

Microsoft.MS-102J.v2026-10-06.q284

試験コード：	MS-102J
試験名称：	Microsoft 365 Administrator (MS-102日本語版)
認証ベンダー：	Microsoft
無料問題の数：	284
バージョン：	v2026-10-06
ページの閲覧量：	111
問題集の閲覧量：	3307
https://www.jpnsshiken.com/shiken/Microsoft.MS-102J.v2026-10-06.q284.html	

質問: 1

Microsoft 365 E5 サブスクリプションをお持ちです。メールが有効な連絡先を作成する必要があります。どのポータルを使用すればよいですか？

- A. Exchange 管理センター
- B. Intune 管理センター
- C. Microsoft Purview コンプライアンス ポータル
- D. Microsoft Entra 管理センター

正解: ([正解を表示します](#))

質問: 2

技術要件を満たすように Office on the Web を構成する必要があります。
あなたは何をすべきか？

- A. グローバル リーダー ロールを User1 に割り当てます。
- B. SharePoint Online および OneDrive で Office ファイルの秘密度ラベルを有効にします。
- C. 機密ラベルを適用する自動ラベル付けポリシーを構成します。
- D. Office アプリ管理者の役割を User1 に割り当てます。

正解: ([正解を表示します](#))

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide>

質問: 3

EU PII データの技術要件を満たす必要があります。
何を作成する必要がありますか？

- A. Security & からの保持ポリシー。コンプライアンス管理センター。
- B. Exchange 管理センターからの保持ポリシー
- C. Exchange 管理センターからのデータ損失防止 (DLP) ポリシー
- D. セキュリティとセキュリティのデータ損失防止 (DLP) ポリシー。コンプライアンス管理センター

正解: ([正解を表示します](#))

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies> EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

質問: **4**

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、サービス正常性の概要が表示されます。

Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

 Report an issue  Customize



Active issues

Issue title	Affected service	Issue type
> Microsoft service health (6)		

Issues in your environment that require action (0)

Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

Service	Status
Exchange Online	 3 advisories
Microsoft 365 suite	 2 advisories
Microsoft Teams	 1 advisory





User1 という名前のユーザーがサービスの健全性の問題を調査するためのアドバイザリを表示できることを確認する必要があります。

User1 にどの役割を割り当てるべきですか？

- A. メッセージ センター リーダー
- B. レポートリーダー
- C. サービス サポート管理者
- D. コンプライアンス管理者

正解: B (コメントを发表する)

Service Support admin

Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:

- Open and manage service requests
- View and share message center posts
- Monitor service health

Incorrect:

* Message center reader

Assign the Message center reader role to users who need to do the following:

- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Microsoft Entra ID services, such as users and groups

* Reports reader

Assign the Reports reader role to users who need to do the following:

- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Microsoft Entra ID
- View data returned by Microsoft Graph reporting API

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

質問: 5

貴社は、comoso.onmicrosoft.com という名前の Microsoft Entra テナントを所有しており、そのテナントには次の表に示すユーザーが含まれています。

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

以下の管理タスクを実行できるユーザーを特定する必要があります。

- * ユーザー4のパスワードをリセットします。
- * User4のマネージャー属性の値を変更します。

各タスクについて、どのユーザーを指定すべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Reset the password of User4:

User1 and User3 only

User1 only

User2 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Modify the value for the manager attribute of User4:

User3 only

User2 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

正解:



Reset the password of User4:

User1 and User3 only
User1 only
User2 only
User1 and User2 only
User1 and User3 only
User1, User2, and User3

Modify the value for the manager attribute of User4:

User3 only
User2 only
User3 only
User1 and User3 only
User2 and User3 only
User1, User2, and User3

Explanation:

Answer Area

Reset the password of User4:

User1 and User3 only

Modify the value for the manager attribute of User4:

User3 only



質問: 6

お客様のオンプレミスネットワークには、Contoso.com という名前の Active Directory ドメインと、macOS、Windows 8.1、Windows 10、または Windows 11 のいずれかを実行する 500 台のデバイスが含まれています。すべてのデバイスは、Microsoft Endpoint Configuration Manager を使用して管理されています。このドメインは、Microsoft Entra ID (Microsoft Entra ID) と同期しています。Microsoft 365 E5 サブスクリプションを導入し、共同管理を有効にする予定です。導入後、どのデバイスを共同管理できるようになりますか？

- A. Windows 11。Windows 10、およびWindows 8.1のみ
- B. Windows 11、Windows 10～Windows 8.1、macOS
- C. Windows 11のみ
- D. Windows 11およびmacOSのみ
- E. Windows 11 および Windows 10 のみ

正解: (正解を表示します)

質問: 7

御社はモントリオール、シアトル、ニューヨーク市にオフィスを構えていますね。お客様は、以下の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションをご利用されています。

Name	Email address
User1	user1@contoso.com
User2	user2@contoso.com

The offices have the IP addresses shown in the following table.

Office	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



Microsoft Defender for Cloud Apps から、次の図に示すアクティビティ 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 ⓘ

Activities matching all of the following ✕ [Edit and preview results](#)

✕

IP address ▼ Raw IP address ▼ equals ▼ ✖

OR ✚

✕

Activity type ▼ equals ▼ Download ▼

✕

User ▼ From group ▼ equals ▼

✕

Application (Defender for Cloud Apps) ▼ as Actor only ▼ ⓘ

[+ Add a filter](#)

Alerts

☒ Create an alert for each matching event with the policy's severity

[Save as default settings](#) [Restore default settings](#)

☐ Send alert as email ⓘ

Daily alert limit per policy ▼

[Create a playbook in Power Automate](#)



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

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
At the Montreal office, if User1 downloads 40 files in 45 seconds, an alert will be created.	☐	☒
At the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.	☒	☐
At the New York City office, if User1 downloads 40 files in 10 seconds, an alert will be created.	☐	☒

正解:

Statements	Yes	No
At the Montreal office, if User1 downloads 40 files in 45 seconds, an alert will be created.	☐	☒
At the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.	☒	☐
At the New York City office, if User1 downloads 40 files in 10 seconds, an alert will be created.	☐	☒

Explanation:

Statement

Answer

At the Montreal office, if User1 downloads 40 files in 45 seconds, an alert will be created.

No

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

Yes

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

No

The policy is a Microsoft Defender for Cloud Apps activity policy configured for Repeated activity by a single user. The threshold is 30 repeated activities within 1 minute, and the activity type is Download.

Microsoft documents that activity policies can be configured for repeated activity, including a minimum activity count and a timeframe, and that activity type filters are used to match app activities such as downloads.

The decisive filter is the Raw IP address condition: 10.10.0.0/24 OR 194.25.2.0/24. Defender for Cloud Apps supports filtering by raw IP address, meaning activities performed from or by those raw IP addresses. For cloud activity, the relevant source address is the externally visible address reported by the cloud app.

Microsoft warns that internal IP addresses audited by connected cloud apps should not be confused with the internal source-network IPs of user devices, because cloud applications are not exposed to those device internal IPs.

Montreal does not match because its public NAT segment is 190.15.1.0/24, not 10.10.0.0/24 or 194.25.2.0/24.

Seattle does match because its public NAT segment is 194.25.2.0/24, and one download per second for two minutes exceeds 30 downloads in one minute. New York does not match because its public NAT segment is 198.35.3.0/24.

質問: 8

あなたは、User1という名前のユーザーを含むMicrosoft 365サブスクリプションを所有しています。

User1がセキュリティとコンプライアンス管理センターからMicrosoft 365の監査ログを検索できることを確認する必要があります。

User1にはどの役割を割り当てるべきですか？

A. セキュリティとコンプライアンス管理センターの閲覧専用監査ログ

B. Exchange 管理センターの閲覧専用監査ログ

C. Microsoft Entra ID 管理センターのセキュリティリーダー

D. セキュリティとコンプライアンス管理センターのセキュリティリーダー

正解: **B** ([コメントを發表する](#))

Reference:

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

質問: **9**

Windows 10 デバイスのコンプライアンス要件を満たす必要があります。

Intune 管理センターから何を作成する必要がありますか？

A. アプリ構成ポリシー

B. デバイスのコンプライアンス ポリシー

C. デバイス構成プロファイル

D. アプリケーションポリシー

正解: ([正解を表示します](#))

質問: **10**

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

Microsoft 365 サブスクリプションをお持ちです。

ドメインをサブスクリプションと同期する必要があります。ソリューションは次の要件を満たしている必要があります。

* オンプレミスの Active Directory パスワードの複雑さのポリシーを適用する必要があります。

* ユーザーは Microsoft Entra セルフサービス パスワード リセット (SSPR) を使用できる必要があります。

何を使うべきでしょうか？

A. パスワードハッシュ同期

B. Microsoft Entra ID 保護

C. Microsoft Entra シームレス シングル サインオン (Microsoft Entra シームレス SSO)

D. パススルー認証

正解: ([正解を表示します](#))

質問: **11**

注: このセクションには、同じシナリオと問題に関する 1 つ以上の質問セットが含まれています。各質問には、問題に対する独自の解決策が提示されています。解決策が、指定された目標を満たしているかどうかを判断する必要があります。

セット内の複数のソリューションが問題を解決できる可能性があります。また、セット内のどのソリューションも問題を解決できない可能性もあります。

このセクションの質問に回答した後は、戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 E5 サブスクリプションがあり、Microsoft Defender for Office 365 を使用しています。

スパム、フィッシング、マルウェアから保護するために、バランスの取れたベースライン保護プロファイルを適用する脅威ポリシーを実装する必要があります。

解決策: フィッシング対策ポリシーを作成します。

これは目標を満たしていますか？

A. いいえ

B. はい

正解: **A** ([コメントを發表する](#))

質問: 12

Microsoft 365 E5 サブスクリプションがあり、Microsoft Defender for Endpoint を使用しています。

Microsoft Defender for Endpoint を Microsoft Intune と統合します。

Microsoft Defender 脆弱性管理から、主要なセキュリティ推奨事項を確認し、Microsoft Edge (Chromium) を新しいバージョンに更新するという推奨事項を見つけます。

推奨事項に対応するには、Intune にセキュリティ タスクが追加されていることを確認する必要があります。

何をすべきでしょうか？

A. Microsoft Intune 管理センターから、Windows Autopatch を構成します。

B. Microsoft Defender ポータルから、[修復の要求] を選択します。

C. Microsoft Defender ポータルからインシデント通知ルールを追加します。

D. Microsoft Intune 管理センターから、セキュリティ ベースラインを構成します。

正解: **B** ([コメントを発表する](#))

質問: 13

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

組織内のすべてのデバイスは Microsoft Defender for Endpoint にオンボードされます。

過去 24 時間以内にデバイス上で悪意のあるアクティビティが検出された場合は、アラートが生成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. [高度なハンティング] から、クエリと検出ルールを作成します。

B. アラート キューから抑制ルールを作成し、アラートを割り当てます。

C. Microsoft Purview コンプライアンス ポータルから、監査ログ検索を作成します。

D. Microsoft Purview コンプライアンス ポータルから、データ損失防止 (DLP) ポリシーを作成します。

正解: ([正解を表示します](#))

質問: 14

Windows 10 バージョン 2004 がプレインストールされている新しいコンピューターを購入するとします。

コンピューターが最新であることを確認する必要があります。ソリューションでは、インストールされる更新プログラムの数を最小限に抑える必要があります。

コンピューターで何をすればいいですか？

A. バージョン 2004 以降にリリースされたすべての機能更新プログラムと、最新の品質更新プログラムのみをインストールします。

B. バージョン 2004 以降にリリースされたすべての機能更新プログラムと、バージョン 2004 以降にリリースされたすべての品質更新プログラムのみをインストールします。

C. 最新の機能更新プログラムと、バージョン 2004 以降にリリースされたすべての品質更新プログラムをインストールします。

D. West 機能更新プログラムと最新の品質更新プログラムのみをインストールします。

正解: ([正解を表示します](#))

質問: 15

Microsoft Intune を使用する Microsoft 365 E5 サブスクリプションを持っています。

携帯電話からサービス正常性アラートにアクセスする必要があります。

何をえばいいのでしょうか？

A. Intune ポータル サイト

B. Microsoft 365 管理モバイル アプリ

C. Intune アプリ

D. Microsoft Authenticator アプリ

正解: B (コメントを发表する)

質問: 16

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

User1 は、午前中に 1,000 件の電子メール メッセージを送信した後、追加の電子メールの送信がブロックされたと報告しました。次のことを特定する必要があります。

* User1 のブロックを解除できる管理者

* User1 がブロックされずに 1 日あたり少なくとも 2,000 件の電子メールを送信できるようにするには何を設定する必要がありますか? 何を識別する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Administrators: 

Admin2 only
Admin1 only
Admin2 only
Admin1 and Admin2 only
Admin2 and Admin3 only
Admin1, Admin2, and Admin3

Settings: 

Anti-spam
Anti-spam
Anti-phishing
Anti-malware
Advanced delivery
Enhanced filtering

正解:

Answer Area

Administrators: 

Admin2 only
Admin1 only
Admin2 only
Admin1 and Admin2 only
Admin2 and Admin3 only
Admin1, Admin2, and Admin3

Settings: 

Anti-spam
Anti-spam
Anti-phishing
Anti-malware
Advanced delivery
Enhanced filtering

Explanation:

	Catalog	
	App governance	
	Audit	
	Content search	
	Communication compliance	
	Data loss prevention	
	eDiscovery	▼
	Data lifecycle management	▼
	Information protection	
	Information barriers	▼
	Insider risk management	
	Records management	
	Privacy risk management	▼
	Subject rights requests	

正解:

Answer Area

	
	Home
	Compliance Manager
	Data classification
	Data connectors
	Reports
Solutions	
	Catalog
	App governance
	Audit
	Content search
	Communication compliance
	Data loss prevention
	eDiscovery
	Data lifecycle management
	Information protection

	Information barriers	▼
	Insider risk management	
	Records management	
	Privacy risk management	▼
	Subject rights requests	

Explanation:

Answer Area



Microsoft

Microsoft Purview

Home

Compliance Manager

Data classification ✓

Data connectors

Reports

Solutions

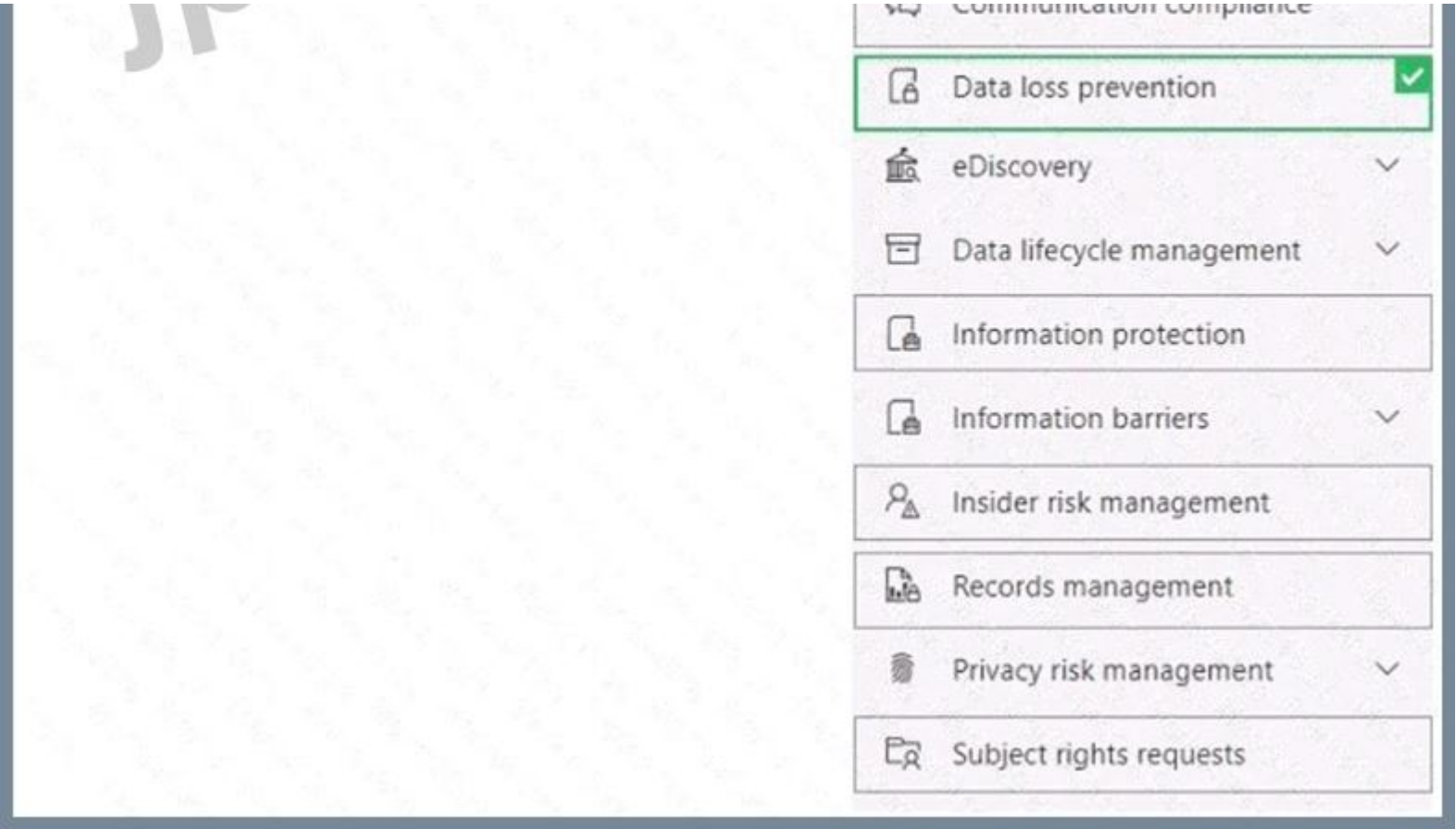
Catalog

App governance

Audit

Content search

Communication compliance



質問: 18

Microsoft 365 テナントには、Group1 と Group2 という名前の 2 つのグループが含まれています。
Microsoft Teamsを使用して、グループ1のメンバーとグループ2のメンバー間の通信を防止する必要があります。このソリューションは、規制要件に準拠し、テナント内の他のユーザーに影響を与えてはなりません。
何を使うべきでしょうか？

- A. コミュニケーションコンプライアンスポリシー
- B. モデレートされた配信グループ
- C. 情報障壁
- D. Microsoft Entra ID(Microsoft Entra ID)の管理者ユニット

正解: (正解を表示します)

質問: 19

あなたは Contoso, Ltd. という名前の会社で働いています。
Contoso には、次の表に示す DNS ドメインを使用するように構成された Microsoft 365 サブスクリプションがあります。
Contoso は Fabrikam, Inc. という会社を買収します。
Contoso は、次のドメインを Microsoft 365 サブスクリプションに追加する予定です。

- *fabrikam.com
- * east.fabrikam.com
- *west.contoso.com

新しいドメイン内のデバイスが自動検出を使用して登録できることを確認する必要があります。
確認する必要があるドメインの数はいくつですか?また、追加する必要があるエンタープライズ登録 DNS レコード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。

Answer Area



Microsoft

Domains:

3	▼
1	
2	
3	

Enterpriseregistration DNS records:

3	▼
1	
2	
3	

Answer Area



Microsoft

Domains:

3	▼
1	
2	
3	

Enterpriseregistration DNS records:

3	▼
1	
2	
3	

Explanation:

Answer Area



Microsoft

Domains: 3 ▼

Enterpriseregistration DNS records: 3 ▼

質問: 20

セキュリティとセキュリティを使用する Microsoft 365 サブスクリプションを持っています。コンプライアンス保持ポリシー。すべてのエグゼクティブユーザーに割り当てられる保持ポリシーに保存ロックを実装します。保持ポリシーに対して実行できる 2 つのアクションはどれですか?それぞれの正解は完全な解決策を示します。
注: 正しい選択はそれぞれ 1 ポイントの価値がありますか?
A. ポリシーから場所を削除します

- B. ポリシーを無効にします
- C. 保険期間を短縮します
- D. ポリシーの期間を延長します
- E. ポリシーに場所を追加します

正解: ([正解を表示します](#))

質問: 21

貴社はオンプレミスサーバーとMicrosoft Entraテナントを所有しています。

数か月前、すべてのサーバーにMicrosoft Entra Connect Healthエージェントがインストールされました。

あなたはすべてのサーバーの稼働状況を定期的に確認します。

最近、Server1という名前のサーバーの稼働状況を確認しようとしたところ、そのサーバーがMicrosoft Entra Connect同期サーバーのリストに表示されていないことがわかりました。

別の管理者がServer1をリストから削除したのではないかと疑っている。

Server1の稼働状況を確認できることを確認する必要があります。

目標を達成するための2つの方法は何ですか？それぞれの正解は完全な解決策を示しています。

注：正解ごとに1ポイントが加算されます。

- A. Azure Cloud Shell から Connect-Microsoft Entra ID コマンドレットを実行します。
- B. Server1 から、Microsoft Entra Connect Health Services のスタートアップの種類を自動に変更します。
- C. Server1 から、Microsoft Entra Connect Health エージェントを再インストールします。
- D. Server1 から、Microsoft Entra Connect Health Services の起動タイプを 自動 (遅延開始)」に変更します。
- E. Windows PowerShell から、Rejister-ArureADConnectHealthsyncAgent コマンドレットを実行します。

正解: ([正解を表示します](#))

質問: 22

Microsoft 365 E5 テナントがあります。

クレジット カード番号を含むドキュメントがテナントに追加されるときに、ドキュメントが暗号化されていることを確認する必要があります。

どのポリシーを使用する必要がありますか？

- A. 保持ポリシー
- B. 保持ラベル ポリシー
- C. 自動ラベル付けポリシー
- D. インサイダー リスク ポリシー

正解: C ([コメントを發表する](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

質問: 23

あなたは、User1という名前のユーザーを含むMicrosoft 365サブスクリプションを所有しています。

ユーザー1は、以下のタスクを実行するために管理者権限が必要です。

Microsoft Exchange Online の設定を管理します。

Microsoft 365グループを作成します。

ユーザー1には管理者権限を8時間のみ付与し、役割割り当てを行う前に承認が必要となるようにする必要があります。

何を使うべきでしょうか？

- A. zure AD Identity Protection
- B. Microsoft Entra 認証済みID
- C. 条件付きアクセス
- D. Microsoft Entra ID 特権ID管理(PJM)

正解: (正解を表示します)

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Microsoft Entra ID and Azure resources
Assign time-bound access to resources using start and end dates
Require approval to activate privileged roles
Enforce multi-factor authentication to activate any role
Use justification to understand why users activate
Get notifications when privileged roles are activated
Conduct access reviews to ensure users still need roles
Download audit history for internal or external audit
Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

質問: 24

Microsoft Defender for Endpoint が Microsoft Endpoint Manager と統合された Microsoft 365 E5 サブスクリプションを持っています。

デバイスは、Microsoft Defender for Endpoint を使用してオンボードされます。

Microsoft Defender for Endpoint によって計算されたマシン リスク スコアの結果に基づいてデバイスをブロックすることを計画しています。

最初に何を作成する必要がありますか？

- A. デバイスの設定ポリシー
- B. デバイスのコンプライアンス ポリシー
- C. 条件付きアクセス ポリシー
- D. エンドポイントの検出および応答ポリシー

正解: B (コメントを发表する)

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure>

質問: 25

貴社はcontoso.onmicrosoft.comという名前のMicrosoft Entraテナントを所有しています。

レジストラからcontoso.comという名前のドメインを購入し、必要なDNSレコードをすべて追加します。

User1という名前のユーザーアカウントを作成します。User1はuser1@contoso.onmicrosoft.comとしてサインインするように構成されています。

User1がuser1@contoso.comとしてサインインするように設定する必要があります。

どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。

Actions

Run Update-MgDomain -DomainId contoso.com.
Modify the email address of User1.
Add contoso.com as a SAN for an X.509 certificate.
Add a custom domain name.
Verify the custom domain.
Modify the username of User1.

Answer Area



正解:

Actions

Run Update-MgDomain -DomainId contoso.com.
Modify the email address of User1.
Add contoso.com as a SAN for an X.509 certificate.
Add a custom domain name.
Verify the custom domain.
Modify the username of User1.

Answer Area

Add a custom domain name.
Verify the custom domain.
Modify the username of User1.



Explanation:

Actions

Run Update-MgDomain -DomainId contoso.com.
Modify the email address of User1.
Add contoso.com as a SAN for an X.509 certificate.



Answer Area

1	Add a custom domain name.
2	Verify the custom domain.
3	Modify the username of User1.



質問: 26

Windows 10 デバイスが 2,500 台あり、Microsoft 365 E5 テナントには User1 と User2 という 2 人のユーザーが含まれています。これらのデバイスは Microsoft Intune に登録されていません。Microsoft Endpoint Manager では、デバイスの制限は、次の図に示すように構成されます。

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

Microsoft Entra ID (Microsoft Entra ID) では、デバイス設定は次の図に示すように構成されます。

Users may register their devices with Azure AD

All

None

Learn more on how this setting works

Require Multi-Factor Auth to join devices

Yes

No

Maximum number of devices per user

5

Microsoft Endpoint Manager から、User2 をデバイス登録マネージャー (DEM) として追加します。
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	☐	☐
User1 can join only five devices to Azure AD.	☐	☐
User2 can enroll all the devices in Intune.	☐	☐

正解:
Answer Area

Statements

Yes

No

User1 can enroll only five devices in Intune.	☐	☒
User1 can join only five devices to Azure AD.	☐	☒
User2 can enroll all the devices in Intune.	☒	☐

Explanation:
Answer Area

Statements

Yes

No

User1 can enroll only five devices in Intune.	☐	☒
User1 can join only five devices to Azure AD.	☐	☒
User2 can enroll all the devices in Intune.	☒	☐

質問: 27

ネットワークには 3 つの Active Directory フォレストが含まれています。フォレスト間にはフォレスト信頼関係があります。

Microsoft Entraテナントを作成します

オンプレミスの Active Directory を Microsoft Entra テナントに同期する予定です。

同期ソリューションを推奨する必要があります。ソリューションでは、1 台のサーバーに障害が発生した場合でも、同期が可能な限り迅速に完了することを保証する必要があります。

推薦書には何を含めるべきでしょうか？

A. 3 つの Microsoft Entra Connect 同期サーバーとステージング モードの 1 つの Microsoft Entra Connect 同期サーバー

B. 3 つの Microsoft Entra Connect 同期サーバーとステージング モードの 3 つの Microsoft Entra Connect 同期サーバー

C. 6 台の Microsoft Entra Connect 同期サーバーとステージング モードの 3 台の Microsoft Entra Connect 同期サーバー

D. 1 台の Microsoft Entra Connect 同期サーバーとステージング モードの 1 台の Microsoft Entra Connect 同期サーバー

正解: ([正解を表示します](#))

質問: 28

Microsoft 365 サブスクリプションをお持ちです。

次の要件を満たすコンプライアンス ソリューションを構成する必要があります。

既存のデータサンプルに基づいて機密データを定義します

サンプルに一致するデータが Microsoft SharePoint または電子メール メッセージで外部に共有されるのを自動的に防止します。どの 2 つのコンポーネントを構成する必要がありますか?それぞれの正解は、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. トレーニング可能な分類子

B. 機密情報の種類

C. インサイダー リスク ポリシー

D. 適応ポリシーのスコープ

E. データ損失防止 (DLP) ポリシー

正解: ([正解を表示します](#))

A: Classifiers

This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.

Where you can use classifiers

Classifiers are available to use as a condition for:

Office auto-labeling with sensitivity labels

Auto-apply retention label policy based on a condition

Communication compliance

Sensitivity labels can use classifiers as conditions, see [Apply a sensitivity label to content automatically](#).

Data loss prevention

E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

質問: 29

Microsoft Defender for Office 365 を使用し、Mailbox1 という名前のメールボックスを含む Microsoft 365 サブスクリプションがあります。

Mailbox1 を使用して、フィルターされていない電子メール メッセージを収集および分析する予定です。

Mailbox1 に配信された受信メールに対して Defender for Office 365 が何もアクションを起こさないようにする必要があります。

あなたは何をするべきか？

- A. メールボックスを構成してください! SecOps メールボックスとして。
- B. Mailbox1 の保持ポリシーを構成します。
- C. メール フロー ルールを作成します。
- D. Mailbox1 に訴訟ホールドを設定します。

正解: [\(正解を表示します\)](#)

質問: 30

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

Microsoft Defender for Cloud Apps を展開し、Microsoft 365 を Defender for Cloud Apps に接続する予定です。

アプリコネクタを追加する際には、すべてのMicrosoft 365コンポーネントを有効にする必要があります。

まず最初に何をすべきでしょうか？

- A. クラウド検出を設定します。
- B. Defender for Cloud Apps のファイル監視を有効にします。
- C. Defender for Cloud AppsにAPIトークンを追加します。
- D. 条件付きアクセスアプリ制御を設定します。

正解: [\(正解を表示します\)](#)

The correct answer is B. Enable file monitoring for Defender for Cloud Apps . Microsoft's Microsoft 365 connector guidance states that when connecting Microsoft 365 to Defender for Cloud Apps, admins select the Microsoft 365 components to protect, and for maximum protection Microsoft recommends selecting all components. However, Microsoft explicitly notes that to enable protection for Microsoft 365 files, you must first enable Defender for Cloud Apps file monitoring under Settings > Cloud Apps > Files > Enable file monitoring . This makes option B the prerequisite action.

Do not select Add an API token . API tokens are commonly used for certain third-party app connectors, but Microsoft 365 connects through the built-in app connector flow and Microsoft 365 audit/API integration.

Cloud Discovery is for discovering cloud app usage from network logs, not enabling Microsoft 365 connector components. Conditional Access app control is for real-time session control and is not required before selecting Microsoft 365 connector components. Microsoft also states that Defender for Cloud Apps integrates directly with Microsoft 365 audit logs and that Microsoft 365 components are selected during the app connector setup.

質問: 31

2,000 人を超えるゲスト ユーザーを含む Microsoft 365 サブスクリプションがあります。

ゲスト ユーザーがサブスクリプション内の Microsoft 365 グループに追加されるときに、そのメンバーシップがグループ所有者によって 30 日ごとに検証されるようにする必要があります。

何を設定すればよいのでしょうか？

- A. グループの有効期限ポリシー
- B. 条件付きアクセスポリシー
- C. アクセスレビュー
- D. 保持ポリシー

正解: C ([コメントを發表する](#))

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%**ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 32

Device1 という名前の Windows 11 デバイスが含まれる Microsoft 365 E5 サブスクリプションがあります。
Device1 は Microsoft Defender for Endpoint にオンボードされています。
Device1 が IP アドレス 131.107.10.15 に接続できないようにする必要があります。
Microsoft Defender エンドポイント設定では何を構成する必要がありますか? 回答するには、回答領域で適切な設定を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



質問: 33

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なくなり、これらの質問はレビュー画面に表示されなくなります。

ネットワークには Active Directory フォレストが含まれています。

Microsoft 365 を展開します。

ディレクトリ同期を実装する予定です。

同期された ID 用のセキュリティ ソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。

* Active Directory が使用できなくなった場合、ユーザーは Microsoft 365 サービスに対して正常に認証できる必要があります。

※ユーザーパスワードは10文字以上にしてください。

解決策: パスワード ハッシュ同期を実装し、Active Directory のデフォルト ドメイン ポリシーからパスワード設定を変更します。

これは目標を達成していますか？

A. はい

B. いいえ

正解: **A** ([コメントを发表する](#))

質問: **34**

Microsoft Intune を使用する Microsoft 365 E5 テナントがあります。

ユーザーがデバイスを Intune に登録するときに部門を選択できる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. スコープタグ

B. デバイス構成プロファイル

C. デバイスのカテゴリ

D. デバイスのコンプライアンス ポリシー

正解: **C** ([コメントを发表する](#))

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

質問: **35**

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザーが高リスクのサインイン イベントをトリガーした場合に、App1 という名前のアプリへのアクセスをブロックする条件付きアクセス ポリシーを作成します。

ユーザーが企業ネットワークからサインインする場合、不可能な移動による誤検知を減らす必要があります。

何を設定すればよいでしょうか？

A. ユーザーリスクポリシー

B. 名前付きの場所

C. 多要素認証 (MFA)

D. 除外グループ

正解: ([正解を表示します](#))

質問: **36**

Microsoft 365 E5 サブスクリプションをお持ちです。

次の要件を満たす、Policy という名前の条件付きアクセス ポリシーを作成する必要があります。

- * 高リスクユーザーに適用されます
- * 多要素認証 (MFA) が必要です

どの 2 つの設定を構成する必要がありますか? 回答するには、回答で適切な設定を選択します。注: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

Policy1

Assignments

Users ⓘ

All users

Target resources ⓘ

No target resources selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

正解:



New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Policy1 ✓

Assignments

Users ⓘ

All users

Target resources ⓘ

No target resources selected

Conditions ⓘ ✓

0 conditions selected

Access controls

Grant ⓘ ✓

0 controls selected

Session ⓘ

0 controls selected

Explanation:

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

Policy1 ✓

Assignments

Users ⓘ

All users

Target resources ⓘ

No target resources selected

Conditions ⓘ

0 conditions selected ✓

Access controls

Grant ⓘ

0 controls selected ✓

Session ⓘ

0 controls selected



質問: 37

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。

グループ メンバーシップを通じて Office 365 のライセンスを付与されているサブスクリプション内のすべてのユーザーを識別する必要があります。ソリューションには、ライセンスの割り当てに使用されたグループの名前が含まれている必要があります。

何をえばいいのでしょうか？

- A. Microsoft 365 管理センターのアクティブ ユーザー
- B. Microsoft Purview コンプライアンス ポータルのレポート
- C. Microsoft Entra 管理センターのライセンス ブレード
- D. Microsoft 365 管理センターのレポート

正解: (正解を表示します)

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center

Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	No ¹	No ¹	No ¹	No ¹
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports>

質問: 38

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	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

AU1 という名前の新しい管理単位を作成し、次の AU1 動的メンバーシップルールを構成します。

サブスクリプションには、次の表に示すロールの割り当てが含まれています。

Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

Statements	Yes	No
Admin1 can reset the password of User1.	☐	☐
Admin1 can reset the password of User2.	☐	☐
Admin2 can reset the password of User3.	☐	☐

正解:

Answer Area



Statements

Admin1 can reset the password of User1.

Admin1 can reset the password of User2.

Admin2 can reset the password of User3.

Yes

☒

No

☐

☐

☒

☒

☐

Explanation:

Admin1 can reset the password of User1: Yes

Admin1 has the User Administrator role within AU1. User1 is a member of Group1, which is included in AU1 ' s dynamic membership rule.

Admin1 can reset the password of User2: No

User2 is a member of both Group1 and Group2. However, User2's job title contains " Executive, " which excludes them from AU1 ' s dynamic membership rule. Therefore, Admin1 cannot reset User2 ' s password.

Admin2 can reset the password of User3: Yes

Admin2 has the Global Administrator role, which grants the ability to reset passwords for any user within the organization, including User3.

質問: 39

ホットスポット

あなたはMicrosoft 365のサブスクリプションをお持ちです。

あなたは組織向けに脅威管理ソリューションを計画しています。

ユーザーが以下の脅威の影響を受ける可能性を最小限に抑える必要があります。

悪意のあるコンテンツを含むファイルをMicrosoft SharePointで開く

電子メールメッセージにおけるなりすまし攻撃およびスプーフィング攻撃

Microsoft Defender XDR で作成すべきポリシーはどれですか？回答するには、回答領域で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Opening files in SharePoint that contain malicious content:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links

Impersonation and spoofing attacks in email messages:

▼

Anti-spam

Anti-Phishing

Safe Attachments

Safe Links



正解:

Answer Area

Opening files in SharePoint that contain malicious content:

Microsoft

▼

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Explanation:

Answer Area

Opening files in SharePoint that contain malicious content:

Microsoft

Impersonation and spoofing attacks in email messages:

▼

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

▼

Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

質問: 40
お客様は、以下の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションを所有しています。

Name	Email	Role
Admin1	Admin1@contoso.com	Password Administrator
Admin2	Admin2@contoso.com	Security Reader
Admin3	Admin3@contoso.com	User Administrator
User1	User1@contoso.com	None

あなたはMicrosoft Entra ID Protectionを使用しています。
「リスクのあるユーザーを検出したアラート」の設定では、以下の項目を設定します。

- * 受信者: Admin1
- * ユーザーリスクレベルが中以上で警告

ユーザー1がMicrosoft 365サービスにサインインすると、次の表に示すリスクレベルが検出されました。

Time	Detected risk level
1:00 PM	Low
2:00 PM	Medium
3:00 PM	Medium
4:00 PM	High

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

Statements	Yes	No
By the end of the day, Admin1 has received two email alerts.	☐	☐
By the end of the day, Admin2 has received three email alerts.	☐	☐
By the end of the day, Admin3 has received three email alerts.	☐	☐

正解:

Statements	Yes	No
By the end of the day, Admin1 has received two email alerts.	☐	☒
By the end of the day, Admin2 has received three email alerts.	☒	☐
By the end of the day, Admin3 has received three email alerts.	☐	☒

Explanation:

Statement

Answer

By the end of the day, Admin1 has received two email alerts.

