# Microsoft.SC-300J.v2025-12-12.q154

| | |
|---|---|
| 試験コード： | SC-300J |
| 試験名称： | Microsoft Identity and Access Administrator (SC-300日本語版) |
| 認証ベンダー： | Microsoft |
| 無料問題の数： | 154 |
| バージョン： | v2025-12-12 |
| ページの閲覧量： | 102 |
| 問題集の閲覧量： | 1545 |

https://www.jpnshiken.com/shiken/Microsoft.SC-300J.v2025-12-12.q154.html

質問**: 1**
contoso.com という名前の Microsoft 365 テナントがあります。
ゲストユーザーアクセスが有効になっています。
次の表に示すように、ユーザーは contoso.com との共同作業に招待されます。
Azure Active Directory 管理センターの外部コラボレーション設定から、次の図に示すようにコラボレーション制限設定を構成します。
ユーザーは、Microsoft SharePoint Online サイトから user3@adatum.com をサイトに招待します。
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。
正解**:**
Explanation:
Box 1: Yes
Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.
Box 2. Yes
Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.
Box 3. No
Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

質問**: 2**
ネットワークには、Azure ADConnectを使用してcontoso.comという名前のAzureActive Directory（Azure AD）テナントにリンクされているcontoso.comという名前のActiveDirectoryフォレストが含まれています。
extensionAttribute15属性がNoSyncに設定されているユーザーの同期を防ぐ必要があります。
Azure AD Connectで何をすべきですか？
**A.** Windows Azure ActiveDirectoryコネクタの受信同期ルールを作成します。

**B.** 完全インポート実行プロファイルを構成します。
**C.** ActiveDirectoryドメインサービスコネクタの受信同期ルールを作成します。
**D.** エクスポート実行プロファイルを構成します。
正解**: (**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

質問**: 3**
Azure サブスクリプションをお持ちです。
エンタープライズ SaaS (Software as a Service) アプリを評価しています。
アプリが Microsoft Entra ユーザーの自動プロビジョニングをサポートしていることを確認する必要があります。
アプリはどの仕様をサポートする必要がありますか?
**A.** SCIM 2.0
**B.** OAuth 2.0
**C.** LDAP3
**D.** WS-Fed
正解**: (**正解を表示します**)**

質問**: 4**
Microsoft 365 テナントがあります。
すべてのユーザーは、Microsoft 365 サービスにアクセスするときに、多要素認証 (MFA) に Microsoft Authenticator アプリを使用する必要があります。
一部のユーザーから、サインイン要求を開始せずに Microsoft Authenticator アプリで MFA プロンプトを受け取ったという報告があります。
ユーザーが開始していない MFA リクエストを報告した場合は、そのユーザーを自動的にブロックする必要があります。
解決策: Azure ポータルから、多要素認証 (MFA) のユーザーのブロック/ブロック解除設定を構成します。
これは目標を満たしていますか?
**A.** はい
**B.** いいえ
正解**: B (**コメントを発表する**)**
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

質問**: 5**

contoso.com という 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。このサブスクリプションには、Group1 というグループと VM1 という仮想マシンが含まれています。
次の要件を満たす必要があります。
* VM1 に対してシステム割り当てマネージド ID を有効にします。
* VM1をGroup1に追加します。
PowerShell スクリプトはどのように完成させるべきでしょうか？適切なコマンドレットを適切なターゲットにドラッグしてください。各コマンドレットは、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、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 6**
5,000人のユーザーがいるMicrosoft 365テナントがあります。そのうち100人は経営幹部で、経営幹部には専任のサポートチームがいます。
サポートチームがパスワードをリセットし、多要素認証（MFA）設定を経営幹部のみに管理できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
どのオブジェクト タイプと Azure Active Directory (Azure AD) ロールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 7**
App1という名前のAzureADエンタープライズアプリケーションを含むcontoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
請負業者はuser1@outlook.comのクレデンシャルを使用します。
請負業者にApp1へのアクセスを提供できることを確認する必要があります。請負業者は、user1 @ outlook.comとして認証できる必要があります。
あなたは何をするべきか？
**A.** New-AzADUserコマンドレットを実行します。
**B.** 外部コラボレーション設定を構成します。
**C.** WS-FedIDプロバイダーを追加します。
**D.** contoso.comでゲストユーザーアカウントを作成します。
正解**: (**正解を表示します**)**
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-usersportal

質問: **8**
次のクラウド プラットフォームのアカウントがあります。
* アズール
* アリババクラウド
* アマゾン ウェブ サービス (AWS)
* Google クラウド プラットフォーム (GCP)
A2ure サブスクリプションを Microsoft Entra Permissions Management を使用して Azure のみの権限管理を行うように設定しています。Permissions Management を使用して管理できる追加のクラウド プラットフォームは何ですか？
**A.** Alibaba Cloud と AWS のみ
**B.** AWSのみ
**C.** Alibaba Cloud、AWS、GCP
**D.** AWS と GCP のみ
**E.** Alibaba Cloud と GCP のみ
正解: **(**正解を表示します**)**

質問: **9**
タスク5
Sg-Retail グループに Windows 10/11 Enterprise E3 ライセンスを割り当てる必要があります。
正解:
See the Explanation for the complete step by step solution.
Explanation:
To assign a Windows 10/11 Enterprise E3 license to the Sg-Retail group, you can follow these steps:
Sign in to the Microsoft Entra admin center:
Make sure you have the role of Global Administrator or License Administrator.
Navigate to the licensing page:
Go toBilling>Licenses1.
Find the Windows 10/11 Enterprise E3 license:
Look for the Windows 10/11 Enterprise E3 license in the list of available products.
Assign licenses to the group:
Select the license and then choose Assign licenses.
Search for and select the Sg-Retail group.
Confirm the assignment and make sure that the correct number of licenses is available for the group.
Review and confirm the assignment:

Ensure that the licenses have been properly assigned to the Sg-Retail group without affecting other groups or users.
Monitor the license status:
Check the license usage and status to ensure that the Sg-Retail group members can utilize the Windows 10/11 Enterprise E3 features.
By following these steps, the Sg-Retail group should now have the Windows 10/11 Enterprise E3 licenses assigned to them.

質問: **10**
ユーザーが 70 歳以上のサインイン アラートをトリガーしたときに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。
次の条件下でポリシーをテストする必要があります。
* ユーザーが別の国からサインインします。
* ユーザーがサインイン リスクを引き起こします。
テストを完了するには何を使用すればよいですか?
**A.** Azure AD のサインイン ログ
**B.** 条件付きアクセス What If ツール
**C.** Azure AD のアクセスレビュー
**D.** Microsoft Defender for Cloud Apps のアクティビティ ログ
正解: **(正解を表示します)**

質問: **11**
contoso.comという名前のAzureActive Directory（Azure AD）テナントがあり、Azure AD IdentityProtectionポリシーが適用されています。
Azure Sentinelインスタンスを作成し、Azure ActiveDirectoryコネクタを構成します。
Azure Sentinelが、Azure AD IdentityProtectionによって発生したリスクアラートに基づいてインシデントを生成できることを確認する必要があります。
あなたは最初に何をすべきですか？
**A.** AzureSentinelデータコネクタを追加します。
**B.** Azure AD IdentityProtectionで通知設定を構成します。
**C.** AzureSentinelプレイブックを作成します。
**D.** AzureADの診断設定を変更します。
正解: **(正解を表示します)**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection

質問: **12**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。
Au1 という名前の管理単位があります。Group1、User2、および User3 は Au1 のメンバーです。
User5 には Au1 のユーザー管理者ロールが割り当てられます。

User5 はどのユーザーのパスワードをリセットできますか?
**A.** ユーザー2とユーザー3のみ
**B.** ユーザー3とユーザー4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、ユーザー3
正解: **(**正解を表示します**)**

