスクリプション ライセンスを購入しました。

Microsoft Azure Active Directory (Azure AD) Connect がインストールされており、デフォルトの認証設定を使用します。ユーザー アカウントはまだ Azure AD に同期されていません。

次の表に示す Microsoft 365 ユーザーとグループがあります。

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

計画された変更

Litware は次の変更を実装する予定です。

電子メール システムを Microsoft Exchange Online に移行する

Azure AD Privileged Identity Management を実装する

セキュリティ要件

Litware では、次のセキュリティ要件が特定されています。

すべての Azure AD ユーザー アカウントを含む Group2 という名前のグループを作成しま

ず。Group2 は次のことに慣れます。

Windows Analytics への制限付きアクセスを提供する

Azure Information Protection ポリシーをパイロットに適用するために使用される Group3 という名前のグループを作成します。

ユーザー。Group3 にはユーザー アカウントのみを含める必要があります

Azure Advanced Threat Protection (ATP) を使用して、フォレストを標的とするセキュリティの脅威を検出します。

Active Directory からロックアウトされたユーザーが Azure AD および Active Directory にサインインできないようにする

User1 に対するコンプライアンス管理者ロールの永続的適格割り当てを実装します。

ドメインに参加しているサーバー上で Windows Defender と Windows Defender ATP を統合する

デフォルトでゲスト ユーザー アカウントの Azure リソースへのアクセスを禁止する

ドメインに参加しているすべてのコンピューターが Azure AD に登録されていることを確認する

多要素認証 (MFA) の要件

Microsoft Office 365 と Azure のセキュリティ機能は、パイロット Azure ユーザー アカウントを使用してテストされます。

MFA をテストするための次の要件を特定します。

パイロット ユーザーは、シカゴ オフィスの内部ネットワークからサインインしない限り、MFA を使用する必要があります。

MFA はシカゴ オフィスの内部ネットワークでは使用しないでください。

認証試行が疑わしい場合は、ユーザーの場所に関係なく、MFA を使用する必要があります。

正当な認証試行の中断は最小限に抑える必要があります

一般的な要件

Litware は、Active Directory フォレストへの追加のサーバーとサービスの展開を最小限に抑えたいと考えています。

最新問題: 259

Microsoft 365 サブスクリプションをお持ちです。監査が有効になっています。

User1 という名前のユーザーは、Group1 という名前の動的セキュリティ グループのメンバーです。

User1 が Group1 のメンバーではなくなっていることがわかります。

User1 が Group1 から削除された理由を特定するには、監査ログを検索する必要があります。

検索ではどの 2 つのアクションを使用する必要がありますか? 回答するには、回答領域で適切なアクティビティを選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Search
Results

Clear

Activities

Show results for all activities

Date ▼ IP address User Activity Item

✕ Clear all to show results for all activities

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal


Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal


Microsoft

Answer:

Search Clear **Results** Microsoft

Activities

Date ▼ IP address User Activity Item

Show results for all activities

✕ Clear all to show results for all activities

Search

User administration activities

- Added user
- Deleted user
- Set license properties
- Reset user password
- Changed user password
- Changed user license
- Updated user
- Set property that forces user to change password

Azure AD group administration activities

- Added group
- Updated group
- Deleted group
- Added member to group
- Removed member from group

Application administration activities

- Added service principal
- Removed a service principal from the directory
- Set delegation entry
- Removed credentials from a service principal
- Added delegation entity
- Added credentials to a service principal

参照：

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

最新問題: 260

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 サブスクリプションがあります。Site1 には、次の表に示すフォルダーが含まれています。

Name	File in folder
Folder1	File1
Folder2	File2

09:00 に、次の図に示すように、Policy1 という名前の Microsoft Cloud App Security ポリシーを作成します。

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

× App equals Microsoft SharePoint...

+

Apply to:
selected folders Currently supports Box, SharePoint, Dropbox, OneDrive.