No

By the end of the day, Admin2 has received three email alerts.

Yes

By the end of the day, Admin3 has received three email alerts.

No

Microsoft Entra ID Protection sends Users at risk detected email alerts when a user's risk level reaches the configured threshold. Here, the threshold is Medium or above, so the 1:00 PM Low risk event does not generate an alert. The 2:00 PM Medium event generates one alert, the 3:00 PM Medium event generates another because Microsoft states that later risk detections can trigger additional emails even if the recalculated risk remains at the configured level, and the 4:00 PM High event generates a third alert because it is still above the configured threshold. Microsoft also states that extra emails are suppressed only within a five- second period; these events are one hour apart, so that suppression rule does not reduce the count.

Admin1 receives the alerts because Admin1 is explicitly configured as a recipient, but the statement says two alerts; the correct count is three, so it is No. Admin2 receives three alerts because Security Reader users are automatically included by default for ID Protection notifications when they have a valid email or alternate email. Admin3 does not receive the alerts because User Administrator is not one of the automatically included roles and is not configured as a recipient.

質問: 41

お客様は、Contoso.com という名前の Microsoft Entra ID (Microsoft Entra ID) テナントをお持ちです。

Contoso IDインスタンス用のMicrosoft Defenderを作成します。

テナントには、以下の表に示すユーザーが含まれています。

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

センサーを識別するには、Defenderの設定を変更する必要があります。

解決策 :ユーザー3に、IDセンサーの設定に関してDefenderを変更するよう指示します。

これは目標を達成していると言えるでしょうか？

A. いいえ

B. はい

正解: (正解を表示します)

質問: 42

ホットスポット

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	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

ユーザー管理者ロールに次の割り当てを追加します。

* スコープタイプ: ディレクトリ

* 選抜メンバー: グループ1

* 割り当てタイプ: アクティブ

- * 割り当て開始日: 2023年3月15日
- * 割り当て終了日: 2023年8月15日
- Exchange 管理者ロールに次の割り当てを追加します。
- * スコープタイプ: ディレクトリ
- * 選抜メンバー: グループ2
- * 割り当てタイプ: 適格
- * 割り当て開始日: 2023年6月15日
- * 割り当て終了日: 2023年10月15日

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

Answer Area

Statements

Microsoft

Yes

No

On July 15, 2023, Admin1 can reset the password of a user.	☐	☐
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	☐	☐
On May 1, 2023, Admin3 can reset the password of a user.	☐	☐

正解:

Answer Area

Statements

Microsoft

Yes

No

On July 15, 2023, Admin1 can reset the password of a user.	☒	☐
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	☐	☒
On May 1, 2023, Admin3 can reset the password of a user.	☒	☐

Explanation:

Answer Area

Microsoft

Statements

On July 15, 2023, Admin1 can reset the password of a user.

On June 20, 2023, Admin2 can manage Microsoft Exchange Online.

On May 1, 2023, Admin3 can reset the password of a user.

Yes

No

Box 1: Yes

Admin1 is member of Group1.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

July 15, 2023 is with the assignment period.

A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.

Box 2: No

Admin2 is member of Group2.

The Exchange Administrator role assignment has Group2 as a member.

The assignment type: Eligible

June 20, 2023 is with the assignment period.

The assignment must be approved.

Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.

Box 3: Yes

Admin3 is member of Gropu1 and Group2.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

May 1, 2023 is with the assignment period.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member-owner>

質問: 43

Microsoft Defender for Endpoint を使用し、次の表に示すデバイスを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Operating system	Tag
Device1	Windows 11	Inventory1
Computer1	Windows 11	Inventory2
Device3	Android	Inventory3



Defender for Endpoint には、次の表に示すデバイス グループがあります。

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	Not applicable

次の表に示すように構成されたインシデント電子メール通知ルールを作成します。

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Microsoft

Statements

If a high-severity incident is triggered for Device1, an incident email notification will be sent.

Yes

☒

No

☐

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

☐☐

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

☐☐

正解:

Answer Area

Statements

If a high-severity incident is triggered for Device1, an incident email notification will be sent.

Yes

☒

No

☐

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

☐☐

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

☐☐

Explanation:

Answer Area

Statements

If a high-severity incident is triggered for Device1, an incident email notification will be sent.

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

Yes

No

☐

☒

☐

☒

☒

☐

Box 1: No
Device1 is in Group2 as Name starts with Device and Tag contains Inventory.
However, the Group2 has alert severity low.

Box 2: No
Computer1 does not belong to either Group1 or Group2

Box 3: Yes
Device3 belongs to both Group1 and Group2.

Note: Understanding alert severity
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.
The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.
Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue>

質問: 44
User1 と User2 という名前の 2 人のユーザーを含む Microsoft 365 テナントがあります。次の図に示すアラート ポリシーを作成します。



User2 は、Microsoft SharePoint Online ライブラリ内のファイルを変更するスクリプトを 4 分ごとに 2 時間実行します。
User1 は何件のアラートを受信しますか？

- A. 10
- B. 25
- C. 5
- D. 2

正解: [\(正解を表示します\)](#)

質問: 45

Microsoft Intune を使用する Microsoft 365 E5 テナントがあります。

次の要件を満たすように Intune を構成する必要があります。

ユーザーが個人のデバイスを登録できないようにします。

ユーザーが最大 10 台のデバイスを登録できるようにします。

それぞれの要件に何を使用する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Prevent users from enrolling personal devices:

Ensure that users can enroll a maximum of 10 devices:

Microsoft

正解:

Prevent users from enrolling personal devices:

Ensure that users can enroll a maximum of 10 devices:

Microsoft

Explanation:

Prevent users from enrolling
personal devices:

▼

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

Ensure that users can enroll a
maximum of 10 devices:

▼

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

Reference:
<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#blocking-personal-windows-devices>

質問: 46
Microsoft 365 E5 テナントがあります。
次の図に示すように、デバイス コンプライアンス ポリシーを構成します。

Compliance settings

Edit

Microsoft Defender ATP

Require the device to be at or under the machine risk score:

Low

Device Health

Rooted devices

Require the device to be at or under the Device Threat Level

Block

System Security

Require a password to unlock mobile devices

Require

Required password type

Device default

Encryption of data storage on device.

Require

Block apps from unknown sources

Block

Actions for noncompliance

Edit

Action

Schedule

Mark device noncompliant

Immediately

Retire the noncompliant device

Immediately

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 a device reports a medium threat level, the device will

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

正解:

When a device reports a medium threat level, the device will

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Explanation:

When a device reports a medium threat level, the device will

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android>

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> **598**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **47**

Microsoft 365 E5 テナントがあります。

ISO 27001:2013 テンプレートに基づいてカスタムのコンプライアンス マネージャー評価テンプレートを作成する予定です。

既存のテンプレートをエクスポートする必要があります。

エクスポートされたテンプレートにはどのファイル形式を使用する必要がありますか？

A. CSV

B. XLSX

C. JSON

D. XML

正解: **B** ([コメントを發表する](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template>

質問: **48**

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Entra のユーザー管理者ロールに Privileged Identity Management (PIM) を構成する予定です。今後 6 か月間は、ユーザーがユーザー管理者ロールのロール割り当てリクエストを行えるようにする必要があります。割り当てはどのように構成すればよいですか？

A. 割り当てタイプを 「適格」に設定する

B. 永続的な適格割り当てを許可するを 「はい」に設定する

C. 割り当てタイプをアクティブに設定します。

D. 永続的なアクティブを許可するを 「はい」に設定する

正解: ([正解を表示します](#))

質問: **49**

Microsoft 365 E5 サブスクリプションをお持ちです。

すべてのユーザーは Mac コンピュータを持っています。ATI コンピューターは Microsoft エンドポイント マネージャーに登録され、Microsoft Defender for Endpoint にオンボードされます。

コンピューター上で Microsoft Defender for Endpoint を構成する必要があります。

Endpoint Management 管理センターから何を作成する必要がありますか？

A. デバイス構成プロファイル

B. iOS のアップデート ポリシー

C. Microsoft Defender for Endpoint のベースライン プロファイル

D. モバイル デバイス管理 (MDM) セキュリティ ベースライン プロファイル

あなたの会社には複数のオフィスがあります。

デバイス管理に Microsoft Intune を使用する Microsoft 365 E5 テナントがあります。各オフィスにはローカル管理者がいます。

ローカル管理者がそれぞれのオフィス内のデバイスのみを管理できるようにする必要があります。

何を使えばいいのでしょうか？

- A. スコープタグ
- B. 構成プロファイル
- C. デバイスのカテゴリ
- D. 条件付きアクセス ポリシー

正解: (正解を表示します)

Reference:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

質問: 51

Group1とGroup2という2つのセキュリティグループを含むMicrosoft 365 E5サブスクリプションをご利用の場合、以下の要件を満たす認証ソリューションを推奨する必要があります。

* グループ 1 のメンバーは、ハードウェア トークンを使用して認証できる必要があります。

* グループ 2 のメンバーは、公開鍵インフラストラクチャ (PKI) を使用して認証できる必要があります。

各グループに推奨する認証方法はどれですか？適切な認証方法を適切なグループにドラッグしてください。各認証方法は、1回、複数回、または全く使用しないことが可能です。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Methods

Passkey (FIDO2)

Certificate-based authentication

Email OTP

Microsoft Authenticator

Temporary Access Pass

Third-party software OATH tokens

Answer Area

Group1:

Group2:

正解:

Methods

Passkey (FIDO2)

Certificate-based authentication

Email OTP

Microsoft Authenticator

Temporary Access Pass

Third-party software OATH tokens

Answer Area

Group1: Temporary Access Pass

Group2: Microsoft Authenticator

Explanation:

Methods

Passkey (FIDO2)

Certificate-based authentication

Email OTP

Microsoft Authenticator

Temporary Access Pass

Third-party software OATH tokens

Answer Area

Group1: Temporary Access Pass

Group2: Microsoft Authenticator

質問: 52

Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Defender for Cloud Apps を評価しています。
条件付きアクセス アプリ制御に依存する 2 つのポリシーの種類はどれですか。それぞれの正解は完全なソリューションを示します。
注意: 正しい選択ごとに 1 ポイントが付与されます。

- A. セッションポリシー
- B. ファイルポリシー
- C. アプリ検出ポリシー
- D. OAuth アプリポリシー
- E. アクセスポリシー
- F. アクティビティポリシー

正解: [\(正解を表示します\)](#)

質問: 53

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	Distribution
Group3	Mail-enabled security
Group4	Security

Label1 という名前の機密ラベルを公開する予定です。
Label1 をどのグループに公開できますか？

- A. グループ 1 のみ
- B. グループ 1 とグループ 2 のみ
- C. グループ 1 とグループ 4 のみ
- D. グループ 1、グループ 2、およびグループ 3 のみ
- E. グループ1、グループ2、グループ3、およびグループ4

正解: (正解を表示します)

In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites>

質問: 54

ホットスポット

お客様のネットワークには、オンプレミスのActive Directoryドメインが含まれています。このドメインには、次の表に示すサーバーが含まれています。

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

Microsoft 365 E5 サブスクリプションをご購入いただきます。

Microsoft Entra Cloud Syncを導入する必要があります。

最初に何をインストールすべきか、またどのサーバーにインストールすべきか？回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Install:

The Azure AD Application Proxy connector

Azure AD Connect

The Azure AD Connect provisioning agent

Active Directory Federation Services (AD FS)

Server:

Server1 only

Server2 only

Server3 only

Server1 or Server2 only

Server1 or Server3 only

Server1, Server2, or Server3

正解:

Answer Area

Install:

The Azure AD Application Proxy connector

Azure AD Connect

The Azure AD Connect provisioning agent

Active Directory Federation Services (AD FS)

Server:

Server1 only

Server2 only

Server3 only

Server1 or Server2 only

Server1 or Server3 only

Server1, Server2, or Server3

Explanation:

Answer Area



Install:

▼

The Azure AD Application Proxy connector
Azure AD Connect
The Azure AD Connect provisioning agent
Active Directory Federation Services (AD FS)

Server:

▼

Server1 only
Server2 only
Server3 only
Server1 or Server2 only
Server1 or Server3 only
Server1, Server2, or Server3

Box 1: The Microsoft Entra Connect Sync provisioning agent

Install the Microsoft Entra Connect Sync provisioning agent

How is Microsoft Entra Cloud Sync different from Microsoft Entra Connect Sync sync?

With Microsoft Entra Cloud Sync, provisioning from AD to Microsoft Entra ID is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Microsoft Entra ID and AD. The provisioning configuration is stored in Microsoft Entra ID and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

- * An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install>

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites>

質問: 55

Microsoft 365 E5 サブスクリプションをお持ちです。

すべてのデバイスを Microsoft Defender for Endpoint にオンボードします

www.contoso.com にある悪意のある Web サイトへのアクセスをブロックするには、Defender for Endpoint を使用する必要があります。

どの 2 つのアクションを実行する必要がありますか?それぞれの正解は、解決策の一部を示しています。

注: 各正解は 1 ポイントの価値があります。

A. 自動調査を有効にします。

B. Web コンテンツ フィルタリング ポリシーを作成します。

C. 適用範囲を構成します。

D. インジケーターを作成します。

E. カスタム ネットワーク インジケーターを有効にします。

正解: **B,E** ([コメントを發表する](#))

質問: **56**

(ネットワークには、contoso という名前のオンプレミスの Active Directory ドメイン サービス (AD DS) フォレストが 2 つ含まれています。

com と fabrikam.com はフォレストの信頼を使用して接続されています。

Microsoft 365 E5 サブスクリプションをお持ちです。

両フォレストのユーザーの一部を Microsoft Entra IDに同期する必要があります。ソリューションはデバイスオブジェクトとデバイスライトバックをサポートしている必要があります。

何を使えばいいのでしょうか？

A. Microsoft Entra Cloud Sync

B. Microsoft Entra ドメイン サービス

C. Microsoft Entra Connect 同期

D. Active Directory フェデレーション サービス (AD FS)

正解: **C** ([コメントを發表する](#))

The correct answer is Microsoft Entra Connect Sync because it is the only Microsoft-supported solution that meets all of the stated requirements.

1. Support for multiple on-premises AD DS forests

Microsoft Entra Connect Sync is designed to synchronize identities from multiple on-premises Active Directory forests into a single Microsoft Entra tenant. Microsoft documentation explicitly states that when multiple forests are present, they can all be synchronized as long as they are reachable by the same Entra Connect server. A forest trust between contoso.com and fabrikam.com is a supported and common configuration.

2. Ability to sync only a subset of users

Microsoft Entra Connect Sync supports filtering and scoping at multiple levels (domain-based, OU-based, or attribute-based). Microsoft documentation lists pilot deployments and limited user synchronization as a primary use case, allowing administrators to synchronize only selected users from each forest.

3. Support for device objects and hybrid device scenarios

Microsoft Entra Connect Sync supports hybrid device identity, including Microsoft Entra hybrid joined devices. These devices are registered both in on-premises Active Directory and in Microsoft Entra ID, which is required for many Microsoft 365 and Conditional Access scenarios.

4. Device writeback support

Device writeback is a feature that allows device objects from Microsoft Entra ID to be written back into on- premises Active Directory. Microsoft documentation clearly identifies device writeback as a feature of Microsoft Entra Connect Sync.

Important documented behavior:

Device writeback is supported when device objects and users are correctly located and configured in the same forest.

Device writeback is not a feature of Cloud Sync or federation services.

Why the other options are incorrect

A). Microsoft Entra Cloud Sync

Cloud Sync is a lightweight provisioning agent and does not provide the full hybrid identity feature set required for this scenario. Microsoft documentation associates advanced device features and device writeback with Microsoft Entra Connect Sync, not Cloud Sync.

B). Microsoft Entra Domain Services

Microsoft Entra Domain Services is a managed domain service used to run legacy, domain-joined workloads in Azure. It does not synchronize on-premises forests into Microsoft Entra ID and is not a replacement for

Entra Connect in hybrid identity scenarios.

D). Active Directory Federation Services (AD FS)

AD FS is an authentication and federation service. It does not synchronize users or devices to Microsoft Entra ID and does not support device writeback. Microsoft documentation positions AD FS as an authentication method, not a directory synchronization solution.

質問: 57

お客様のネットワークには、オンプレミスのActive Directoryドメインサービス(AD DS)ドメインが含まれています。このドメインには2,000個のユーザーアカウントが存在します。

お客様はMicrosoft Entraテナントをお持ちです。

ドメインをMicrosoft Entraテナントと同期する必要があります。ソリューションは以下の要件を満たす必要があります。

インフラ要件を最小限に抑える。

単一障害点を最小限に抑える。

管理業務の手間を最小限に抑える。

何を使うべきでしょうか？

A. Active Directory フェデレーション サービス (AD FS)

B. Microsoft Entra Cloud Sync

C. Microsoft Entra Connect Sync

D. パススルー認証

正解: (正解を表示します)

Microsoft Entra Cloud Sync is the correct choice because the requirement is directory synchronization with the least infrastructure, least administrative overhead, and reduced single points of failure. Microsoft describes Entra Cloud Sync as a cloud-managed hybrid identity synchronization service for synchronizing users, groups, and contacts between Active Directory and Microsoft Entra ID, using a lightweight agent-based model.

Microsoft also positions Cloud Sync as its strategic direction for hybrid identity synchronization.

For resilience, Cloud Sync supports multiple active provisioning agents. Microsoft states that high availability is achieved by having multiple active agents installed and running, so synchronization can continue if one agent fails, and Microsoft recommends three active agents for high availability. This directly satisfies

"minimize single points of failure."

Microsoft Entra Connect Sync can synchronize AD DS to Entra ID, but it requires a more substantial dedicated synchronization server design and more operational management. Microsoft's migration guidance notes that Cloud Sync's lightweight provisioning agent model requires minimal server resources compared with Connect Sync's fuller installation. AD FS and pass-through authentication are authentication/sign-in solutions, not the best answer for directory synchronization. References/topics: Microsoft Entra Cloud Sync, hybrid identity synchronization, provisioning agents, high availability, Microsoft Entra Connect comparison.

質問: 58

Microsoft 365 サブスクリプションをお持ちです。

Microsoft Defender for Cloud Apps を Microsoft Defender for Endpoint と統合します。

リスク スコアが 4 以下の検出されたアプリにユーザーがアクセスできないようにするポリシーを作成する必要があります。

どの 2 つの設定を構成する必要がありますか? 回答するには、回答領域で適切な設定を選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Apps matching all of the following

Select a filter

+ Add a filter

Apply to:

All continuous reports

☐ Trigger a policy match if all the following occur on the same day:

Alerts

☐ Create an alert for each matching event with the policy's severity

Governance actions

☐ Tag app as sanctioned

☒ Tag app as unsanctioned

☐ Tag app as monitored

☐ Tag app with custom tag

Select app tag

正解:

Answer Area

Apps matching all of the following

Select a filter

+ Add a filter

Apply to:

All continuous reports

☐ Trigger a policy match if all the following occur on the same day:

Alerts

☐ Create an alert for each matching event with the policy's severity

Governance actions

☐ Tag app as sanctioned

☒ Tag app as unsanctioned

☐ Tag app as monitored

☐ Tag app with custom tag

Select app tag

Explanation:

Answer Area

Apps matching all of the following

Select a filter

+ Add a filter

Apply to:

All continuous reports

☐ Trigger a policy match if all the following occur on the same day:

Alerts

☐ Create an alert for each matching event with the policy's severity

Governance actions

☐ Tag app as sanctioned

☒ Tag app as unsanctioned

☐ Tag app as monitored

☐ Tag app with custom tag

Select app tag

質問: 59

貴社は、contoso.com という名前の Microsoft Entra テナントを使用する Microsoft 365 サブスクリプションを保有しています。このテナントには、次の表に示すユーザーが含まれています。

Name	Role	Office 365 role group
User1	None	Compliance Data Administrator
User2	Global Administrator	None

「ラベル1」という名前の保持ラベルを作成し、以下の設定を行います。

- * コンテンツを5年間保持します
- * 5年以上前のコンテンツを自動的に削除します

Policy1という名前のポリシーを使用して、Label1の自動ラベル付けを有効にします。Policy1には、次の設定があります。

- * 「合併」という単語を含むコンテンツに適用されます
- * OneDriveアカウントとSharePointサイトの場所を指定します

以下のコマンドを実行します。

Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention True -Force 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」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	☐	☐
User2 can remove SharePoint sites from Policy1.	☐	☐
User2 can add the word Acquisition to Policy1.	☐	☐

正解:

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	☒	☐
User2 can remove SharePoint sites from Policy1.	☐	☒
User2 can add the word Acquisition to Policy1.	☒	☐

Explanation:

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	☒	☐
User2 can remove SharePoint sites from Policy1.	☐	☒
User2 can add the word Acquisition to Policy1.	☒	☐

質問: 60

Microsoft Defender for Office 365 を使用する Microsoft 365 サブスクリプションがあります。
事前設定されたセキュリティ ポリシー内の標準保護プロファイル設定よりも安全性が低い設定を特定する必要があります。

何を使うべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Portal:

Microsoft Defender portal

Microsoft 365 admin center

Microsoft Defender portal

Microsoft Purview portal

Feature:

Configuration analyzer

Preset security policies

Threat tracker

正解:

Feature:

Configuration analyzer

Preset security policies

Threat tracker

Explanation:

Answer Area

Portal:

Microsoft 365 admin center

Feature:

Configuration analyzer

質問: 61

ネットワークには Active Directory フォレストが含まれています。

Microsoft 365 を展開します。

ディレクトリ同期を実装する予定です。

同期された ID のセキュリティ ソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。

* Active Directory が利用できなくなった場合、ユーザーは Microsoft 365 サービスに対して正常に認証できる必要があります。

* ユーザーパスワードは10文字以上である必要があります。

解決策: パススルー認証を実装し、Microsoft Entra パスワード保護を構成します。これで目標は達成されますか?

A. はい

B. いいえ

正解: (正解を表示します)

有効的な**MS-102J**問題集はJPNTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTest.comは今最新**MS-102J**試験問題集を提供します。JPNTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 62

Microsoft J65 E5 サブスクリプションをお持ちです。

Microsoft Defender for Endpoint を Microsoft Intune と統合します。

デバイスが Intune に登録されるときに、Defender for Endpoint に自動的にオンボードされるようにする必要があります。

解決策: デバイス構成プロファイルを構成します。

これは目標を満たしていますか？

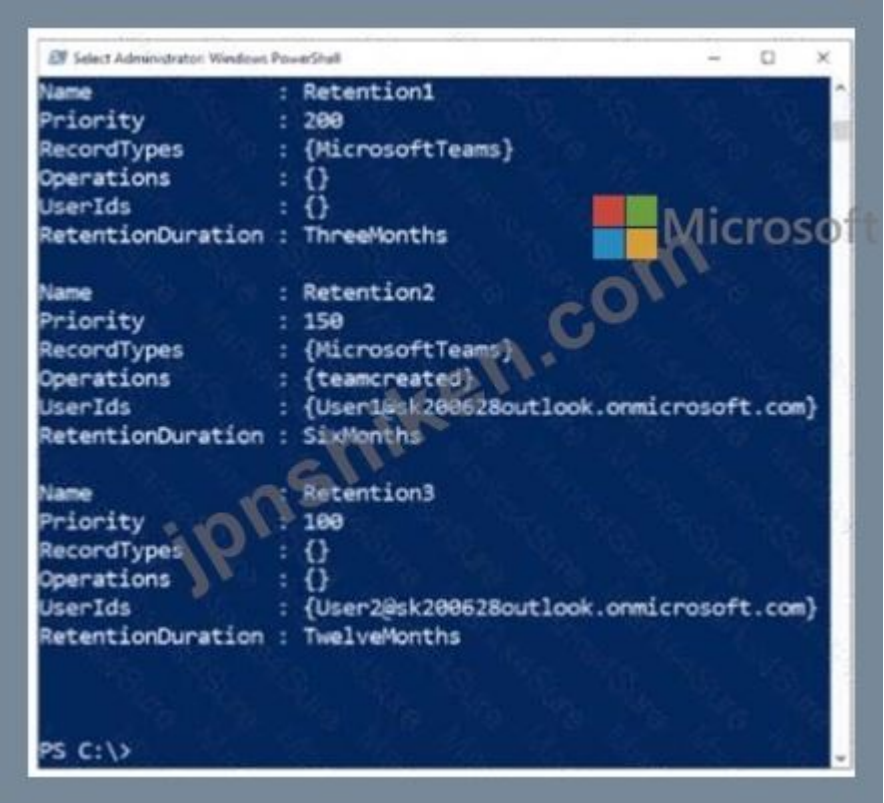
A. いいえ

B. はい

正解: (正解を表示します)

質問: 63

次の図に示すように、3 つの自動保持ポリシーを持つ Microsoft 365 ES サブスクリプションがあります。



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 正しい選択肢はそれぞれ 1 ポイントの価値があります。

Answer Area	If User1 creates a team in Microsoft Teams, the event is [answer choice]	not retained retained for 90 days retained for six months retained for one year
	If User2 adds a channel in Microsoft Teams, the event is [answer choice]	not retained retained for 90 days retained for six months retained for one year

正解:

Answer Area



If User1 creates a team in Microsoft Teams, the event is [answer choice]

not retained

retained for 90 days

retained for six months

retained for one year

If User2 adds a channel in Microsoft Teams, the event is [answer choice]

not retained

retained for 90 days

retained for six months

retained for one year

Explanation:

Answer Area



If User1 creates a team in Microsoft Teams, the event is [answer choice] retained for six months

If User2 adds a channel in Microsoft Teams, the event is [answer choice] retained for 90 days

質問: 64

お客様は、以下の表に示すデバイスを含む Microsoft 365 E5 サブスクリプションをお持ちです。

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

午前8時に、以下の設定を持つインシデント通知ルールを作成します。

- * 名前: 通知!
- * 通知設定
 - o アラート70で通知：低
 - o デバイスグループの範囲: すべて (3)
 - o 詳細 :インシデントごとの最初の通知
- * 受信者: User1@contoso.com、User2@contoso.com

午前8時02分に、以下の設定を持つインシデント通知ルールを作成します。

- * 名前: 通知
- * 通知設定
 - アラートの深刻度に応じて通知する: 低、中
 - o デバイスグループの範囲: DeviceGroup1、DeviceGroup2
- * 受信者: User1@contoso.com

Microsoft Defender XDRでは、アラートは次の表に示すようにログに記録されます。

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

以下の各記述について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

User2@contoso.com will receive an incident notification email for the alert at 08:07.

User1@contoso.com will receive an incident notification email for the alert at 08:20.

Yes

No

☐☐☐☐☐☐

正解:

Answer Area	
Statements	
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	Yes No
User2@contoso.com will receive an incident notification email for the alert at 08:07.	Yes No
User1@contoso.com will receive an incident notification email for the alert at 08:20.	Yes No

Explanation:

Answer Area

Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

User2@contoso.com will receive an incident notification email for the alert at 08:07.

User1@contoso.com will receive an incident notification email for the alert at 08:20.

Yes

No



Microsoft

質問: 65

Azure ATP センサーはどのサーバーにインストールする必要がありますか?

- A. サーバー 1
- B. サーバー 2
- C. サーバー 3
- D. サーバー 4
- E. サーバー 5

正解: (正解を表示します)

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning> However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

質問: 66

Microsoft 365 E5 サブスクリプションをお持ちです。

次の要件を満たすように Microsoft Defender for Office 365 を構成する必要があります。

- * スプーフィング防止のため、誤検知を最小限に抑えるために、ユーザーの電子メール送信パターンを使用する必要があります。
 - * Microsoft Teams、SharePoint Online、OneDrive にアップロードされたドキュメントは、Defender for Office 365 を使用して保護する必要があります。
- それぞれの要件に対して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。

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:

Domains to protect

Domains to protect

Mailbox intelligence

Users to protect

Global settings for safe attachments

Global settings for safe attachments

The Safe Attachments policy settings

The Safe Links policy settings

正解:

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:

Domains to protect ▼
Domains to protect
Mailbox intelligence
Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:

Global settings for safe attachments ▼
Global settings for safe attachments
The Safe Attachments policy settings
The Safe Links policy settings

Explanation:

Answer Area

A user's email sending **patterns** must be used to minimize false positives for spoof protection: Domains to protect ▼

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365: Global settings for safe attachments ▼

質問: 67

Microsoft 365 F5 サブスクリプションをお持ちです。

あなたは 100 台の新しい Windows 10 デバイスを展開する予定です。

新しいデバイスに適したバージョンの Windows 10 を注文する必要があります。バージョンは次の要件を満たす必要があります。

最低 24 か月はサービスを受けてください。

Microsoft Application Virtualization (App-V) のサポート

どのバージョンを特定すればよいでしょうか？

- A. Windows 10 Pro、バージョン 1909
- B. Windows 10 Pro、バージョン 2004
- C. Windows 10 Pro、バージョン 1909
- D. Windows 10 Enterprise、バージョン 2004

正解: D ([コメントを发表する](#))

Reference:

<https://docs.microsoft.com/en-us/windows/release-health/release-information>

<https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations>

質問: 68

Microsoft 365 テナントがあります。

会社のポリシーでは、すべての Windows 10 デバイスが次の最小要件を満たすことが求められています。
複雑なパスワードを要求します。
データストレージデバイスの暗号化を要求します。

Microsoft Defender ウイルス対策のリアルタイム保護を有効にします。

要件を満たさないデバイスがテナント内のリソースにアクセスできないようにする必要があります。

どの 2 つのコンポーネントを作成する必要がありますか?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. 構成ポリシー

B. コンプライアンス ポリシー

C. セキュリティベースラインプロファイル

D. 条件付きアクセス ポリシー

E. 構成プロファイル

正解: ([正解を表示します](#))

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

質問: **69**

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。

Windows 10 を実行しているコンピューターがあります。

どのバージョンの Windows 10 がインストールされているかを確認する必要があります。

解決策: 設定アプリから [システム] を選択し、[バージョン情報] を選択してシステムに関する情報を表示します。

これは目標を達成していますか?

A. はい

B. いいえ

正解: ([正解を表示します](#))

Reference:

<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808>

質問: **70**

contoso.com という名前の Microsoft Entra テナントにリンクされた Microsoft 365 E5 サブスクリプションがあります。

Microsoft 365 Business Voice アドオン ライセンスを 100 個購入します。

Voice という名前のグループのメンバーに Microsoft 365 Business Voice アドオン ライセンスが自動的に割り当てられていることを確認する必要があります。

あなたは何をすべきか?

A. Microsoft Entra 管理センターから、Voice グループの設定を変更します。

B. Microsoft 365 管理センターの [ライセンス] ページから、ライセンスを割り当てます。

C. Microsoft 365 管理センターから、Voice グループの設定を変更します。

正解: **A** ([コメントを發表する](#))

質問: 71

Office 365 では Microsoft Defender を使用します。

攻撃シミュレーション キャンペーンを自動化する予定です。

シミュレーションに失敗したユーザーは、シミュレーション結果に基づいて追加のトレーニングを受ける必要があります。

シミュレーション後にユーザーがトレーニングを利用できる日数は最大何日ですか？

- A. 7
- B. 45
- C. 15
- D. 30

正解: (正解を表示します)

質問: 72

contoso.com というドメインを含む Microsoft 365 ES サブスクリプションがあり、user1@contoso.com というユーザーに対してユーザー偽装保護が有効になっている Policy1 という新しい Microsoft Defender (または Office 365 フィッシング対策ポリシー) を展開します。

Policy1 では、usei1@fabnkam.com という通常の連絡先からの電子メール メッセージがブロックされていることがわかります。

メッセージが正常に配信されることを確認する必要があります

ポリシー1では何をすべきでしょうか？

- A. フィッシングメールのしきい値設定を構成します。
- B. 保護するドメインを有効にするを選択します。
- C. 保護するユーザーを構成します。
- D. メールボックスインテリジェンスを有効にするを選択します

正解: (正解を表示します)

質問: 73

次の表に示すように、Microsoft エンドポイント マネージャーに 3 つのデバイスが登録されています。

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

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

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

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	Assigned to
Policy1	Group3
Policy2	Group2

次の表に示すように、ポリシー1の値が「はい」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

Microsoft

Statements	Yes	No
Device1 is compliant.	☐	☐
Device2 is compliant.	☐	☐
Device3 is compliant.	☐	☐

正解:

Answer Area

Microsoft

Statements	Yes	No
Device1 is compliant.	☐	☒
Device2 is compliant.	☐	☒
Device3 is compliant.	☒	☐

Explanation:

Answer Area

Microsoft

Statements	Yes	No
Device1 is compliant.	☐	☒
Device2 is compliant.	☐	☒
Device3 is compliant.	☒	☐

質問: 74

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

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

すべてのデバイスが Microsoft Defender for Endpoint にオンボードされています
次の要件を満たすために Microsoft Defender 脆弱性管理を使用する予定です。
* オペレーティング システムの脆弱性を検出します。

Answer Area

Detect operating system vulnerabilities:

- Device1, Device2, and Device3 only
- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only**
- Device1, Device2, and Device4 only

Perform a configuration assessment of the operating system:

- Device1 and Device2 only
- Device1 only**
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3, and Device4



正解:

Answer Area

Detect operating system vulnerabilities:

- Device1, Device2, and Device3 only
- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only**
- Device1, Device2, and Device4 only

Perform a configuration assessment of the operating system:

- Device1 and Device2 only
- Device1 only**
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3, and Device4



Explanation:

Answer Area

Detect operating system vulnerabilities:

Device1, Device2, and Device3 only

Perform a configuration assessment of the operating system:

Device1 and Device2 only



Group1 というグループを含む Microsoft 365 E5 サブスクリプションがあります。このサブスクリプションでは Microsoft Defender for Cloud Apps を使用しています。クラウド検出を構成します。

Group1 のメンバーによるシャドー IT の使用状況を詳細に示すカスタム レポートを作成できることを確認する必要があります。

まず何をすべきでしょうか？

- A. ユーザーエンリッチメントを構成します。
- B. 匿名化を無効にします。
- C. ユーザー監視を構成します。
- D. アプリコネクタを追加します。

正解: ([正解を表示します](#))

質問: 76

ホットスポット

Group1 という名前の Microsoft 365 グループを含む Microsoft 365 サブスクリプションがあります。Group1 は、次の図に示すように構成されています。



User1 という名前の外部ユーザーの電子メール アドレスは user1@outlook.com です。

User1 を Group1 に追加する必要があります。

最初に何をすべきか、どのポータルを使用すべきか？ 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Action:

Add User1 to the subscription as an active user.

For Group1, change the Privacy setting to Public.

For Group1, select Allow external senders to email this group.

Invite User1 to collaborate with your organization as a guest.

Portal:

The Microsoft Entra admin center

The Exchange admin center

The Microsoft 365 admin center

The Microsoft Purview compliance portal

正解:

Answer Area

Microsoft

Action:

Add User1 to the subscription as an active user.

For Group1, change the Privacy setting to Public.

For Group1, select Allow external senders to email this group.

Invite User1 to collaborate with your organization as a guest.

Portal:

The Microsoft Entra admin center

The Exchange admin center

The Microsoft 365 admin center

The Microsoft Purview compliance portal

Explanation:

Answer Area

Action:

Add User1 to the subscription as an active user.

For Group1, change the Privacy setting to Public.

For Group1, select Allow external senders to email this group.

Invite User1 to collaborate with your organization as a guest.

Portal:

The Microsoft Entra admin center

The Exchange admin center

The Microsoft 365 admin center

The Microsoft Purview compliance portal

Box 1: Invite User1 to collaborate with your organization as a guest.

To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.

Navigate with your Web browser to <https://admin.microsoft.com>.

On the left pane, click on "Users", then click "Guest Users".

On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Microsoft Entra ID to add guest users" link at the bottom of the page. Both of these links will take you to the Microsoft Entra ID portal, which is located at <https://aad.portal.azure.com>.

On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format `username@tenantdomain.dot.com`. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.

Box 2: The Microsoft Entra admin center

Microsoft Entra admin center unites Microsoft Entra ID with family of identity and access products Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Microsoft Entra ID (Microsoft Entra ID) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Microsoft Entra admin center (aad.portal.azure.com).