質問: **13**
contoso.com と fabhkam.com という 2 つの Microsoft Entra テナントがあります。Contoso.com には、次の表に示すユーザーが含まれています。
Contoso.com には、次の表に示すグループが含まれています。
contoso.com から fabrikam.com へのテナント間同期を構成し、User3 と Group2 のテナント間同期を有効にします。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:

質問: **14**
Azure サブスクリプションをお持ちです。
Azure AD ログは Log Analytics ワークスペースに送信されます。
ログをクエリし、ユーザーごとのサインイン数をグラフで表示する必要があります。
クエリをどのように完了すればよいですか? 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。
正解:
Explanation:
Box 1 =
SigninLogs
| where ResultType == 0
| summarize login_count = count() by identity
| render piechart
This query retrieves the sign-in logs, filters the successful sign-ins,summarizesthe count of sign-ins per user, and renders the result as a pie chart.
Box 2 = Render

質問: **15**
User1 という名前のユーザーを含む Azure AD テナントがあります
ユーザー 1 は、ライセンスの割り当てを管理し、ユーザー パスワードをリセットする必要があります。

User1 に割り当てるべきロールはどれですか?
**A.** ヘルプデスク管理者
**B.** ライセンス管理者
**C.** 課金管理者
**D.** ユーザー管理者
正解: **(**正解を表示します**)**

質問: **16**
contoso.com の SMTP アドレス スペースを使用するオンプレミスの Microsoft Exchange 組織があります。
ユーザーが Microsoft 365 サービスへのセルフサービス サインアップに自分のメール アドレスを使用していることがわかりました。
自己署名ユーザーが含まれる Azure Active Directory (Azure AD) テナントに対するグローバル管理者権限を取得する必要があります。
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。
正解:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover



質問: **17**
Microsoft 365 テナントがあります。
資格情報が漏洩したユーザーを特定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。
* 資格情報が漏洩した疑いのあるユーザーによる ID サインイン。
* サインインを高リスクイベントとして禁止します。
* ユーザーがアプリケーションにアクセスできるようにしながら、リスクを軽減するための制御を直ちに実施します。
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。
正解:

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

質問**: 18**
Sub1 という名前の Azure サブスクリプションがあります。
Microsoft Entra Permissions Management ライセンスを購入します。
You need to onboard Permissions Management.
実行すべき 2 つのアクションはどれですか? それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。
**A.** Microsoft Entra アプリケーション プロキシを実装します。
**B.** Microsoft Entra 管理センターから、アプリ登録を作成します。
**C.** Microsoft Entra Permissions Management からデータ収集を構成します。
**D.** Sub1 のロールの割り当てを作成します。
**E.** Azure ポータルから、データ収集ルール (DCR) を作成します。
**F.** Microsoft Entra 管理センターから、診断設定を構成します。
正解**: (**正解を表示します**)**

質問**: 19**
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。
グループのライフサイクルを管理する予定です。
どのグループに有効期限を設定できますか。また、設定できるグループの有効期間の最短はどれくらいですか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 20**
次の表に示す Azure Active Directory (Azure AD) ユーザーを作成します。
2021 年 2 月 1 日に、次の図に示すように多要素認証 (MFA) 設定を構成します。
次の表に示すように、デバイス上の Azure AD に対するユーザー認証。
2021 年 2 月 26 日、各ユーザーの多要素認証ステータスはどうなりますか?
**A.**
**B.**
**C.**
**D.**
正解**: (**正解を表示します**)**

質問: **21**
次の表に示すユーザーを含むハイブリッド Microsoft 365 サブスクリプションがあります。
オンプレミスの app1 を展開する予定です。app1 は Azure AD に登録され、Azure AD アプリケーション プロキシを使用します。
アプリケーションプロキシコネクタのインストールを委任し、User1 が Azure AD に App1 を登録できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
どのユーザーがインストールを実行し、Users1 に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。
正解**:**
Explanation:

質問: **22**
SSPR の計画された変更を実装します。
User3 が SSPR を使用しようとすると何が起こりますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**

質問: **23**
User1 という名前のユーザーと、次の表に示すグループを含む Azure Active Directory (Azure AD) テナントがあります。
テナントでは、次の表に示すグループを作成します。
グループAとグループBに追加できるメンバーは誰ですか? 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。
正解**:**
Explanation:
Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

質問: **24**
Microsoft Entra テナントがあります。
次の表に示すエンドユーザー デスクトップ環境があります。
Global Secure Access を展開する必要があります。
Global Secure Access クライアントはどのような環境にインストールできますか?
**A.** 開発者、オフィススタッフ、上級管理職のみ

**B.** 請負業者、開発者、最前線で働く人々、オフィススタッフ、そして上級管理職
**C.** 最前線の従業員と上級管理職のみ
**D.** 請負業者とオフィススタッフのみ
正解: **(**正解を表示します**)**

質問: **25**
Azure サブスクリプションをお持ちです。
権限を自動的に監視し、適切な規模のロールを作成して実装するには、Microsoft Entra Permissions Management を使用する必要があります。このソリューションは、最小権限の原則に従う必要があります。
権限管理のサービス プリンシパルに割り当てるべきロールはどれですか?
**A.** ユーザー アクセス管理者
**B.** 所有者
**C.** リーダー
**D.** 貢献者
正解: **(**正解を表示します**)**

質問: **26**
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。その結果、これらの質問はレビュー画面には表示されません。
アマゾン ウェブ サービス (AWS) アカウント、Google Workspace サブスクリプション、および GitHub アカウントがある Azure サブスクリプションをデプロイし、Microsoft 365 Defender を有効にします。
Microsoft Defender for Cloud Apps を使用して OAuth 認証要求を監視できることを確認する必要があります。
解決策: Microsoft 365 Defender ポータルから、GitHub アプリ コネクタを追加します。これは目標を達成していますか?
**A.** いいえ
**B.** はい
正解: **A (**コメントを発表する**)**

質問: **27**
Microsoft Defender for Cloud Apps および Yammer を使用する Microsoft 365 ES サブスクリプションがあります。
ユーザーがリスクの高い場所から Yammer にサインインできないようにする必要があります。
Microsoft Defender for Cloud Apps ポータルでは何をすればよいですか?

**A.** アクティビティ ポリシーを作成します。
**B.** アクセス ポリシーを作成します。
**C.** ヤマーを不当に扱う。
**D.** 異常検出ポリシーを作成します。
正解**:** **(**正解を表示します**)**

質問**: 28**
次の表に示すユーザーを含む Azure AD テナントがあります。
Azure AD Identity Protection では、次の設定を持つユーザー リスク ポリシーを構成します。
* 課題:
o ユーザー: グループ1
o ユーザーリスク: 低以上
* コントロール:
o アクセス: アクセスをブロックする
* ポリシーの適用: オン
Azure AD Identity Protection では、次の設定を持つサインイン リスク ポリシーを構成します。
* 課題:
o ユーザー: グループ2
o サインインリスク: 低以上
* コントロール:
o アクセス: 多要素認証を要求する
* ポリシーを強制する。オン
次の設定:
設定:
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 29**
User1 という名前のユーザーを含む Azure Active Directory (Azure AD) テナントがあります。
管理者が User1 を削除します。
次のことを特定する必要があります。
* User1 のアカウントが削除されてから何日後にアカウントを復元できますか?
* User1 を復元するために使用できる最も権限の低いロールはどれですか?
何を特定すべきでしょうか？ 回答するには、回答エリアで適切な選択肢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。
正解**:**
Explanation:

質問: **30**
Microsoft 365 E5 サブスクリプションがあり、その中に Site1 という Microsoft SharePoint Online サイトが含まれています。ユーザーが Site1 から 1 分間に 50 件を超えるファイルをダウンロードした場合に通知を受け取る必要があります。
Microsoft Defender for Cloud Apps ポータルで作成する必要があるポリシーの種類は何ですか?
**A.** アクティビティポリシー
**B.** 異常検出ポリシー
**C.** ファイルポリシー
**D.** セッションポリシー
正解: **(**正解を表示します**)**

質問: **31**
Contoso という Azure AD テナントがあり、Terms1 という利用規約 (ToU) とアクセス パッケージが含まれています。Contoso ユーザーは、Fabrikam という外部組織と共同作業を行っています。Fabrikam ユーザーは、アクセス パッケージを使用する前に、Terms1 に同意する必要があります。
どのユーザーが利用規約1に同意したか、または拒否したかを特定する必要があります。
何を使うべきでしょうか?
**A.** 使用状況と分析レポート
**B.** プロビジョニングログ
**C.** サインインログ
**D.** 監査ログ
正解: **(**正解を表示します**)**



質問: **32**
Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という名前の 3 人のユーザーが含まれています。
次の表に示すようにユーザーを構成する必要があります。
各ユーザーを設定するにはどのポータルを使用すればよいでしょうか？適切なポータルを適切なユーザーにドラッグしてください。各ポータルは1回、複数回、または全く使用されない場合があ

ります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。
正解:
Explanation:

質問: **33**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Microsoft365テナントがあります。
10の部門に編成された100人のIT管理者がいます。
展示に表示されるアクセスレビューを作成します。 [展示]タブをクリックします。）
すべてのアクセスレビューリクエストがMeganBowenによって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取るようにする必要があります。
解決策：各マネージャーをフォールバックレビューアとして追加します。
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://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

質問: **34**
タスク3
LinkedInアプリケーションをSales and Marketingアクセスパッケージのリソースとして追加する必要があります。このソリューションでは、アクセスパッケージから他のリソースを削除しないでください。
正解:
See the Explanation for the complete step by step solution.
Explanation:
To add the LinkedIn application as a resource to the Sales and Marketing access package without removing any other resources, you can follow these steps:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Identity Governance Administrator.

Navigate to Entitlement Management:
Go to Identity governance > Entitlement management > Access packages1.
Select the Sales and Marketing access package:
Find and select the Sales and Marketing access package to modify it.
Add a new resource:
Within the access package details, select Resources.
Click on + Add resource.
Search for and select the LinkedIn application from the list of available resources.
Configure the resource role:
Assign the appropriate role for the LinkedIn application that users in the Sales and Marketing access package will have.
Review and update the access package:
Ensure that the LinkedIn application has been added as a resource.
Confirm that no other resources have been removed from the access package.
Save the changes:
After reviewing, save the changes to the access package.
Communicate the update:
Notify the relevant users about the addition of the LinkedIn application to their access package.
By following these steps, you will successfully add the LinkedIn application to the Sales and Marketing access package without affecting the other resources.

質問**: 35**
Group! と Group2 という 2 つのグループと、次の表に示すユーザーを含む Microsoft Entra テナントがあります。
グループ2はグループ1のメンバーです。
次の設定を持つアクセス レビューを構成します。
* 名前: レビュー 1
* レビュー対象を選択: チーム + グループ
* レビュー範囲: チーム + グループを選択
* グループ: グループ1
* 対象: ゲストユーザーのみ
* レビュー担当者を選択: グループ所有者
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 36**

Active Directoryフォレストと同期するAzure Active Directory (Azure AD)テナントがあります。テナントは認証を介して使用します。
企業のセキュリティポリシーには次のように記載されています。
ドメイン コントローラーはインターネットと直接通信してはなりません。
サーバーには必要なソフトウェアのみをインストールする必要があります。
Active Directory ドメインには、次の表に示すオンプレミス サーバーが含まれています。
サーバーに障害が発生した場合でも、ユーザーが Azure AD に対して認証できることを確認する必要があります。
追加のパススルー認証エージェントを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2
**B.** サーバー4
**C.** サーバー1
**D.** サーバー3
正解**: B (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

質問**: 37**
App1という名前のAzureADエンタープライズアプリケーションを含むcontoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
請負業者はuser1@outlook.comのクレデンシャルを使用します。
請負業者にApp1へのアクセスを提供できることを確認する必要があります。請負業者は、user1 @ outlook.comとして認証できる必要があります。
あなたは何をするべきか？
**A.** New-AzureADMSInvitationコマンドレットを実行します。
**B.** 外部コラボレーション設定を構成します。
**C.** WS-FedIDプロバイダーを追加します。
**D.** Azure ADConnectを実装します。
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal
https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

質問**: 38**
タスク7
サインイン試行が 10 回失敗したら、アカウントを 5 分間ロックアウトする必要があります。
正解**:**
See the Explanation for the complete step by step solution.

Explanation:
To configure the account lockout settings so that accounts are locked out for five minutes after 10 failed sign- in attempts, you can follow these steps:
Open the Microsoft Entra admin center:
Sign in with an account that has the Security Administrator or Global Administrator role.
Navigate to the lockout settings:
Go to Security > Authentication methods > Password protection.
Adjust the Smart Lockout settings:
Set the Lockout threshold to 10 failed sign-in attempts.
Set the Lockout duration (in minutes) to 5.
Please note that by default, smart lockout locks an account from sign-in after 10 failed attempts in Azure Public and Microsoft Azure operated by 21Vianet tenants1. The lockout period is one minute at first, and longer in subsequent attempts.However, you can customize these settings tomeet your organization's requirements if you have Microsoft Entra ID P1 or higher licenses for your users1.

質問**: 39**
次の表に示すユーザーを含む Azure AD テナントがあります。
Azure AD Privileged Identity Management (PIM) では、次の図に示すようにグローバル管理者ロールを構成します。
ユーザー 1 は、グローバル管理者ロールの対象となります。
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 40**
contoso.com の SMTP アドレス スペースを使用する Microsoft Exchange 組織があります。
複数のユーザーが、1 Microsoft Entra へのセルフサービス サインアップに contoso.com の電子メール アドレスを使用しています。
自己署名ユーザーを含む Microsoft Entra テナントに対するグローバル管理者権限を取得します。
ユーザーが Microsoft 365 サービスにセルフサービスでサインアップできるように、contoso.com 2 Microsoft Entra テナントにユーザー アカウントを作成できないようにする必要があります。
どの PowerShell コマンドレットを実行する必要がありますか?
**A.** Update-MgPolicyAuthorizationPolicy
**B.** Update-MgDomain
**C.** Update-MgDomainFederationConfiguration
**D.** Update-MgPolicyPermissionGrantPolicyExclude
正解**: (**正解を表示します**)**

質問: **41**
Automation1 という名前の Azure Automation アカウントと、Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。Vault1 には Secret 1 という名前のシークレットが含まれています。
Automation1 に対してシステム割り当てマネージド ID を有効にします。
Automation! が Secret1 の内容を読み取れるように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。
* Automation1 が Vault1 に保存されている他のシークレットにアクセスできないようにします。
* 最小権限の原則に従ってください。
何をすべきでしょうか?
**A.** Secret1からアクセス制御（1AM）設定を構成します
**B.** Vault1 から、アクセス制御 (1AM) 設定を構成します。
**C.** Automation1 から、ID 設定を構成します。
**D.** Automation1 から、実行アカウント設定を構成します。
正解: **(**正解を表示します**)**