Folder1 (Microsoft SharePoint Online) ×

[Add more folder\(s\)](#)

Apply to:
all file owners

Inspection method
None Alerts

Create an alert for each matching file [Restore default settings](#)

Daily alert limit 5

Send alert as email ⓘ

Send alert as text message ⓘ

[Save as default settings](#)

Send alerts to Flow [Create a playbook in Flow](#)

Policy1 を作成した後、次の表に示すようにファイルを Site1 にアップロードします。

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
File1 triggers an alert from Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>

参照：

<https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

最新問題: 261

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー閲覧者の役割はどのユーザーにも割り当てられていません。
User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないよ
うにする解決策を推奨する必要があります。

解決策: コンプライアンス マネージャー閲覧者の役割を User1 に割り当てることをお勧めしま
す。

これは目標を達成していますか?

A. いいえ

B. はい

Answer: A ([メッセージを残す](#))

最新問題: 262

Azure AD Connect 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: 正しく選択するたびに 1 ポイントの価値があります。

User sign-in settings:

	▼
Password Synchronization with single-sign on	
Pass-through authentication with single sign-on	
Federation with Active Director Federation Services (ADFS)	

Device options:

	▼
Hybrid Azure AD Join	
Enable Device writeback	
Disable Device writeback	

Answer:

ADGroup1:

None	v
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

ADGroup2:

None	v
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

説明

User sign-in settings:

Microsoft	▼
Password Synchronization with single sign on	
Pass-through authentication with single sign-on	
Federation with Active Director Federation Services (AD FS)	

Device options:

	▼
Hybrid Azure AD Join	
Enable Device writeback	
Disable Device writeback	

最新問題: 263

Microsoft 365 サブスクリプションをお持ちです。

次の図に示すように、Retention1 という名前の保持ポリシーを作成しています。

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... ▾ 2 years ▾

Retain the content based on when it was last modified ▾ ⓘ

Do you want us to delete it after this time? ⓘ

Yes No

No, just delete content that's older than ⓘ

1 years ▾

Need more options?

Use advanced retention settings ⓘ

Back **Next** Cancel

Retention1 を SharePoint サイトと OneDrive アカウントに適用します。

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

注: 正しく選択するたびに 1 ポイントの価値があります。

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained	▾
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	▾
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

Answer:



If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained	▼
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	▼
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

最新問題: 264

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 サブスクリプションがあります。Site1 には、次の表に示すフォルダーが含まれています。

Name	File in folder
Folder1	File1
Folder2	File2

09:00 に、次の図に示すように、Policy1 という名前の Microsoft Cloud App Security ポリシーを作成します。

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

× App equals Microsoft SharePoint...
+

Apply to:

selected folders

Currently supports Box, SharePoint, Dropbox, OneDrive.

Folder1 (Microsoft SharePoint Online) ×

Add more folder(s)

Apply to:

all file owners

Microsoft
Inspection method

None

Alerts

Create an alert for each matching file [Restore default settings](#)

Daily alert limit 5

Send alert as email ⓘ

Send alert as text message ⓘ

[Save as default settings](#)

Send alerts to Flow

[Create a playbook in Flow](#)

Policy1 を作成した後、次の表に示すようにファイルを Site1 にアップロードします。

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

説明

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

参照 :