Reference:

<https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users>

<https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-access-products>

有効的な**MS-102J**問題集はJPNTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTest.comは今最新**MS-102J**試験問題集を提供します。JPNTest.com MS-102J試験問題集はもう更新されました。ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 77

Microsoft 365 E5 サブスクリプションが Microsoft Entra ID (Microsoft Entra ID) テナントにリンクされています。このテナントには Group1 という名前のグループと、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

テナントには、以下の設定を含む条件付きアクセス ポリシーが設定されています。

名前: ポリシー1

課題 :

- ユーザーとグループ: グループ1
- クラウドアプリまたはアクション: すべてのクラウドアプリ

アクセス制御:

許可する、多要素認証を要求する

ポリシーを有効にする: レポート専用

テナントの「セキュリティを有効にする」設定は、デフォルトで「はい」になります。

以下の各設定項目について、該当する記述が正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Microsoft	Statements	Yes	No
	Admin1 can set Enable policy for Policy1 to On .	☐	☐
	Admin2 can set Enable policy for Policy1 to Off .	☐	☐
	Admin3 can set Users and groups for Policy1 to All users .	☐	☐

正解:

Microsoft	Statements	Yes	No
	Admin1 can set Enable policy for Policy1 to On .	☒	☐
	Admin2 can set Enable policy for Policy1 to Off .	☒	☐
	Admin3 can set Users and groups for Policy1 to All users .	☒	☐

Explanation:

Microsoft	Statements	Yes	No
	Admin1 can set Enable policy for Policy1 to On .	☐	☐
	Admin2 can set Enable policy for Policy1 to Off .	☐	☐
	Admin3 can set Users and groups for Policy1 to All users .	☐	☐

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode: Conditional Access policies can be enabled in report-only mode. During sign-in, policies in report-only mode are evaluated but not enforced.

Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only>

質問: 78

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	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

Microsoft 365 には、次の表に示すようなラベルがあります。

Name	Type
Label1	Sensitivity
Label2	Retention

Microsoft 365 のコンテンツには、次の表に示すラベルが割り当てられます。

Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

次の表に示すように、Microsoft 365 にはラベルがあります。

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。

Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	☐	☐
Admin2 can view the contents of File1 by using Content explorer.	☐	☐
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	☐	☐

正解:

Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	☒	☐
Admin2 can view the contents of File1 by using Content explorer.	☐	☒
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	☐	☒

Explanation:

Answer Area		
Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	☒	☐
Admin2 can view the contents of File1 by using Content explorer.	☐	☒
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	☐	☒

質問: 79

Microsoft 365 サブスクリプションをお持ちです。

Enterprise Mobility + Security プランを持つすべてのユーザーを特定し、ユーザーのリストを CSV 形式で提供する必要があります。

Microsoft 365 管理センターではどの設定を使用する必要がありますか?また、どのオプションを選択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。



質問: 80

Microsoft 365 E5 サブスクリプションをお持ちです。

次の要件を満たすために Microsoft Purview ポリシーを実装する予定です。

Microsoft Teams および SharePoint に保存されている、個人を特定できる情報 (PII) を含むドキュメントを特定します。

PII を含む共有ドキュメントに関するレポート。

何を作成する必要がありますか？

A. データ損失防止 (DLP) ポリシー

B. 保持ポリシー

C. アラート ポリシー

D. Microsoft Defender for Cloud Apps ポリシー

正解: **A** ([コメントを发表する](#))

Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities.

With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

From the Security & Compliance tab of your browser, click Home.

Click Data loss prevention > Policy.

Click + Create a policy.

In Start with a template or create a custom policy, click Custom > Custom policy > Next.

In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b.

Description: Protect the personally identifiable information of European citizens Etc.

Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment>

質問: **81**

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。

このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。

お客様のネットワークには、Microsoft Entra ID (Microsoft Entra ID) と同期された、contoso.com という名前の Active Directory ドメインが含まれています。

Microsoft System Center Configuration Manager (Current Branch) を使用して、Windows 10 デバイスを管理します。

共同管理のためのパイロット版を設定します。

ドメインにDevice1という名前の新しいデバイスを追加します。Device1にConfiguration Managerクライアントをインストールします。

Microsoft IntuneとConfiguration Managerを使用してDevice1を管理できることを確認する必要があります。

解決策 :Configuration Managerのデバイスコレクションをパイロットコレクションとして定義します。Device1をコレクションに追加します。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解: **A** ([コメントを发表する](#))

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

質問: 82

どのサーバーで Defender for ID センサーを使用する必要がありますか?

A. サーバー1

B. サーバー2

C. サーバー3

D. サーバー4

E. サーバー5

正解: (正解を表示します)

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

質問: 83

Microsoft Intune に登録されたデバイスを含む Microsoft 365 テナントがあります。デバイスは次の表のように構成されています。

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

Microsoft Endpoint Manager で次のデバイス管理タスクを実行する予定です。

* VPN デバイス構成プロファイルを使用して VPN 接続を展開します。

* Endpoint Protection デバイス構成プロファイルを使用してセキュリティ設定を構成します。

管理業務をサポートします。

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

VPN device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

正解:

VPN device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Explanation:

VPN device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure>

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos>

質問: 84

お客様は、contoso.com という名前の Microsoft Entra テナントを使用する Microsoft 365 サブスクリプションをご利用になっています。このテナントには、次の表に示すユーザーが含まれています。Microsoft Entra 管理センターの [サインイン] ブレードから、User1 と User2 はどのユーザーのサインイン情報を表示できますか？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：正解ごとに1ポイントが加算されます。

Answer Area

User1 can view the sign-ins for the following users:

- User1, User2, User3, and User4
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

User2 can view the sign-ins for the following users:

- User1 and User2 only
- User2 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4



正解:

Answer Area

User1 can view the sign-ins for the following users:

- User1, User2, User3, and User4
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

User2 can view the sign-ins for the following users:

- User1 and User2 only
- User2 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4



Explanation:

Answer Area

User1 can view the sign-ins for the following users:

User1, User2, User3, and User4

User2 can view the sign-ins for the following users:

User1 and User2 only



質問: 85

ホットスポット

あなたの会社では、100 人のユーザーを含む従来のオンプレミス LDAP ディレクトリを使用しています。

会社は Microsoft 365 サブスクリプションを購入します。

Microsoft 365 管理センターを使用して、100 人のユーザーを Microsoft 365 にインポートする必要があります。
どのタイプのファイルを使用する必要がありますか、どのプロパティが必要ですか？ 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

File type to use:

CSV

JSON

PST

XML

Required properties for each user:

Display Name and Department

First Name and Last Name

User Name and Department

User Name and Display Name

正解:
Answer Area

File type to use:

CSV

JSON

PST

XML

Required properties for each user:

Display Name and Department

First Name and Last Name

User Name and Department

User Name and Display Name

Explanation:

File type to use:

CSV
JSON
PST
XML

Required properties for each user:

Display Name and Department
First Name and Last Name
User Name and Department
User Name and Display Name

Box 1: CSV

Add multiple users in the Microsoft 365 admin center

Sign in to Microsoft 365 with your work or school account.

In the admin center, choose Users > Active users.

Select Add multiple users.

On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.

Etc.

Note: More information about how to add users to Microsoft 365

Not sure what CSV format is?

A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

Box 2: User Name and Display Name

What if I don ' t have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don ' t have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time>

質問: 86

Microsoft 365 サブスクリプションをお持ちです。

Group! という名前の 2 つのグループを作成する必要があります。そしてグループ2。ソリューションは次の要件を満たす必要があります。

* Group1 はメールが有効であり、Microsoft SharePoint Online サイトが関連付けられている必要があります。

* Group2 は動的なメンバーシップと役割の割り当てをサポートする必要がありますが、メールを有効にしてはなりません。

どのタイプのグループを作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。注記：

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

Group1:



Microsoft 365
Distribution
Dynamic distribution
Microsoft 365
Security

Group2:

Security
Distribution
Dynamic distribution
Microsoft 365
Security

正解:

Answer Area



Group1:

Microsoft 365
Distribution
Dynamic distribution
Microsoft 365
Security

Group2:

Security
Distribution
Dynamic distribution
Microsoft 365
Security

Explanation:

Answer Area

Group1:

Microsoft 365

▼

Group2:

Security

▼

質問: 87

Windows 11 デバイスを含む Microsoft 365 E5 サブスクリプションがあります。すべてのデバイスは、Microsoft Defender for Endpoint にオンボードされています。デバイスの構成を業界標準のベンチマークと比較する必要があります。何を使用すればよいでしょうか？

- A. イベント
- B. セキュリティベースライン評価
- C. 攻撃対象領域マップ
- D. 取り組み

正解: [\(正解を表示します\)](#)

質問: 88

次の表に示すユーザーを含む Microsoft 365 E5 テナントがあります。

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

次の表に示すように、ユーザーには Microsoft Store for Business のロールが割り当てられます。

User	Role
User1	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

ビジネス向け Microsoft Store のプライベート ストアにアプリを追加できるのはどのユーザーですか。また、プライベート ストアからアプリをインストールできるのはどのユーザーですか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。



Add apps to the private store:

	▼
User3 only	
User2 and User3 only	
User1 and User3 only	
User1, User2 and User3 only	
User1, User2, User3, and User4	

Install apps from the private store:

	▼
User3 only	
User2 and User3 only	
User1 and User3 only	
User2, User3 and User4 only	
User1, User2, User3, and User4	

正解:

	
Add apps to the private store:	▼
User3 only	
User2 and User3 only	
User1 and User3 only	
User1, User2 and User3 only	
User1, User2, User3, and User4	
Install apps from the private store:	▼
User3 only	
User2 and User3 only	
User1 and User3 only	
User2, User3 and User4 only	
User1, User2, User3, and User4	

Explanation:

Add apps to the private store:

User3 only

User2 and User3 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Install apps from the private store:

User3 only

User2 and User3 only

User1 and User3 only

User2, User3 and User4 only

User1, User2, User3, and User4

Reference:
<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business>
<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store>

質問: 89
Microsoft 365 E5 サブスクリプションをお持ちです。
次の表に示すデータ損失防止 (DLP) ポリシーを作成する予定です。

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

ポリシーごとに DLP ルールを作成する必要があります。
送信者の条件とファイル拡張子の条件をサポートするポリシーはどれですか?回答するには、回答領域で適切なオプションを選択してください。
注: 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

Sender is condition:

File extension is condition:

Microsoft

Options for Sender is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

Options for File extension is condition:

- DLP1, DLP2, and DLP3
- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

正解:

Answer Area

Sender is condition:

File extension is condition:

Microsoft

Options for Sender is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

Options for File extension is condition:

- DLP1, DLP2, and DLP3
- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

Explanation:



質問: 90

お客様は、Microsoft Entra IDansidential Threat Protection (ATP) を使用する Microsoft 365 E5 サブスクリプションをご利用中です。
Azure ATPで検出除外を作成する必要があります。
どのツールを使うべきでしょうか？

- A. セキュリティとコンプライアンス管理センター
- B. Microsoft Defender セキュリティセンター
- C. Microsoft 365 管理センター
- D. Microsoft Entra IDandian Threat Protection ポータル
- E. クラウドアプリセキュリティポータル

正解: D (コメントを发表する)

Reference:
<https://docs.microsoft.com/en-us/defender-for-identity/what-is>
<https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections>

質問: 91

次の表に示すアラートを含む Microsoft 365 サブスクリプションがあります。

Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

アラートのどのプロパティを変更できますか？

- A. ステータスのみ
- B. ステータスとコメントのみ
- C. ステータスと重大度のみ
- D. ステータス、重大度、コメントのみ
- E. ステータス、重大度、コメント、カテゴリ

正解: B (コメントを发表する)

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations>

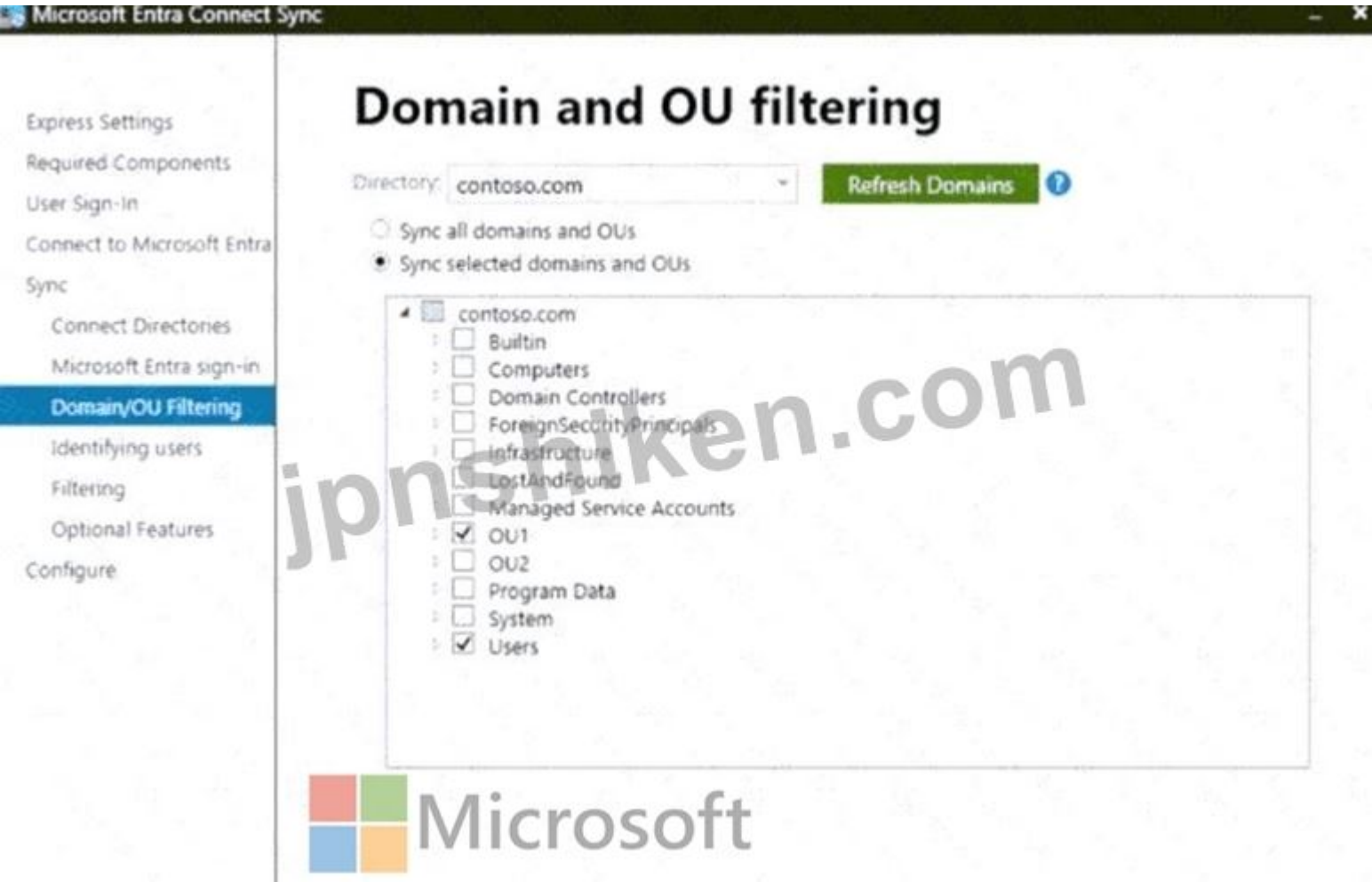
質問: 92

お客様のネットワークには、contoso という名前のオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。com。このドメインには、次の表に示すユーザーが含まれています。

Name	In organizational unit (OU)
User1	OU1
User2	OU1

Microsoft Entra Connect Syncを使用してcontoso.comと同期するMicrosoft Entraテナントをお持ちです。

Microsoft Entra Connect Syncは、図に示すように構成されています。(図」タブをクリックしてください。)



Microsoft Entraテナントには、次の表に示すように、Group1という名前のクラウド専用グループが含まれています。

Members	On-premises sync
User1	Enabled
User2	Disabled

午前10時に以下の作業を行います。

* contoso.comでは、User1をOU2に移動します。

* Microsoft Entra テナントで、User2 を削除します。

* contoso.com で、OU1 に Comp1 という名前のコンピュータ アカウントを作成し、Comp1 の説明を更新します。

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

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
By 11 AM, User1 has become a member of Group1.	☐	☐
At 11 AM, User2 is removed from contoso.com.	☐	☐
At 11 AM, the Description property of Comp1 syncs to the Microsoft Entra tenant.	☐	☐

正解:

Statements	Yes	No
By 11 AM, User1 has become a member of Group1.	☐	☒
At 11 AM, User2 is removed from contoso.com.	☐	☒
At 11 AM, the Description property of Comp1 syncs to the Microsoft Entra tenant.	☐	☒

Explanation:

Statement

Answer

By 11 AM, User1 has become a member of Group1.

No

At 11 AM, User2 is removed from contoso.com.

No

At 11 AM, the description property of Comp1 syncs to the Microsoft Entra tenant.

No

Microsoft Entra Connect Sync OU filtering controls which on-premises objects appear in Microsoft Entra ID.

Microsoft states that when previously synchronized objects are later filtered out, those objects are deleted in Microsoft Entra ID. Since User1 is moved from synced OU1 to unsynced OU2, User1 is no longer in scope and is removed from the active Microsoft Entra sync result, so User1 does not newly become/remain an active Group1 member by 11 AM. Microsoft also states that the sync scheduler runs every 30 minutes by default, so the change can be processed before 11 AM.

User2 is cloud-only in Microsoft Entra ID because on-premises sync is disabled. Deleting that cloud object does not delete the separate on-premises AD DS user. Microsoft Entra Connect's normal direction is on-premises AD DS to Microsoft Entra ID; writeback is limited to specific configured scenarios such as password writeback, not cloud deletion of users back into AD DS.

Comp1 also does not satisfy the statement. Microsoft documents that Windows domain-joined computer /device synchronization includes only specific device attributes, such as displayName, objectGUID, operatingSystem, operatingSystemVersion, objectSID, and userCertificate. description is not listed as a synchronized device attribute.

質問: 93

ネットワークにはcontoso.comというActive Directoryドメインが含まれています。このドメインには、次の表に示すオブジェクトが含まれています。

Name	Microsoft Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2

Answer Area

Microsoft

Statements	Yes	No
User2 will synchronize to the Microsoft Entra tenant.	☐	☐
Group2 will synchronize to the Microsoft Entra tenant.	☐	☐
User3 will synchronize to the Microsoft Entra tenant.	☐	☐

正解:

Answer Area

Microsoft

Statements	Yes	No
User2 will synchronize to the Microsoft Entra tenant.	☐	☒
Group2 will synchronize to the Microsoft Entra tenant.	☒	☐
User3 will synchronize to the Microsoft Entra tenant.	☒	☐

Explanation:

Answer Area

Microsoft

Statements	Yes	No
User2 will synchronize to the Microsoft Entra tenant.	☐	☒
Group2 will synchronize to the Microsoft Entra tenant.	☒	☐
User3 will synchronize to the Microsoft Entra tenant.	☒	☐

質問: 94

あなたの会社は 5 つの都市にオフィスを構えています。
会社には Microsoft 365 テナントがあります。
各オフィスはローカル管理者によって管理されます。
Microsoft Intune を展開する予定です。
Intune でリソースを管理するには、次の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。
ローカル管理者は、それぞれのオフィス内のリソースのみを管理できる必要があります。
ローカル管理者が他のオフィスのリソースを管理できないようにする必要があります。
管理上の労力は最小限に抑える必要があります。
推奨事項には何を含めるべきですか？

- A. デバイスのカテゴリ
- B. スコープタグ
- C. 構成プロファイル
- D. 条件付きアクセス ポリシー

正解: (正解を表示します)

Reference:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

質問: 95

多要素認証 (MFA) の使用を評価しています。
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。

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	☐	☐
Users must use the Microsoft Authenticator app to complete MFA.	☐	☐
After registering, users must use MFA for every sign-in.	☐	☐

正解:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	☒	☐
Users must use the Microsoft Authenticator app to complete MFA.	☒	☐
After registering, users must use MFA for every sign-in.	☐	☒

Explanation:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	☒	☐
Users must use the Microsoft Authenticator app to complete MFA.	☒	☐
After registering, users must use MFA for every sign-in.	☐	☒

Site1 という名前の SharePoint サイトを含む Microsoft 365 E5 サブスクリプションがあります。Site1 には、次の表に示すファイルが含まれています。

Name	Number of IP addresses in the file
File1	2
File2	5

次の表に示すユーザーがいます。

Name	Role
User1	Site owners for Site1
User2	Site members for Site1
Admin1	SharePoint admins

高度な DLP ルールを使用してデータ損失防止 (DLP) ポリシーを作成し、そのポリシーを Site1 に適用します。DLP ルールは、次の図に示すように構成されています。

Edit rule

^ **Conditions**

We'll apply this policy to content that matches these conditions.

^ **Content contains**

Default Any of these

Sensitive info types

IP Address High confidence instance count 3 to Any

Add

Create group

+ Add condition

^ **Exceptions**

^ **Actions**

Use actions to protect content when the conditions are met.

^ **Restrict access or encrypt the content in Microsoft 365 locations**

☒ **Restrict access or encrypt the content in Microsoft 365 locations**

☒ Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

☒ Block everyone

☐ Block only people outside your organization.

☐ Block only people who were given access to the content through the "Anyone with the link" option.

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

Answer Area

Statements	Yes	No
User1 can open File2.	☐	☐
User2 can open File1.	☐	☐
Admin1 can open File2.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 can open File2.	☐	☒
User2 can open File1.	☒	☐
Admin1 can open File2.	☒	☐

Explanation:

User1 can open File2: No

User2 can open File1: Yes

Admin1 can open File2: Yes

User1 can open File2: No

The DLP policy specifies that if a file contains 3 or more IP addresses, access to that content should be restricted. File2 contains 5 IP addresses, which exceeds the threshold set by the DLP policy. Therefore, User1, who is a site owner, will not be able to access File2 because it matches the conditions set in the DLP rule to block access.

User2 can open File1: Yes

File1 contains only 2 IP addresses, which is below the threshold of 3 set by the DLP policy. Since the DLP policy does not apply to files with fewer than 3 IP addresses, User2, who is a site member, can access File1 without any restrictions.

Admin1 can open File2: Yes

Admin1 is part of the SharePoint admins group, which typically has elevated privileges. Despite the DLP rule, SharePoint admins are generally not restricted by the same DLP rules that apply to regular users. Therefore, Admin1 can access File2.

質問: 97

あなたはMicrosoft 365のサブスクリプションをお持ちです。

すべてのユーザーのメールはMicrosoft Exchange Onlineに保存されています。

User1という名前のユーザーのメールボックスで、ProjectXという単語を含むすべてのメールメッセージのコピーを保存する必要があります。

まず最初に何をすべきでしょうか？

A. Microsoft Purview コンプライアンス ポータルから、ラベルとラベル ポリシーを作成します。

B. Microsoft Defender XDR からメッセージ トレースを開始します。

- C. Exchange 管理センターからメールフロールールを作成します。
- D. Microsoft Defender for Cloud Apps からアクティビティ ポリシーを作成します。

正解: (正解を表示します)

質問: 98

100 台の Windows 10 デバイスを含む Microsoft 365 テナントがあります。デバイスは Microsoft Endpoint Manager を使用して管理されます。

ASR1 と ASR2 という名前の 2 つの攻撃対象領域削減 (ASR) ポリシーを作成する予定です。ASR1 は、Microsoft Defender Application Guard の構成に使用されます。ASR2 は、Microsoft Defender SmartScreen の構成に使用されます。

各ポリシーにはどの ASR プロファイル タイプを使用する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

ASR1:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

ASR2:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

正解:

ASR1:

Device control

Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

ASR2:

Device control

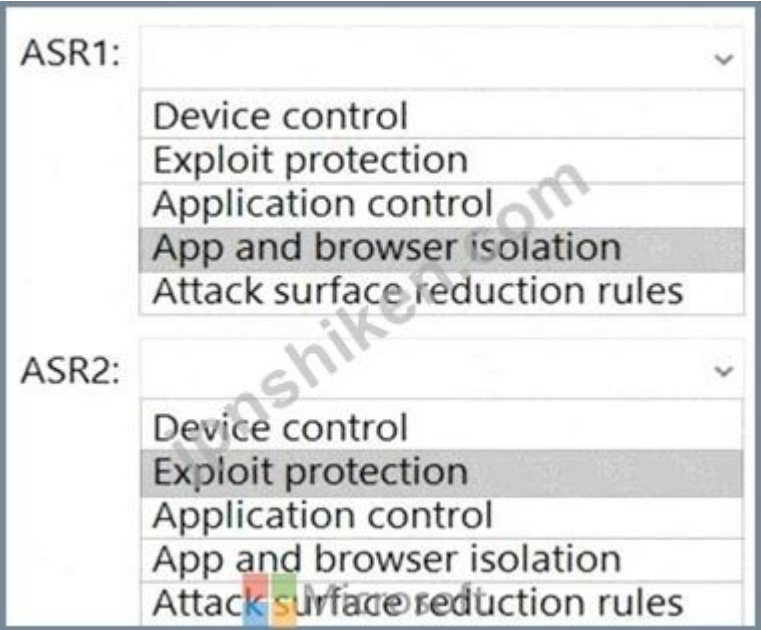
Exploit protection

Application control

App and browser isolation

Attack surface reduction rules

Explanation:



Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

質問: 99

Device1 という名前の Windows 10 デバイスと、次の表に示す Microsoft エンドポイント マネージャー ポリシーを含む Microsoft 365 テナントがあります。

Name	Type	 Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

- A. ポリシーの設定のみです。
- B. 設定なし
- C. Policy3 の設定のみ
- D. Policy2の設定のみ

正解: C ([コメントを发表する](#))

質問: 100

Microsoft 365 サブスクリプションをお持ちです。

機密データが電子メール メッセージで共有されるのをブロックするデータ損失防止 (DLP) ポリシーがある。

機密データを含む電子メール メッセージが外部受信者と内部受信者の両方に送信される場合、メッセージが外部受信者にのみ配信されないようにポリシーを変更する必要があります。

何を修正する必要がありますか？

- A. ポリシー ルールの例外
- B. ポリシールールの条件
- C. DLP ポリシーの場所
- D. ポリシールールのアクション

正解: **B** ([コメントを発表する](#))

質問: **101**

お客様は、以下の表に示すデバイスを含む Microsoft 365 E5 サブスクリプションをお持ちです。

Platform	Count
Windows 10	50
Android	50
Linux	50

Windows 10 デバイスでのみアラートが発生したときにトリガーされるインシデントメール通知ルールを設定する必要があります。このソリューションは、管理作業を最小限に抑える必要があります。まず最初に何をすべきでしょうか？

- A. Microsoft 365 管理センターから、メールが有効になっているセキュリティグループを作成します。
- B. Microsoft Defender XDR ポータルから、デバイス グループを作成します。
- C. Microsoft Endpoint Manager 管理センターから、デバイスカテゴリを作成します。
- D. Microsoft Entra ID 管理センターから、動的デバイスグループを作成します。

正解: **B** ([コメントを発表する](#))

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide>
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide>

質問: **102**

Microsoft 365 E5 テナントがあります。

機密ラベルは、機密ラベルの図に示すように構成されています。(機密ラベル タブをクリックします。)



Sensitivity 1

Scope

File.Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns

None

自動ラベル付けポリシーの図に示すように、自動ラベル付けポリシーがあります。([自動ラベル付けポリシー] タブをクリックします。)

Auto-labeling policy



Edit Policy



Delete Policy

Policy name

Auto-labeling policy

Description

Label in simulation

Sensitivity1

Info to label

IP Address



Apply to content in these locations

Exchange email All

Rules for auto-applying this label

Exchange email 1 rule

Mode

On

Comment

ユーザーは、次の表に示すコンポーネントを含む電子メールを送信します。

Type	File	Includes IP address
Mail body	Not applicable	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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

Statements	Yes	No
Sensitivity1 is applied to the email.	☐	☐
A watermark is added to File1.docx.	☐	☐
A header is added to File2.xml.	☐	☐

正解:

Statements	Yes	No
Sensitivity1 is applied to the email.	☒	☐
A watermark is added to File1.docx.	☐	☒
A header is added to File2.xml.	☐	☒

Explanation:

Statements	Yes	No
Sensitivity1 is applied to the email.	☒	☐
A watermark is added to File1.docx.	☐	☒
A header is added to File2.xml.	☐	☒

Reference:

質問: 103

モバイル デバイス管理用に登録されたデバイスを含む Microsoft 365 テナントがあります。デバイスは次の表に示すように構成されています。

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

デバイスの VPN アクセスを有効にする予定です。
必要な構成ポリシーの最小数はどれくらいですか？

- A. 3
- B. 4
- C. 5
- D. 1

正解: (正解を表示します)

質問: 104

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	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

AU1 という名前の新しい管理単位を作成し、次の AU1 動的メンバーシップ ルールを構成します。

Statements	Yes	No
Admin1 can reset the password of User1.	☐	☐
Admin1 can reset the password of User2.	☐	☐
Admin2 can reset the password of User3.	☐	☐

正解:

Statements	Yes	No
Admin1 can reset the password of User1.	☒	☐
Admin1 can reset the password of User2.	☐	☒
Admin2 can reset the password of User3.	☒	☐

Explanation:

Statements	Yes	No
Admin1 can reset the password of User1.	☒	☐
Admin1 can reset the password of User2.	☐	☒
Admin2 can reset the password of User3.	☒	☐

質問: 105

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。

このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。

お客様のネットワークには、contoso.com という名前のオンプレミス Active Directory ドメインが含まれています。このドメインには、次の表に示すユーザーが含まれています。

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

図に示すように、ドメインはcontoso.comという名前のMicrosoft Entraテナントと同期されます。(図」タブをクリックしてください。)

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	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

ユーザー2がuser2@fabrikam.comとしてサインインしようとした際、Microsoft Entra IDへの認証に失敗しました。User2がMicrosoft Entra IDのリソースにアクセスできることを確認する必要があります。

解決策 :オンプレミスのActive Directoryドメインから、User2のUPNサフィックスを@contoso.comに設定します。あなたはユーザー2に対し、user2@contoso.comとしてログインするよう指示します。これは目標を達成していると言えるでしょうか？

- A. はい
 - B. いいえ
- 正解: (正解を表示します)

The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

質問: 106

ハイブリッド Microsoft Entra テナントにリンクされた Azure サブスクリプションがあります。

すべてのユーザーは、Microsoft Entra Connect の高速設定を使用して、Active Directory ドメイン サービス (AD DS) からテナントに同期します。

セルフサービス パスワード リセット (SSPR) を実装する予定です。

ユーザーがパスワードをリセットまたは変更するときに、パスワードが AD DS と同期することを確認する必要があります。

どのアクションを順番に実行する必要がありますか？ 答えるには、適切なアクションを正しい順序にドラッグします。各アクションは、1 回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。

Actions

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2:

Step 3:

正解:

Actions

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.

Step 3: Select Password writeback in Microsoft Entra Connect.

Explanation:

Actions

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.

Step 3: Select Password writeback in Microsoft Entra Connect.

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%**ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 107

Microsoft Defender for Cloud Apps 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内のユーザー情報またはデータへのアクセス許可を要求する禁止されたアプリが検出されたときに電子メール アラートを生成するポリシーを作成する必要があります。

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。

Answer Area

Policy type:

Activity
App discovery
OAuth app
Session

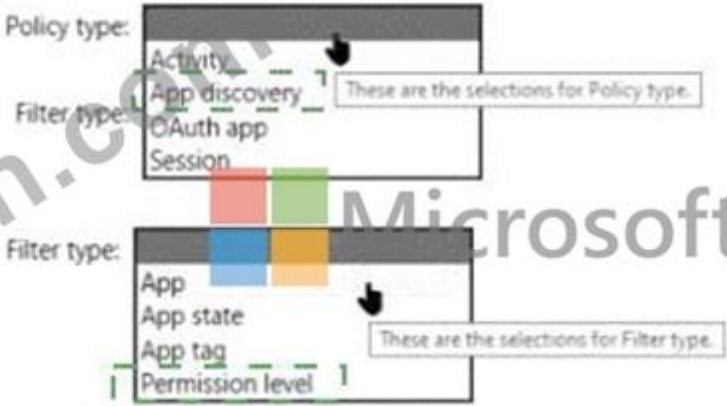
These are the selections for Policy type.

Filter type:

App
App state
App tag
Permission level

These are the selections for Filter type.

正解:



Explanation:



質問: 108

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 テナントがあります。Site1 には、次の表に示すファイルが含まれています。

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

Sensitivity1 という名前の機密ラベルと、次の構成を持つ自動ラベル ポリシーを作成します。

名前: AutoLabel1

自動適用するラベル: Sensitivity1

SharePoint Online サイトのルール: Rule1-SPO

ラベルを適用する場所を選択します: Site1

Rule1-SPO は次のように構成されています。

Edit rule



Name *

Rule1-SPO

Description

Rule1 description

^ Conditions

We'll apply this policy to content that matches these conditions.

^ Content contains sensitive info types

Default

All of these

Sensitive info types

IP Address

Accuracy

85

to

100

Instance count

2

to

Any

Add

Create group

+ Add condition

Save

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。
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

Sensitivity1 is applied to File1.docx.

Sensitivity1 is applied to File2.txt.

Sensitivity1 is applied to File3.xlsx.

正解:

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	☐	☐
Sensitivity1 is applied to File2.txt.	☐	☐
Sensitivity1 is applied to File3.xlsx.	☐	☐

Explanation:

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	☐	☒
Sensitivity1 is applied to File2.txt.	☒	☐
Sensitivity1 is applied to File3.xlsx.	☒	☐

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

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

質問: 109

Microsoft 365 E5 テナントがあります。

ユーザーがマルウェアを含む電子メール メッセージを受信したときに管理者に通知されるように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。

どの種類のポリシーを作成する必要がありますか?また、ポリシーを作成するにはどの Microsoft 365 コンプライアンス センターの役割が必要ですか?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 Area

Policy type:

Alert
Threat
Compliance

Role:

Quarantine
Security Administrator
Organization Configuration
Communication Compliance Admin

正解:



Explanation:



質問: 110

次の表に示すグループを含む Microsoft 365 テナントがあります。

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

新しい Windows 10 セキュリティ ベースライン プロファイルを作成する予定です。
どのグループにプロファイルを割り当てることができますか？

- A. グループ 3 のみ
- B. グループ 1 とグループ 3 のみ
- C. グループ 2 とグループ 3 のみ
- D. グループ 1、グループ2、とグループ3

正解: (正解を表示します)

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile>
<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

質問: 111

ユーザー1が技術要件を満たすデバイスを登録できるようにする必要があります。どうすればよいですか？

- A. Microsoft Entra ID 管理センターから、User1 にクラウド デバイス管理者の役割を割り当てます。
- B. Microsoft Entra ID 管理センターから、ユーザーごとの最大デバイス数の設定を構成します。
- C. Intune 管理センターから、User1 をデバイス登録マネージャーとして追加します。
- D. Intune 管理センターから、登録制限を構成します。

正解: (正解を表示します)

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

質問: 112

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。

Windows 10 を実行しているコンピューターがあります。

どのバージョンの Windows 10 がインストールされているかを確認する必要があります。

解決策: 設定アプリから、[更新と更新] を選択します。更新履歴を表示するためのセキュリティ。

これは目標を達成していますか？

A. はい

B. いいえ

正解: (正解を表示します)

質問: 113

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 には次の表のファイルがあります。

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.docx	2
File4.png	3
File5.docx	3

Site1 ユーザーには、次の表に示すロールが割り当てられます。

Name	Role
User1	Owner
User2	Visitor

次の図に示すように、Policy1 というデータレス防止 (DLP) ポリシーを作成します。



ポリシー」を適用した後に、ユーザー 1 とユーザー 2 に表示されるファイルの数はいくつですか。回答領域で適切なオプションを選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



質問: 114

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。

このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。

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

Microsoft Entra テナントをデプロイします。

別の管理者が、ドメインを Microsoft Entra ID と同期するように設定します。

組織単位(OU)内の10個のユーザーアカウントが Microsoft Entra ID と同期されていないことが判明しました。その他のユーザーアカウントはすべて正常に同期されています。

Microsoft Entra Connect Healthを確認したところ、すべてのユーザーアカウントの同期が正常に完了していたことがわかりました。

10個のユーザーアカウントが Microsoft Entra ID と同期されていることを確認する必要があります。

解決策 :Microsoft Entra Connect Sync から、フィルタリング設定を変更します。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解: ([正解を表示します](#))

質問: 115

貴社には本社が3つと支店が1つあります。支店は研究目的で使用されています。

同社は Microsoft 365 テナントを導入し、多要素認証を展開する予定だ。

支店内のユーザーのみに多要素認証が適用されるようにするには、Microsoft 365 ソリューションを推奨する必要があります。

推薦状には何を含めるべきでしょうか？

A. Microsoft Entra 条件付きアクセス

B. Microsoft Entra ID パスワード保護

C. Microsoft Intune デバイス構成プロファイル

D. Microsoft Intune デバイスコンプライアンスポリシー

正解: A (コメントを发表する)

質問: 116

あなたはMicrosoft 365 E5サブスクリプションをご利用で、Microsoft Defender for Cloud Appsを使用しています。

あなたはサブスクリプションのアクティビティログを確認しています。

オンプレミスネットワークから発生するイベントが自動的に「管理」として分類されるようにする必要があります。

あなたは何を制作すべきでしょうか？

A. 重要な資産分類

B. IPアドレスを示す指標

C. IPアドレス範囲

D. 名前の付いた場所

正解: C (コメントを发表する)

The correct answer is C. an IP address range . In Microsoft Defender for Cloud Apps, IP address ranges are used to identify known network locations, such as physical offices, datacenters, VPN egress addresses, and administrative networks. Microsoft states that IP address ranges let you tag, categorize, and customize how logs and alerts are displayed and investigated. Each IP range can be assigned to a preset IP category, such as Administrative , Corporate , VPN , or other categories, so events from those IP addresses are categorized automatically in the Activity log.