質問: **42**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。
Admin4 は、「Azure 管理に多要素認証を要求する」テンプレートを使用して、Policy1 という名前の条件付きアクセス ポリシーを作成します。
次回サインイン時に多要素認証 (MFA) の使用が求められるユーザーはどれですか?
**A.** Admin2とAdmin3のみ
**B.** Admin1とAdmin4のみ
**C.** Admin1、Admin2、Admin3のみ
**D.** 管理者1、管理者2、管理者3、および管理者4
正解: **(**正解を表示します**)**
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Entra ID Conditional Access policies, the "Require multifactor authentication for Azure management" template, and the roles assigned to the users, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding the "Require multifactor authentication for Azure management" Template:
Microsoft Entra ID Conditional Access policies allow administrators to enforce security controls, such as requiring multi-factor authentication (MFA), based on specific conditions.
The "Require multifactor authentication for Azure management" template is a predefined Conditional Access policy template in Microsoft Entra ID. This template is designed to secureaccess to Azure management interfaces, such as the Azure portal, Azure PowerShell, Azure CLI, and other Azure management endpoints.
Key Details of the Template:

Cloud Apps or Actions:The template targets the "Microsoft Azure Management" cloud app. This includes all Azure management interfaces but does not apply to other cloud apps (e.g., Microsoft 365 apps).
Users:By default, the template applies to "All users," but it can be modified to include or exclude specific users or groups. The question does not specify any modifications, so we assume the default "All users" scope.
Conditions:Typically, there are no specific conditions (e.g., device state, location) in this template unless modified.
Grant Controls:The template enforces "Require multi-factor authentication" as the access control.
Therefore, this policy will require MFA for any user who attempts to access Azure management interfaces.
Understanding the Roles and Their Interaction with Azure Management:
Let's examine the roles assigned to each user and whether they are likely to interact with Azure management interfaces:
Admin1: Global Administrator
A Global Administrator has full access to all Microsoft Entra ID and Azure resources, including the ability to manage Azure subscriptions, resources, and the Azure portal.
Global Administrators frequently access Azure management interfaces (e.g., the Azure portal) to perform administrative tasks. Therefore, Admin1 will be subject to the Conditional Access policy when they sign in to access Azure management.
Admin2: Conditional Access Administrator
A Conditional Access Administrator can manage Conditional Access policies in Microsoft Entra ID but does not have direct access to Azure management interfaces by default.
This role is focused on Microsoft Entra ID, not Azure resource management. Unless Admin2 has been granted additional Azure roles (e.g., Contributor, Owner), they are unlikely to access Azure management interfaces.
The question does not indicate any additional roles for Admin2, so we assume they do not interact with Azure management.
Admin3: Authentication Policy Administrator
An Authentication Policy Administrator can manage authentication methods and policies in Microsoft Entra ID (e.g., MFA settings, passwordless authentication).
Like the Conditional Access Administrator, this role is specific to Microsoft Entra ID and does not grant access to Azure management interfaces by default. Admin3 would not typically access Azure management unless assigned additional Azure roles, which are not specified.
Admin4: Global Administrator
Like Admin1, Admin4 is a Global Administrator and has full access to Azure management interfaces.
Admin4 will be subject to the Conditional Access policy when accessing Azure management.
Applying the Conditional Access Policy:
The policy applies to "All users" (default scope of the template) and targets the "Microsoft Azure Management" cloud app.

The policy requires MFA for any user who accesses Azure management interfaces.
Admin1 and Admin4 (Global Administrators):
As Global Administrators, both Admin1 and Admin4 will access Azure management interfaces (e.g., the Azure portal) as part of their administrative duties.
The next time they sign in to access Azure management, the Conditional Access policy (Policy1) will enforce MFA.
Admin2 (Conditional Access Administrator) and Admin3 (Authentication Policy Administrator):
These roles do not inherently grant access to Azure management interfaces. Their responsibilities are limited to Microsoft Entra ID tasks, such as managing Conditional Access policies or authentication methods.
Unless Admin2 or Admin3 attempts to access Azure management (which they are not authorized to do by default), the policy will not apply to them. The question asks about the "next time they sign in," but the policy only triggers MFA when accessing the targeted cloud app (Microsoft Azure Management). If Admin2 and Admin3 sign in to Microsoft Entra ID or other apps (e.g., Microsoft 365), the policy does not apply.
Analysis of the Options:
A). Admin2 and Admin3 only:
Incorrect. Admin2 and Admin3 are not likely to access Azure management interfaces based on their roles, so the policy will not require MFA for them.
B). Admin1 and Admin4 only:
Correct. Admin1 and Admin4 are Global Administrators who will access Azure management interfaces, triggering the policy to require MFA the next time they sign in to those interfaces.
C). Admin1, Admin2, and Admin3 only:
Incorrect. Admin2 and Admin3 are not subject to the policy for the reasons stated above.
D). Admin1, Admin2, Admin3, and Admin4:
Incorrect. While the policy applies to "All users," only Admin1 and Admin4 (Global Administrators) are likely to access Azure management interfaces, triggering the MFA requirement.
Additional Considerations:
If Admin2 or Admin3 were assigned additional Azure roles (e.g., Contributor, Owner) that grant access to Azure management, they would also be subject to the policy. However, the question does not indicate any such roles.
The phrase "the next time they sign in" can be misleading. The policy only enforces MFA when the user signs in to the targeted cloud app (Microsoft Azure Management). IfAdmin2 or Admin3 signs in to a different app (e.g., Microsoft 365), the policy does not apply.
If the policy were modified to target a different cloud app (e.g., "All apps") or to include specific users, the answer might change. However, the question specifies the default template behavior.
Conclusion:The Conditional Access policy (Policy1) created using the "Require multifactor authentication for Azure management" template will require MFA for users who access Azure management interfaces. Based on their roles:
Admin1 and Admin4 (Global Administrators) will be required to use MFA the next time they sign in to Azure management.

Admin2 and Admin3 (Conditional Access Administrator and Authentication Policy Administrator) are not likely to access Azure management, so the policy does not apply to them.Therefore, the correct answer isB.
References:
Microsoft Entra ID Conditional Access documentation: "Common Conditional Access policies - Require MFA for Azure management" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/conditional- access/concept-conditional-access-policy-common#require-mfa-for-azure-management) Microsoft Entra ID role documentation: "Administrator role permissions in Microsoft Entra ID" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Conditional Access policies and their application to specific roles and cloud apps.

質問**: 43**
次の表に示すグループを含む Azure AD テナントがあります。
次の表に示すように、Group1 のアクセス レビューを作成します。
次の表に示すように、Group2 のアクセス レビューを作成します。
各グループに必要なAzure AD Premium P2ライセンスの最小数はいくつですか？ 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：正解は1つにつき1ポイントです。
正解**:**
Explanation:

質問**: 44**
Microsoft 365 サブスクリプションをお持ちです。
ユーザーが企業アプリケーションに自分のプロファイルへのアクセスを許可できるようにする必要があります。ソリューションでは、ユーザーが委任されたユーザー権限（読み取り権限とプロファイル権限）にのみ同意できるようにする必要があります。
最初に何を設定する必要がありますか?
**A.** セキュリティのデフォルト
**B.** 個人情報保護設定
**C.** 管理者の同意設定
**D.** 権限の分類
正解**: (**正解を表示します**)**

質問**: 45**
Azure AD Identity Protection を使用し、次の表に示すリソースを含む Azure AD テナントがあります。
Azure Multi-Factor Authentication (MFA) はすべてのユーザーに対して有効になっています。
User1 は、追加調査を必要とする中程度の重大度のアラートをトリガーします。

次回サインインするときに、User1 にパスワードをリセットさせる必要があります。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。
何をすべきでしょうか?
**A.** サインイン リスク ポリシーを構成します。
**B.** 中程度または低程度の重大度でトリガーされるようにユーザー リスク ポリシーを再構成します。
**C.** User1 を侵害ありとしてマークします。
**D.** User1 の Azure MFA 登録をリセットします。
正解: **(**正解を表示します**)**