<https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

最新問題: 265

次のものを含むオンプレミスの Hyper-V インフラストラクチャがあります。

Active Directory ドメイン

Server1 という名前のドメイン コントローラー

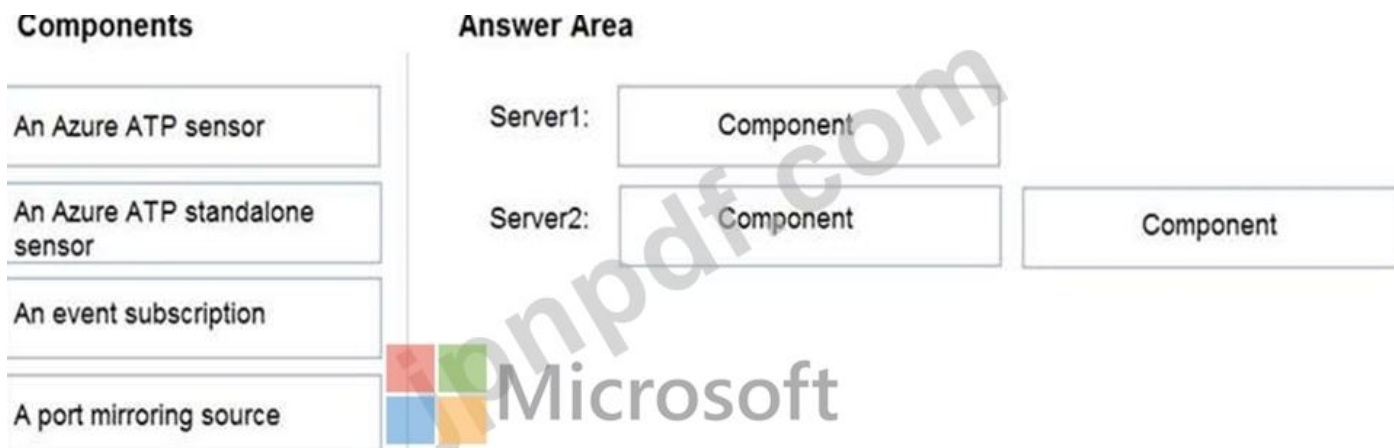
Server2 という名前のメンバー サーバー

セキュリティ ポリシーでは、Server1 がインターネットに接続できないように指定されています。Server2 はインターネットに接続できます。

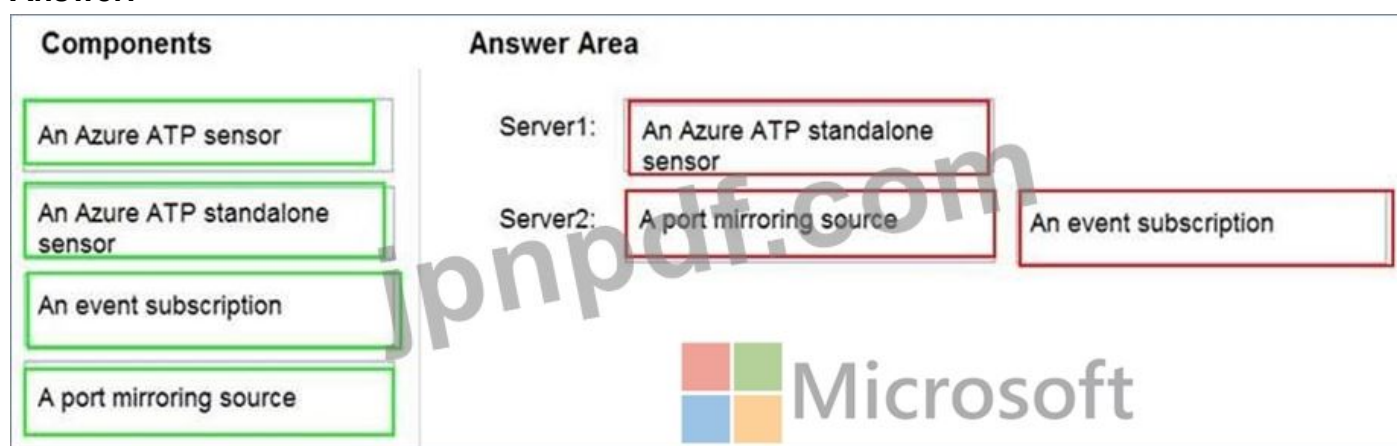
ドメインのセキュリティを監視するには、Azure Advanced Threat Protection (ATP) を実装する必要があります。

各サーバーで何を構成する必要がありますか? 答えるには、適切なコンポーネントを正しいサーバーにドラッグします。各コンポーネントは 1 回だけ使用することも、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、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題: 266

User1、User2、User3 という 3 人のユーザーが含まれる Microsoft 365 E5 テナントがあります。次の表に示すように、ユーザーに役割または役割グループを割り当てる必要があります。

User	Role or role group
User1	SharePoint admin
User2	Data Investigator
User3	User admin

各ユーザーに役割または役割グループを割り当てるには何を使用する必要がありますか？ 回答するには、適切なツールを正しい役割または役割グループにドラッグします。各ツールは 1 回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

Tools	Answer Area
Azure Defender for Servers	User1: Tool
Compliance Manager	User2: Tool
Microsoft 365 admin center	User3: Tool
Security & Compliance admin center	
Trust Center	