This directly matches the requirement: events originating from the on-premises network must be categorized automatically as Administrative . To do that, you create an IP address range for the on-premises public IP addresses and assign the range the Administrative category. Defender for Cloud Apps then uses that categorization when displaying and filtering activity log events. Microsoft also confirms that IP address category can be manually overridden by using IP address ranges.

A named location is a Microsoft Entra Conditional Access construct, not the Defender for Cloud Apps activity-log categorization mechanism. An indicator for IP addresses is used for threat indicators in security tooling, not for activity-log categorization. A critical asset classification is unrelated to IP-based event categorization.

質問: 117

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Defender ポータルでアラートを生成した疑わしい電子メール メッセージを調査しています。

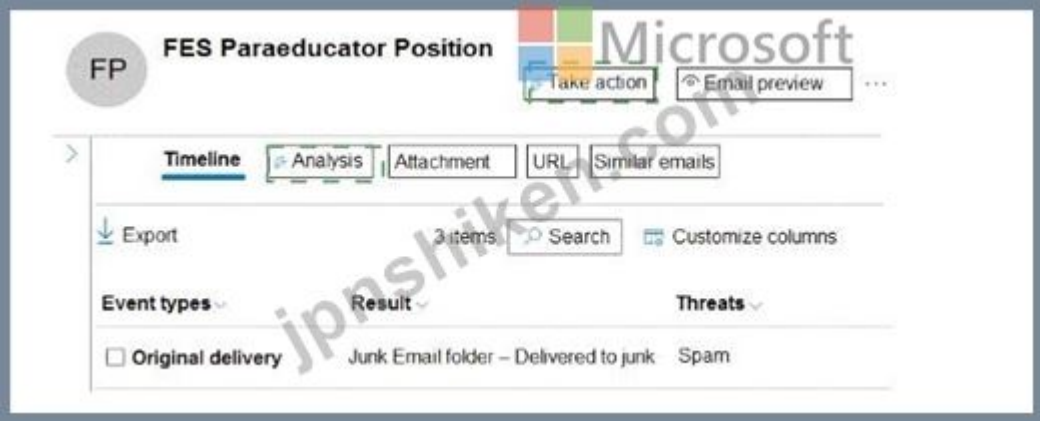
電子メール メッセージのヘッダーを確認し、メッセージを Microsoft に送信して確認を受ける必要があります。

どの 2 つの設定を使用する必要がありますか？ 回答するには、回答領域で適切な設定を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:
1. Analysis 2. Take Action

質問: 118

Microsoft intune 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には、次の表に示すリソースが含まれています。

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 は Device1 の所有者です。
次の表に示すように、Microsoft 365 Apps Windows 10 以降のアプリの種類を Intune に追加します。
木曜日に、アプリのデプロイメントの結果を確認します。

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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

Word is installed on Device1.

App3 is displayed in the Company Portal.

Excel is installed on Device1.

Yes

No

正解:

Answer Area

Microsoft

Statements

Word is installed on Device1.		
App3 is displayed in the Company Portal.		
Excel is installed on Device1.		

Explanation:

Microsoft

Statements

Word is installed on Device1.		
App3 is displayed in the Company Portal.		
Excel is installed on Device1.		

質問: 119

あなたはMicrosoft 365のサブスクリプションをお持ちです。
App1という名前の新しいMicrosoft Entra IDエンタープライズアプリケーションを構成します。App1を使用するには、ユーザーにレポート閲覧者ロールを割り当てる必要があります。
レポート閲覧者ロールを割り当て、App1にアクセスするには、どのタイプのグループを使用すればよいですか？

- A. メンバーシップが割り当てられている Microsoft 365 グループ
- B. 動的なユーザーメンバーシップを持つ Microsoft 365 グループ
- C. メンバーシップが割り当てられたセキュリティグループ
- D. 動的なユーザーメンバーシップを持つセキュリティグループ

正解: (正解を表示します)

To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Microsoft Entra ID and open in the Roles and Administrators list for that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.

Note: You can add the following types of groups:

Assigned groups - Manually add users or devices into a static group.

Dynamic groups (Requires Microsoft Entra ID Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.

Note:

Security groups

Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.

Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.

Security groups can be configured for dynamic membership in Microsoft Entra ID, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.

Security groups can be added to a team.

Microsoft 365 Groups can ' t be members of security groups.

Microsoft 365 Groups

Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps>

<https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?>

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy>

質問: 120

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、アラート ポリシーを作成します。

Policy1

Edit policy

Delete policy

Status ☒ On

Name your alert

Description

Add a description

Severity

Low

Category

Threat management

Policy contains tags

-

Create alert settings

Conditions

Activity is FileMalwareDetected

Aggregation

Aggregated

Activity is monitored on the following scope:

Scope: All users

Window: 2 hours

Threshold: 20

Severity: Low

Set your recipients

Recipients: User1@sk220912outlook.onmicrosoft.com

Daily notification limit: 100

Microsoft

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

Policy1 will trigger an alert if malware is detected in [answer choice].

The maximum number of email messages that Policy1 will generate per day is [answer choice].

SharePoint or OneDrive only

Exchange Online only

SharePoint only

SharePoint or OneDrive only

Exchange Online, SharePoint , or OneDrive

5

5

12

20

100

正解:

Answer Area

Policy1 will trigger an alert if malware is detected in [answer choice].

SharePoint or OneDrive only
Exchange Online only
SharePoint only
SharePoint or OneDrive only
Exchange Online, SharePoint, or OneDrive

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5
5
12
20
100

Explanation:

Answer Area

Policy1 will trigger an alert if malware is detected in [answer choice].

SharePoint or OneDrive only

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5

質問: 121

Microsoft 365 サブスクリプションをお持ちです。

ネットワークは 51.40.15.0/24 の IP アドレス空間を使用します。

Exchange Online 管理者は最近、ネットワーク上のコンピューターから Role1 という名前のロールを作成しました。

監査ログ検索を使用して管理者の名前を特定する必要があります。

監査ログ検索ではどのアクティビティを検索し、どのフィールドでフィルタリング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。

Activities to search for:

Field to filter by:

Exchange mailbox activities
Site administration activities
Show results for all activities
Role administration activities

Item
User
Detail
IP address

正解:

Microsoft

Activities to search for:

Field to filter by:

Exchange mailbox activities
Site administration activities
Show results for all activities
Role administration activities

Item
User
Detail
IP address

Explanation:

Microsoft

Activities to search for:

Field to filter by:

Exchange mailbox activities
Site administration activities
Show results for all activities
Role administration activities

Item
User
Detail
IP address

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

次の表に示すグループを含む Microsoft 365 テナントがあります。

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

Compliance1 という名前のコンプライアンス ポリシーを作成する予定です。

次の要件を満たすグループを特定する必要があります。

- * コンプライアンス1に非準拠通知の受信者として追加できます
- * コンプライアンス1に割り当てることができます

回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Can be added to Compliance1 as recipients of noncompliance notifications:

Microsoft

Group 1 and Group4 only

Group3 and Group4 only

Group1, Group2 and Group3 only

Group1, Group3, and Group4 only

Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

Group1 and Group4 only

Group3 and Group4 only

Group1, Group2 and Group3 only

Group1, Group3, and Group4 only

Group1, Group2, Group3, and Group4

正解:

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

Reference:
<https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manager-intune/>

質問: 123
Microsoft Entra ID Protectionの週刊ダイジェストメールを有効にします。
次の表に示すユーザーを作成します。

Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

どのユーザーが毎週のダイジェストメールを自動的に受信しますか？

- A. Admin2、Admin3、Admin4のみ
- B. Admin1、Admin2、Admin3、およびAdmin4
- C. Admin2とAdmin3のみ
- D. 管理者3のみ
- E. Admin1とAdmin3のみ

正解: E (コメントを发表する)

By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

質問: 124

Group1とGroup2という2つのグループを含むMicrosoft 365 E5サブスクリプションを所有しています。以下の要件を満たすデータ損失防止(DLP)戦略を構成する予定です。

- * グループ 1 のメンバーは、クレジットカード番号が含まれるドキュメントを共有できないようにする必要があります。
- * Group2 のメンバーは、Microsoft Purview Information Protection によって内部として分類されたドキュメントを共有できないようにする必要があります。
- * ソリューションは管理上の労力を最小限に抑える必要があります

グループごとに DLP ポリシーを作成する必要があります。

各グループの各 DLP ポリシー ルールにどの条件を追加する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

 Microsoft

Group1:

Select Document name contains words or phrases.

Select Document property is.

Set Content contains to Sensitive info types.

Set Content contains to Sensitivity labels.

Group2:

Select Document name contains words or phrases.

Select Document property is.

Set Content contains to Sensitive info types.

Set Content contains to Sensitivity labels.

正解:

Answer Area

 Microsoft

Group1:

Select Document name contains words or phrases.

Select Document property is.

Set Content contains to Sensitive info types.

Set Content contains to Sensitivity labels.

Group2:

Select Document name contains words or phrases.

Select Document property is.

Set Content contains to Sensitive info types.

Set Content contains to Sensitivity labels.

Explanation:

Answer Area

 Microsoft

Group1:

Set Content contains to Sensitive info types.

Group2:

Set Content contains to Sensitivity labels.

Microsoft 365 サブスクリプションをお持ちです。
contoso.com という名前のドメインを追加します。
ドメインを確認しようとすると、確認メールを admin@contoso.com に送信するように求められます。
ドメインの認証に使用するメール アドレスを変更する必要があります。
あなたは何をすべきか？
A. ドメインの NS レコードを変更します。
B. ドメインの DNS ゾーンに TXT レコードを追加します。
C. ドメイン レジストラーから、ドメインの連絡先情報を変更します。
D. Microsoft 365 管理センターから、Microsoft 365 サブスクリプションの全体管理者を変更します。
正解: (正解を表示します)

質問: 126
Microsoft 365 ES テナントがあります。
次の図に示すアラートがあります。

View alerts

	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
☐	Medium	Alert1	Active		Threat management	2	3 minutes ago
☐	High	Alert5	Resolved		Permissions	1	8 minutes ago

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

For Alert1, you can change Status to

For Alert5, you can

Answer Area

For Alert1, you can change Status to

For Alert5, you can

Explanation:
Answer Area

For Alert1, you can change Status to Investigating only

For Alert5, you can not change Status

質問: 127

ネットワークには Contoso という名前の Active Directory フォレストが含まれています。地元。

Microsoft 365 サブスクリプションをお持ちです。

パスワード ハッシュ同期を使用するディレクトリ同期ソリューションを実装する予定です。

Microsoft 365 管理センターから、contoso.com ドメイン名が正常に検証されました。

計画されたディレクトリ同期ソリューション用に環境を準備する必要があります。

まず何をすべきでしょうか？

- A. Active Directory ドメインと信頼関係から、contoso.com を UPN サフィックスとして追加します。
- B. Microsoft 365 管理センターから Contoso を確認します。ローカルドメイン名。
- C. [Active Directory ユーザーとコンピューター] から、すべてのユーザーの UPN サフィックスを変更します。
- D. contoso.com のパブリック DNS ゾーンから、新しいメール エクスチェンジャー (MX) レコードを追加します。

正解: (正解を表示します)

質問: 128

サードパーティの多要素認証 (MFA) 製品を使用する Microsoft 365 サブスクリプションがあります。

Microsoft Secure Score を確認しているときに、すべてのユーザーに対して多要素認証が有効になっていることを確認する」推奨事項にポイントがリストされていないことがわかりました。

推奨ポイントをすべて確実に取得する必要があります。ソリューションは管理上の手間を最小限に抑える必要があります。

何をすべきでしょうか？

- A. 推奨事項のステータスを変更します。
- B. Microsoft Defender for Identity センサーを展開します。
- C. データ コネクタを構成します。
- D. 推奨タグを変更します。

正解: (正解を表示します)

質問: 129

お客様は、contoso.onmicrosoft.com という名前の Microsoft Entra ID (Microsoft Entra ID) テナントにリンクされた 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は、Microsoft OneDrive にドキュメントを保存します。

User1 の OneDrive アカウントの内容を電子情報開示保留にする必要があります。

eDiscovery ホールドにはどの URL を使用すべきですか？ 回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

https://

	▼		▼
onedrive.live.com/		User1	
contoso.onmicrosoft.com/		Sites/User1	
contoso.sharepoint.com/		contoso_onmicrosoft_com/User1	
contoso-my.sharepoint.com/		personal/User1_contoso_onmicrosoft_com	

正解:

https://

	▼		▼
onedrive.live.com/		User1	
contoso.onmicrosoft.com/		Sites/User1	
contoso.sharepoint.com/		contoso_onmicrosoft_com/User1	
contoso-my.sharepoint.com/		personal/User1_contoso_onmicrosoft_com	

Explanation:

https://

	▼		▼
onedrive.live.com/		User1	
contoso.onmicrosoft.com/		Sites/User1	
contoso.sharepoint.com/		contoso_onmicrosoft_com/User1	
contoso-my.sharepoint.com/		personal/User1_contoso_onmicrosoft_com	

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds>

質問: 130

米国、ヨーロッパ、アジアのユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Microsoft Entra ID Protection を使用します。

仮想デスクトップインフラストラクチャ (VDI) を導入しています。すべての VDI サーバーは米国に設置されています。

ユーザーはラップトップと VDI から Microsoft 365 に接続します。

一部の VDI ユーザーからは、サインイン リスクが高いために Microsoft 365 へのサインインがブロックされているという報告があります。

VDI ユーザーが誤って Microsoft へのサインインをブロックされる可能性を減らす必要があります。

365. ソリューションでは、ID 保護を使用して VDI 環境からのサインインが保護されるようにする必要があります。

- A. 条件付きアクセスポリシー
- B. 衛星地理位置
- C. Microsoft 365 向け ExpressRoute
- D. 信頼できる場所

正解: (正解を表示します)

質問: 131

お客様のネットワークには、contoso.local という名前のオンプレミスの Active Directory ドメインが含まれています。このドメインには 5 台のドメイン コントローラーがあります。

貴社はMicrosoft 365を購入し、contoso.onmicrosoftという名前のMicrosoft Entraテナントを作成します。

と。

あなたは、メンバーサーバーにMicrosoft Entra Connect Syncをインストールし、パススルー認証を実装する予定です。

パススルー認証の実装を計画しているため、そのための環境を準備する必要があります。

実行すべき3つの行動はどれですか？それぞれの正解は、解決策の一部を示しています。

注：正解ごとに1ポイントが加算されます。

A. ドメインコントローラーから認証エージェントをインストールします

B. Microsoft Entra 管理センターから認証方法を設定します。

C. Active Director から、ドメインと信頼関係に UPN サフィックスを追加します

D. 各ユーザーアカウントのメールアドレス属性を変更します。

E. Microsoft Entra 管理センターから、カスタムドメイン名を追加します。

F. 各ユーザーアカウントのユーザーログオン名を変更します。

正解: ([正解を表示します](#))

Deploy Microsoft Entra ID Pass-through Authentication

Step 1: Check the prerequisites

Ensure that the following prerequisites are in place.

In the Entra admin center

1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Microsoft Entra tenant. This way, you can manage the configuration of your tenant should your on- premises services fail or become unavailable.

(E) 2. Add one or more custom domain names to your Microsoft Entra tenant. Your users can sign in with one of these domain names.

(A) In your on-premises environment

1. Identify a server running Windows Server 2016 or later to run Microsoft Entra Connect Sync. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.

2. Install the latest version of Microsoft Entra Connect Sync on the server identified in the preceding step. If you already have Microsoft Entra Connect Sync running, ensure that the version is supported.

3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.

4. Etc.

(B) Step 2: Enable the feature

Enable Pass-through Authentication through Microsoft Entra Connect Sync.

If you ' re installing Microsoft Entra Connect Sync for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Microsoft Entra Connect Sync. In addition, the Pass-through Authentication feature is enabled on your tenant.

Incorrect:

Not C: From Active Directory Domains and Trusts, add a UPN suffix

Not D. Modify the email address attribute for each user account.

Not F. Modify the User logon name for each user account.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start>

質問: 132

ホットスポット

Microsoft 365 サブスクリプションをお持ちです。

次の図に示すフィッシング対策ポリシーを展開します。

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

Add trusted senders and domains

Enable domains to protect

Enable users to protect

Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Add trusted senders and domains

Enable intelligence for impersonation protection

Enable spoof intelligence

正解:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

Add trusted senders and domains

Enable domains to protect

Enable users to protect

Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Add trusted senders and domains

Enable intelligence for impersonation protection

Enable spoof intelligence

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Add trusted senders and domains

Enable domains to protect

Enable users to protect

Phishing email threshold

Add trusted senders and domains

Enable intelligence for impersonation protection

Enable spoof intelligence

Box 1: Enable users to protect

Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.

User impersonation protection

User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.

You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).

When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender ' s email address, the action for impersonated users is applied to the message.

Box 2: Add trusted senders and domains

Trusted senders and domains

Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren ' t applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

質問: 133

Microsoft 365 サブスクリプションをお持ちです。

導入スコアを使用する予定であり、デバイスとソフトウェアのメトリクスを取得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. サポート統合を構成します。
- B. エンドポイント分析を有効にします。
- C. 各デバイスで Microsoft 365 ネットワーク接続テストを実行します。
- D. 特権アクセスを有効にします。

正解: (正解を表示します)

質問: 134

ホットスポット

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	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

「サポート」という単語が含まれるすべての部門のゲスト ユーザーを含む動的ユーザー グループを構成する必要があります。

会員規約をどのように完了すればよいですか? 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

(user.userType

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

正解:

Answer Area

(user.userType

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

Explanation:

Answer Area

(user.userType

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

Box 1: -eq " Guest "

Dynamic membership rules for groups in Microsoft Entra ID

Supported expression operators

The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

- * Equals
- eq
- * Contains
- contains
- * Etc.

Box 2: -contains " Support "

Incorrect:

- * -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notin operators.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

質問: 135

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

次の表に示すように、Intune に登録されているデバイスがあります。

Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1, Group3	Tag1
Device2	Android	Group2	Tag2

次の表に示すデバイス構成プロファイルを作成します。

Name	Platform	Assignments:		Scope tags
		Included groups	Excluded groups	
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	None	Default

各デバイスにはどのプロファイルが適用されますか? 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。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

正解:

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

Explanation:

Device 1:  Microsoft

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

質問: 136

あなたの会社は Microsoft 365 E5 サブスクリプションを持っています。

研究部門のユーザーは機密データを扱います。

電子メール メッセージやドキュメントに埋め込まれたハイパーリンクを使用して、研究部門のユーザーが安全でない可能性のある Web サイトにアクセスするのを防ぐ必要があります。他の部門のユーザーを制限してはなりません。

あなたは何をするべきか？

- A. コンテンツが共有されるという条件を持つデータ損失防止 (DLP) ポリシーを作成します。
- B. 安全なリンク ポリシーのグローバル設定を変更します。
- C. コンテンツが含まれる条件を持つデータ損失防止 (DLP) ポリシーを作成します。
- D. 新しい安全なリンク ポリシーを作成します。

正解: (正解を表示します)

Use the Microsoft Defender XDR portal to create Safe Links policies

In the Microsoft Defender XDR portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies & Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use <https://security.microsoft.com/safelinksv2>.

1. On the Safe Links page, select Create to start the new Safe Links policy wizard.

2. On the Name your policy page, configure the following settings:

Name: Enter a unique, descriptive name for the policy.

Description: Enter an optional description for the policy.

3. When you 're finished on the Name your policy page, select Next.

4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):

Users: The specified mailboxes, mail users, or mail contacts.

*- > Groups:

Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren ' t supported).

The specified Microsoft 365 Groups.
Domains: All recipients in the specified accepted domains in your organization.
Etc.
Reference:
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure>

有効的な**MS-102J**問題集はJPNTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTest.comは今最新**MS-102J**試験問題集を提供します。JPNTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> **598**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 137
Microsoft 365 E5 サブスクリプションをお持ちです。
貴社の Microsoft Secure Score は、次の資料に示されているアクションを推奨します。

Microsoft Secure Score

Overview

Recommended actions

History

Metrics & trends

↓ Export

	Rank	Recommended action	Score impact	Points achieved	Status
☐	1	Require multifactor authentication for administrative roles	+4.15%	0/10	☐ To address
☐	2	Ensure all users can complete multifactor authentication	+3.73%	0/9	☐ To address
☐	3	Create Safe Links policies for email messages	+3.73%	0/9	☐ To address
☐	4	Enable policy to block legacy authentication	+3.32%	0/8	☐ To address
☐	5	Turn on Safe Attachments in block mode	+3.32%	0/8	☐ To address
☐	6	Ensure that intelligence for impersonation protection is enabled	+3.32%	0/8	☐ To address
☐	7	Move messages that are detected as impersonated users by mailbox intelligence	+3.32%	0/8	☐ To address
☐	8	Enable impersonated domain protection	+3.32%	0/8	☐ To address

電子メール メッセージに対して [安全なリンクの作成] ポリシーを選択し、[ステータスとリスク] で [ステータス] を [リスクが受け入れられました] に変更します。アクションプランの設定。
この変更はセキュア スコアにどのような影響を与えますか？
A. 1ポイント減少

- B. 1ポイント増加
- C. 9 ポイント減少
- D. 9ポイント増加
- E. 変わらない
- 正解: (正解を表示します)

質問: 138

ホットスポット

会社では Microsoft Defender for Endpoint を使用しています。Microsoft Defender for Endpoint には、次の表に示すデバイス グループが含まれています。

Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	Not applicable

次の図に示すように、computer1 という名前のコンピューターを Microsoft Defender for Endpoint にオンボードします。

Settings > Endpoints > computer1

Microsoft

 **computer1**

Device summary

Risk level ⓘ

 None

Device details

Domain
adatum.com

OS
Windows 10 64-bit
Version 21H2
Build 19044.2130

ドロップダウンメニューを使用して、各ステートメントを完了する回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

正解:

Answer Area

Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

Explanation:

Answer Area

Microsoft

Computer1 will be a member of [answer choice].

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

Group1 only

Group1 and Group2 only

Group1, Group2, Group3, and Group4

Ungrouped devices

Box 1: Group3 and Group4 only
Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10.
Box 2: Group1, Group2, Group3 and Group4

質問: 139

会社には Microsoft 365 E5 サブスクリプションがあります。
会社のネットワーク上のデバイスを Microsoft Defender for Endpoint にオンボードします。
Microsoft Defender ポータルで、デバイス インベントリに、オンボード状態がオンボード可能となっているデバイスが多数表示されていることがわかります。
オンボードされたデバイスがデバイス検出のためにネットワークをポーリングできないようにしながらも、直接通信するデバイスは検出できるようにする必要があります。
Microsoft Defender ポータルでは何を構成する必要がありますか？

- A. ネットワーク評価ジョブ
- B. 基本的な検出
- C. デバイス検出の除外
- D. 標準検出

正解: [\(正解を表示します\)](#)

質問: 140

User1 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。
次の図に示すように、Policy1 という名前の送信スパム対策ポリシーを作成します。

Protection settings

Set your outbound anti-spam settings for this policy.

Message limits

Set an external message limit

10

Set an internal message limit

20



Set a daily message limit

1000

Restriction placed on users who reach the message limit

Restrict the user from sending mail until the following day

Forwarding rules

Automatic forwarding rules

Automatic - System-controlled

Notifications

- ☐ Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups
- ☐ Notify these users and groups if a sender is blocked due to sending outbound spam

Policy1 を User1 に割り当てます。
ユーザー 1 が 24 時間に送信できる電子メール メッセージの最大数はいくつですか？
A. 1030
B. 30
C. 1000
D. 720
正解: [\(正解を表示します\)](#)

質問: 141
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	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

次の図に示すように、登録ステータス ページのプロファイルを構成します。

Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress.

Yes No

Show time limit error when installation takes longer than specified number of minutes.

60

Show custom message when time limit error occurs.

Yes No

Allow users to collect logs about instalattion errors.

Yes No

Only show page to devices provisioned by out-of-box experience (OOBE)

Yes No

Block device use until all apps and profiles are installed

Yes No

ポリシーを Group1 に割り当てます。

次の表に示すデバイスを購入します。

Name	Platform
Device1	Windows 10
Device2	Android

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 User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	☐	☐
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	☐	☐
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	☐	☐

正解:

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	☒	☐
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	☐	☒
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	☐	☒

Explanation:

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	☒	☐
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	☐	☒
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	☐	☒

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>

質問: 142

Microsoft 365 サブスクリプションがあり、Microsoft Defender for Office 365 を使用しています。ソーシャル エンジニアリングのリスクに関連するトピックについてユーザーを教育するためのソリューションを推奨する必要があります。ユーザーは、学習タスクを完了するためのリマインダーを毎週受け取る必要があります。

Microsoft Defender ポータルでは何を使用すればよいですか？

- A. 学習ハブ
- B. 攻撃シミュレーション訓練
- C. キャンペーン
- D. 脅威トラッカー

正解: B (コメントを发表する)

質問: 143

お客様は、以下の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションをご利用されています。

Name	Assigned role
User1	Groups Administrator
User2	User Administrator
User3	Teams Administrator

ユーザーオブジェクトを作成できるユーザーと、Microsoft 365 グループを作成できるユーザーはどれですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area



User objects:

User2 only

User2 onlyUser1 and User2 onlyUser2 and User3 onlyUser1, User2, and User3

Microsoft 365 groups:

User1 onlyUser1 and User2 onlyUser1 only User3 onlyUser1, User2, and User3

正解:

User objects:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Microsoft 365 groups:

- User1 only
- User1 and User2 only
- User1 only User3 only
- User1, User2, and User3



Explanation:



User objects:

Microsoft 365 groups:

質問: 144

Microsoft Intune と Microsoft Defender XDR が含まれる 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 Windows 11 を実行するデバイスを所有しています。Microsoft Defender ポータルから、Microsoft Secure Score の推奨事項を確認します。最も重要な推奨事項の 1 つは、すべての Microsoft Office アプリケーションによる子プロセスの作成をブロックすることです。推奨事項に対処して、セキュリティ スコアを高める必要があります。何をすべきでしょうか？

- A. エンドポイント検出および応答 (EDR) ポリシーを構成します。
- B. Office アプリケーションのポリシーを作成します。
- C. Office クライアントの安全なドキュメントを選択します。
- D. 攻撃対象領域縮小 (ASR) ポリシーを作成します。

正解: [\(正解を表示します\)](#)

質問: 145

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。ユーザー認証方法としてPasskey(FIDO2)を使用する認証ポリシーを実装する予定です。登録時に、各Passkey(FIDO2)がFIDO Allianceメタデータサービスを使用して検証されるようにする必要があります。どの設定を有効にする必要がありますか？

- A. キー制限の適用
- B. 特定のキーを制限する

- C. 認証を強制する
- D. セルフサービス設定を許可する

正解: C ([コメントを发表する](#))

質問: 146

外部ユーザーとのクレジット カード情報の共有を保護するデータ損失防止 (DLP) ポリシーをテストしています。テスト中に、ユーザーが電子メールを使用して外部ユーザーとクレジット カード情報を共有できることがわかりました。ただし、ユーザーは Microsoft SharePoint を使用してクレジット カード情報を含むファイルを共有することはできません。ユーザーが電子メールや SharePoint を使用してクレジット カード情報を共有できないようにする必要があります。何を設定すればよいでしょうか？

- A. DLP ポリシーのステータス
- B. DLP ポリシー ルールの条件
- C. DLP ポリシー ルールのユーザー オーバーライド
- D. DLP ポリシーの場所

正解: ([正解を表示します](#))

質問: 147

Microsoft 365 テナントがあります。Endpoint Protection デバイス構成プロファイルを実装する予定です。プロファイルを使用して管理できるプラットフォームはどれですか？

- A. アンドロイド
- B. CentOS Linux
- C. iOS
- D. ウィンドウ 10

正解: ([正解を表示します](#))

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure>

質問: 148

User1 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1は、1日あたりのメール送信数の上限を超えており、制限対象エンティティリストに登録されています。ユーザー1を制限対象エンティティリストから削除する必要があります。どのような方法がありますか？

- A. Microsoft Purview ポータル
- B. Microsoft Entra 管理センター
- C. Microsoft 365 管理センター
- D. Exchange 管理センター
- E. Microsoft Defender ポータル

正解: ([正解を表示します](#))

質問: 149

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

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

このセクションの質問に回答した後は、戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 E5 サブスクリプションがあり、Microsoft Defender for Office 365 を使用しています。

スパム、フィッシング、マルウェアから保護するために、バランスの取れたベースライン保護プロファイルを適用する脅威ポリシーを実装する必要があります。

解決策: 標準のプリセット セキュリティ ポリシーを作成します。

これは目標を満たしていますか？

- A. はい
 - B. いいえ
- 正解: [\(正解を表示します\)](#)

質問: 150

Microsoft 365 E5 サブスクリプションをお持ちです。

Microsoft Entra のユーザー管理者ロールに対して Privileged Identity Management (PIM) を構成する必要があります。対象ユーザーは、次の要件を満たしている必要があります。

- * 常にユーザー管理者ロールをリクエストできます。
- * ユーザー管理者ロールを申請する際には理由を明記する必要があります
- * ユーザー管理者ロールをアクティブ化するときには多要素認証 (MFA) を要求する必要があります。ソリューションでは、管理の労力を最小限に抑える必要があります。

Answer Area

Always be able to request the User Administrator role:

Select Require approval to activate.

Set Allow permanent active assignment to Yes.

Set Allow permanent eligible assignment to Yes.

Must provide a reason when requesting the User Administrator role:

Select Require justification on activation.

Select Require ticket information on activation.

Set Require justification on active assignment to Yes.

Must require MFA when activating the User Administrator role:

Set On activation require to Azure MFA.

Set On activation require to Microsoft Entra Conditional Access authentication context.

Set Require Azure Multi-Factor Authentication on active assignment to Yes.

正解:

Answer Area

The screenshot shows three configuration settings for the User Administrator role in Microsoft Entra ID:

- Always be able to request the User Administrator role:** A dropdown menu with the selected option "Require approval to activate". Below it are two checkboxes: "Set Allow permanent active assignment to Yes" and "Set Allow permanent eligible assignment to Yes".
- Must provide a reason when requesting the User Administrator role:** A dropdown menu with the selected option "Require justification on activation". Below it are two checkboxes: "Set Require justification on activation" and "Set Require justification on active assignment to Yes".
- Must require MFA when activating the User Administrator role:** A dropdown menu with the selected option "Require Azure Multi-Factor Authentication on active assignment to Yes". Below it are two checkboxes: "Set On activation require to Azure MFA" and "Set On activation require to Microsoft Entra Conditional Access authentication context".

Explanation:

Always be able to request the User Administrator role: Setting " Allow permanent eligible assignment to Yes

" ensures that users can always request the User Administrator role when needed.

Must provide a reason when requesting the User Administrator role: Selecting " Require justification on activation " ensures that users must provide a reason each time they activate the User Administrator role, which adds a layer of accountability and tracking.

Must require MFA when activating the User Administrator role: Setting " Require Azure Multi-Factor Authentication on active assignment to Yes " ensures that users must perform MFA to activate the User Administrator role, enhancing security.

質問: 151

お客様のネットワークには、オンプレミスのActive Directoryドメインサービス(AD DS)ドメインが含まれています。このドメインには、500台のWindows 11デバイスが接続されています。

Sub1という名前のMicrosoft 365サブスクリプションをお持ちです。

あなたは、Microsoft Entra Connect Syncを使用して、ドメインをSub1にリンクされているMicrosoft Entraテナントと同期させる予定です。

ユーザーが認証を求められることなく、デバイスからSub1にアクセスできることを確認する必要があります。

解決策は、管理上の負担を最小限に抑えるものでなければならない。

あなたはすべきでしょうか？

A. パスワードハッシュの同期を設定します。

B. パススルー認証を設定します。

C. デバイスをハイブリッド結合します。

D. デバイスをテナントに参加させます。

正解: C ([コメントを发表する](#))

The correct answer is Hybrid join the devices. The devices already belong to an on-premises AD DS domain and run Windows 11, so the lowest-impact approach is to configure Microsoft Entra hybrid join. A Microsoft Entra hybrid joined device remains joined to the on-premises AD DS domain while also being registered in Microsoft Entra ID, which is the correct identity state for existing domain-joined Windows devices that need cloud access with single sign-on behavior. Microsoft's hybrid join guidance shows that Microsoft Entra Connect can be used to configure Microsoft Entra hybrid join through Configure device options, minimizing manual device-by-device work.

Password hash synchronization and pass-through authentication are user sign-in methods; they do not by themselves join or register the Windows 11 devices to Microsoft Entra ID. They address how credentials are validated, not whether the device has a cloud device identity for seamless access. Joining the devices directly to the tenant would mean Microsoft Entra joining them, which is more disruptive for existing AD DS domain-joined devices. Microsoft Entra joined devices are joined only to Microsoft Entra ID, while hybrid joined devices are intended for organizations that still use on-premises AD DS.

Therefore, select C. Hybrid join the devices.

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> **598**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 152

Microsoft Purview コンプライアンス ポータルから、Policy 1 という名前の保持ポリシーを作成します。
すべてのユーザーがポリシーを無効にしたり、保存期間を短縮したりできないようにする必要があります。
Azure PowerShell コマンドは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。

Answer Area

Set-RetentionCompliancePolicy

Set-ComplianceTag

Set-HoldCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Set-RetentionPolicyTag

-Identity "Policy1"

-RestrictiveRetention

enabled

-Force

-RestrictiveRetention

-RetentionPolicyTagLinks

-SystemTag

\$true

正解:

Answer Area

Set-RetentionCompliancePolicy

Set-ComplianceTag

Set-HoldCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Set-RetentionPolicyTag

-Identity "Policy1"

-RestrictiveRetention

enabled

-Force

-RestrictiveRetention

-RetentionPolicyTagLinks

-SystemTag

\$true

Explanation:

Answer Area

Set-RetentionCompliancePolicy

-Identity "Policy1"

-RestrictiveRetention

\$true

質問: 153

500 台の Windows 10 デバイスを含む Microsoft 365 E5 テナントがあります。デバイスは Microsoft intune に登録されています。
エンドポイント分析を使用してハードウェアの問題を特定する予定です。
エンドポイント分析をサポートするには、デバイス上で Windows ヘルス モニタリングを有効にする必要があります。
A. Windows 10 セキュリティ ベースライン プロファイルを作成する
B. コンプライアンス ポリシーを作成します。

- C. 構成プロファイルを作成します。
- D. エンドポイント分析のベースライン回帰しきい値を構成します。

正解: C ([コメントを発表する](#))

質問: 154

Microsoft 365 E5 サブスクリプションがあり、Microsoft Defender for Cloud Apps を使用しています。
Cloud Discovery によって検出されたすべてのアプリのセキュリティ監査を実行する予定です。
監査されたアプリを追跡する必要があります。ソリューションでは、監査対象アプリのリストがクラウドアプリカタログに表示されるようにする必要があります。

- A. 各アプリを重要な資産として定義します。
- B. 条件付きアクセス アプリ制御を展開します。
- C. 各アプリにカスタム アプリ タグを適用します。
- D. Cloud Discovery スナップショット レポートを生成します。
- E. アプリガバナンスを有効にします。

正解: ([正解を表示します](#))

質問: 155

Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Teams メッセージによる財務データの共有を防ぐ、DLP1 という新しいデータ損失防止 (DLP) ポリシーを作成します。このポリシーを財務部門のユーザーに適用します。
User1 という財務部門のユーザーが、外部メンバーを含む Teams チャンネルで財務データを共有すると、インシデントが発生します。
User1 が Teams を使用して 1 対 1 のチャットまたはプライベート チャンネルで同じメッセージを送信すると、メッセージは予想どおりにブロックされます。
User1 が外部メンバーを含む Teams チャンネルで財務データを共有できないようにする必要があります。
何をすべきでしょうか？

- A. DLP1 の場所設定を編集します。
- B. User1 に割り当てられたライセンスを変更します。
- C. DLP1 のポリシー ルールを編集します。
- D. チャンネルを含むチームの設定を編集します。

正解: C ([コメントを発表する](#))

質問: 156

ホットスポット

Microsoft 365 E3 サブスクリプションをお持ちです。
すべてのユーザーを対象に攻撃シミュレーション トレーニングを開始する予定です。
どのようなソーシャル エンジニアリング手法とトレーニング エクスペリエンスが利用可能でしょうか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area



Social engineering technique:

☐ Credential harvest
☐ Link to malware
☐ Malware attachment

Training experience:

☐ Identity Theft
☐ Mass Market Phishing
☐ Web Phishing

正解:

Answer Area



Social engineering technique:

☒ Credential harvest
☒ Link to malware
☐ Malware attachment

Training experience:

☒ Identity Theft
☒ Mass Market Phishing
☐ Web Phishing

Explanation:

Answer Area

Social engineering technique:

Credential harvest

Link to malware

Malware attachment

Training experience:

Identity Theft

Mass Market Phishing

Web Phishing

Box 1: Credential Harvest

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select ' ISA Phishing ' or ' Mass Market Phishing ' training experiences. No other capabilities are part of the E3 trial offering.