質問: **46**
litware.com に計画されている変更を適用する必要があります。何を設定すればよいですか？
**A.** litware.com ドメインを含めるための Azure AD Connect
**B.** litware.com ドメインの Azure AD Connect のステージング モード
**C.** Azure AD テナントと litware.com 間の Azure AD Connect クラウド同期
正解: **(**正解を表示します**)**



質問: **47**
次のグループを含む Azure Active Directory (Azure AD) テナントがあります。
名前: グループ1
メンバー: ユーザー1、ユーザー2
所有者: ユーザー3
2021 年 1 月 15 日に、図に示すようにアクセス レビューを作成します。([図] タブをクリックします。)
ユーザーは、次の表に示すように Review1 の質問に回答します。
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。
正解:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access

質問: **48**
オンプレミスネットワークには、Azure AD Connect を使用して Azure AD テナントと同期する Active Directory ドメインが含まれています。以下の要件を満たすように Azure AD Connect を構成する必要があります。
* Azure AD へのユーザー サインインは、Active Directory ドメイン コントローラーによって認証される必要があります。
* Active Directory ドメイン ユーザーは、Azure AD 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。
各要件には何を使用すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:

質問: **49**
Package1 という名前のアクセス パッケージと User1 という名前のユーザーを含む Azure AD テナントがあります。
Package1 は次の図に示すように構成されています。
User1 が Package1 のレビュー頻度を変更できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
User1 に割り当てるべきロールはどれですか?
**A.** セキュリティ管理者
**B.** ユーザー管理者
**C.** 特権ロール管理者
**D.** 外部IDプロバイダー管理者
正解: **(正解を表示します)**

質問: **50**
ネットワークには、Microsoft Entraテナントと同期するオンプレミスのActive Directoryドメインサービス（AD DS）ドメインが含まれています。AD DSドメインに対してパスワードを検証することで、ユーザー認証が常に確実に行われるようにする必要があります。どのような設定を行い、どのようなツールを使用すればよいでしょうか？回答するには、回答欄から適切な選択肢を選択してください。注：各選択肢は1点です。
正解:
Explanation:

質問: **51**

Azure Monitor を使用して、Azure Active Directory (Azure AD) アクティビティ ログを分析します。
追跡された Azure Al) ユーザーのサインイン試行に関する電子メール アラートを毎日 100 件以上受信します。
新しいセキュリティ管理者があなたに代わってアラートを受信するようにする必要があります。
解決策: Azure モニターからデータ収集ルールを作成します。
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**: 52**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Microsoft365テナントがあります。
10の部門に編成された100人のIT管理者がいます。
展示に表示されるアクセスレビューを作成します。 [展示]タブをクリックします。）
すべてのアクセスレビューリクエストがMeganBowenによって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取るようにする必要があります。
解決策 :IT管理者ユーザーアカウントのプロパティを変更します。
これは目標を達成していますか？
**A.** はい
**B.** いいえ
正解**: (**正解を表示します**)**
Reference:
D18912E1457D5D1DDCBD40AB3BF70D5D
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

質問**: 53**
Azure Active Directory (Azure AD) に登録されている、App1 という名前のカスタム クラウド アプリがあります。
App1 は次の図に示すように構成されています。
ドロップダウン メニューを使用して、グラフィックに表示された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 ポイントが加算されます。
正解**:**
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

質問**: 54**
次の表に示すユーザーを含む AzureAD テナントがあります。
次の表に示す場所があります。
テナントには、次の構成を持つ名前付き場所が含まれます。
* 名前: location1
* 信頼できる場所としてマーク: 有効
* IPv4範囲: 10.10.0.0/16
MFA には、193.17.17.0/24 の信頼できる iPad ドレス シリーズがあります。
次の設定を持つ条件付きアクセス ポリシーがあります。
* 名前: CAPolicy1
* 課題
o ユーザーまたはワークロード ID: 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
* 条件
* 場所 信頼できるすべての場所
* アクセス制御
o と
* アクセスを許可する: 多要素認証を要求する
* セッション: 選択されたコントロールは 0 件です
* ポリシーを有効にする: オン
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：正しい選択は1つにつき1点となります。
正解**:**
Explanation:

質問**: 55**
User1 と User2 という 2 人のユーザーを含む Azure AD テナントがあり、以下のアクションを実行する予定です。
* 「グループ 1」という名前のグループを作成します。
* User1 と User2 を Group1 に追加します。
* Group1 に Azure AD ロールを割り当てます。
Group1を作成する必要があります。

どの2つの設定を使用できますか？ それぞれの正解は完全な解決策を示します。注：正解の選択は1ポイントです
**A.** グループタイプ セキュリティ メンバーシップタイプ: 動的ユーザー
**B.** グループの種類: Microsoft 365 メンバーシップの種類: 割り当て済み
**C.** グループの種類: セキュリティ メンバーシップの種類: 動的デバイス
**D.** グループの種類: Microsoft 365 メンバーシップの種類: 動的ユーザー
**E.** グループタイプ セキュリティ メンバーシップタイプ: 割り当て済み
正解: **(**正解を表示します**)**

質問: **56**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Microsoft365テナントがあります。
10の部門に編成された100人のIT管理者がいます。
展示に表示されるアクセスレビューを作成します。 [展示]タブをクリックします。）
すべてのアクセスレビューリクエストがMeganBowenによって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取るようにする必要があります。
解決策 :レビュー担当者をメンバー（自己）に設定します。
これは目標を達成していますか？
**A.** いいえ
**B.** はい
正解: **A (**コメントを発表する**)**

質問: **57**
Site! という名前の Microsoft SharePoint Online サイトが含まれる Microsoft 365 E5 サブスクリプションがあります。Site!
PDFファイルをホストする
ユーザーが Sitel から直接ファイルを印刷できないようにする必要があります。
Microsoft Defender for Cloud Apps ポータルで作成する必要があるポリシーの種類は何ですか?
**A.** アクティビティポリシー
**B.** セッションポリシー
**C.** アクセスポリシー
**D.** ファイルポリシー
正解: **(**正解を表示します**)**

質問: **58**
Azure サブスクリプションをお持ちです。
Role1とRole2という2つのカスタムロールを作成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。
* Role1 が割り当てられたユーザーは、Azure Container Apps のインスタンスを作成または削除できます。
* Role2 が割り当てられたユーザーは、適応型ネットワーク強化ルールを適用できます。
各ロールにはどのリソース プロバイダーのアクセス許可が必要ですか? 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。
正解**:**
Explanation:

質問: **59**
User1 という名前のユーザーを含む Microsoft Entra テナントがあります。
管理者がUser1を削除します。以下の点を確認する必要があります。
* User1 アカウントを復元できるオプションがある最大日数は何ですか?
* User1 を復元するために使用できる最も権限の低いロールはどれですか?
回答するには、回答エリアで適切な選択肢を選択してください。注: 正解ごとに1ポイント加算されます。
正解**:**
Explanation:

質問: **60**
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 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。
正解**:**
Explanation:

質問: **61**
AU1 という管理単位を含む Microsoft Entra テナントがあります。AU1 は割り当てられたメンバーシップ用に構成されています。
テナントには次の表に示すユーザーが含まれます。
AU1 の場合、次の構成を更新します。
会員種別: ダイナミックユーザー
動的メンバーシップルール: (user.department -eq "hr")