Answer:

Tools	Answer Area
Azure Defender for Servers	User1: Microsoft 365 admin center
Compliance Manager	User2: Security & Compliance admin center
Microsoft 365 admin center	User3: Microsoft 365 admin center
Security & Compliance admin center	
Trust Center	

説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーション、チャットまたはテキスト メッセージ 説明が自動的に生成

User1:	Microsoft 365 admin center
User2:	Security & Compliance admin center
User3:	Microsoft 365 admin center

参照：

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-com>

最新問題: 267

次の図に示すように、ネットワークには、Azure Active Directory (Azure AD) と同期するオンプレミスの Active Directory ドメインが含まれています。

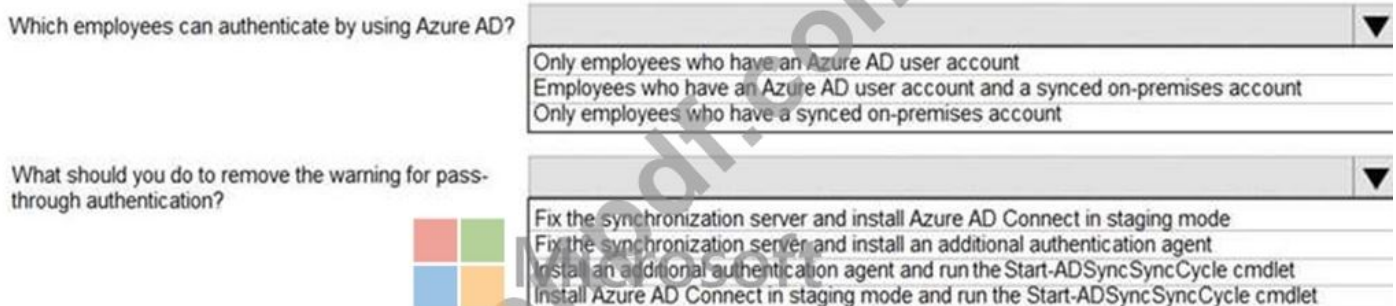


同期スケジュールは次のように構成されています。



ドロップダウンメニューを使用して、図に示されている情報に基づいて各質問に答える回答の選択肢を選択します。

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:

Which employees can authenticate by using Azure AD?

- Only employees who have an Azure AD user account
- Employees who have an Azure AD user account and a synced on-premises account
- Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

- Fix the synchronization server and install Azure AD Connect in staging mode
- Fix the synchronization server and install an additional authentication agent
- Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
- Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

最新問題: 268

Site1 という名前の Microsoft SharePoint Online サイトと、次の表のデータ損失防止 (DIP) ポリシーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

The DLP rules are configured as shown in the following table.

Rule	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	On	Tip 1	Enabled
Rule2	On	Tip 2	Disabled
Rule3	On	Tip 3	Enabled
Rule4	On	Tip 4	Disabled

すべてのポリシーが Site1 に割り当てられます。

ユーザーがすべてのルールに一致するドキュメントを Site1 にアップロードした場合、そのユーザーにヒント 2 のポリシー ヒントが表示されるようにする必要があります。

あなたは何をするべきか？

- A. Rule2 に一致する場合、ポリシーの追加処理を防止します。
- B. DLP2 の優先度を 3 に変更します。
- C. Rule1 に一致する場合、ポリシーの追加処理を有効にします。
- D. DLP2 の優先度を 0 に変更します。

Answer: [\(解答を表示する\)](#)

最新問題: 269

Microsoft 365 サブスクリプションでいくつかの Advanced Threat Protection (ATP) ポリシーを構成します。

User1 という名前のユーザーが脅威管理ダッシュボードで ATP レポートを表示できるようにする必要があります。

User1 に必要なロール権限を提供するのはどのロールですか？

- A. セキュリティリーダー
- B. メッセージセンター リーダー

C. コンプライアンス管理者

D. 情報保護管理者

Answer: A ([メッセージを残す](#))

参照 :

<https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are-needed-to-view-the-atp-reports>