Note: In Attack simulation training, multiple types of social engineering techniques are available:

Credential Harvest

Malware Attachment

Link to Malware

Etc.

Box 2: Mass Market Phishing

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started>

質問: 157

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

Name	Platform
Device1	Windows 11
Device2	Linux
Device3	MacOS

Defender Update コントロール テンプレートを使用してエンドポイント セキュリティ ポリシーを作成する予定です。どのデバイスにポリシーを適用できますか？

- A. デバイス1とデバイス2のみ
- B. Devke1、Device2、および Devke3
- C. Devke1 と Device3 のみ
- D. デバイス1のみ

正解: (正解を表示します)

質問: 158

Microsoft Defender for Office 365 を使用する Microsoft 365 E5 サブスクリプションがあります。次の表に示すポリシーがあります。

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

すべてのポリシーは、悪意のある電子メール メッセージを検疫に送信するように構成されています。カスタマイズされた隔離保持期間をサポートするポリシーはどれですか？

- A. ポリシー 1 とポリシー 2 のみ
- B. ポリシー 2 とポリシー 4 のみ
- C. ポリシー 3 とポリシー 4 のみ
- D. ポリシー 1 およびポリシー 3 のみ

正解: (正解を表示します)

質問: 159

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

Microsoft Defender ポータルから、次の表に示す Microsoft Secure Score の改善アクションを確認します。

Recommended action	Status	Points achieved
Enable Conditional Access policies to block legacy authentication	To address	0/9
Ensure user consent to apps accessing company data on their behalf is not allowed	To address	0/4
Create an app discovery policy to identify new and trending cloud apps in your org	To address	0/3

次の表に示すように、改善アクションのステータスを更新する予定です。

Recommended action	Status
Enable Conditional Access policies to block legacy authentication	Risk accepted
Ensure user consent to apps accessing company data on their behalf is not allowed	Resolved through third party
Create an app discovery policy to identify new and trending cloud apps in your org	Planned

アップデート後、セキュア スコアは何ポイント増加しますか？

- A. 7
- B. 4
- C. 0
- D. 13
- E. 16

正解: (正解を表示します)

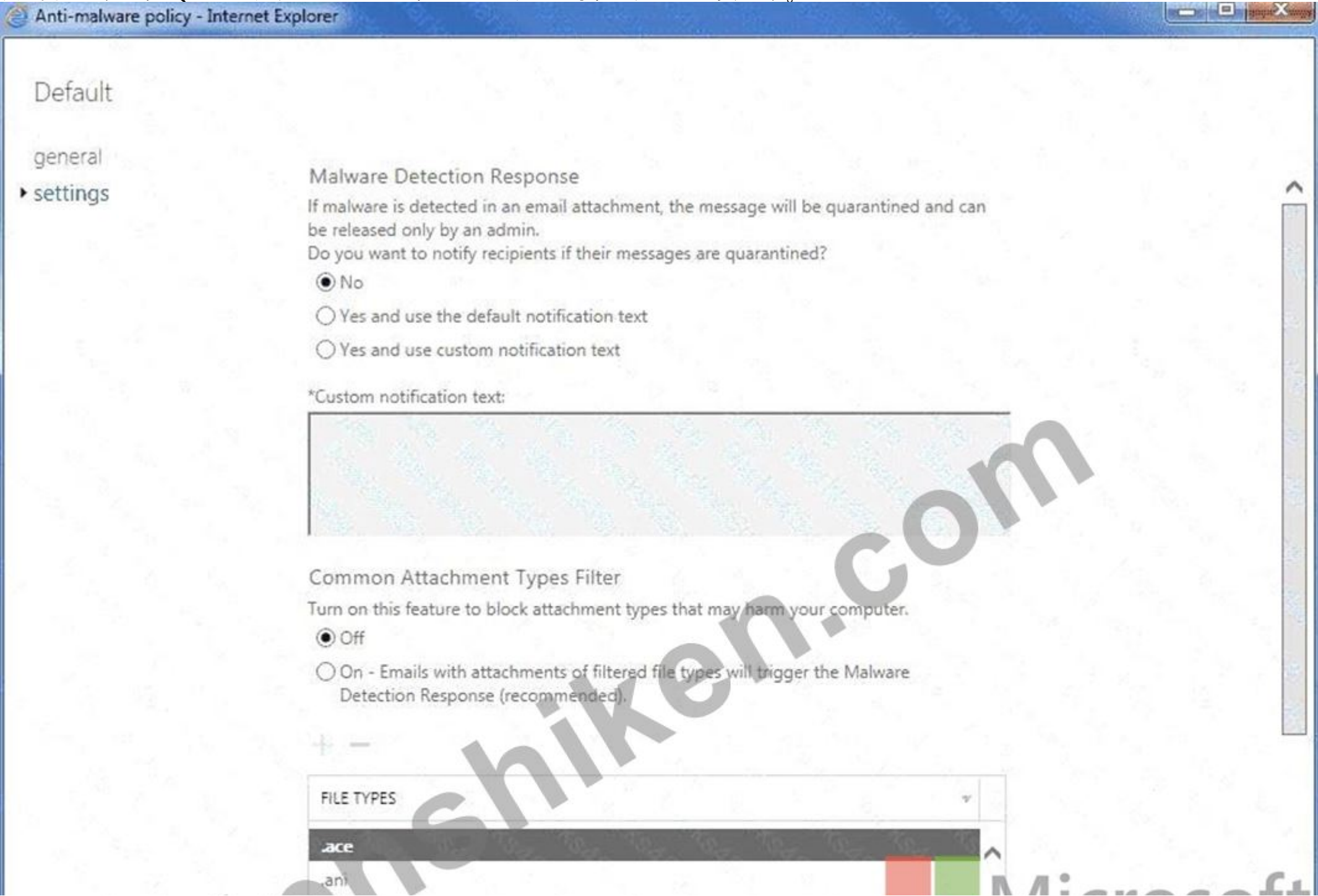
質問: 160

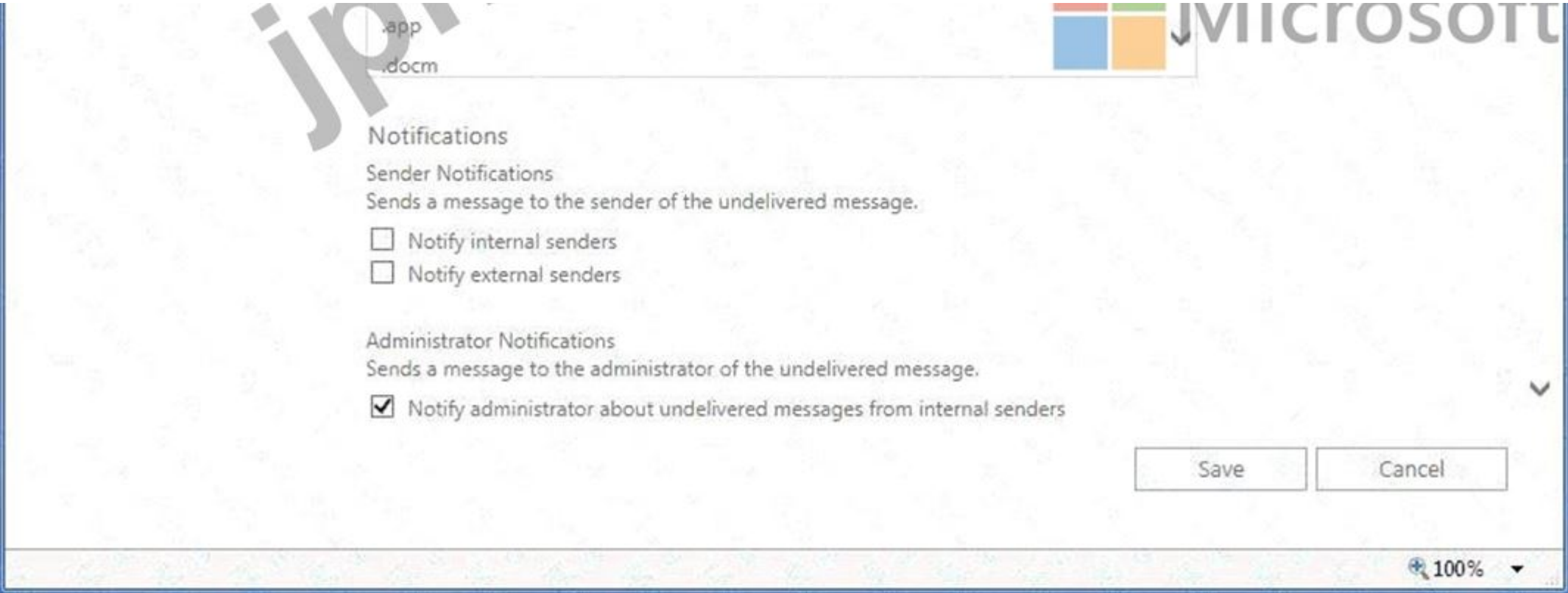
Microsoft 365 E5 サブスクリプションをお持ちです。
ユーザーのメールボックスのアクティビティを監視するには、Microsoft Defender for Cloud Apps を使用する必要があります。どうすればよいでしょうか？

A. アクティビティ ポリシーを作成します。
B. メールボックス監査ログを有効にします。
C. アクセス ポリシーを作成します。
D. Microsoft 365 用のアプリ コネクタを作成します。

正解: (正解を表示します)

質問: 161
User1 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。
次の図に示すように、サブスクリプションには単一のマルウェア対策ポリシーがあります。





テキストと 2 つの添付ファイルを含む電子メール メッセージが User1 に送信されます。添付ファイルの 1 つがマルウェアに感染しています。

電子メール メッセージと添付ファイルはどのように処理されますか？

- A.** 両方の添付ファイルが削除されます。電子メール メッセージは隔離され、使用者は添付ファイルのない電子メール メッセージと、「マルウェアは削除されました。」というテキストを含む電子メール メッセージを受け取ります。
- B.** 電子メール メッセージは隔離され、メッセージは配信されないままになります。
- C.** 両方の添付ファイルが削除されます。電子メール メッセージは隔離され、User1 は元のテキストを含むメッセージのコピーと、次のテキストを含む新しい添付ファイルを受信します。
「マルウェアは削除されました。」
- D.** マルウェアに感染した添付ファイルは削除されます。電子メール メッセージは隔離され、User1 は感染していない添付ファイルのみを含むメッセージのコピーを受け取ります。

正解: (正解を表示します)

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies>

質問: 162

次の表に示すセキュリティ 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	Membership type	Membership rule
Group1	Assigned	Not applicable
Group2	Dynamic	(user.department -eq "Finance")
Group3	Dynamic	(user.department -eq "R&D")

サブスクリプションには、次の表に示すユーザーが含まれます。

Name	Department	Assigned group membership
User1	Finance	Group1
User2	Technical	None
User3	R&D	Group1

次の設定を持つ条件付きアクセス ポリシーがあります。

* Assignments

o Users

Include: Group1

Exclude: Group2, Group3

o Target resources

Cloud apps

App1

Access controls

Grant

Block access

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Statements	Yes	No
User1 can sign in to App1.	☐	☐
User2 can sign in to App1.	☐	☐
User3 can sign in to App1.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 can sign in to App1.	☒	☐
User2 can sign in to App1.	☐	☒
User3 can sign in to App1.	☐	☒

Explanation:

Answer Area

Statements	Yes	No
User1 can sign in to App1.	☒	☐
User2 can sign in to App1.	☐	☒
User3 can sign in to App1.	☐	☒

質問: 163

Microsoft 365 E5 サブスクリプションをお持ちで、Microsoft Defender for Cloud Apps をご利用です。このサブスクリプションには、Windows 11 デバイスを所有するユーザーが含まれています。デバイス上のクラウドアプリの使用状況を分析するには、Cloud Discovery スナップショットレポートを使用する必要があります。レポートを生成する前に何をすればよいでしょうか？

- A. アプリ検出ポリシーを作成します。
- B. アクティビティ ポリシーを作成します。
- C. ファイアウォールとプロキシからトラフィック ログをエクスポートします。
- D. デバイスに Azure Monitor エージェントをデプロイします。

正解: (正解を表示します)

質問: 164

Admin1 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。

あなたの会社は、Branch という名前の新しいブランチ オフィスを展開します。

Admin1にBranch1を管理する権限を与える必要があります。ソリューションは以下の要件を満たす必要があります。

- * Admin1 は、Office の場所が Branch1 に設定されているユーザーのみを管理できる必要があります。
- * Admin1 は、Branch1 内のユーザーに対してのみ、パスワードのリセット、ユーザー ライセンスの管理、ユーザー属性の変更を行える必要があります。

Branch1 ユーザーを整理するには何を使用すればいいですか。また、Admin1 にはどのロールを割り当てる必要がありますか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Use:	An administrative unit An administrative unit A Microsoft 365 group A security group
Role:	User Administrator Help Desk Administrator Password Administrator User Administrator

正解:

Answer Area



Use:

Role:

Explanation:

Answer Area

Use:

Role:

質問: 165

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。

このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。

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

Microsoft Entra テナントをデプロイします。

別の管理者が、ドメインを Microsoft Entra ID と同期するように設定します。

組織単位(OU)内の10個のユーザーアカウントが Microsoft Entra ID と同期されていないことが判明しました。その他のユーザーアカウントはすべて正常に同期されています。

Microsoft Entra Connect Healthを確認したところ、すべてのユーザーアカウントの同期が正常に完了していたことがわかりました。

10個のユーザーアカウントが Microsoft Entra ID と同期されていることを確認する必要があります。

解決策：同期ルールエディタから、新しい送信同期ルールを作成します。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解: ([正解を表示します](#))

The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

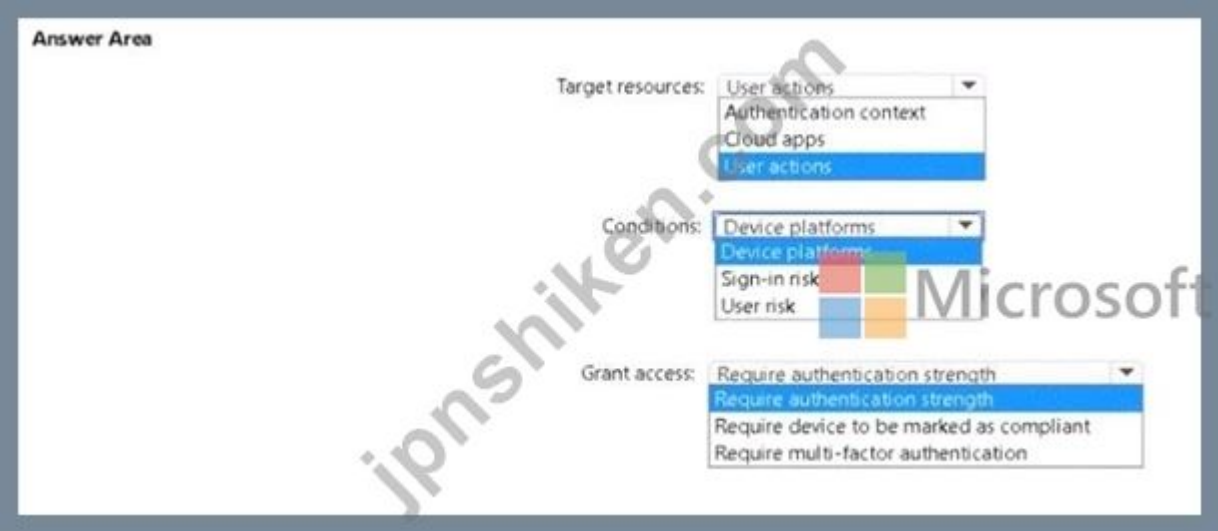
質問: 166

Microsoft 365 E5 サブスクリプションをお持ちです。

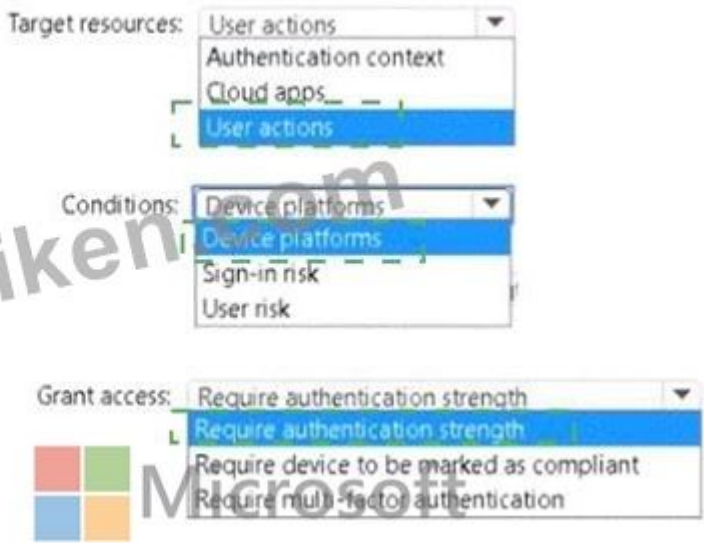
ユーザーが Windows デバイスを Microsoft Entra ID に参加させる場合にのみ FID02 セキュリティ キーの使用を要求する条件付きアクセス ポリシーを作成する必要があります。

ポリシーは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。

注意 正しい選択はそれぞれ 1 ポイントの価値があります。



正解:



Explanation:



有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 167
ホットスポット
Microsoft 365 E5 サブスクリプションをお持ちです。
ID 保護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。

- * ユーザーの資格情報が侵害され、ダークウェブ上で共有されたことを識別します。
 - * 資格情報が侵害されたユーザーに自己修復機能を提供します。
- どうすればいいのでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
- 注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area



To identify when **users** have compromised credentials, configure:

A registration policy

A sign-in risk policy

A user risk policy

A multifactor authentication registration policy

To enable self-remediation, select:

Generate a temporary password

Require multi-factor authentication

Require password change

正解:

Answer Area



To identify when users have compromised credentials, configure:

A registration policy

A sign-in risk policy

A user risk policy

A multifactor authentication registration policy

To enable self-remediation, select:

Generate a temporary password

Require multi-factor authentication

Require password change

Explanation:

Answer Area

To identify when users have compromised credentials, configure:

A registration policy

A sign-in risk policy

A user risk policy

A multifactor authentication registration policy

 Microsoft

To enable self-remediation, select:

Generate a temporary password

Require multi-factor authentication

Require password change

Box 1: A user risk policy

Identify when a user ' s credentials are compromised and shared on the dark web.

User risk-based Conditional Access policy

Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:

Block access

Allow access but require a secure password change.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.

Box 2: Require password change

Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#user-risk-based-conditional-access-policy>

質問: 168

営業部門のすべてのユーザーが Project1 と Project2 中に正常に認証できることを確認する必要があります。

パイロット プロジェクトにはどの認証戦略を実装する必要がありますか？

- A. パススルー認証
- B. パススルー認証とシームレスな SSO
- C. パスワード ハッシュ同期とシームレスな SSO
- D. パスワードハッシュ同期

正解: (正解を表示します)

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

Fabrikam does NOT plan to implement identity federation.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

質問: 169

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	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

Exchange 電子メールに発行される Retention1 という名前の Microsoft Office 365 保持ラベルがあります。
すべてのメールボックスに適用される Microsoft Exchange Online アイテム保持ポリシーがあります。保持ポリシーには、Retention2 という名前の保持タグが含まれています。
どのユーザーが自分の電子メールに Retention1 と Retention2 を割り当て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。

Users who can assign Retention1:

User4 only
User3 and User4 only
User2, User3, and User4 only
User1, User2, User3, and User4

Users who can assign Retention2:

User4 only
User3 and User4 only
User2, User3, and User4 only
User1, User2, User3, and User4

正解:

Users who can assign Retention1:

User4 only
User3 and User4 only
User2, User3, and User4 only
User1, User2, User3, and User4

Users who can assign Retention2:

User4 only
User3 and User4 only
User2, User3, and User4 only
User1, User2, User3, and User4

Explanation:

Microsoft

Users who can assign Retention1:

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

Users who can assign Retention2:

User4 only

User3 and User4 only

User2, User3, and User4 only

User1, User2, User3, and User4

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

質問: 170

ログ分析の技術要件を満たす必要があります。
Microsoft Cloud App Security から作成する必要があるデータ ソースとログ コレクターの最小数はいくつですか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Microsoft

Minimum number of data sources:

1

3

6

Minimum number of log collectors:

1

3

6

正解:

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6

Explanation:

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6

References:

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

質問: 171

Microsoft 365 E5 サブスクリプションをお持ちです。

条件付きアクセスは、すべてのユーザーのリスクの高いサインインをブロックするように構成されています。

すべてのユーザーはフランスにおり、多要素認証 (MFA) に登録されています。

メディア部門のユーザーは来月中にさまざまな国を旅行します。

メディア部門のユーザーが旅行中にサインインできない場合でも、ユーザーが管理者の介入なしに問題を解決できることを確認する必要があります。

何を設定すればよいのでしょうか？

- A. 除外グループ
- B. MFA 登録ポリシー
- C. 名前付きの場所
- D. セルフサービス パスワード リセット (SSPR)

正解: D ([コメントを发表する](#))

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

質問: 172

あなたの会社にはシアトルとデンバーにオフィスがあります。

Microsoft 365 サブスクリプションをお持ちです。

多要素認証 (MFA) を適用する Policy1 という名前の条件付きアクセス ポリシーを作成する予定です。

シアトルオフィスのユーザーがMFAから除外されていることを確認する必要があります。デンバーオフィスのユーザーには常にMFAの入力を求める必要があります。

Policy1 には何を設定する必要がありますか？

- A. シアトルオフィスからのVPN接続
- B. 認証の強度
- C. IP範囲の場所がシアトルオフィスに設定されている名前付き場所
- D. 国が米国に設定されている名前付き場所

正解: (正解を表示します)

質問: 173

Microsoft 365 E5 サブスクリプションがあり、その中に user1@contoso.com と user2@contoso.com という 2 人のユーザーと、Site1 という Microsoft SharePoint サイトが含まれています。

次の表に示す高度な DLP ルールを持つ、DLP1 という名前のデータ損失防止 (DLP) ポリシーを作成します。

Name	Content contains	User notifications	Priority
Rule1	4 or more IP addresses	User1@contoso.com	0
Rule2	2 or more IP addresses	User1@contoso.com	1
Rule3	3 or more IP addresses	User2@contoso.com	2

DLP1 は Site1 に適用されます。

次の表に示すファイルがあります。

Name	Number of IP addresses in the file
File1.xlsx	2
File2.doc	3
File3.pptx	4
File4.txt	1

ファイルを Site1 にコピーします。

各ユーザーが受け取る通知の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。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

User1@contoso.com:

User2@contoso.com:

Microsoft

正解:

Answer Area

Microsoft

User1@contoso.com:

User2@contoso.com:

Explanation:

User1@contoso.com: 2 notifications

User2@contoso.com: 1 notification

User1@contoso.com: 2 notifications

File3.pptx contains 4 IP addresses, which matches Rule1 (4 or more IP addresses), triggering a notification to User1.
File4.txt contains 6 IP addresses, which also matches Rule1, triggering another notification to User1.
Therefore, User1 receives 2 notifications.
User2@contoso.com: 1 notification
File2.doc contains 3 IP addresses, which matches Rule3 (3 or more IP addresses), triggering a notification to User2. Therefore, User2 receives 1 notification.

質問: 174

あなたの会社には Microsoft E5 テナントがあります。
企業は ISO/IEC 27001:2013 規格の要件を満たさなければなりません。
会社の現在のコンプライアンス状態を評価する必要があります。
何をえばいいのでしょうか？

- A. 電子情報開示
- B. 情報ガバナンス
- C. コンプライアンスマネージャー
- D. データ主体リクエスト (DSR)

正解: (正解を表示します)

Reference:
<https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001>

質問: 175

Microsoft 365 E5 サブスクリプションがあり、Microsoft Purview を使用しています。サブスクリプションには、次の表に示すデバイスが含まれています。

Name	Platform
Device1	Windows 11
Device2	macOS
Device3	Android
Device4	Linux

すべてのデバイスが Microsoft Defender for Endpoint にオンボードされています。エンドポイント データ損失防止 (エンドポイント DLP) ポリシーを展開する予定です。DLP ポリシーを使用して保護できるデバイスはどれですか。

- A. デバイス1、デバイス2、デバイス3のみ
- B. デバイス1、デバイス2、デバイス3、デバイス4
- C. デバイス1、デバイス3、デバイス4のみ
- D. デバイス1のみ
- E. デバイス1とデバイス2のみ

正解: (正解を表示します)

質問: 176

Microsoft Intune に登録された 500 台の Android デバイスを含む Microsoft 365 E5 テナントがあります。
マネージド Google Play アプリをデバイスに展開するには、Microsoft エンドポイント マネージャーを使用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

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

Answer Area

正解:

Actions

Create an app configuration policy

Link the account to Intune

Create a Microsoft account

Configure a mobile device management (MDM) push certificate

Add the app

Create a Google account

Assign the app

Answer Area

Create a Google account

Link the account to Intune

Add the app

Assign the app

Explanation:



Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a-managed-google-play-app-to-android-enterprise-fully-managed-devices>

質問: 177

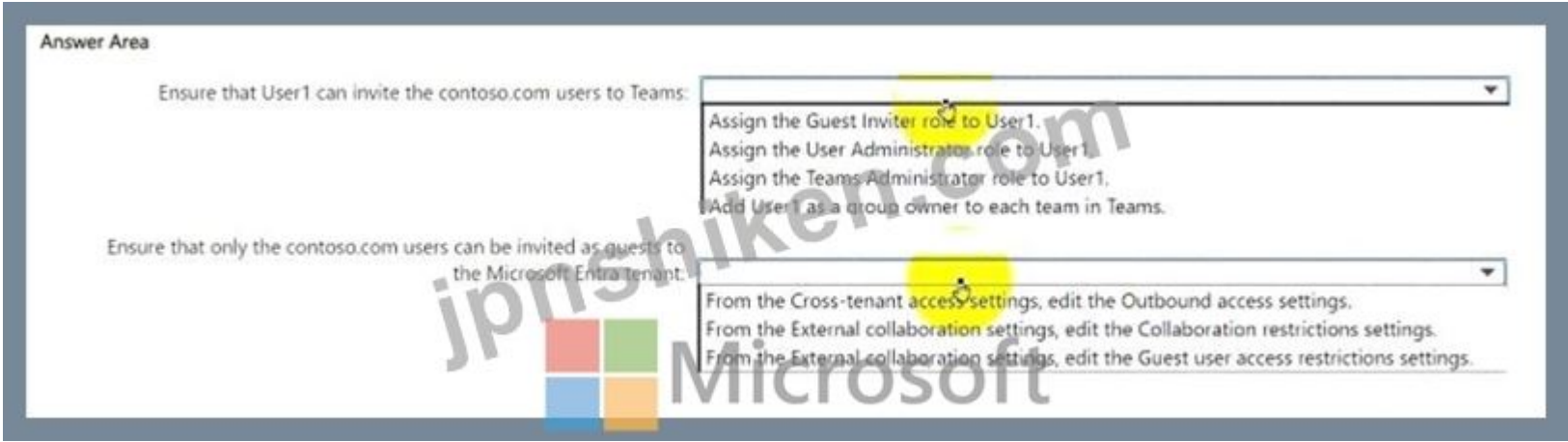
adatum.com というドメイン名を使用する Microsoft 365 サブスクリプションがあります。

Microsoft Entra ID では、ゲスト招待の制限を、特定の管理者ロールに割り当てられたユーザーのみがゲスト ユーザーを招待できるように設定しました。

used@adatum.com というユーザーは、contoso.com というドメインの外部ユーザーを Microsoft Teams での共同作業に招待できなくなったと報告しています。

次の要件を満たすように Microsoft Entra ID 構成を変更する必要があります。

- * User1 が contoso.com ユーザーを Teams に招待できることを確認します。
 - * contoso.com ユーザーのみを Microsoft Entra テナントにゲストとして招待できるようにします。
 - * 最小権限の原則に従う
- 各要件に対して何をすべきか」に回答するには、回答領域で適切なオプションを選択します。



正解:

Answer Area

Ensure that User1 can invite the contoso.com users to Teams:

- Assign the Guest Inviter role to User1.
- Assign the User Administrator role to User1.
- Assign the Teams Administrator role to User1.
- Add User1 as a group owner to each team in Teams.

Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant:

- From the Cross-tenant access settings, edit the Outbound access settings.
- From the External collaboration settings, edit the Collaboration restrictions settings.
- From the External collaboration settings, edit the Guest user access restrictions settings.

Explanation:

Ensure that User1 can invite the contoso.com users to Teams: Assign the Guest Inviter role to User1 Assigning the Guest Inviter role ensures that User1 has the necessary permissions to invite external users, such as those from contoso.com, to Microsoft Teams.

Ensure that only the contoso.com users can be invited as guests to the Microsoft Entra tenant: From the External collaboration settings, edit the Guest user access restrictions settings Modifying the Guest user access restrictions settings under External collaboration ensures that only users from specific domains, like contoso.com, can be invited as guests to the Microsoft Entra tenant.

質問: 178

Microsoft 365 サブスクリプションをお持ちです。
Microsoft 365 管理センターから、次の図に示すように Microsoft 365 Apps 使用状況レポートを開きます。

Username ⓘ	Last activation date (UTC)	Last activity date (UTC)	Choose columns
431B8D0D1D05D877FDC4416			
2F2747649D4150B686307383			
659213C0E1D99EA1A4AD56D	Wednesday, August 3, 2022		
FE185622F642B0381DB633EC			
988D39ED225FC80FF2A5684			

レポートが次の要件を満たしていることを確認する必要があります。
* [ユーザー名] 列には、各ユーザーの実際の名前が表示される必要があります。

※ Microsoft Teams モバイル アプリの使用状況が表示される必要があります。
それぞれの要件に対して何を変更する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

The Username column must display the actual name of each user:

Microsoft

Reports in Org settings

Privacy profile in Org settings

Reports in Org settings

The membership of the Reports Reader role

Microsoft Teams in Org settings

Microsoft Teams in Org settings

The columns in the report

The Teams license assignment

正解:

Answer Area

The Username column must display the actual name of each user:

Usage of the Teams mobile app must be displayed:

Reports in Org settings

Privacy profile in Org settings

Reports in Org settings

The membership of the Reports Reader role

Microsoft Teams in Org settings

Microsoft Teams in Org settings

The columns in the report

The Teams license assignment

Explanation:

Answer Area

The Username column must display the actual name of each user:

Usage of the Teams mobile app must be displayed:

Reports in Org settings

Microsoft Teams in Org settings

質問: 179

あなたはMicrosoft 365のサブスクリプションをお持ちです。

このサブスクリプションのMicrosoft Secure Scoreは60で、達成可能なスコアは75です。

信頼できないデバイスから接続する際に、ユーザーに多要素認証(MFA)の使用を要求する条件付きアクセス ポリシーを適用する必要があります。

この政策はスコアにどのような影響を与えるでしょうか？

- A. 安全スコアは低下し、達成可能なスコアは上昇します。
- B. 安全スコアと達成可能スコアが上昇します。
- C. セキュアスコアと達成可能スコアは変更されません。
- D. 安全スコアが上昇し、達成可能なスコアが低下します。

正解: (正解を表示します)

The correct exam selection is D. The Secure Score will increase, and the achievable score will decrease .

Microsoft Secure Score measures security posture, and Microsoft states that a higher score indicates that more recommended security actions have been taken. Microsoft also states that points are awarded for configuring recommended security features, and Conditional Access/MFA-related controls are part of the Microsoft 365 security posture model.

When you implement a Conditional Access policy requiring MFA from untrusted devices, you are applying a control that strengthens identity protection. That increases the current Secure Score because the tenant has completed or partially completed a recommended security action. The "achievable score" represents the remaining score opportunity available from your current licenses and risk posture. After you complete an improvement action, the remaining achievable gap is reduced, so the achievable score decreases in the exam's scoring logic. Microsoft's Secure Score documentation confirms that completed actions grant points and that Secure Score views include current score, current license score, planned score, and achievable score.

質問: 180

あなたはMicrosoft 365 ESのサブスクリプションをお持ちです。

Microsoft Defender XDR ポータルから、会社の Microsoft Secure Score を確認できます。

多数の推奨アクションが表示されます。

特定の部署名に基づいてアクションをフィルタリングできることを確認する必要があります。

最初に何を作るべきでしょうか？

- A. 行政単位
- B. タグ
- C. カスタム検出ルール
- D. 動的なセキュリティグループ

正解: A (コメントを発表する)

質問: 181

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

ユーザーは、自身のノートパソコンと企業の仮想デスクトップインフラストラクチャ(VDI)ソリューションの両方からMicrosoft 365にアクセスできます。

Microsoft Entra ID Protection では、サインインリスクポリシーを有効にできます。

ユーザーからは、VDIソリューションを使用している際に、Microsoft 365へのアクセスを試みると頻繁にブロックされるという報告が寄せられている。

何を設定すればよいですか？

- A. Microsoft Entra ID のテナント制限設定
- B. 信頼できる場所
- C. Microsoft 365 のセキュリティ接続設定
- D. 条件付きアクセスポリシーの接続設定

正解: (正解を表示します)

There are two types of risk policies in Microsoft Entra ID (Microsoft Entra ID) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:

Sign-in risk policy

User risk policy

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

Reference:

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

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 182

Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには、Windows 11 デバイスを所有するユーザーが含まれています。

デバイスをMicrosoft Defender for Endpointにオンボードする予定です。デバイスはプロキシサービスを介してDefender for Endpointに接続します。

Defender for Endpoint に接続する際に、デバイスが統合された URL と静的 IP 範囲を使用していることを確認する必要があります。どうすればよいでしょうか？

- A. 標準の接続タイプを使用します。
- B. デバイスの検出を有効にします。
- C. 合理化された接続タイプを使用します。
- D. デバイス グループを構成します。

正解: ([正解を表示します](#))

質問: 183

セキュリティ管理者向けに解決策を提案する必要があります。その解決策は技術要件を満たしていなければなりません。

推奨状には何を含めるべきでしょうか？

- A. Microsoft Microsoft Entra ID (Microsoft Entra ID) 特権ID管理
- B. マイクロソフト エントラ ID (Microsoft Entra ID) ID 保護
- C. Microsoft Entra ID (Microsoft Entra ID) 条件付きアクセス ポリシー
- D. Microsoft Entra ID (Microsoft Entra ID) 認証方法

正解: ([正解を表示します](#))

References:

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

質問: 184

User1 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。

App1 という名前のクラウドベースのアプリに条件付きアクセス ポリシーが適用されています。App1 には条件付きアクセス アプリ制御が展開されています。

User1 が App1 から印刷するのをブロックするには、Microsoft Defender for Cloud Apps ポリシーを作成する必要があります。

- A. セッションポリシー
- B. アクティビティポリシー

- C. OAuth アプリポリシー
- D. Cloud Discovery 異常検出ポリシー
- 正解: (正解を表示します)

質問: 185

あなたは、Label1 と Label2 という名前の 2 つの機密ラベルを含む Microsoft 365 E5 サブスクリプションを所有しています。
このサブスクリプションには、Microsoft Purview にオンボーディングされた Device1 という名前の Windows デバイスが含まれています。Device1 には、次の表に示すファイルが含まれています。

Name
Location
Sensitivity label
File1.docx
C:\Temp\
Label1
File2.docx
C:\Temp\Folder1\
Label2
File3.docx
C:\Temp\Folder2\
Label1

Policy1という名前のデータ損失防止(DLP)ポリシーを作成し、以下の設定を行います。

- * 場所: デバイス: すべてのユーザーとグループ
- * 条件: コンテンツにはセンシティブラベルラベル1が含まれています
- * アクション: デバイス上のアクティビティを監査または制限する
- * 印刷: ブロック

データ損失防止設定から、C:\Temp\ のファイルパス除外を設定します。
以下の各記述について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

Statements	Yes	No
A user on Device1 can print File1.docx.	☐	☐
A user on Device1 can print File2.docx.	☐	☐
A user on Device1 can print File3.docx.	☐	☐

正解:

Statements	Yes	No
A user on Device1 can print File1.docx.	☒	☐
A user on Device1 can print File2.docx.	☒	☐
A user on Device1 can print File3.docx.	☐	☒

Explanation:

A user on Device1 can print File1.docx.