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
**正解:**
Explanation:
HR is a member of AU1: No
User1 is a member of AU1: Yes
User2 is a member of AU1: No
Let's break this down step by step based on Microsoft Entra ID dynamic membership rules, administrative units, and group membership, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Administrative Units and Dynamic Membership in Microsoft Entra ID:
Administrative Units (AUs):Administrative Units in Microsoft Entra ID are used to delegate administrative tasks to a subset of users, groups, or devices. They allow you to scope administrative roles (e.g., User Administrator) to specific users or groups within the AU.
Membership Types for AUs:
Assigned Membership:Members (users, groups, or devices) are manually added to the AU by an administrator.
Dynamic Membership:Members are automatically added or removed based on a dynamic membership rule, similar to dynamic groups. Dynamic membership for AUs can be applied to users or devices (but not groups directly).
The question states that AU1 is initially configured for assigned membership but is then updated to useDynamic Usermembership with the rule (user.department -eq "HR").
Dynamic Membership Rule:The rule (user.department -eq "HR") means that AU1 will automatically include all users whose department attribute in Microsoft Entra ID is set to "HR". This rule applies to users, not groups or devices, because the membership type is "Dynamic User." Impact of Changing AU1 to Dynamic Membership:
When AU1's membership type is changed from assigned to dynamic, the existing assigned memberships (e.
g., User2, HR group, IT group) are no longer relevant. Thedynamic rule takes over, and AU1's membership is determined solely by the rule (user.department -eq "HR").
Dynamic User Membership:Only users whose attributes match the rule will be members of AU1. Groups (like HR and IT) are not evaluated by this rule because the membership type is "Dynamic User," not "Dynamic Group." Let's evaluate the users based on the rule:
User1:Department = "HR". The rule (user.department -eq "HR") matches, so User1 will be dynamically added to AU1.
User2:Department = "IT". The rule does not match, so User2 will not be a member of AU1, even though they were previously assigned to AU1 and are a member of the IT group.
Groups (HR and IT):The dynamic membership rule for AU1 applies to users, not groups. Therefore, groups like HR and IT are not directly evaluated by the rule. However, we need toconsider whether group membership in AU1 affects the statements.

Statement 1: HR is a member of AU1:
Analysis:
The HR group is listed in the second table with AU1 as its administrative unit, indicating that it was initially assigned to AU1 when AU1 used assigned membership.
However, AU1's membership type has been updated to "Dynamic User" with the rule (user.department -eq
"HR"). Dynamic User membership applies to users, not groups.
In Microsoft Entra ID, administrative units with dynamic user membership do not include groups as members unless the AU's membership type is explicitly set to "Dynamic Group" (which is not the case here).
When AU1 was changed to dynamic membership, the HR group would no longer be considered a member of AU1 because the dynamic rule only evaluates users. Groups are not dynamically added to AUs based on user attributes.
Conclusion:The HR group is not a member of AU1 after the change to dynamic membership.
Therefore, this statement isNo.
Statement 2: User1 is a member of AU1:
Analysis:
User1 has the department attribute set to "HR" (from the first table).
The dynamic membership rule for AU1 is (user.department -eq "HR"), which matches User1's department.
Therefore, User1 will be automatically added to AU1 as a member based on the dynamic rule.
Additionally, User1 is a member of the HR group, which was initially assigned to AU1. However, since AU1 now uses dynamic membership, the HR group's assignment to AU1 is irrelevant.
User1's membership in AU1 is determined solely by the dynamic rule, not their group membership.
Conclusion:User1 is a member of AU1 because their department matches the dynamic rule.
Therefore, this statement isYes.
Statement 3: User2 is a member of AU1:
Analysis:
User2 has the department attribute set to "IT" (from the first table).
The dynamic membership rule for AU1 is (user.department -eq "HR"), which does not match User2's department.
User2 was initially assigned to AU1 (as shown in the first table) and is a member of the IT group, which was also assigned to AU1. However, when AU1's membership type was changed to "Dynamic User," the assigned memberships (including User2 and the IT group) are no longer relevant.
The dynamic rule only includes users with the department "HR," so User2 is not added to AU1.
Conclusion:User2 is not a member of AU1 because their department does not match the dynamic rule.
Therefore, this statement isNo.
Additional Considerations:

If AU1's membership type were "Dynamic Group" instead of "Dynamic User," we would evaluate whether the HR and IT groups match a group-based rule. However, the question specifies "Dynamic User," so the rule applies to user attributes only.
The initial assigned memberships (e.g., User2, HR group, IT group) are overridden by the dynamic membership rule. Microsoft Entra ID does not retain assigned memberships when an AU or group is converted to dynamic membership.
The HR and IT groups being assigned to AU1 initially does not affect the dynamic membership of users, but it might be relevant for administrative scoping (e.g., if an admin role is scoped to AU1). However, the statements are about membership, not administrative roles.
Conclusion:Based on the dynamic membership rule (user.department -eq "HR") for AU1:
HR group:Not a member of AU1 because dynamic user membership does not apply to groups.
User1:A member of AU1 because their department is "HR," matching the rule.
User2:Not a member of AU1 because their department is "IT," which does not match the rule.Therefore, the answers are:
HR is a member of AU1:No
User1 is a member of AU1:Yes
User2 is a member of AU1:No
References:
Microsoft Entra ID documentation: "Dynamic membership rules for groups and administrative units" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership) Microsoft Entra ID documentation: "Manage administrative units" (Microsoft Learn:https://learn.microsoft.
com/en-us/entra/identity/role-based-access-control/administrative-units) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers dynamic membership rules and administrative units in Microsoft Entra ID.



質問: **62**
contoso.onmicrosoft.com というドメイン名を使用する新しい Microsoft 365 テナントがあります。
ドメイン レジストラに contoso.com という名前を登録します。
新しい Microsoft 365 ユーザーの既定のドメイン名として contoso.com 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、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。
正解:
Explanation:
Reference:
https://practical365.com/configure-a-custom-domain-in-office-365/

質問: **63**
App1 という名前の Web アプリが含まれる Microsoft 365 E5 サブスクリプションがあります。
ゲストユーザーには、App1 へのアクセスが定期的に許可されます。
過去 30 日間に App1 にアクセスしていないゲスト ユーザーのアクセスが削除されるように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。
何を設定すればよいでしょうか?
**A.** 条件付きアクセスポリシー
**B.** ゲストアクセスレビュー
**C.** アプリケーションアクセスのアクセスレビュー
**D.** コンプライアンスポリシー
正解: **(**正解を表示します**)**

質問: **64**
SecAdmin1という名前のユーザーを含むAzureActive Directory（Azure AD）テナントがあります。
SecAdmin1には、セキュリティ管理者の役割が割り当てられています。
SecAdmin1は、Azure AD IdentityProtectionポータルからパスワードをリセットできないと報告しています。
SecAdmin1が非管理ユーザーに代わってパスワードを管理し、セッションを無効にできることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
SecAdmin1にどの役割を割り当てる必要がありますか？
**A.** 認証管理者
**B.** ヘルプデスク管理者
**C.** 特権認証管理者
**D.** セキュリティオペレーター
正解: **C (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

質問: **65**
Department1 という名前の管理単位を含む Azure Active Directory (Azure AD) テナントがあります。
Department1 には、[ユーザー] 展示に示されているユーザーがいます。([ユーザー] タブをクリックします。)

Department1 には、[グループ] 展示に示されているグループがあります。([グループ] タブをクリックします。)
Department1 には、[割り当て] 展示に示されているユーザー管理者の割り当てがあります。([割り当て] タブをクリックします。)
グループ 2 のメンバーは、グループ 2 展示に表示されます。([グループ 2] タブをクリックします。)
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。
正解:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

質問: **66**
監視要件を満たすには、多段階攻撃の検出を構成する必要があります。
何をすべきでしょうか?
**A.** Azure Sentinel データ コネクタを追加します。
**B.** Azure Sentinel プレイブックを追加します。
**C.** ワークブックを作成します。
**D.** Azure Sentinel ルールのロジックをカスタマイズします。
正解: **(正解を表示します)**