最新問題: 270

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

Name	Permanent role assignment
User1	Global Administrator
User2	Security Administrator
User3	Privileged Role Administrator
User4	None

ユーザー管理者ロールは、次の図に示すように、Azure AD Privileged Identity Management (PIM) で構成されます。

User Administrator



Save Discard

Activations

Maximum activation duration (hours) ⓘ

4

Notifications

Send email notifying admins of activation ⓘ

Enable Disable

Incident/Request ticket

Require incident/request ticket number during activation ⓘ

Enable Disable

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation ⓘ

Enable Disable

Require approval

Require approval to activate this role ⓘ

Enable Disable



If no approvers are selected, Privileged Role Administrators will be approvers by default.

SELECTED APPROVER

ACTION

No results

Select approvers

No approver selected



User4 にユーザー管理者ロールの資格を与えます。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input type="radio"/>
User2 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input type="radio"/>
User3 receives an email notification when User4 requests activation of the User Administrator role.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>
User3 receives an email notification when User4 requests activation of the User Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>

最新問題: 271

contoso.com という名前の Microsoft Azure Active Directory (Azure AD) テナントがあり、次の表に示すユーザーが含まれています。

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

次の設定を持つ Azure AD Identity Protection サインイン リスク ポリシーを作成して適用します。

割り当て: グループ 1 を含む、グループ 2 を除外


条件: サインインリスクが低以上

アクセス: アクセスを許可、パスワード多要素認証を要求

ポリシーが User1 と User2 にどのような影響を与えるかを特定する必要があります。

各ユーザーが匿名 IP アドレスからサインインするとどうなりますか? 回答するには、回答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。

User1:  Microsoft ▼


Blocked
Can sign in without MFA
Prompted for MFA

User2: ▼

Blocked
Can sign in without MFA
Prompted for MFA

Answer:

User1: ▼

 Microsoft
Blocked
Can sign in without MFA
Prompted for MFA


User2: ▼

Blocked
Can sign in without MFA
Prompted for MFA

説明

User1:

	▼
Blocked	
Can sign in without MFA	
Prompted for MFA	



User2:

	▼
Blocked	
Can sign in without MFA	
Prompted for MFA	

有効な **MS-500** 問題集は GoShiken.com が提供された合格しやすい MS-500 試験問題集！
 GoShiken.com が最新の **MS-500** 試験問題集を提供しています。GoShiken.com MS-500 試験問題は最新で、解答が正確でございます。最新の GoShiken.com MS-500 問題集をゲットする人はこちら: <https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (**32930%OFF**問題集 溶と正解付きで **30%**w特別割引コード: **Freepdfdumps**)

最新問題: 272

100 人のユーザーを含む Microsoft 365 サブスクリプションがあります。
 サブスクリプションの Microsoft セキュア スコアは、次の図に示されています。
 ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
 注: 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

If you set Enable Security defaults to Yes in Azure Active Directory (Azure AD), Microsoft Secure Score will increase by [answer choice].

If you enable multi-factor authentication (MFA) for 30 users, Microsoft Secure Score will increase by [answer choice].



Answer:

以下の答えを参照してください。

説明

下の画像で答えてください。



最新問題: 273

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

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

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

サブスクリプション内のすべてのユーザーがコンプライアンス マネージャー レポートにアクセスできることがわかります。

コンプライアンス マネージャー閲覧者の役割はどのユーザーにも割り当てられていません。

User5 という名前のユーザーがコンプライアンス マネージャー レポートにアクセスできないようにする解決策を推奨する必要があります。

解決策: コンプライアンス マネージャー閲覧者の役割を User1 に割り当てることをお勧めします。

これは目標を達成していますか?

A. はい

B. いいえ

Answer: ([解答を表示する](#))

Valid MS-500 Dumps shared by GoShiken.com for Helping Passing MS-500 Exam!

GoShiken.com now offer the **newest MS-500 exam dumps**, the GoShiken.com MS-500 exam **questions have been updated** and **answers have been corrected** get the **newest**

GoShiken.com MS-500 dumps with Test Engine here:

<https://www.goshiken.com/Microsoft/MS-500-mondaishu.html> (329 Q&As Dumps, 30%OFF

Special Discount: **Freepdfdumps**)