Yes

A user on Device1 can print File2.docx.

Yes

A user on Device1 can print File3.docx.

No

The DLP rule blocks printing only when the file is subject to Endpoint DLP enforcement and the content matches the configured condition: sensitivity label Label1. Microsoft Purview Endpoint DLP can enforce protective actions on onboarded devices, and Microsoft lists Print as an auditable and restrictable endpoint activity for protected files.

The path exclusion is the deciding detail. Microsoft states that file path exclusions turn off DLP monitoring, alerts, and policy enforcement for files in excluded locations. For Windows file path syntax, a path ending with a backslash, such as C:\Temp\, excludes only files directly under that specified folder. A path ending with * excludes files within subfolders, while a path without trailing \ or * excludes both the folder and all subfolders.

Therefore, File1.docx can be printed because it has Label1 but is directly under C:\Temp\, so DLP enforcement does not apply. File2.docx can be printed because it is in a subfolder and not excluded, but it has Label2, so it does not match the Label1 blocking condition. File3.docx cannot be printed because it is in a subfolder, is not excluded by C:\Temp\, and has Label1, so the print action is blocked.

質問: 186

Microsoft 365 E5 テナントがあります。

機密の個人データを含む添付ファイル付きの電子メールが外部の受信者に送信された場合は、通知を受ける必要があります。

どの 2 つのポリシーを使用できますか?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. Microsoft Cloud App Security ファイル ポリシー

B. 秘密度ラベル ポリシー

C. データ損失防止 (DLP) ポリシー

D. 通信コンプライアンス ポリシー

E. 保持ラベルポリシー

正解: ([正解を表示します](#))

質問: 187

ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。このドメインには、次の表に示すユーザーが含まれています。

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

ドメインは、図に示すように、contoso.com という名前の Microsoft Entra テナントに同期されます。(図タブをクリックします。) User2 は、usef2@fabfikam.com としてサインインするときに、Microsoft Entra テナントへの認証に失敗します。User2 が Microsoft Entra ID のリソースにアクセスできることを確認する必要があります。

解決策: Microsoft Entra 管理センターから、カスタム ドメインとして <abrlkam.com を追加します。User2 に user2@fabrikam.com としてサインインするように要求します。これで目標は達成されますか?

A. いいえ

B. はい

正解: ([正解を表示します](#))

質問: 188

次の図に示すように、フィッシング対策ポリシーを構成します。

Policy setting	Policy name	Managers	
	Description		
	Applied to	If the email is sent to: IvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.onmicrosoft.com	Edit
	Safety tips > User impersonation	Off	Edit
	Safety tips > Domain impersonation	Off	
	Safety tips > Unusual characters	Off	
	Mailbox intelligence	Off	
Spool	Enable antispooofing protection	On	
	Action	Quarantine the message	Edit
Advanced settings	Advanced phishing thresholds	3 - More Aggressive	Edit

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

Answer Area

If a message is identified as a domain impersonation, [answer choice]

the message is delivered to the Inbox folder

the message is moved to the Deleted Items folder

the messages is moved to the Junk Email folder

the message is NOT delivered

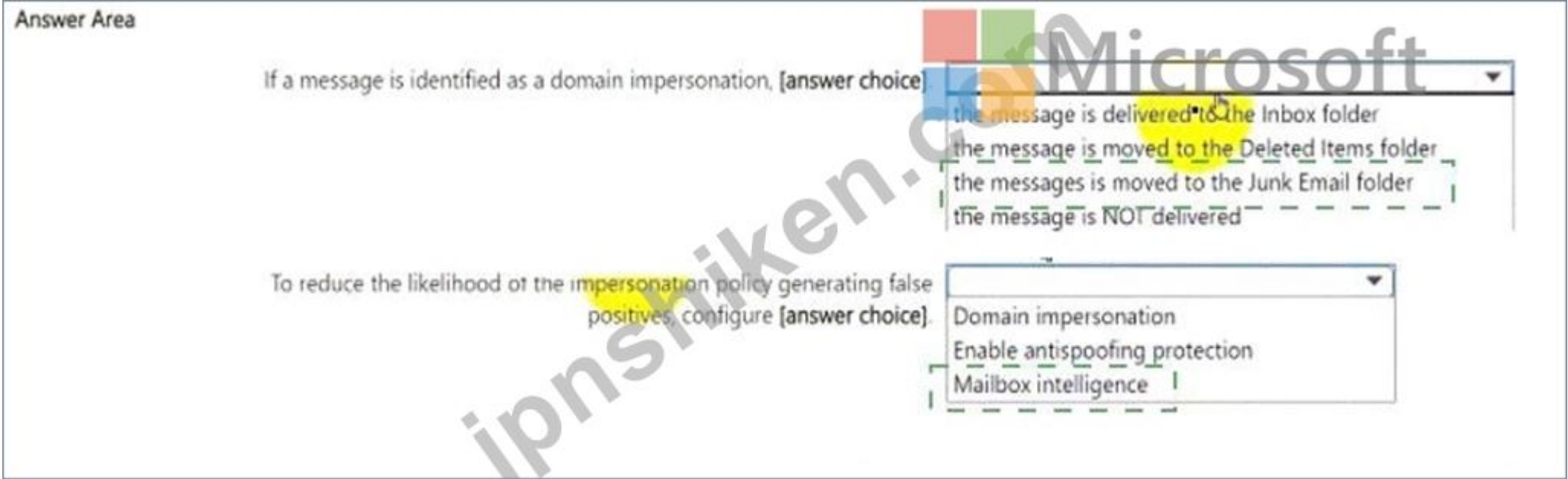
To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice]

Domain impersonation

Enable antispooofing protection

Mailbox intelligence

正解:



Explanation:

If a message is identified as a domain impersonation: the message is moved to the Junk Email folder According to the anti-phishing policy settings shown in the exhibit, messages identified as domain impersonation should be moved to the Junk Email folder to reduce the risk of phishing attacks.

To reduce the likelihood of the impersonation policy generating false positives, configure: Mailbox intelligence Mailbox intelligence helps in reducing false positives by using machine learning and historical email patterns to make better decisions about which emails are legitimate and which are not.

質問: 189

Microsoft 365 テナントと LinkedIn 会社ページがあります。
LinkedIn コネクタを使用して、LinkedIn ページから Microsoft 365 にデータをアーカイブする予定です。
LinkedIn コネクタからのデータはどこに保存できますか？

- A. Microsoft OneDrive for Business フォルダー
- B. Microsoft SharePoint Online ドキュメント ライブラリ
- C. Microsoft 365 メールボックス
- D. Azure ファイル

正解: (正解を表示します)

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide>

質問: 190

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。Microsoft 365 サブスクリプションを所有しています。
パススルー認証を使用するディレクトリ同期ソリューションを実装します。
次の図に示すように、Microsoft Entra パスワード保護を構成します。



Active Directory ユーザーがカスタム禁止パスワード リスト内のパスワードを使用できることがわかります。
禁止されたパスワードがすべてのユーザーに対して禁止されていることを確認する必要があります。
実行すべき 3 つのアクションはどれですか？それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。

- A. ドメイン コントローラーから、Microsoft Entra アプリケーション プロキシ コネクタをインストールします。
- B. Windows Server Active Directory のパスワード保護から、モード設定を変更します。
- C. ドメイン コントローラーから、Microsoft Entra Password Protection Proxy をインストールします。
- D. すべてのドメイン コントローラーから、Microsoft Entra Password Protection DC エージェントをインストールします。
- E. カスタム禁止パスワードから、カスタム リストの強制設定を変更します。
- F. Active Directory から、既定のドメイン ポリシーを変更します。

正解: **B,C,D** ([コメントを发表する](#))

質問: 191

お客様は、Microsoft 365 Multi-Geo を使用する Microsoft 365 サブスクリプションをご利用中です。このサブスクリプションには、異なる Multi-Geo リージョンに保存されている Site1 と Site2 という名前の 2 つの Microsoft SharePoint Online サイトが含まれています。

Microsoft 365 バックアップ ポリシーを構成する予定です。

ポリシーにSite1とSite2を追加し、利用可能な最長の保持期間を設定する必要があります。

どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。



正解:



Explanation:

To add the sites

Upload a list of the sites in a CSV file

Set the retention period to

1 year

The correct method for adding the sites is Upload a list of the sites in a CSV file. The key exam detail is Microsoft 365 Multi-Geo. Microsoft states that Microsoft 365 Backup supports backup of sites and user accounts from both central and satellite Multi-Geo locations, but for Multi-Geo policy creation, sites or user accounts from all geos must be added by using the CSV file upload method. Microsoft also states that adding sites through the site picker, search, or filter rules does not currently support Multi-Geo, and the UI supports only sites in the tenant's central location.

The longest retention period is 1 year. Microsoft's Microsoft 365 Backup feature summary lists the retention period for OneDrive, SharePoint, and Exchange Online as 1 year. Since this question concerns SharePoint Online sites, the applicable maximum retention period is one year, not five or ten years.

Therefore, select Upload a list of the sites in a CSV file and 1 year.

質問: 192

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。ドメインには以下が含まれます

1,000 台の Windows 10 デバイス。

10 台のテスト デバイスに対して Microsoft Defender for Endpoint の概念実証 (PoC) 展開を実行します。

オンボーディング プロセス中に、Microsoft Defender for Endpoint 関連のデータが米国に保存されるように構成します。

すべてのデバイスを Microsoft Defender for Endpoint にオンボードする予定です。

Microsoft Defender for Endpoint データをヨーロッパに保存する必要があります。

まず何をすべきでしょうか？

- A. ワークスペースを削除します。
- B. ワークスペースを作成します。
- C. 新しいデバイスをオンボードします。
- D. テストデバイスをオフボードにします。

正解: (正解を表示します)

Storage locations

Understand where Defender for Cloud stores data and how you can work with your data:

* Machine information

- Stored in a Log Analytics workspace.

- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace>

質問: 193

次の図に、Microsoft Defender XDR レポートのスケジュールを示します。

Manage your report schedules here

Refresh

2 items

Search

☐	Schedule start date	Schedule name	Report type	Frequency
☐	Feb 8, 2025 1:00 AM	Schedule1	MailFlowStatus	Monthly
☐	Feb 8, 2025 1:00 AM	Schedule2	Zap	Monthly

レポートのスケジュール設定によって、レポートが可能な限り頻繁に生成されるようにする必要があります。
各スケジュールにおける「頻度」設定は、それぞれどのくらいに設定すべきでしょうか？回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Schedule1:

Daily

Weekly

Monthly

Schedule2:

Daily

Weekly

Monthly

正解:



Explanation:



質問: 194

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
アプリケーションへのアクセスを監視および報告するためのソリューションを推奨する必要があります。そのソリューションは、以下の要件を満たす必要があります。

- * データクエリにKQLをサポートします。
- * レポートデータは少なくとも1年間保管してください。

推薦状には何を含めるべきでしょうか？

- A. エンドポイント分析
- B. Microsoft 365 使用状況分析
- C. Microsoft Defender XDR のセキュリティ レポート
- D. Azure Monitor ワークブック

正解: D ([コメントを发表する](#))

質問: 195

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。

User1 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。

User1 がコンプライアンス マネージャー評価を作成できるようにする必要があります。

解決策: Microsoft 365 管理センターから、User1 にコンプライアンス管理者のロールを割り当てます。

これは目標を達成していますか？

- A. はい

B. いいえ

正解: (正解を表示します)

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

質問: 196

お客様はMicrosoft 365 E5サブスクリプションと、contoso.comという名前のMicrosoft Entraテナントをお持ちです。

すべてのユーザーは、Windows 11を搭載したコンピューターを使用しており、contoso.comに加入しており、BitLockerドライブ暗号化(BitLocker)によって保護されています。

あなたは、以下のタスクを実行するAdmin1という名前のユーザーを作成する予定です。

* BitLocker回復キーを表示します。

* contoso.com のユーザーの利用場所を設定します。

要件を満たすために、Admin1に役割を割り当てる必要があります。解決策は最小権限の原則に従う必要があります。どの2つの役割を割り当てるべきですか？回答するには、回答領域で適切な役割を選択してください。

注：正解ごとに1ポイント獲得できます。

Answer Area

Devices

☐ Cloud Device Administrator ⓘ

☐ Desktop Analytics Administrator ⓘ

☐ Intune Administrator ⓘ

☐ Printer Administrator ⓘ

☐ Printer Technician ⓘ

☐ Windows 365 Administrator ⓘ

Global

☐ Global Administrator ⓘ

Identity

☐ Application Administrator ⓘ

☐ Application Developer ⓘ

☐ Authentication Administrator ⓘ

☐ Cloud Application Administrator ⓘ

☐ Conditional Access Administrator ⓘ

- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

正解:

Answer Area



Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ

☐ Application Developer ⓘ

☐ Authentication Administrator ⓘ

☐ Cloud Application Administrator ⓘ

☐ Conditional Access Administrator ⓘ

☐ Domain Name Administrator ⓘ

☐ External Identity Provider Administrator ⓘ

☐ Guest Inviter ⓘ

☐ Helpdesk Administrator ⓘ

☐ Hybrid Identity Administrator ⓘ

☐ License Administrator ⓘ

☐ Password Administrator ⓘ

Explanation:

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☒ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☒ Helpdesk Administrator ⓘ ✓
- ☐ Hybrid Identity Administrator ⓘ
- ☒ License Administrator ⓘ ✓
- ☐ Password Administrator ⓘ



有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 197

Microsoft 365 E5 サブスクリプションをお持ちです。

次の図に示すように、場所に適用されるデータ損失防止 (DLP) ポリシーを作成しています。

Location		Scope	
☒	Exchange email	All groups	Edit
☒	SharePoint sites	All sites	Edit
☒	OneDrive accounts	All users & groups	Edit
☒	Teams chat and channel messages	All users & groups	Edit
☒	Microsoft Defender for Cloud Apps	All instances	Edit
☒	On-premises repositories	All repositories	Edit
☐	Power BI workspaces	Turn on location to scope	

ポリシーの DIP ルールで利用できる条件はどれですか？

- A. コンテンツ検索クエリ
- B. 機密情報の種類
- C. キーワード
- D. 機密ラベル

正解: B (コメントを发表する)

質問: 198

Microsoft 365 E5 テナントがあります。

機密ラベルを構成します。

ユーザーから、Web 用 Microsoft Word で [感度] ボタンが使用できないと報告されています。感度ボタンは Word for Microsoft 365 で使用できます。

ユーザーが Web 用 Word を使用するときに秘密度ラベルを適用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. 自動ラベル付けポリシーを作成する
- B. Azure Information Protection から Microsoft 365 コンプライアンス センターにポリシーをコピーします。
- C. 機密ラベルを公開します。
- D. Microsoft SharePoint Online および OneDrive のファイルの秘密度ラベルを有効にします。

正解: (正解を表示します)

質問: 199

お客様は、以下のサービスを利用するMicrosoft 365サブスクリプションをお持ちです。

- * マイクロソフトが参入
- * Exchange Online
- * Microsoft Teams

* SharePoint Online。
あなたは、Microsoft 365 Backup を利用したバックアップソリューションを計画しています。
どのMicrosoft 365サービスをバックアップできるか、また利用可能な最長の保存期間を推奨する必要があります。
何を推奨しますか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

Services:

Exchange Online only
SharePoint Online only
Exchange Online and SharePoint Online only
Microsoft Entra, Exchange Online, and SharePoint Online only
Exchange Online, SharePoint Online, and Teams only
Microsoft Entra, Exchange Online, SharePoint Online, and Teams

Retention period:

6 months
1 year
5 years
10 years

正解:

Services:

Exchange Online only
SharePoint Online only
Exchange Online and SharePoint Online only
Microsoft Entra, Exchange Online, and SharePoint Online only
Exchange Online, SharePoint Online, and Teams only
Microsoft Entra, Exchange Online, SharePoint Online, and Teams

Retention period:

6 months
1 year
5 years
10 years

Explanation:
Services: Exchange Online and SharePoint Online only
Retention period: 1 year
The correct dropdown selection is Exchange Online and SharePoint Online only. Microsoft 365 Backup supports backup and recovery for OneDrive, SharePoint, and Exchange Online workloads. From the services listed in this question, Exchange Online and SharePoint Online are the only supported services. Microsoft Entra is not a Microsoft 365 Backup workload because it is an identity and directory platform, not a content workload protected by Microsoft 365 Backup. Microsoft Teams is also not selected as a separate backup service. Teams files are stored in SharePoint or OneDrive, but Microsoft 365 Backup does not list "Teams" as an independent backup workload. Microsoft's backup policy documentation also separates backup policy configuration into SharePoint, Exchange, and OneDrive tabs, reinforcing that those are the protected workload categories.

The longest available retention period is 1 year. Microsoft's Microsoft 365 Backup FAQ states that when backed-up OneDrive or Exchange content is removed from the backup policy or the user is deleted, the backup is retained for one year from the date the backup was created. Therefore, among the given retention choices, the correct maximum is 1 year, not 5 or 10 years.

質問: 200

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

Microsoft Entra テナントを展開します。

別の管理者が Microsoft Entra テナントと同期するようにドメインを構成する 組織単位 (OU) 内の 10 個のユーザー アカウントが Microsoft Entra テナントと同期していないことがわかります。他のすべてのユーザー アカウントは正常に同期されました。

Microsoft Entra Connect Health を確認すると、すべてのユーザー アカウントの同期が正常に完了したことがわかります。

10 個のユーザー アカウントが Microsoft Entra テナントに同期されていることを確認する必要があります。

解決策: Microsoft Entra Connect から Microsoft Entra 資格情報を変更します。

これは目標を達成していますか？

A. いいえ

B. はい

正解: ([正解を表示します](#))

質問: 201

Microsoft 365 テナントがあります。

Microsoft 365 セキュリティ センターを使用してテナント内のインシデントを管理する予定です。

Microsoft 365 セキュリティ センターの [インシデント] ページに表示される Microsoft サービス ソースはどれですか？

A. Microsoft Defender for Cloud を使用します。

B. Microsoft の権限

C. アズールアーク

D. ID 用 Microsoft Defender

正解: ([正解を表示します](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

質問: 202

Intune で自動登録を構成する必要があります。ソリューションは技術要件を満たしている必要があります。

何を設定する必要がありますか?また、その設定をどのグループに割り当てる必要がありますか?回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Configure:  ▼

Device configuration profiles	Enrollment restrictions
The mobile device management (MDM) user scope	
The mobile application management (MAM) user scope	

Group:  ▼

UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

正解:

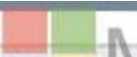
Configure:  ▼

Device configuration profiles	Enrollment restrictions
The mobile device management (MDM) user scope	
The mobile application management (MAM) user scope	

Group:  ▼

UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

Explanation:

Configure:  ▼

Device configuration profiles	Enrollment restrictions
The mobile device management (MDM) user scope	
The mobile application management (MAM) user scope	

Group:  ▼

UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

Reference:

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

質問: 203

お客様は、Microsoft Intuneに登録された500台のWindowsデバイスを含むMicrosoft 365サブスクリプションをご利用中です。

デバイスの脆弱性管理に関する推奨事項を確認できる体制を整える必要があります。また、管理作業を最小限に抑えるソリューションを採用する必要があります。

Microsoft Defender ポータルでは、どのポリシー テンプレートを選択すべきですか？

- A. エンドポイント検出および応答
- B. デバイス制御
- C. Microsoft Defender ウイルス対策
- D. Windows セキュリティ エクスペリエンス

正解: **A** ([コメントを發表する](#))

The correct policy template is Endpoint Detection and Response because vulnerability management recommendations require the devices to be onboarded to Microsoft Defender for Endpoint, where Defender Vulnerability Management can assess the endpoint inventory, detected weaknesses, exposure, and security recommendations. Microsoft states that after Intune is integrated with Defender for Endpoint, Defender Vulnerability Management identifies vulnerabilities on managed devices and allows security admins to review endpoint vulnerabilities and create remediation tasks.

For Intune-managed Windows devices, the lowest-administration deployment path is to use an endpoint security policy rather than manually deploying onboarding scripts or packages. Microsoft's Defender portal endpoint security policy documentation states that when Defender for Endpoint is integrated with Intune, administrators use endpoint detection and response endpoint security policies to manage EDR settings and onboard devices to Microsoft Defender for Endpoint. Microsoft's onboarding guidance also identifies deploying an endpoint detection and response policy with Intune as an onboarding deployment method.

Device Control manages removable/device access controls, Microsoft Defender Antivirus configures antivirus behavior, and Windows Security Experience controls end-user Windows Security app experience. None of those templates is the direct onboarding mechanism needed for Defender Vulnerability Management recommendations. References/topics: Microsoft Defender for Endpoint onboarding, Intune endpoint security policies, Endpoint Detection and Response policy, Defender Vulnerability Management recommendations.

質問: **204**

あなたはMicrosoft 365 E5サブスクリプションをご利用で、Office 365向けMicrosoft Defenderを使用しています。

あなたは、すべてのユーザーを標的とし、認証情報窃盗というソーシャルエンジニアリング手法を用いる攻撃シミュレーション訓練を設定しています。

シミュレーションでは、カスタムのフィッシングリンクと企業独自の用語やブランドを含むメールメッセージを送信するようにする必要があります。

シミュレーションはどのように設定すればよいですか？

- A. カスタムエンドユーザー通知を選択します。
- B. テナントペイロードを作成します。
- C. テナントランディングページを作成します。
- D. グローバルペイロードを選択します。

正解: ([正解を表示します](#))

The correct answer is Create a Tenant payload. In Microsoft Defender for Office 365 Attack simulation training, the payload is the simulated phishing email content presented to users. Microsoft defines a payload as the link, QR code, or attachment in the simulated phishing email message. For the Credential Harvest technique, the payload is the phishing email that drives the user to interact with a simulated credential-capture scenario. Microsoft also states that while Attack simulation training includes built-in payloads, administrators can create custom payloads that work better for their organization. Tenant payloads are the organization- created payloads, so they are the correct choice when the email must contain organization-specific wording, branding, and a custom phishing link.

A Global payload is Microsoft-provided and generic, so it will not satisfy the requirement for company-based terminology and branding. Custom end-user notifications are used for training or notification messages after simulation events, not for defining the phishing email itself. A tenant landing page controls the page shown after the user interacts with the phishing link; it does not define the email message content. Therefore, the simulation must use a Tenant payload.

質問: **205**

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	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

Group1 のセルフサービス パスワード リセット (SSPR) を有効にします。SSPR の唯一の認証方法としてセキュリティの質問を構成します。
SSPR を使用できるのはどのユーザーですか?また、パスワードをリセットするにはセキュリティの質問に答える必要があるのはどのユーザーですか?回答するには、回答領域で適切なオプションを選択してください。
注記;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

Users that can use SSPR:

User1, User2, and User4 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

Users that must answer security questions to reset their password:

User1 and User2 only

User1 only

User2 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

正解:



Microsoft

Users that can use SSPR:

User1, User2, and User4 only
User1 and User2 only
User1, User2, and User3 only
User1, User2, and User4 only
User1, User2, User3, and User4

User1 and User2 only
User1 only
User2 only
User1 and User2 only
User1, User2, and User3 only
User1, User2, and User4 only
User1, User2, User3, and User4

Explanation:

Answer Area

Users that can use SSPR: User1, User2, and User4 only

Users that must answer security questions to reset their password: User1 and User2 only

質問: 206

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。

User1 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。

User1 がコンプライアンス マネージャー評価を作成できるようにする必要があります。

解決策: Microsoft 365 コンプライアンス センターから、User1 をコンプライアンス マネージャー評価者役割グループに追加します。

これは目標を達成していますか?

A. はい

B. いいえ

正解: (正解を表示します)

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

質問: 207

ホットスポット

Microsoft 365 テナントがあります。

次の図に示すように、保持ポリシーを作成する予定です。

Information governance > Create retention policy

✓ Name

✓ Locations

✓ Retention settings

● Finish

Review and finish

It might take up to one day to apply this policy to the locations you selected.

Policy name
contoso
Edit

Description
Edit

Locations to apply the policy
Exchange email (All Recipients)
SharePoint sites (All Sites)
OneDrive accounts (All Accounts)
Microsoft 365 Groups (All Groups)
Edit

Retention settings
Delete items at end of retention period
Delete items that are older than 7 years based on when they were created
Edit

⚠ Items that are currently older than 7 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted.

Microsoft

BackSubmitCancel

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

Answer Area

Microsoft SharePoint files that are affected by the policy will be [answer choice].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [answer choice].

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

正解:

Answer Area

Microsoft SharePoint files that are affected by the policy will be [answer choice].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [answer choice].

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Explanation:

Answer Area

Microsoft SharePoint files that are affected by the policy will be [answer choice].

recoverable for up to seven years

deleted seven years after they were created

retained for only seven years from when they were created

Once the policy is created, [answer choice].

some data may be deleted immediately

data will be retained for a minimum of seven years

users will be prevented from permanently deleting email messages for seven years

Box 1: Deleted seven years after they were created.

From the exhibit:

The retention policy applies to SharePoint sites.

Delete items that are older than 7 years based on when they were created.

Box 2: data will retained for a minimum of seven years

The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.

Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).

For example, if all documents in a SharePoint site should be retained for 5 years, it's more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5 years and others retained for 10 years, a retention policy wouldn't be able to do this. When you need to specify retention settings at the item level, use retention labels.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention>

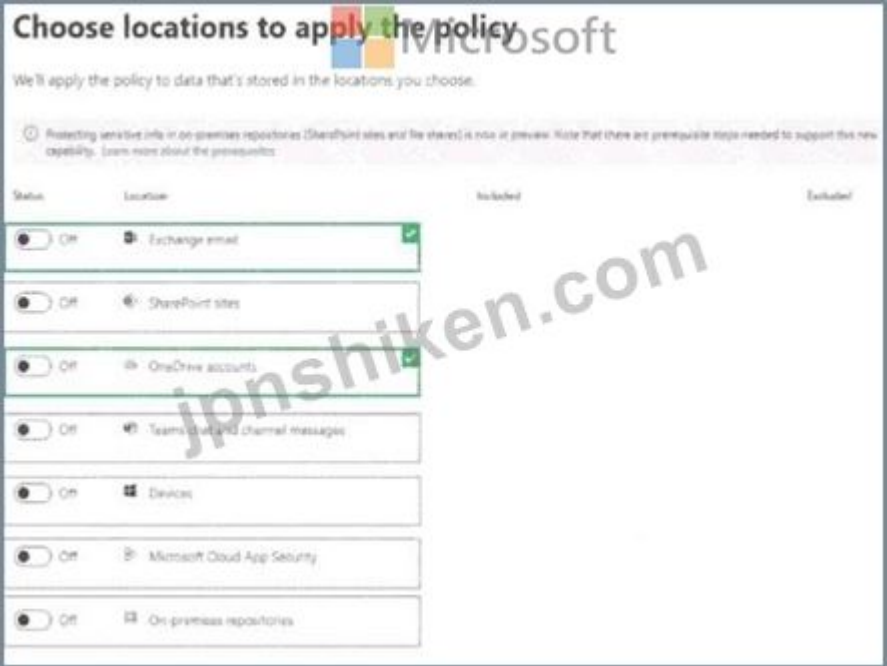
質問: 208

Microsoft 365 E5 テナントがある

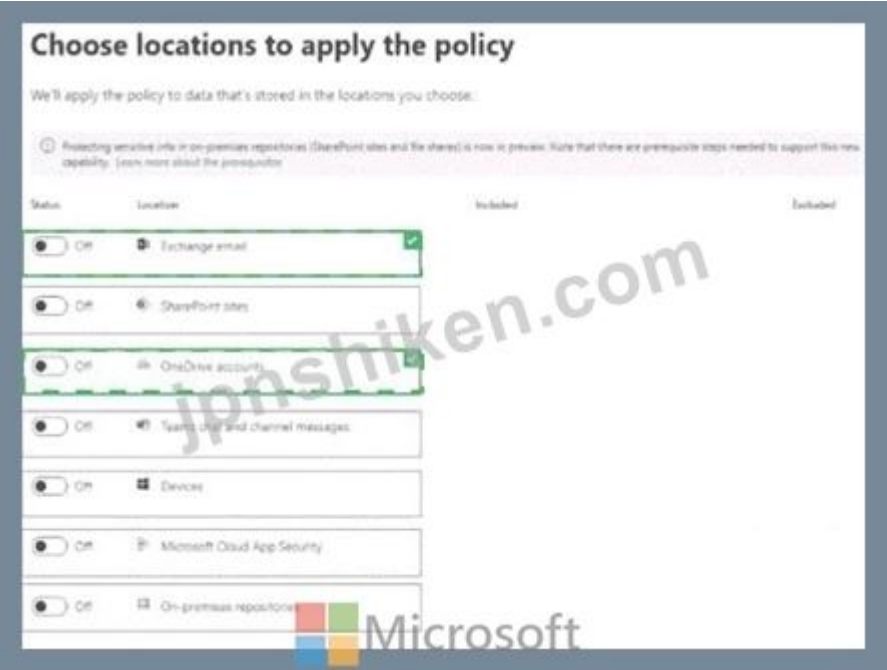
データ投げ捨て防止 (DLP) ポリシーを作成して、ユーザーが Microsoft Teams を使用して内部ドキュメントを外部ユーザーと共有できないようにします。

どの 2 つの場所にポリシーを適用する必要がありますか?回答するには、回答領域で適切な場所を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。



正解:



質問: 209

Microsoft 365 E5 サブスクリプションをお持ちです。
クラウド アプリ用に Microsoft Defender を実装しています。
OAuth アプリ ポリシーを作成できることを確認する必要があります。
解決策: Cloud Discovery を構成します。
これは目標を満たしていますか?

- A. いいえ
- B. はい

正解: A ([コメントを发表する](#))

質問: 210

User1 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。次の設定を持つ Policy! という名前のフィッシング対策ポリシーを作成します。

* 次のユーザー、グループ、ドメインを含めます: User1

* フィッシングメールの閾値: 3 - より攻撃的

ユーザー1 は、次の表に示す電子メール メッセージを受信します。

Name	Phishing confidence level (PCL)
Mail1	Low
Mail2	Medium
Mail3	High
Mail4	Very high

どのメッセージがフィッシングメールですか？

A. メール3とメール4のみ

B. メール2、メール3、メール4のみ

C. メール4のみ

D. メール1、メール2、メール3、メール4

正解: (正解を表示します)

質問: 211

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。

このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

SecAdmin1という名前の新しいセキュリティ管理者アカウントを作成します。

SecAdmin1 が、Microsoft Teams、SharePoint、および OneDrive の Office 365 Advanced Threat Protection (ATP) の設定とポリシーを管理できることを確認する必要があります。

解決策 :Microsoft Entra ID管理センターから、SecAdmin1にセキュリティ管理者ロールを割り当てます。

これは目標を達成していると言えるでしょうか？

A. いいえ

B. はい

正解: B (コメントを發表する)

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 212

あなたの会社には Microsoft 365 E5 テナントがあります。

ユーザーは、個人所有の Android デバイスと会社所有の Android デバイスの両方を使用して、テナント内のリソースにアクセスします。会社のポリシーでは、Microsoft Exchange Online メールボックスにアクセスするには、デバイスの脅威レベルが中以下であることが必要です。

デバイスの脅威レベルを特定し、リソースへのデバイスのアクセスを制御するソリューションを推奨する必要があります。

各デバイスタイプのソリューションには何を含め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デバイスにドラッグします。各コンポーネントは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。

Solutions

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

Answer Area

Company-owned devices:

Solution

Personal devices:

Solution

正解:

Solutions

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

Answer Area

Company-owned devices:

A compliance policy

Personal devices:

An app protection policy

Explanation:

Company-owned devices:

A compliance policy

Personal devices:

An app protection policy

質問: 213

Microsoft Endpoint Managerには、複数のデバイスが登録されています。
お客様は、以下の表に示すユーザーを含む Microsoft Entra ID (Microsoft Entra ID) テナントを所有しています。

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

Endpoint Managerにおけるデバイスタイプの制限は、次の表に示すように構成されます。

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Answer Area



Microsoft

Statements

Yes

No

User1 can enroll Windows devices in Endpoint Manager.

☐

☐

User2 can enroll Android devices in Endpoint Manager.

☐

☐

User3 can enroll iOS devices in Endpoint Manager.

☐

☐

正解:

Answer Area



Microsoft

Statements

Yes

No

User1 can enroll Windows devices in Endpoint Manager.

☐

☒

User2 can enroll Android devices in Endpoint Manager.

☐

☒

User3 can enroll iOS devices in Endpoint Manager.

☒

☐

Explanation:

Answer Area



Microsoft

Statements

Yes

No

User1 can enroll Windows devices in Endpoint Manager.

☐

☒

User2 can enroll Android devices in Endpoint Manager.

☐

☒

User3 can enroll iOS devices in Endpoint Manager.

☒

☐

質問: 214

Microsoft 365 E5 サブスクリプションをお持ちです。

次の表に示すように、Microsoft Defender for Endpoint にデバイスがオンボードされています。

Name	Platform
Device1	Windows 11
Computer2	Windows 11
Device3	Android

次の表に示すデバイス グループを作成します。

Rank	Name	Matching rule
1	Group1	Name Starts with Dev
2	Group2	OS Is Windows 11
Last	Ungrouped devices (default)	Not applicable

IP アドレス インジケータは、次の表に示すように定義されます。

IP address	Action	Scope
131.107.10.50	Block	Group2
20.30.40.50	Block	Group1
2.23.10.15	Block	UnassignedGroup

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

注意: 正解を選ぶごとに1ポイント獲得できます

Answer Area

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	☐	☐
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	☐	☐
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	☐	☐

正解:

Answer Area

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	☒	☐
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	☐	☒
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	☐	☒

Explanation:

Answer Area

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	☒	☐
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	☐	☒
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	☐	☒

質問: 215

Microsoft 365 テナントがあります。

Microsoft 365 セキュリティ センターを使用してテナント内のインシデントを管理する予定です。

Microsoft 365 セキュリティ センターの [インシデント] ページに表示される Microsoft サービス ソースはどれですか？

A. Microsoft Cloud App Security

B. アズールセンチネル

C. Azure Web アプリケーション ファイアウォール

D. アズール ディフェンダー

正解: A (コメントを发表する)

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

質問: 216

100 台の Windows 10 デバイスを含む Microsoft 365 E5 テナントがあります。

Windows 10 デバイスの攻撃対象表面削減 (ASR) ルールを計画しているとします。

ASR ルールを監査モードで構成し、Log Analytics ワークスペースで監査データを収集します。

デバイス上のアクティビティに一致する ASR ルールを見つける必要があります。
Kusto クエリをどのように完了する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

▼

AlertInfo

DeviceEvents

DeviceInfo

▼

ActionType startswith 'ASR'

lookup

project

render

where

正解:

▼

AlertInfo

DeviceEvents

DeviceInfo

▼

ActionType startswith 'ASR'

lookup

project

render

where

Explanation:

▼

AlertInfo

DeviceEvents

DeviceInfo

▼

ActionType startswith 'ASR'

lookup

project

render

where

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction-rules-part-3/ba-p/1360968>

質問: 217

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。

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 2019 を実行するドメイン コントローラーが含まれています。フォレストとドメインの機能レベルは Windows Server 2012 R2 です。

ドメインには、Windows 10 を実行する 100 台のコンピューターと、Windows Server 2012 R2 を実行する Server1 という名前のメンバー サーバーが含まれています。

Server1 を使用してドメインを管理し、Windows 10 グループ ポリシー設定を構成する予定です。

Server1 にグループ ポリシー管理コンソール (GPMC) をインストールします。

Server1 で Windows Update for Business のグループ ポリシー設定を構成する必要があります。

解決策: フォレストの機能レベルを Windows Server 2016 に引き上げます。グループ ポリシー管理用テンプレートを Windows 10 コンピューターからすべてのドメイン コントローラーの Netlogon 共有にコピーします。

これは目標を達成していますか?