質問: **67**
Microsoft 365 サブスクリプションがあり、その中に Site1 という Microsoft SharePoint Online サイトと Group1 という Microsoft 365 グループが含まれています。Group1 のメンバーが Site1 に 90 日間アクセスできるようにする必要があります。管理の手間を最小限に抑えるソリューションが必要です。どのようなソリューションを使用すればよいでしょうか？
**A.** ライフサイクルワークフロー
**B.** アクセスレビュー
**C.** アクセスパッケージ
**D.** 条件付きアクセスポリシー
正解: **(正解を表示します)**

質問: **68**
Microsoft 365 テナントがあります。
Azure Active Directory (Azure AD) テナントと同期する Active Directory ドメインがあります。
ユーザーは、社内のハードウェアファイアウォールを使用してインターネットに接続します。
ユーザーは、Active Directory の資格情報を使用してファイアウォールに認証します。

Azure AD を使用して外部アプリケーションへのアクセスを管理する予定です。
管理されていない外部アプリケーションとそれらにアクセスするユーザーのリストを作成するには、ファイアウォール ログを使用する必要があります。
情報を収集するには何を使用すればよいでしょうか?
**A.** Microsoft Defender for Cloud Apps の Cloud App Discovery
**B.** Azure AD のアクセスレビュー
**C.** Azure AD のエンタープライズ アプリケーション
**D.** Azure Monitor の Application Insights
正解: **(**正解を表示します**)**

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。
Microsoft 365 E5 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を作成します。
User1 が ID セキュア スコア改善アクションのステータスを更新できることを確認する必要があります。
解決策: SharePoint 管理者ロールを User1 に割り当てます。
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**)**

質問: **70**
User1 という名前のユーザーと、次の表に示す条件付きアクセス ポリシーを含む Azure AD テナントがあります。
User1 がさまざまな IP アドレスからサインインしようとしたときに、User1 に適用されるポリシーを評価する必要があります。
どの機能を使用すべきでしょうか?
**A.** What Ifツール
**B.** アクセスレビュー
**C.** アイデンティティセキュリティスコア
**D.** Microsoft 365 ネットワーク接続テスト ツール
正解: **(**正解を表示します**)**

質問: **71**

役割の割り当てを管理するために使用する役割を特定する必要があります。ソリューションは委任要件を満たす必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。
正解:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

質問: **72**
Microsoft 365 サブスクリプションには、User1、User2、User3 という 3 人のユーザーと、Appl というエンタープライズ アプリが含まれています。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。
サブスクリプションには、次の表に示すグループが含まれています。
次の設定を持つ 2 つの条件付きアクセス ポリシーを作成します。
* 名前: ポリシー1
* ユーザー:
o 含める: グループ 1
o 除外: グループ3
* 対象リソース:
o 含める: すべてのリソース
* アクセス制御: アクセスをブロックする
* 名前: ポリシー2
* ユーザー:
o 含める: グループ2
* 対象リソース:
o 含める: App1
* アクセス制御:
* アクセスを許可する: デバイスが準拠していることを示すマークを付ける必要がある
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: **73**
ネットワークには、Azure Active Directory (Azure AD) テナントと同期するオンプレミスの ActiveDirectory ドメインが含まれています。テナントには、次の表に示すユーザーが含まれています。
すべてのユーザーはリモートで作業します。

次の図に示すように、Azure ADConnectはAzureADで構成されています。
オンプレミスドメインからインターネットへの接続が失われます。
どのユーザーがAzureADにサインインできますか？
**A.** User1とUser3のみ
**B.** User1のみ
**C.** User1、User2、およびUser3
**D.** User1とUser2のみ
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations

質問**: 74**
ネットワークには、Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory ドメインが含まれています。ユーザーは、Windows 10 を実行し、ドメインに参加しているコンピューターにサインインします。
Azure AD シームレス シングル サインオン (Azure AD シームレス SSO) を実装する予定です。
Azure AD シームレス SSO 用にコンピューターを構成する必要があります。
何をすべきでしょうか?
**A.** Enterprise State Roaming を有効にします。
**B.** サインイン オプションを構成します。
**C.** Azure AD Connect 認証エージェントをインストールします。
**D.** イントラネット ゾーンの設定を変更します。
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

質問**: 75**
ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。
正解**:**

質問**: 76**
次の表に示すオブジェクトを含むAzureActive Directory（Azure AD）テナントがあります。
Group3にメンバーとして追加できるオブジェクトはどれですか？
**A.** User2とGroup2のみ
**B.** User2、Group1、およびGroup2のみ
**C.** User1、User2、Group1、Group2

**D.** User1とUser2のみ
**E.** User2のみ
正解: **(**正解を表示します**)**
Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/



質問: **77**
User! という名前のユーザーと、RG1 および RG2 という名前の 2 つのリソース グループを含む Azure サブスクリプションがあります。
User1 が次のタスクを実行できることを確認する必要があります。
* すべてのリソースを表示します。
* 仮想マシンを再起動します。
* RG1 でのみ仮想マシンを作成します。
* RG1 でのみストレージ アカウントを作成します。
必要なロールベース アクセス制御 (RBAC) ロール割り当て* の最小数はいくつですか?
**A.** 3
**B.** 1
**C.** 4
**D.** 2
正解: **D** (コメントを発表する)

質問: **78**
Microsoft365テナントがあります。
すべてのユーザーは、Windows 10を実行するコンピューターを持っています。ほとんどのコンピューターは会社所有であり、Azure Active Directory（Azure AD）に参加しています。一部のコンピューターはユーザー所有であり、AzureADにのみ登録されます。
ユーザーが所有するコンピューターでMicrosoftSharePoint Onlineに接続するユーザーが、ファイルをダウンロードまたは同期できないようにする必要があります。他のユーザーを制限してはなりません。
どのポリシータイプを作成する必要がありますか？

**A.** Microsoft Office365ガバナンスアクションが構成されているMicrosoftCloud AppSecurityアクティビティポリシー
**B.** セッションコントロールが構成されているAzureAD条件付きアクセスポリシー
**C.** クライアントアプリの条件が構成されているAzureAD条件付きアクセスポリシー
**D.** ガバナンスアクションが構成されているMicrosoft Cloud AppSecurityアプリ検出ポリシー
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad

質問: **79**
既定のドメイン名 contosso.com を使用するように新しい Microsoft 36S テナントを構成します。条件付きアクセス ポリシーを使用して、Microsoft 365 リソースへのアクセスを制御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.** ユーザーの同意設定を無効にします。
**B.** セキュリティのデフォルトを無効にします。
**C.** Windows Server Active Directory のパスワード保護を構成します。
**D.** 多要素認証 (MLA) 登録ポリシー1 を構成します。
正解: (正解を表示します)

質問: **80**
タスク1
多要素認証 (MFA) を導入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。
* Sg-Finance グループのメンバーに対してのみ MFA 登録が必要です。
* Debra Berger を MFA に登録する必要がないようにします。
* 条件付きアクセス ポリシーを使用せずにソリューションを実装します。
正解:
See the Explanation for the complete step by step solution.
Explanation:
To deploy Multi-Factor Authentication (MFA) for only the members of the Sg-Finance group, excluding Debra Berger, and without using a Conditional Access policy, you can follow these steps:
Open the Microsoft Entra admin center:
Sign in as a Security Administrator or Global Administrator.
Navigate to MFA settings:
Go to Users > Active users.
On the Active users page, select Multi-factor authentication.
Manage user settings:
Find and select the Sg-Finance group.