A. はい

B. いいえ

正解: [\(正解を表示します\)](#)

質問: 218

Microsoft 365 E5 サブスクリプションをお持ちです。

グループの名前付けポリシーを構成する必要があります。

どのポータルを使用する必要がありますか?また、ポリシーはどのタイプのグループに適用されますか?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。

Answer Area

Portal:

The Microsoft 365 admin center

The Microsoft 365 admin center

The Microsoft 365 Defender portal

The Microsoft Entra admin center

The Microsoft Purview compliance portal

Group types:

Security only

Microsoft 365 only

Security only

Security and mail-enabled security only

Microsoft 365 and distribution only

Microsoft 365, mail-enabled security, and distribution only

Security, Microsoft 365, mail-enabled security, and distribution

正解:

Answer Area

Portal:

Group types:

Group types:

Group types:

Group types:

Group types:

Group types:

Group types:

Explanation:

Answer Area

Portal:

Group types:

質問: 219

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、指定された問題を満たす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 E5 サブスクリプションをお持ちです。

SecAdmin1 という名前の新しいセキュリティ管理者のアカウントを作成します。

SecAdmin1 が Microsoft Defender for Office 365 の設定と Microsoft Teams、SharePoint のポリシーを管理できることを確認する必要があります。そしてOneDrive。

解決策: Microsoft 365 管理センターから、SecAdmin1 に SharePoint 管理者ロールを割り当てます。

これは目標を達成していますか？

A. いいえ

B. はい

正解: (正解を表示します)

質問: 220

Microsoft 365 E5 サブスクリプションをお持ちです。

次の設定を持つ保持ラベルを定義します。

※保存期間は7年です

* 保存期間の開始日はアイテムの作成日です

ラベル K が嘘に適用された後は、ラベルが削除されないようにする必要があります。保持ラベルの設定で何を選択する必要がありますか？

- A. アイテムを永久に保持します
- B. アイテムを規制記録としてマークします
- C. 項目をレコードとしてマークします
- D. ユーザーが削除してもアイテムを保持します

正解: C (コメントを发表する)

質問: 221

Microsoft 365 E5 サブスクリプションがあり、その中には Microsoft Defender for Endpoint にオンボードされたデバイスが含まれています。Microsoft Defender for Cloud Apps を Defender for Endpoint と統合します。過去 30 日間に最も多く使用されたクラウドアプリとサービスを特定する必要があります。何をすればよいでしょうか。

- A. Cloud Discovery エグゼクティブ レポートを生成する
- B. 月次セキュリティ概要レポートを生成する
- C. 脅威分析アラート通知を作成します。
- D. Cloud Discovery スナップショット レポートを生成します。

正解: (正解を表示します)

質問: 222

お客様のオンプレミスネットワークには、Active Directory ドメインと Microsoft Endpoint Configuration Manager サイトが含まれています。

お客様は、Microsoft Intune を使用する Microsoft 365 E5 サブスクリプションをご利用中です。

Microsoft Entra Connect Sync を使用してユーザーオブジェクトとグループオブジェクトを Azure Directory (Microsoft Entra ID) に同期しますが、パスワードハッシュの同期は無効になっています。

あなたは共同経営を導入する予定です。

共同管理をサポートするには、Microsoft Entra Connect Sync とドメインを設定する必要があります。

どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area



To configure Azure AD Connect:

Configure hybrid Azure AD join.

Enable device writeback.

Enable password hash synchronization.

To configure the domain:

Add an alternative UPN suffix.

Register a service connection point.

Register a service principal name (SPN).

正解:

Answer Area

To configure Azure AD Connect:

- Configure hybrid Azure AD join.
- Enable device writeback.
- Enable password hash synchronization.

To configure the domain:

- Add an alternative UPN suffix.
- Register a service connection point.
- Register a service principal name (SPN).



Explanation:

Answer Area

To configure Azure AD Connect: Enable password hash synchronization.

To configure the domain: Add an alternative UPN suffix.



質問: 223

あなたはMicrosoft 365のサブスクリプションをお持ちです。

あなたはApp1とApp2という名前の2つのアプリケーションをMicrosoft Entra IDに登録します。

App1に接続するユーザーには多要素認証(MFA)を必須とする必要があります。MFAはApp1のみで必要です。どうすればよいですか？

- A. Microsoft Entra 管理センターから、条件付きアクセス ポリシーを作成します。
- B. Microsoft 365 管理センターから、モデム認証設定を構成します。
- C. Microsoft Entra 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、ユーザー設定を構成します。
- D. 多要素認証から、サービス設定を構成します。

正解: (正解を表示します)

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication>

質問: 224

注: このセクションには、同じシナリオと問題に関する 1 つ以上の質問セットが含まれています。各質問には、問題に対する独自の解決策が提示されています。解決策が、指定された目標を満たしているかどうかを判断する必要があります。

セット内の複数のソリューションが問題を解決できる可能性があります。また、セット内のどのソリューションも問題を解決できない可能性もあります。

このセクションの質問に回答した後は、戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 E5 サブスクリプションがあり、Microsoft Defender for Office 365 を使用しています。

スパム、フィッシング、マルウェアから保護するために、バランスの取れたベースライン保護プロファイルを適用する脅威ポリシーを実装する必要があります。

解決策: 厳格なプリセット セキュリティ ポリシーを作成します。

これは目標を満たしていますか？

- A. はい

B. いいえ

正解: ([正解を表示します](#))

質問: **225**

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

以下の要件を満たすには、条件付きアクセス ポリシーを作成する必要があります。

社内ネットワーク外からサインインするユーザーは、全員多要素認証(MFA)を使用する必要があります。

ユーザーは、準拠したデバイスからサインインする場合に限り、社内ネットワーク外からサインインできる必要がある。

米国およびカナダ国外からのログインは、すべてのユーザーに対してブロックされなければならない。

研究開発部門のユーザーのみが、AndroidおよびiOSデバイスの両方からサインインできないようにブロックする必要があります。

財務部門のユーザーのみが、App1という名前のMicrosoft Entra IDエンタープライズアプリケーションにサインインできるようにする必要があります。その他のすべてのユーザーは、App1にサインインできないようにする必要があります。

作成すべき条件付きアクセス ポリシーの最小数はいくつですか？

A. 3

B. 4

C. 5

D. 6

E. 7

F. 8

正解: **B** ([コメントを發表する](#))

* Only users in the finance department must be able to sign in to an Microsoft Entra ID enterprise application named App1. All other users must be blocked from signing in to App1.

One Policy.

* Only users in the R & D department must be blocked from signing in from both Android and iOS devices.

One Policy.

* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

One policy

* All users must be blocked from signing in from outside the United States and Canada.

Only users in the R & D department must be blocked from signing in from both Android One Policy Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>

質問: **226**

500 台の Windows 10 デバイスと Windows 10 コンプライアンス ポリシーを含む Microsoft 365 E5 テナントがあります。

サードパーティのウイルス対策ソリューションをデバイスに展開します。

デバイスが準拠としてマークされていることを確認する必要があります。

コンプライアンス ポリシーで変更する必要がある 3 つの設定はどれですか?回答するには、回答領域で適切な設定を選択します。

注: 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

Windows 10 compliance policy
Windows 10 and later

Encryption

Encryption of data storage on device	Require	Not configured
--------------------------------------	---------	----------------

Device Security

Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender

Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

正解:

Answer Area

Windows 10 compliance policy
Windows 10 and later

Encryption

Encryption of data storage on device	Require	Not configured
--------------------------------------	---------	----------------

Device Security

Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender

Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

Explanation:

Windows 10 compliance policy

Windows 10 and later

Encryption

Encryption of data storage on device

Require

Not configured

Device Security

Firewall

Require

Not configured

Trusted Platform Module (TPM)

Require

Not configured

Antivirus

Require

Not configured

Antispyware

Require

Not configured

Defender

Microsoft Defender Antimalware

Require

Not configured

Microsoft Defender Antimalware minimum version

Not configured

Microsoft Defender Antimalware security intelligence up-to-date

Require

Not configured

Real-time protection

Require

Not configured

Reference:
<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

有効的な**MS-102J**問題集はJPNTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTest.comは今最新**MS-102J**試験問題集を提供します。JPNTest.com MS-102J試験問題集はもう更新されました。ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 227
次の表に示すデバイスを含む Microsoft 365 E5 テナントがあります。

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

攻撃対象領域削減 (ASR) ルールを実装する予定です。どのデバイスが ASR ルールをサポートしますか？
A. デバイス 1、デバイス 2、およびデバイス 3 のみ
B. デバイス 3 のみ

C. デバイス 2 とデバイス 3 のみ

D. デバイス 1、デバイス 2、デバイスおよびデバイス 4

正解: ([正解を表示します](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements>

質問: **228**

Microsoft 365 サブスクリプションをお持ちです。

Microsoft Exchange Online サービスの問題が発生した場合、個人の電子メール アドレスに通知を受け取る必要があります。どうすればよいでしょうか？

A. Exchange 管理センターから連絡先を作成します。

B. Microsoft 365 管理センターから、技術連絡先の詳細を更新します。

C. Microsoft Outlook クライアントから受信トレイ ルールを構成します。

D. Microsoft 365 管理センターから、サービス正常性設定をカスタマイズします。

正解: ([正解を表示します](#))

質問: **229**

あなたの会社には 3 つの本社と 1 つの支社があります。支社は研究のために使用されています。

同社は、Microsoft 365 テナントを実装し、多要素認証を展開する予定です。

ブランチ オフィスのユーザーに対してのみ多要素認証が実施されるようにするには、Microsoft 365 ソリューションを推奨する必要があります。

推薦書には何を含めるべきでしょうか？

A. Microsoft Entra 条件付きアクセス

B. Microsoft Intune デバイス構成プロファイル

C. Microsoft Intune デバイス コンプライアンス ポリシー

D. Microsoft Entra パスワード保護

正解: ([正解を表示します](#))

質問: **230**

次の表に示すように、Microsoft Intune に登録された 5 台のデバイスを含む Microsoft 365 E5 テナントがあります。

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

すべてのデバイスに App1 という名前のアプリがインストールされています。
ユーザーが App1 からデータをコピーして他のアプリに貼り付けることを防ぐ必要があります。
Microsoft Endpoint Manager で作成する必要があるポリシーはどれですか。また、必要なポリシーの最小数はいくつですか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Policy to create in Microsoft Endpoint Manager:

▼

An app configuration policy

An app protection policy

A conditional access policy

A device compliance policy

Minimum number of required policies:

▼

1

2

3

5

正解:

Policy to create in Microsoft Endpoint Manager:

Minimum number of required policies:

Microsoft

	▼
An app configuration policy	
An app protection policy	
A conditional access policy	
A device compliance policy	

	▼
1	
2	
3	
5	

Explanation:

Policy to create in Microsoft Endpoint Manager:

Minimum number of required policies:

Microsoft

	▼
An app configuration policy	
An app protection policy	
A conditional access policy	
A device compliance policy	

	▼
1	
2	
3	
5	

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy>

質問: 231

Microsoft 365 E5 サブスクリプションをお持ちです。

次の要件を満たすように、Microsoft 365 の脅威保護を構成する必要があります。

- * ユーザー 1 というユーザーが 1 日に 30 件を超える電子メール メッセージを送信できないように制限します。
- * ファイルハッシュに基づいて特定のファイルの配信を防止します。

Microsoft Defender for Office 365 で構成する必要がある 2 つの脅威ポリシーはどれですか? 回答するには、回答領域で適切な脅威ポリシーを選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。



	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected.
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps.

Rules

	Tenant Allow/Block Lists	Manage allow or block entries for your organization.
	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users.
	Advanced delivery	Manage overrides for special system use cases.
	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first.
	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own.

正解:

Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take, and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Rules

	Tenant Allow/Block Lists	Manage allow or block entries for your organization.
	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
	Advanced delivery	Manage overrides for special system use cases.
	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

Explanation:

Limit a user named User 1 from sending more than 30 email messages per day: Anti-spam policy The anti-spam policy in Microsoft Defender for Office 365 allows you to configure outbound spam settings, including limiting the number of email messages a user can send per day. This helps prevent spam and potential email abuse within the organization.

Prevent the delivery of a specific file based on the file hash: Safe Attachments policy The Safe Attachments policy in Microsoft Defender for Office 365 can be configured to block or quarantine emails with attachments that match specific file hashes. This ensures that potentially malicious files are not delivered to users' inboxes.

質問: 232

Device1 という名前の Windows 10 デバイスと、次の表に示す Microsoft エンドポイント マネージャー ポリシーを含む Microsoft 365 テナントがあります。

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

ポリシーは Device1 に割り当てられます。

Device1 にはどのポリシー設定が適用されますか？

- A. Policy2の設定のみ
 - B. 設定なし
 - C. Policy1 の設定のみ
 - D. Policy3 の設定のみ
- 正解: ([正解を表示します](#))

質問: 233

お客様は、以下の表に示すユーザーを含む、Microsoft 365 のハイブリッド展開環境をご利用になっています。

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Microsoft Entra Connect Syncには、以下の設定があります。

パスワードハッシュ同期：有効

パススルー認証：有効

オンプレミスのActive Directoryとインターネット間の接続が失われた場合に、Microsoft Entra IDを使用して認証できるユーザーを特定する必要があります。

どのユーザーを特定すべきでしょうか？

- A. なし
- B. 使用回数1回のみ
- C. ユーザー1とユーザー2のみ
- D. ユーザー1、ユーザー2、およびユーザー3

正解: ([正解を表示します](#))

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

質問: 234

User1 という名前のユーザーと、次の表に示す管理者を含む Microsoft 365 E5 サブスクリプションがあります。

Name	Role
Admin1	Exchange Administrator
Admin2	Security Administrator
Admin3	User Administrator

ユーザー1から、午前中に1,000通のメールを送信した後、それ以上のメール送信がブロックされたという報告がありました。以下の点を確認する必要があります。

Answer Area

Administrators:

Admin1 only
Admin2 only
Admin1 and Admin2 only
Admin2 and Admin3 only
Admin1, Admin2, and Admin3

Configure:

Microsoft
Anti-spam
Anti-phishing
Anti-malware
Advanced delivery
Enhanced filtering

正解:

Configure:

Microsoft
Anti-spam
Anti-phishing
Anti-malware
Advanced delivery
Enhanced filtering

Explanation:

Answer Area

Administrators:

Admin2 only

Configure:

Anti-spam

質問: 235

ネットワークにはオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
ドメインと同期し、パスワードハッシュ同期が有効になっているMicrosoft Entraテナントがあります。テナントには、次の表に示すユーザーが含まれています。

Name	Source location	Authentication method
User1	On-premises	Password hash
User2	On-premises	Password hash
User3	On-premises	Password hash
User4	On-premises	Password hash
User5	Cloud	Cloud-only
User6	Cloud	Cloud-only

すべてのユーザーがMicrosoft 365ポータルを使用してパスワードを変更できるようにする必要があります。ソリューションはコストを最小限に抑える必要があります。
必要な Microsoft Entra ID Free ライセンスと Microsoft Entra ID P1 ライセンス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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Microsoft Entra ID Free:

Microsoft

0
1
2
3
4
5
6
7
8

Microsoft Entra ID P1:

0
1
2
3
4
5
6
7
8

正解:

Microsoft Entra ID Free:

0
1
2
3
4
5
6
7
8

Microsoft Entra ID P1:

0
1
2
3
4
5
6
7
8

Explanation:

From the table in the question:

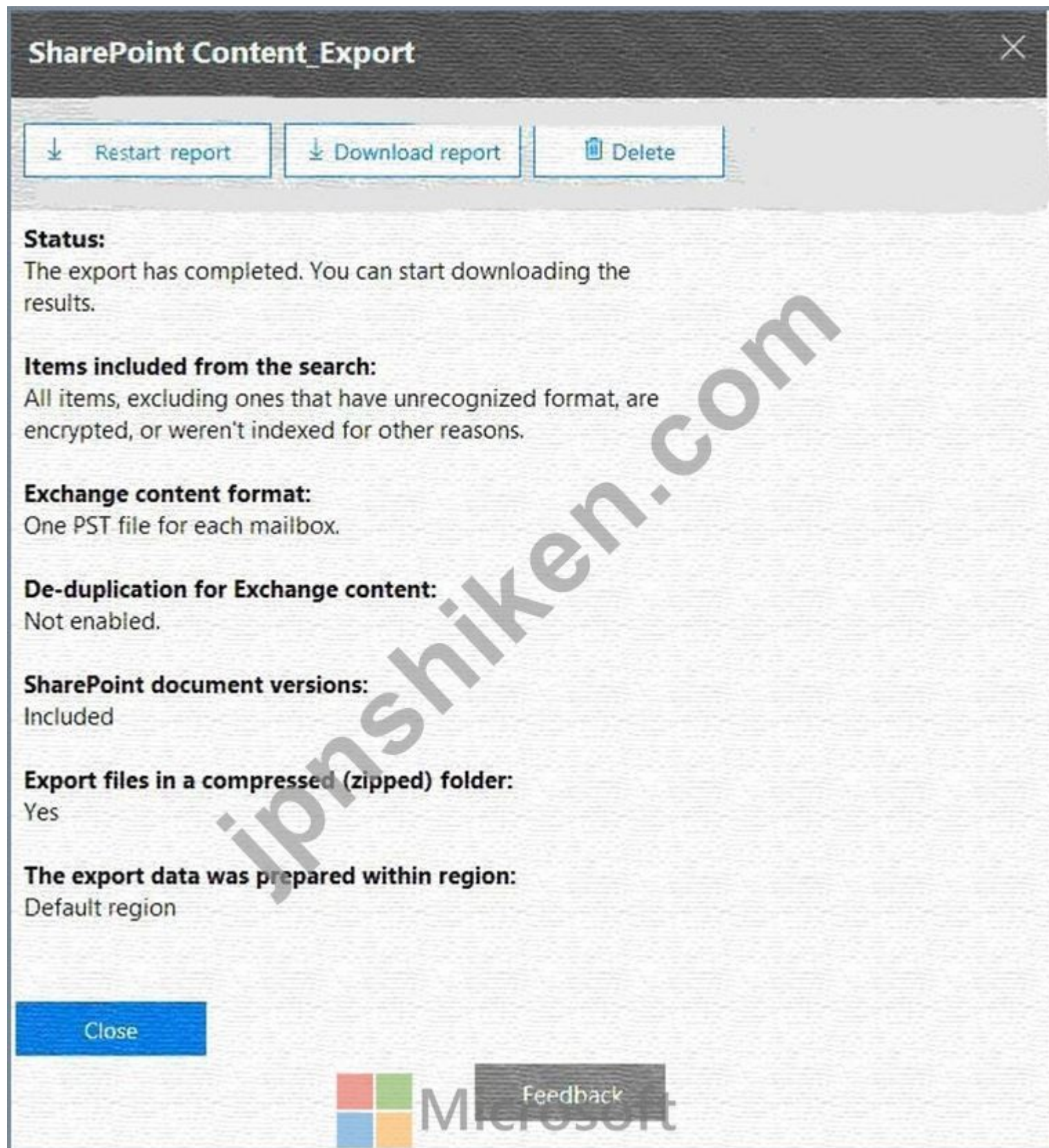
User1-User4 are On-premises (synced) with Password hash authentication.

User5-User6 are Cloud users (cloud-only).

Microsoft's licensing guidance for Self-Service Password Reset (SSPR) scenarios (which includes password change) states:
Cloud-only user password change (user knows their password and wants to change it) is available in Microsoft Entra ID Free.
Exact extract: "Cloud-only user password change ... Microsoft Entra ID Free" Hybrid user password change or reset with on-prem writeback (synced from on-prem using Entra Connect and writing the password back) requires Microsoft Entra ID P1 or P2 (or Microsoft 365 Business Premium).
Exact extract: "Hybrid user password change or reset with on-prem writeback ... Microsoft Entra ID P1 or P2" Because User1-User4 are synced (hybrid) users and must change passwords using a Microsoft 365 portal and keep passwords consistent with on-premises AD DS, they require password writeback, which requires P1 for those users.
Because User5-User6 are cloud-only users, they can change passwords with Entra ID Free.
Minimum licenses (cost-optimized)
Microsoft Entra ID P1 licenses: 4 (User1-User4)
Microsoft Entra ID Free licenses: 2 (User5-User6)

質問: 236

セキュリティとセキュリティからコンプライアンス管理センターでは、図に示すようにコンテンツ エクスポートを作成します。(展示」タブをクリックします。)



何が輸出から除外されますか？

- A. 10 MB の XLSX ファイル
- B. 5MBのMP3ファイル
- C. 5 KB の RTF ファイル
- D. 80 MB PPTX ファイル

正解: ([正解を表示します](#))

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don ' t contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don ' t perform full-text indexing on these types of files.

These types of files are considered to be unsupported file types.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide>

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

質問: 237

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 365 admin role	Microsoft Exchange Online admin role
User1	Global Administrator	None
User2	Exchange Administrator	None
User3	Service Support Administrator	None
User4	None	Organization Management

Exchange Online を使用して DNS ドメインの電子メールを管理する予定です。

管理者は DNS ドメインをサブスクリプションに追加します。

DNS ドメインのステータスは「セットアップが完了していません」です。

どのユーザーが DNS ドメインのセットアップを完了できるかを識別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。

どのユーザーを特定する必要がありますか？

A. ユーザー 4

B. ユーザー2

C. ユーザー1

D. ユーザー 3

正解: (正解を表示します)

質問: 238

Microsoft 365 サブスクリプションをお持ちです。

[ヘッダーの設定] アクションを使用するように構成されたデータ損失防止 (DLP) ポリシーを作成する必要があります。

ポリシーはどの場所に適用できますか？

A. SharePoint サイト

B. メールを交換する

C. OneDrive アカウント

D. チームのチャットとチャネル メッセージ

正解: B (コメントを发表する)

質問: 239

Microsoft Defender for Endpoint を使用します。

次の表に示す Microsoft Defender for Endpoint デバイス グループがあります。

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	Not applicable

次の表に示すように、コンピューターを Microsoft Defender for Endpoint にオンボードする予定です。

Computer1-London: [Group1, Group2, Group3, Ungrouped machines]

Server1-London: [Group1, Group2, Group3, Ungrouped machines]

Computer1-London: [Group1, Group2, Group3, Ungrouped machines]

Server1-London: [Group1, Group2, Group3, Ungrouped machines]

正解:
Answer Area

Explanation:
Answer Area

Computer1-London: Group1

Server1-London: Group2

質問: 240

次の表に示すユーザーを含む Microsoft 365 E5 テナントがあります。

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

テナントには、次の表に示すデバイスが含まれます。

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	None	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	None	iOS	Not enrolled

次の表に示すアプリがあります。

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

Microsoft Endpoint Manager を使用してユーザーのアプリを管理する予定です。
次の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Statements

Yes

No

App1 can be assigned as a required install for User3.

☐

☐

App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.

☐

☐

App3 can be installed automatically for UserGroup1.

☐

☐

正解:

Statements

Yes

No

App1 can be assigned as a required install for User3.

☐

☒

App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.

☐

☒

App3 can be installed automatically for UserGroup1.

☒

☐

Explanation:

Statements	Yes	No
App1 can be assigned as a required install for User3.	☒	☐
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	☐	☒
App3 can be installed automatically for UserGroup1.	☒	☐

Reference:
<https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy>
<https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy>

質問: 241
あなたは、User1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を所有しています。
ユーザー1は、許可されている1日のメール送信数のデフォルト制限を超えており、制限対象エンティティリストに登録されています。
制限対象エンティティリストからUser1を削除する必要があります。
何を使うべきでしょうか？
A. Exchange 管理センター
B. Microsoft Purview コンプライアンス ポータル
C. Microsoft 365 管理センター
D. Microsoft Defender XDR ポータル
E. Microsoft Login 管理センター

正解: D (コメントを发表する)
Admins can remove user accounts from the Restricted entities page in the Microsoft Defender XDR portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft Defender XDR portal In the Microsoft Defender XDR portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>.
Reference:
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam>

有効的な**MS-102J**問題集はJPNTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTest.comは今最新**MS-102J**試験問題集を提供します。JPNTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 242
ホットスポット
Microsoft 365 サブスクリプションをお持ちです。
次の指標を確認する必要があります。

Microsoft Teamsの毎日のアクティブユーザー数
最近の Microsoft サービスの問題
何を使うべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Teams daily active users:

Microsoft Secure Score

Adoption Score

Service health

Usage reports

Recent Microsoft service issues:

Microsoft Secure Score

Adoption Score

Service health

Usage reports

Microsoft

正解:

Answer Area

Teams daily active users:

Microsoft Secure Score

Adoption Score

Service health

Usage reports

Recent Microsoft service issues:

Microsoft Secure Score

Adoption Score

Service health

Usage reports

Microsoft

Explanation:

Answer Area



Box 1: Usage reports

The daily active users in Microsoft Teams

Microsoft 365 Reports in the admin center - Microsoft Teams usage activity The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.

Box 2: Service Health

Recent Microsoft service issues

You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft 365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams-usage-activity>

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health>

質問: 243

注: このセクションには、同じシナリオと問題に関する 1 つ以上の質問セットが含まれています。各質問には、問題に対する独自の解決策が提示されています。解決策が、指定された目標を満たしているかどうかを判断する必要があります。

セット内の複数のソリューションが問題を解決できる可能性があります。また、セット内のどのソリューションも問題を解決できない可能性もあります。

このセクションの質問に回答した後は、戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 E5 サブスクリプションがあり、Microsoft Defender for Office 365 を使用しています。

スパム、フィッシング、マルウェアから保護するために、バランスの取れたベースライン保護プロファイルを適用する脅威ポリシーを実装する必要があります。

解決策: マルウェア対策ポリシーを作成します。

これは目標を満たしていますか?

A. いいえ

B. はい

正解: ([正解を表示します](#))

質問: 244

Microsoft 365 E5 サブスクリプションをお持ちです。
Mailbox1 という名前のメールボックスを使用して、悪意のある電子メール メッセージを分析する予定です。
次の要件を満たすように Microsoft Defender for Office 365 を構成する必要があります。

- * 受信メールが Mailbox1 でフィルタリングされていないことを確認してください。
- * サブスクリプション内の他のすべてのメールボックスに対するなりすましおよびスプーフィング攻撃を検出します。

どの 2 つの設定を構成する必要がありますか?回答するには、回答領域で適切な設定を選択します。

Answer Area

Policies

-  Anti-phishing
-  Anti-spam
-  Anti-malware
-  Safe Attachments
-  Safe Links

Rules

-  Tenant Allow/Block Lists
-  Email authentication settings
-  DKIM
-  Advanced delivery
-  Enhanced filtering
-  Quarantine policies

正解:

Answer Area

Policies

Anti-phishing

Anti-spam

Anti-malware

Safe Attachments

Safe Links

Rules

Tenant Allow/Block Lists

Email authentication settings

DKIM

Advanced delivery

Enhanced filtering

Quarantine policies



Explanation:

Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments. This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.

Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

質問: 245

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。

このセクションの質問に回答すると、後から戻って回答内容を確認することはできません。そのため、これらの質問は復習画面には表示されません。

お使いのネットワークには、Active Directoryフォレストが含まれています。

Microsoft 365 を導入します。

ディレクトリ同期を実装する予定です。

同期されたIDに対するセキュリティソリューションを推奨する必要があります。ソリューションは以下の要件を満たす必要があります。

* Active Directoryが利用できなくなった場合でも、ユーザーはMicrosoft 365サービスに対して正常に認証できる必要があります。

* ユーザーパスワードは10文字以上である必要があります。

解決策 :Microsoft Entraテナントでパススルー認証を実装し、パスワード保護を設定します。これで目標は達成されますか？

A. はい

B. いいえ

正解: (正解を表示します)

質問: 246

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

現在のセーフリンクの設定を、マイクロソフトが推奨する設定と比較する必要があります。

何を使うべきでしょうか？

A. Microsoft Secure Score

B. Microsoft Entra ID Protection

C. 構成アナライザー

D. マイクロソフトのパービュー

正解: A (コメントを発表する)

質問: 247

contoso.com という名前の Microsoft Entra テナントがあり、次の表に示すようにテナント間アクセスが構成されています。

Direction	Type	Applies to	Status
Inbound	B2B collaboration	External users and groups	All allowed
Inbound	B2B collaboration	Applications	All allowed
Inbound	B2B direct connect	External users and groups	All blocked
Inbound	B2B direct connect	Applications	All blocked
Inbound	Trust settings	Not applicable	Disabled
Outbound	B2B collaboration	Users and groups	All allowed
Outbound	B2B collaboration	External applications	All allowed
Outbound	B2B direct connect	Users and groups	All allowed
Outbound	B2B direct connect	External applications	All allowed

貴社にはFabrikamとAdatum Corporationという2つのパートナー組織があります。FabrikamはMicrosoftと提携しています。

fabrikam.com という名前の 365 ドメインがあります。データムは、adatum.com という名前の Microsoft 365 ドメインを持っています。

fabrikam.com のテナント間アクセスは、以下の表に示すように設定します。

Direction	Type	Applies to	Status
Inbound	B2B collaboration	External users and groups	All blocked
Inbound	B2B collaboration	Applications	All blocked
Inbound	B2B direct connect	External users and groups	All allowed
Inbound	B2B direct connect	Applications	All allowed
Inbound	Trust settings	<i>Not applicable</i>	Disabled
Outbound	B2B collaboration	Users and groups	All blocked
Outbound	B2B collaboration	External applications	All blocked
Outbound	B2B direct connect	Users and groups	All blocked
Outbound	B2B direct connect	External applications	All blocked

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

Statements	Yes	No
A user in contoso.com can send a guest invitation to a user that has an email address of user1@fabrikam.com.	☐	☐
A user in contoso.com can send a guest invitation to a user that has an email address of user1@adatum.com.	☐	☐
A user in contoso.com can accept a guest invitation from a user that has an email address of user1@fabrikam.com.	☐	☐

正解:

Statements	Yes	No
A user in contoso.com can send a guest invitation to a user that has an email address of user1@fabrikam.com.	☐	☒
A user in contoso.com can send a guest invitation to a user that has an email address of user1@adatum.com.	☒	☐
A user in contoso.com can accept a guest invitation from a user that has an email address of user1@fabrikam.com.	☐	☒

Explanation:

Statement

Answer

A user in contoso.com can send a guest invitation to a user that has an email address of user1@fabrikam.com.

No

A user in contoso.com can send a guest invitation to a user that has an email address of user1@adatum.com.

Yes

A user in contoso.com can accept a guest invitation from a user that has an email address of user1@fabrikam.com.

No

This question is testing B2B collaboration, not B2B direct connect. A guest invitation creates or uses a B2B collaboration guest relationship. Microsoft states that cross-tenant access settings determine both inbound access by external users to your resources and outbound access by your users to external organizations.

Inbound access controls whether users from an external Microsoft Entra organization can access resources in your tenant, while outbound access controls whether your users can access resources in an external organization. Microsoft also states that default cross-tenant access settings apply to all external organizations unless organization-specific settings exist.

For fabrikam.com, organization-specific settings override the default settings. Because Inbound B2B collaboration is All blocked, a Contoso user cannot invite a Fabrikam user as a guest into Contoso. Therefore, the first statement is No. For adatum.com, no organization-specific blocking rule is shown, so the default tenant setting applies; B2B collaboration is enabled by default for external Microsoft Entra organizations, so the second statement is Yes.

For the third statement, a Contoso user accepting an invitation from Fabrikam means the Contoso user is accessing Fabrikam as an external guest, which uses Outbound B2B collaboration from Contoso to Fabrikam. Since outbound B2B collaboration for fabrikam.com is All blocked, the answer is No.

質問: 248

エンドポイント セキュリティを使用する Microsoft 365 E5 サブスクリプションがあります。

グループを作成し、そのグループにエンドポイント セキュリティ マネージャーの役割を割り当てる必要があります。

どのタイプのグループを使用できますか？

A. セキュリティのみ

B. メールが有効なセキュリティ、Microsoft 365、およびセキュリティのみ

C. 配布、メール対応セキュリティ、Microsoft 365、およびセキュリティ

D. Microsoft 365 のみ

E. メールが有効なセキュリティとセキュリティのみ

正解: B ([コメントを发表する](#))

質問: 249

次のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

名前: ユーザー1

UPN: user1@contoso.com

電子メール アドレス: user1@marketmg.contoso.com

MFA 登録ステータス: 無効

User1 が user1@marketing.contoso.com の電子メール アドレスを使用して Web 上の Outlook にサインインしようとする、ユーザーはサインインできません。

User1 が user1@marketing.contoso.com を使用して Web 上の Outlook にサインイン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. MFA 登録ポリシーを User1 に割り当てます。

- B.** User1 のパスワードをリセットします。
- C.** User1 の代替電子メール アドレスを追加します。
- D.** User1 の UPN を変更します。

正解: ([正解を表示します](#))

Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.

Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user ' s email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.

Configure the Microsoft Entra ID multifactor authentication registration policy Microsoft Entra ID (Microsoft Entra ID) Identity Protection helps you manage the roll-out of Microsoft Entra ID multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you ' re signing in to.

Reference:

<https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname>

質問: **250**

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

セキュリティのデフォルトが無効になっている Microsoft Entra テナントがあります。

Microsoft Entra Connect Sync はディレクトリ同期用に構成されています。パスワード ハッシュ同期とパススルー認証は無効になっています。

漏洩した資格情報を検出するには、Microsoft Entra ID Protection 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 Entra 管理センターから、検証可能な資格情報を構成します。
- B.** Microsoft Entra Connect から、パススルー認証を有効にします。
- C.** Microsoft Entra Connect から、パスワード ハッシュ同期を有効にします。
- D.** Microsoft Entra 管理センターから、セキュリティの既定値を有効にします。

正解: ([正解を表示します](#))

質問: **251**

Microsoft 365 E5 テナントがあります。

顧客データに関する欧州連合のプライバシー規制への準拠を評価する必要があります。

Microsoft 365 コンプライアンス センターでは何をすべきですか？

- A.** データ主体リクエスト (DSR) を作成します。
- B.** 一般データ保護規則 (GDPR) データに対するデータ損失防止 (DLP) ポリシーを作成します。
- C.** EU GDPR 評価テンプレートに基づいて評価を作成します
- D.** データ保護ベースライン評価テンプレートに基づいて評価を作成します

正解: ([正解を表示します](#))

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan>

質問: **252**

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。

User1 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。
User1 がコンプライアンス マネージャー評価を作成できるようにする必要があります。
解決策: Microsoft 365 管理センターから、User1 にコンプライアンス データ管理者ロールを割り当てます。
これは目標を達成していますか？

- A. はい
 - B. いいえ
- 正解: ([正解を表示します](#))

Reference:
<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

質問: 253

Microsoft Defender for Office 365 を使用する Microsoft 365 サブスクリプションがあります。
受信メール メッセージがスパムとしてマークされ、その後隔離された場合、メール受信者に通知するまでに数日かかることに気付きました。
電子メールの受信者に 24 時間以内に通知が届くようにする必要があります。
A. DefaultFullAccessPolicy 検疫ポリシーを変更します。
B. 検疫ポリシーのグローバル設定を変更します。
C. カスタム検疫ポリシーを追加します。
D. デフォルトの受信スパム対策ポリシーを変更します。

正解: B ([コメントを發表する](#))

質問: 254

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 サブスクリプションをお持ちです。
ユーザーがオンプレミス ネットワークに接続していない限り、ユーザーが Microsoft SharePoint Online サイトにアクセスできないようにする必要があります。

解決策: Endpoint Management 管理センターから、デバイス構成プロファイルを作成します。
これは目標を達成していますか？

- A. はい
 - B. いいえ
- 正解: ([正解を表示します](#))

You need to create a trusted location and a conditional access policy.

質問: 255

Microsoft 365 E5 サブスクリプションをお持ちです。
サポートされているファイアウォール デバイスから Microsoft Defender for Cloud Apps に syslog データを取り込む予定です。
自動ログアップロードを設定する必要があります。
ログ コレクター用に構成する必要がある 2 つのコンポーネントはどれですか。それぞれの正解は完全なソリューションを示します。
注意: 正しい選択ごとに 1 ポイントが付与されます。

- A. 受信者タイプ
- B. 接続文字列
- C. ユーザー名とパスワード
- D. ホストのIPアドレスまたはFQDN
- E. データソース

正解: ([正解を表示します](#))

質問: 256

あなたはMicrosoft 365テナントをお持ちです。

Microsoft Defender XDR を使用してテナント内のインシデントを管理する予定です。Microsoft Defender ポータルのインシデント ページには、どの Microsoft サービス ソースが表示されますか？

- A. Microsoft Defender for Cloud
- B. アズールアーク
- C. Azure Web Application Firewall
- D. Microsoft Defender for Identity

正解: ([正解を表示します](#))

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> **598**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 257

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

ユーザーがパートナー企業のポータルにアクセスしようとする、次のようなメッセージが表示されます。



パートナー企業のポータルへのユーザー アクセスを有効にする必要があります。
どの Microsoft Defender for Endpoint 設定を変更する必要がありますか？

- A. アラート通知
- B. アラートの抑制
- C. カスタム検出
- D. 高度な狩猟
- E. インジケーター

正解: (正解を表示します)



This Website Is Blocked By Your Organization
Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.
Reference:
<https://jadexstrategic.com/web-protection/>

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
過去7日間に匿名IPアドレスからMicrosoft Office 365にアクセスしたユーザーを特定する必要があります。
あなたはどうすべきでしょうか？

A. Cloud App Security 管理センターから、[ユーザーとアカウント] を選択します。
B. Microsoft Entra ID 管理センターから、危険なサインイン レポートを表示します。
C. Microsoft 365 セキュリティ センターから脅威トラッカーを表示します。
D. 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 レポートを表示します。

正解: ([正解を表示します](#))

質問: 259

あなたはMicrosoft 365のサブスクリプションをお持ちです。
すべてのユーザーのメールはMicrosoft Exchange Onlineに保存されています。
User1という名前のユーザーのメールボックスで、ProjectXという単語を含むすべてのメールメッセージのコピーを保存する必要があります。
まず最初に何をすべきでしょうか？

A. Microsoft Defender XDR からメッセージ トレースを開始します。
B. Microsoft Purview コンプライアンス ポータルから、ラベルとラベル ポリシーを作成します。
C. Microsoft Defender for Cloud Apps からアクティビティ ポリシーを作成します。
D. Exchange 管理センターからメールフロールールを作成します。

正解: ([正解を表示します](#))

質問: 260

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
Site1 上のクレジット カード番号を含むドキュメントに自動的にラベルを付ける必要があります。
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
Create a sensitivity label.	
Create an auto-labeling policy.	
Create a sensitive information type.	
Wait 24 hours, and then turn on the policy.	
Publish the label.	
Create a retention label.	
Wait eight hours, and then turn on the policy.	

正解:

Actions	Answer Area
Create a sensitivity label.	Create a sensitivity label.
Create an auto-labeling policy.	
Create a sensitive information type.	Publish the label.
Wait 24 hours, and then turn on the policy.	
Publish the label.	Create an auto-labeling policy.
Create a retention label.	
Wait eight hours, and then turn on the policy.	

Explanation:

Create a sensitivity label.
Publish the label.
Create an auto-labeling policy.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-label-policies-can-do>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

質問: 261

Microsoft Intune に登録された 1,000 台の iOS デバイスを含む Microsoft 365 テナントがあります。一括購入型アプリを購入し、そのアプリをデバイスに展開する予定です。Intune を使用して、使用済みライセンスを追跡し、アプリを管理する必要があります。アプリの購入には何を使用すればよいですか？

- A. ビジネス向け Microsoft ストア
- B. Apple ビジネスマネージャー
- C. Apple iTunes ストア
- D. Apple コンフィギュレータ

正解: (正解を表示します)

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios>

質問: 262

Microsoft 365 サブスクリプションをお持ちです。

onmicrosoft.com ドメインをサブスクリプションに追加する必要があります。追加のドメインは、ユーザーの電子メール アドレスとして割り当て可能である必要があります。サブスクリプションに含めることができる onmicrosoft.com ドメインの最大数は何ですか？

- A. 1
- B. 2

C. 5

D. 10

正解: (正解を表示します)

You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq>

質問: 263

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	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

Microsoft エンドポイント マネージャーには、次の表に示す Office アプリのポリシー設定があります。

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

ポリシーでは、次の表に示す設定が使用されます。

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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 has their cache cleared on close.	☐	☐
User2 has Cursor movement set to Visual.	☐	☐
User3 has Cursor movement set to Visual.	☐	☐

正解:

Statements	Yes	No
User1 has their cache cleared on close.	☐	☐
User2 has Cursor movement set to Visual.	☐	☐
User3 has Cursor movement set to Visual.	☐	☐

Explanation:

Statements	Yes	No
User1 has their cache cleared on close.	☐	☐
User2 has Cursor movement set to Visual.	☐	☐
User3 has Cursor movement set to Visual.	☐	☐

Reference:

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

質問: 264

お客様は、以下の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションをご利用されています。

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

Microsoft Defender for Endpoint を実装しました

Microsoft Defender XDR ポータルへのアクセスを制限するには、ロールベースのアクセス制御 (RBAQ) を有効にする必要があります。

どのユーザーがRBACを有効にできるか、またRBACが有効になった後、どのユーザーがMicrosoft Defender XDRポータルにアクセスできなくなるか。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：正解ごとに1ポイントが加算されます。

Answer Area

Users that can enable RBAC:

Users that will no longer have access to the Microsoft 365 Defender portal:

正解:

ANSWER AREA

Users that can enable RBAC:

Users that will no longer have access to the Microsoft 365 Defender portal:

Explanation:

Answer Area

Users that can enable RBAC:

Users that will no longer have access to the Microsoft 365 Defender portal:

質問: 265

コンプライアンス要件を満たすには、条件付きアクセス ポリシーを構成する必要があります。
Exchange Online をクラウド アプリとして追加します。
Policy1 で構成する必要がある 2 つの追加設定はどれですか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

New

Info

* Name

Policy1

Assignments

Users and groups

0 users and groups selected

Cloud apps

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

OnOff

Conditions

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Device state (preview)

Info

Configure

YesNo

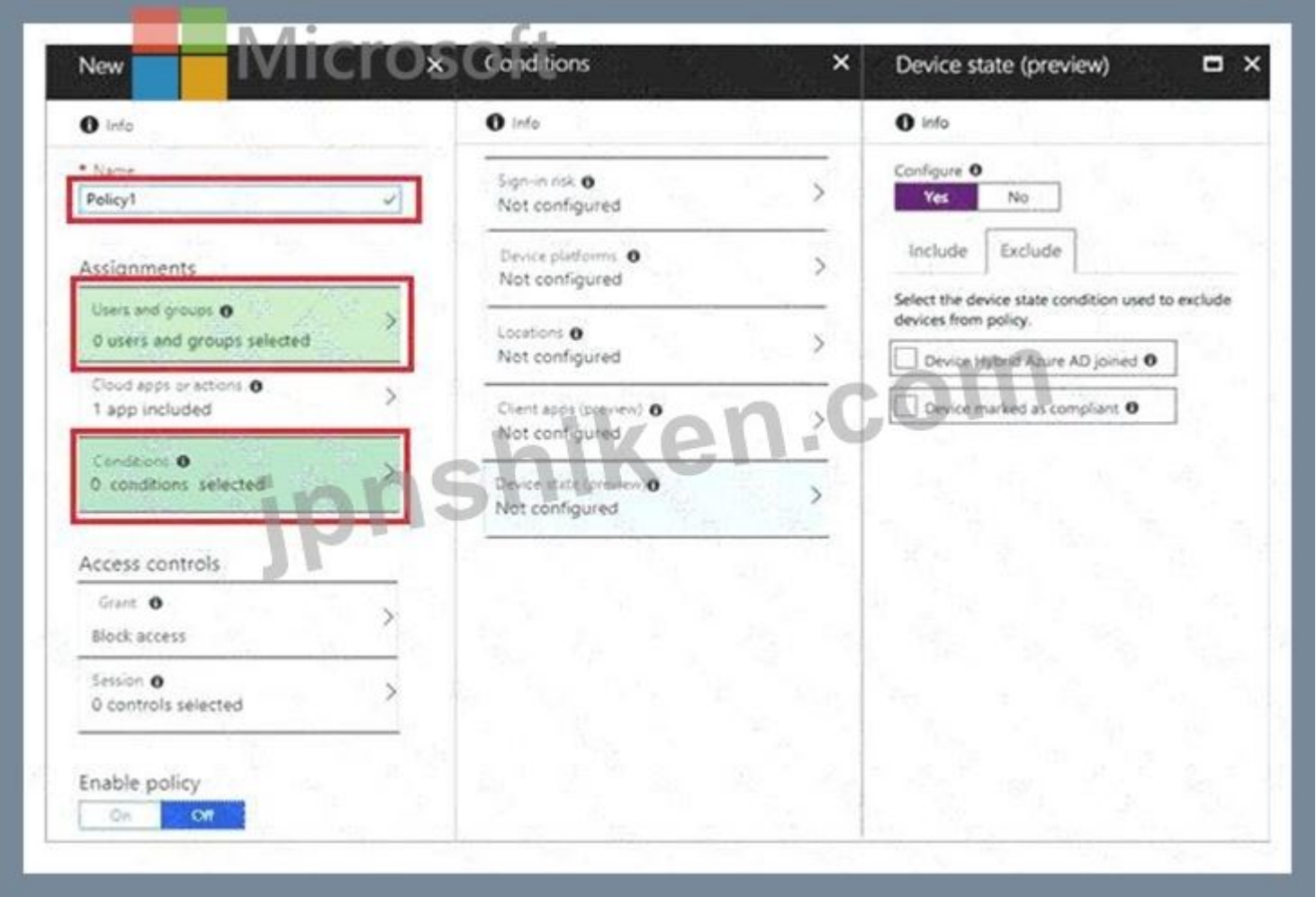
IncludeExclude

Select the device state condition used to exclude devices from policy.

Device Hybrid Azure AD joined

Device marked as compliant

Explanation:
Suggested answer:



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

Topic 1, Contoso, LtdOverview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

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

Contoso recently purchased a Microsoft 365 ES subscription.

Existing Environment

Requirement

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

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

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Microsoft Entra ID (Microsoft Entra ID) and includes the users shown in the following table.

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

The domain also includes a group named Group1.

Planned Changes

Contoso plans to implement the following changes:

- *Implement Microsoft 365.
- *Manage devices by using Microsoft Intune.
- *Implement Microsoft Entra IDvanced Threat Protection (ATP).
- *Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- *When a Windows 10 device is joined to Microsoft Entra ID, the device must enroll in Intune automaticity.
- *Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- *User1 must be able to enroll all the New York office mobile devices in Intune.
- *Azure ATP sensors must be installed and must NOT use port mirroring.
- *Whenever possible, the principle of least privilege must be used.
- *A Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

- *Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- *Configure Windows Information Protection (W1P) for the Windows 10 devices.

質問: 266

Microsoft 365 サブスクリプションをお持ちです。

一部の外部ユーザーが Microsoft SharePoint サイトのセンターにアクセスしたことがわかりました。

SharePoint 共有ポリシーを変更して、組織外での共有を防止します。

SharePoint 共有ポリシーが将来変更された場合は、通知を受ける必要があります。

解決策: Security \$ Compliance 管理センターから、脅威管理ポリシーを作成します。

これは目標を達成していますか？

- A. はい
 - B. いいえ
- 正解: B ([コメントを发表する](#))

質問: 267

次の表に示す管理単位を含む Microsoft 365 サブスクリプションがあります。

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

グループには、次の表に示すメンバーが含まれます。

Name	Members
Group1	User1
Group2	User2, User4

ユーザーには、次の表に示す役割が割り当てられます。

Name	Role	Scope
User1	None	Not applicable
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	None	Not applicable

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。

注記;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
User2 can reset the password of User1.	☐	☐
User2 can reset the password of User4.	☐	☐
User3 can assign licenses to User1.	☐	☐

正解:

Answer Area

Statements

User2 can reset the password of User1.

Yes

☐

No

☐

User2 can reset the password of User4.

☐☐

User3 can assign licenses to User1.

☐☐

Explanation:

Answer Area

Statements

User2 can reset the password of User1.

Yes

☒

No

☐

User2 can reset the password of User4.

☐☒

User3 can assign licenses to User1.

☒☐

質問: 268

Microsoft Entra ID (Microsoft Entra ID) でセキュリティの既定値を有効にする設定が「いいえ」になっている Microsoft 365 テナントがあります。テナントは、以下の表に示すように、2件のコンプライアンスマネージャーによる評価を受けています。

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

SP800評価には、以下の表に示す改善策が含まれています。

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

あなたは以下の操作を実行します。
データ保護ベースライン評価については、**脅威インテリジェンスプログラムの確立**のテストステータスを **実装済み**に変更してください。
すべてのユーザーに対して**多要素認証(MFA)**を有効にしてください。
以下の各記述について、正しい場合は **はい**を選択してください。そうでない場合は **いいえ**を選択してください。
注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	☐	☐
The SP800 assessment score will increase by 54 points.	☐	☐
The Data Protection Baseline score will increase by 9 points.	☐	☐

正解:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	☐	☒
The SP800 assessment score will increase by 54 points.	☐	☒
The Data Protection Baseline score will increase by 9 points.	☒	☐

Explanation:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	☐	☒
The SP800 assessment score will increase by 54 points.	☐	☒
The Data Protection Baseline score will increase by 9 points.	☒	☐

Reference:

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

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide#action-types-and-points>

質問: 269

あなたの会社には Microsoft 365 テナントがあります

Engineering という名前のグループのメンバーであるユーザーが、自分のモバイル デバイスをモバイル デバイス管理 (MDM) に登録できるようにする予定です。デバイス タイプの制限は、次の表に示すように構成されます。

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

デバイス制限は次の表のように設定されています。

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users



正解:



Explanation:



<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority>

質問: 270

お客様は、Contoso.com という名前の Microsoft Entra ID (Microsoft Entra ID) テナントをお持ちです。

Contoso IDインスタンス用のMicrosoft Defenderを作成します。
テナントには、以下の表に示すユーザーが含まれています。

MICROSOFT		
Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

センサーを識別するには、Defenderの設定を変更する必要があります。
解決策 :ユーザー4に、IDセンサーの設定に関してDefenderを変更するよう指示します。
これは目標を達成していると言えるでしょうか？

- A. はい
B. いいえ
正解: A (コメントを发表する)

質問: 271
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、指定された問題を満たす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。
ネットワークには Active Directory ドメインが含まれています。
Microsoft Entra テナントを展開します。
別の管理者は、Microsoft Entra テナントと同期するようにドメインを構成します。
組織単位 (OU) 内の 10 個のユーザー アカウントが Microsoft Entra テナントに同期されていないことがわかりました。他のすべてのユーザー アカウントは正常に同期されました。
Microsoft Entra Connect Health を確認すると、すべてのユーザー アカウントの同期が正常に完了したことがわかります。
10 個のユーザー アカウントが Microsoft Entra テナントに同期されていることを確認する必要があります。
解決策: Microsoft Entra Connect からフィルタリング設定を変更します。
これは目標を達成していますか？
A. いいえ
B. はい
正解: A (コメントを发表する)

有効的な**MS-102J**問題集はJPNTTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTTest.comは今最新**MS-102J**試験問題集を提供します。JPNTTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%**ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 272
Site1 と Site2 という名前の 2 つの Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
次の表に示す文書があります。

Name	Number of credit card numbers in the document	Number of SWIFT codes in the document	Stored on
Document1	3	3	Site1
Document2	7	2	Site2
Document3	15	0	Site1

図に示すように、高度な DLP ルールを持つ DLP1 という名前のデータ損失防止 (DLP) ポリシーを作成します。

Sensitive info types

Credit Card Number	Low confidence	Instance count	1	to	5
SWIFT Code	Low confidence	Instance count	1	to	2

Add

Group name *

Group2

Group operator

Any of these

Sensitive info types

Credit Card Number	Low confidence	Instance count	10	to	Any
--------------------	----------------	----------------	----	----	-----

Add

Evaluate predicate for (available for Exchange workload only)

☒ Message or attachment ☐ Message only ☐ Attachments only

Create group

Save Cancel

Create rule

Content contains

Group name *

Group1

Group operator

All of these

If you specify "All of these" for the "Content contains" condition, you can't add more than one retention label and one sensitivity label to a group. This is because emails and documents can have only one retention label and one sensitivity label assigned to them at a time.

Sensitive info types

Credit Card Number

Low confidence

Instance count

1

to

5

SWIFT Code

Low confidence

Instance count

1

to

2

Add

OR

Group name *

Group2

Group operator

Any of these

Sensitive info types

Credit Card Number

Low confidence

Instance count

10

to

Any

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

Statements	Yes	No
DLP1 applies to Document1.	☐	☐
DLP1 applies to Document2.	☐	☐
DLP1 applies to Document3.	☐	☐

正解:

Statements	Yes	No
DLP1 applies to Document1.	☐	☒
DLP1 applies to Document2.	☐	☒
DLP1 applies to Document3.	☒	☐

Explanation:

NO

No

Yes

In the Content contains condition, Microsoft Purview DLP lets you combine conditions using logical operators:

"Any of these" = logical OR

"All of these" = logical AND

From the exhibit, the rule is effectively:

Group1 (All of these / AND)

Credit Card Number: 1 to 5 instances

SWIFT Code: 1 to 2 instances

OR

Group2 (Any of these)

Credit Card Number: 10 to Any instances

So the rule matches if:

(Credit Card is 1-5 AND SWIFT is 1-2) OR (Credit Card is #10).

Evaluate each document against the rule

Document1: Credit Card = 3, SWIFT = 3

Group1 requires SWIFT 1-2, but Document1 has 3 # Group1 = false

Group2 requires Credit Card #10, but Document1 has 3 # Group2 = false Result: DLP1 does NOT apply # No Document2: Credit Card = 7, SWIFT = 2 Group1 requires Credit Card 1-5, but Document2 has 7 # Group1 =

false Group2 requires Credit Card #10, but Document2 has 7 # Group2 = false Result: DLP1 does NOT apply # No Document3: Credit Card = 15, SWIFT = 0 Group2 requires Credit Card #10, and Document3 has 15 #

Group2 = true Result: DLP1 DOES apply # Yes

質問: 273

Microsoft 365 テナントがあります。

Microsoft Intune に登録するすべての Windows 10 デバイスに対して、BitLocker ディスク暗号化 (BitLocker) を自動的に有効にする予定です。

何をえばいいのでしょうか？

A. 攻撃対象領域削減 (ASR) ポリシー

B. アプリ構成ポリシー

C. デバイスのコンプライアンス ポリシー

D. デバイス構成プロファイル

正解: D (コメントを发表する)

Reference:
<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

質問: 274

ホットスポット

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

8月1日にMicrosoft Entra ID Protectionから、以下の設定を含む多要素認証登録ポリシーを構成します。

割り当て: すべてのユーザー

コントロール: Microsoft Entra ID 多要素認証の登録を必須にする ポリシーの適用: オン 8 月 3 日に、User1 と User2 という名前の 2 人のユーザーを作成します。

ユーザーは、次の表に示す日付に初めて Azure 多要素認証 (MFA) を使用して認証を行います。

User	Date
User1	August 5
User2	August 7

User1とUser2は、いつまでにAzure MFAの登録を完了する必要がありますか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

User1:

▼

August 6

August 17

August 19

September 3

September 5

User2:

▼

August 8

August 17

August 19

August 21

September 7

正解:

User1:
August 6
August 17
August 19
September 3
September 5

User2:
August 8
August 17
August 19
August 21
September 7

Explanation:

Answer Area

User1:
August 6
August 17
August 19
September 3
September 5

User2:
August 8
August 17
August 19
August 21
September 7

Box 1: August 19

Note: Security defaults will trigger a 14 day grace period for registration after a user ' s first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.

Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period.

Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi-Factor Authentication, then the user must be able to pass that MFA request.

Box 2: August 21

Reference:

質問: 275

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。

Microsoft	
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

サブスクリプションには、次の 2 つのスパム対策ポリシーがあります。

* 名前: AntiSpam1

* 優先度: 0

* これらのユーザー、グループ、ドメインを誘導する

o ユーザー: ユーザー3

o グループ: グループ1

* これらのユーザー、グループ、ドメインを除外する

o グループ: グループ2

* メッセージの制限

o 1日のメッセージ制限を100に設定する

* 名前: AntiSpam2

* 優先度: 1

* これらのユーザー、グループ、ドメインを含める

o ユーザー: User! o グループ: Group2

* これらのユーザー、グループ、ドメインを除外する

o ユーザー: ユーザー3

* メッセージの制限

o 1日のメッセージ制限を50に設定する

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	☐	☐
User2 can send a maximum of 50 email messages per day.	☐	☐
User3 can send a maximum of 100 email messages per day.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	☐	☒
User2 can send a maximum of 50 email messages per day.	☒	☐
User3 can send a maximum of 100 email messages per day.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	☐	☒
User2 can send a maximum of 50 email messages per day.	☒	☐
User3 can send a maximum of 100 email messages per day.	☐	☒

質問: 276

Microsoft J65 E5 サブスクリプションをお持ちです。

Microsoft Defender for Endpoint を Microsoft Intune と統合します。

デバイスが Intune に登録されるときに、Defender for Endpoint に自動的にオンボードされるようにする必要があります。

解決策: 共同管理を有効にします。

これは目標を満たしていますか？

A. はい

B. いいえ

正解: **A** ([コメントを發表する](#))

質問: **277**

Microsoft エンドポイント マネージャーを使用して管理されている Windows 10 デバイスがあります。

Microsoft Edgeでセキュリティ設定を構成する必要があります。

Microsoft エンドポイント マネージャーで何を作成する必要がありますか？

A. アプリ構成ポリシー

B. アプリ

C. デバイス構成プロファイル

D. デバイスのコンプライアンス ポリシー

正解: ([正解を表示します](#))

Reference:

<https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune>

質問: **278**

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に onmicrosoft.com サフィックスを持つドメインを追加する必要があります。追加したドメインは、ユーザーのメールアドレスとして割り当て可能である必要があります。

サブスクリプションに含めることができる onmicrosoft.com ドメインの最大数はいくつですか？

A. 10

B. 5

C. 2

D. 1

正解: **D** ([コメントを發表する](#))

質問: **279**

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

Name	Type
User1	User
Group1	Microsoft 365 group
Group2	Mail-enabled security group
Group3	Distribution group

Shared1 という名前の共有メールボックスを作成します。

Shared1 にメンバーとして追加できる ID はどれですか？

A. ユーザー1、グループ2、グループ3のみ

B. ユーザー1とグループ3のみ

C. ユーザー1とグループ1のみ

- D. ユーザー1のみ
- E. ユーザー1とグループ2のみ
- 正解: E (コメントを发表する)

質問: 280

Site1 という名前の Microsoft SharePoint サイトを含む Microsoft 365 E5 サブスクリプションがあります。サイト！ 次の表に示すファイルが含まれています。

Name	Number of IP addresses in the file
File1	2
File2	3

次の表に示す高度な DLP ルールを持つ DLP1 という名前のデータ損失防止 (DLP) ポリシーがあります。

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

DLP1 を Site1 に適用します。

各ファイルにはどのポリシー ヒントが表示されますか?回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area



File1:

Tip2 onlyTip2 onlyTip3 onlyTip2 and Tip3

File2:

Tip1 and Tip2 onlyTip1 onlyTip3 onlyTip1 and Tip2 onlyTip1, Tip2, and Tip3

正解:

Answer Area

Microsoft

File1: Tip2 only
Tip2 only
Tip3 only
Tip2 and Tip3

File2: Tip1 and Tip2 only
Tip1 only
Tip3 only
Tip1 and Tip2 only
Tip1, Tip2, and Tip3

Explanation:

Answer Area

Microsoft

File1: Tip2 only

File2: Tip1 and Tip2 only

質問: 281

Microsoft 365 E5 サブスクリプションがあり、Microsoft Defender for Cloud Apps を使用しています。次の要件を満たす Policy1 という名前のファイル ポリシーを作成する必要があります。

- * 接続されたSaaS サービスとしてのソフトウェア)アプリ内のファイルを検査します
- * 保護されたファイルを検査する

どの 2 つの設定を構成する必要がありますか? 回答するには、回答で適切な設定を選択します。注: 正しい選択ごとに 1 ポイントが付与されます。

Information Protection

- Admin quarantine
- Microsoft Information Protection ☒
- Azure security
- Files ☒

Conditional Access App Control

- General Settings
- User monitoring
- Device identification
- App onboarding/maintenance
- Edge for Business protection

App governance

- Service status



正解:

Information Protection

- Admin quarantine
- Microsoft Information Protection ☒
- Azure security
- Files ☒

Conditional Access App Control



- General Settings
- User monitoring
- Device identification
- App onboarding/maintenance
- Edge for Business protection

App governance

- Service status

Explanation:

Information Protection

Admin quarantine

Microsoft Information Protection

Azure security

Files

Conditional Access App Control

General Settings

User monitoring

Device identification

App onboarding/maintenance

Edge for Business protection

App governance

Service status

質問: 282

Admin1 と Admin2 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。すべてのユーザーに Microsoft 365 Enterprise E5 ライセンスが割り当てられ、監査が有効になっています。図に示す監査保持ポリシーを作成します。(図タブをクリックします。)

New audit retention policy

Name *: Policy1

Description

Record Types AzureActiveDirectory

Activities Added user, Deleted user, Reset user password, Changed user password, Changed user license, ...(7)

Users: Admin1

Duration *: ☒ 90 Days ☐ 6 Months ☐ 1 Year

Priority *: 100

Save Cancel

Policy1 が作成されると、次のアクションが実行されます。

* Admin1 は User1 という名前のユーザーを作成します。

* Admin2 は User2 という名前のユーザーを作成します。

User1 と User2 の作成に関する監査イベント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ます。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Microsoft

User1: ▼

0 days
30 days
90 days
180 days
365 days

User2: ▼

0 days
30 days
90 days
180 days
365 days

正解:

Microsoft

User1: ▼

0 days
30 days
90 days
180 days
365 days

User2: ▼

0 days
30 days
90 days
180 days
365 days

Explanation:

User1:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

User2:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

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

質問: 283

Microsoft 365 E5 サブスクリプションをお持ちです。
あなたは、記録管理を実装し、ユーザーが文書を規制記録として指定できるようにする予定です。
保持ラベルを作成するときに、コンテンツを規制記録としてマークするオプションが表示されるようにする必要があります。
まず何をすべきでしょうか？

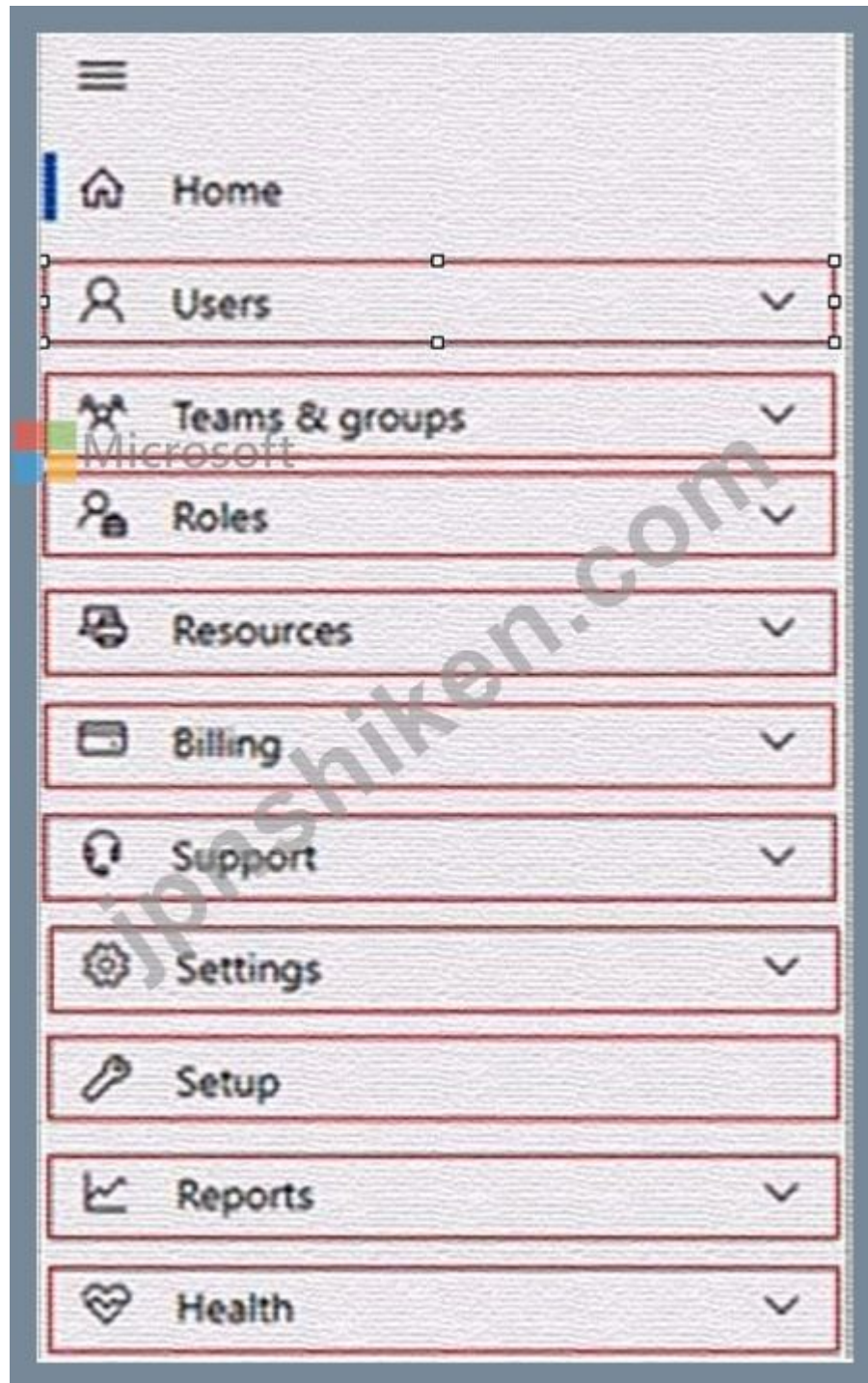
- A. カスタム検出ルールを構成します。
- B. 完全データ一致 (EDM) スキーマを作成します。
- C. Sec-RegulacoryComplianceUI コマンドレットを実行します。
- D. Sec-LabelPolicy コマンドレットを実行します。

正解: C (コメントを发表する)

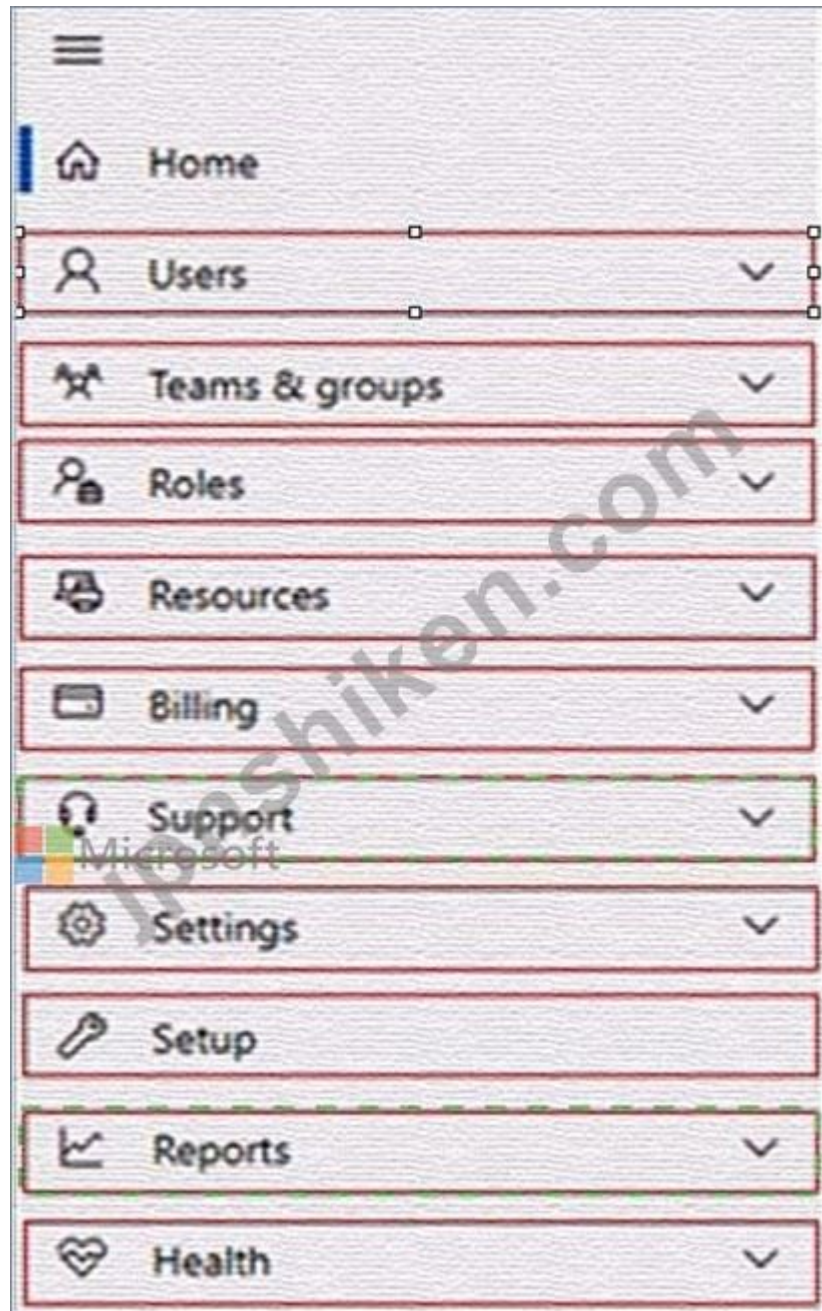
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide>

質問: 284

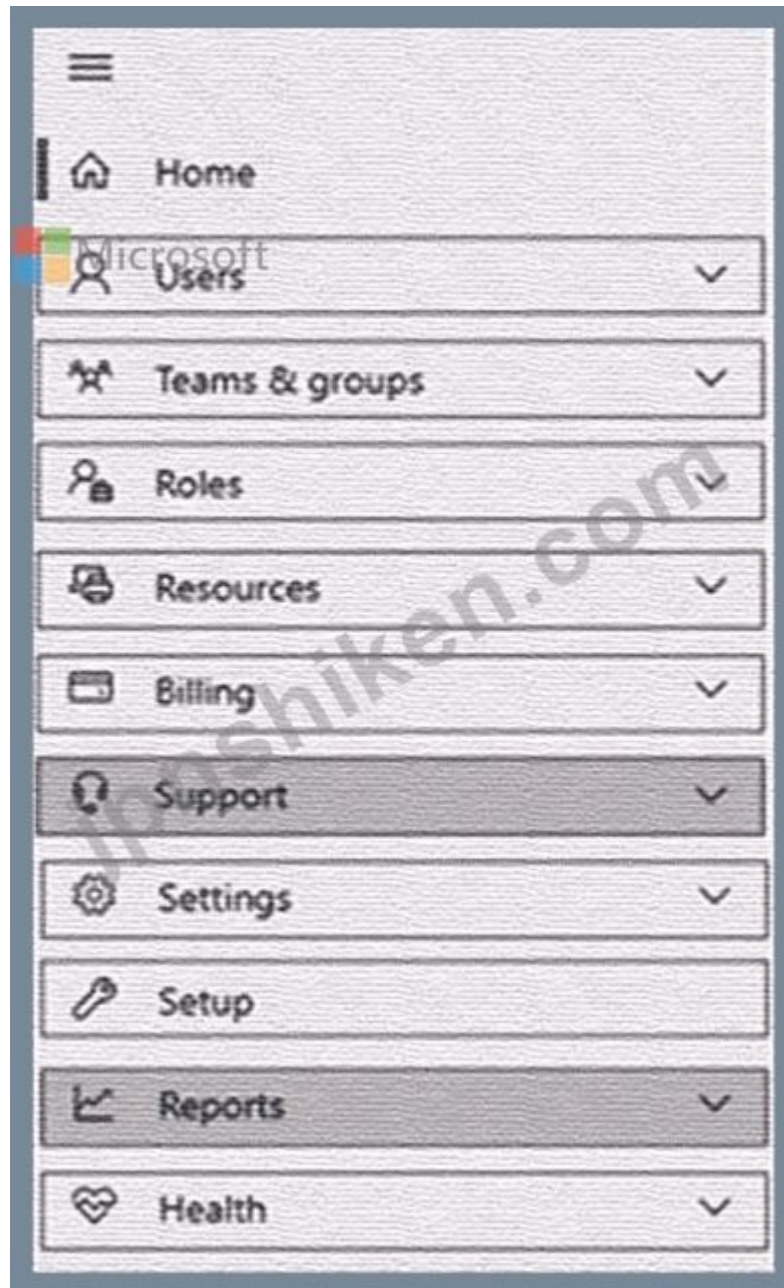
ホットスポット
あなたの会社には Microsoft 365 E5 サブスクリプションがあります。
次のタスクを実行する必要があります。
会社の採用スコアを表示します。
Microsoft への新しいサービス リクエストを作成します。
Microsoft 365 管理センターでは、どの 2 つのオプションを使用する必要がありますか？ 回答するには、回答領域で適切なオプションを選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score

To enable Adoption Score:

Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score Select enable Adoption Score. It can take up to 24 hours for insights to become available.

Box 2: Support

Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request.

If you 're in the admin center, select Support > New service request.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score>

<https://support.microsoft.com/en-us/topic/contact-microsoft-office-support-fd6bb40e-75b7-6f43-d6f9-c13d10850e77>

有効的な**MS-102J**問題集はJPNTest.com提供され、**MS-102J**試験に合格することに役に立ちます！JPNTest.comは今最新**MS-102J**試験問題集を提供します。JPNTest.com MS-102J試験問題集はもう更新されました。
ここで**MS-102J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/MS-102J-mondaishu> 598問、30%**ディスカウント**、特別な割引コード: **JPNshiken**」