Enable MFA for this group by setting the requirement status to Enabled.
Exclude a user from MFA:
In the Multi-factor authentication page, search for Debra Berger.
Set her MFA status to Disabled to exclude her from MFA registration.
Verify the configuration:
Ensure that all members of the Sg-Finance group have MFA enabled except for Debra Berger.
Communicate the change:
Inform the Sg-Finance group members about the MFA requirement and provide instructions on how to register for MFA.
Monitor the setup:
Check the sign-in logs to confirm that MFA is being prompted for the Sg-Finance group members and not for Debra Berger.

質問**: 81**
User1 という名前のユーザーを含む Microsoft 365 サブスクリプションがあります。
User1 が Azure AD ロールのアクセスレビューを作成できるようにする必要があります。このソリューションでは、最小限の権限のプリンシパルを使用する必要があります。
User1 に割り当てるべきロールはどれですか?
**A.** ユーザーアクセス管理
**B.** 特権ロール管理者
**C.** ユーザー管理者
**D.** ガバナンス管理者を特定する
正解**: C (**コメントを発表する**)**

質問**: 82**
ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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 ポイントが加算されます。
正解**:**
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies
Topic 2, Litware, Inc
Overview
Litware, Inc. is a pharmaceutical company that has a subsidiary named fabrikam, inc Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.
Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development. Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.
com by using gu est accounts in the litware.com tenant.
Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector.
Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
On-premises Environment
The on-premises network contains the severs shown in the following table.
Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Delegation Requirements
Litware identifies the following delegation requirements:
* Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant-
* Use custom catalogs and custom programs for Identity Governance.
* Ensure that User1 can create enterprise applications in Azure AD. Use the principle of least privilege.
Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to Microsoft
365 group that he appropriate license assigned.
Management Requirement
Litware wants to create a group named LWGroup1 will contain all the Azure AD user accountsfor Litware but exclude all the Azure AD guest accounts.
Authentication Requirements
Litware identifies the following authentication requirements:
* Implement multi-factor authentication (MFA) for all Litware users.

* Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
* Implement a banned password list for the litware.com forest.
* Enforce MFA when accessing on-premises applications.
* Automatically detect and remediate externally leaked credentials
Access Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

質問: **83**
オンプレミス ネットワークには、Active Directory ドメイン サービス (AD DS) ドメインと、CAT という名前の証明機関 (CA) が含まれています。
Microsoft Entra テナントがあります。
Microsoft Entra 証明書ベースの認証を実装する必要があります。このソリューションでは、ユーザーが CAT が発行した証明書を使用してサインインできることを保証する必要があります。まず何をすべきでしょうか？
**A.** Azure キー コンテナーをデプロイします。
**B.** Windows Hello for Business を展開します。
**C.** CAT の自動登録を有効にします。
**D.** CA1 を証明機関として Microsoft Entra テナントに追加します。
正解: **(**正解を表示します**)**

質問: **84**
Appl というオンプレミスアプリがあります。Microsoft Entra テナントがあり、Microsoft Entra Private Access を使用して App1 を公開する予定です。Private Access プロファイルを有効にする必要があります。Microsoft Entra 管理センターではどのブレードを使用すればよいですか？
**A.** セキュリティプロファイル
**B.** コネクタ
**C.** リモートネットワーク
**D.** トラフィック転送
正解: **A (**コメントを発表する**)**

質問: **85**
Microsoft 365 テナントがあります。
現在、基本認証を使用する電子メール クライアントが Microsoft Exchange Online に接続することを許可しています。
ユーザーが Exchange に接続し、最新の認証プロトコルを使用する電子メール クライアントのみを実行できるようにする必要があります。

何を実装する必要がありますか?
モダン認証を使用する必要がある
**A.** Azure Active Directory (Azure AD) の条件付きアクセス ポリシー
**B.** Microsoft Endpoint Manager のアプリケーション制御プロファイル
**C.** Microsoft Endpoint Manager のコンプライアンス ポリシー
**D.** Microsoft Cloud App Security の OAuth ポリシー
正解**: (**正解を表示します**)**

質問**: 86**
Microsoft 365 テナントがあります。
すべてのユーザーは、Microsoft 365 サービスにアクセスするときに、多要素認証 (MFA) に Microsoft Authenticator アプリを使用する必要があります。
一部のユーザーから、サインイン要求を開始せずに Microsoft Authenticator アプリで MFA プロンプトを受け取ったという報告があります。
ユーザーが開始していない MFA リクエストを報告した場合は、そのユーザーを自動的にブロックする必要があります。
解決策: Azure ポータルから、多要素認証 (MFA) のアカウント ロックアウト設定を構成します。
これは目標を満たしていますか?
**A.** はい
**B.** いいえ
正解**: (**正解を表示します**)**
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

質問**: 87**
次の表に示すユーザーを含む Azure AD テナントがあります。
エンタープライズ アプリケーションのユーザー設定には次の構成があります。
* ユーザーは、アプリが自分に代わって会社のデータにアクセスすることに同意できます。
* ユーザーは、自分が所属するグループの企業データへのアクセスをアプリに許可することができます。
* ユーザーは、同意できないアプリに対して管理者の同意をリクエストできます: はい
* 管理者の同意リクエストを確認できるユーザー: Admin2、User2
ユーザー1 は、会社のデータにアクセスするために同意が必要なアプリを追加しようとします。
どのユーザーが同意できますか?
**A.** ユーザー1
**B.** 管理者1
**C.** 管理者2
**D.** ユーザー2
正解**: B (**コメントを発表する**)**

質問: **88**
contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
Azure AD 外部 ID の価格が月間アクティブ ユーザー数 (MAU) に基づいていることを確認する必要があります。
何を設定すればよいでしょうか?
**A.** アクセスレビュー
**B.** 使用条件
**C.** リンクされたサブスクリプション
**D.** ユーザーフロー
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing

質問: **89**
Azure AD テナントがあります。
テンプレート ファイルをアップロードして、25 個の新しいユーザー アカウントを一括作成する必要があります。
テンプレート ファイルにはどのようなプロパティが必要ですか?
**A.** オプションC
**B.** オプションB
**C.** オプションD
**D.** オプションA
正解: **(**正解を表示します**)**

質問: **90**
会社では、2 つの新しい Microsoft 365 ES サブスクリプションと、App という名前のアプリを購入します。
App1 に対して Microsoft Defender for Cloud Apps アクセス ポリシーを作成する必要があります。
まず何をすべきでしょうか? (microsoft.com の Microsoft Identity and Access Administrator に基づいて正しい回答を選択してください)
**A.** App1 のトークン構成を構成します。
**B.** App1 の API 権限を追加します。
**C.** アプリで適用される制限を使用するように条件付きアクセス ポリシーを構成します。
**D.** 条件付きアクセス アプリ制御を使用するように条件付きアクセス ポリシーを構成します。
正解: **D (**コメントを発表する**)**
https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad To create a Microsoft Defender for Cloud Apps access policy for App1, you should configure a Conditional Access

policy to use app-enforced restrictions. This will allow you to control access to your cloud apps based on conditions such as user, device, location, and app state. You can also use app-enforced restrictions to control access to your cloud apps based on the state of the app, such as whether it's running on a managed or unmanaged device.

質問**: 91**
タスク8
Microsoft Entra ID への認証時に、すべてのユーザーが従来の認証プロトコルを使用しないようにする必要があります。
正解**:**
See the Explanation for the complete step by step solution.
Explanation:
To prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID, you can create a Conditional Access policy that blocks legacy authentication. Here's how to do it:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Conditional Access Administrator.
Navigate to Conditional Access:
Go to Security > Conditional Access.
Create a new policy:
Select + New policy.
Give your policy a name that reflects its purpose, like "Block Legacy Auth".
Set users and groups:
Under Assignments, select Users or workload identities.
Under Include, select All users.
Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication.It's recommended to exclude at least one account to prevent lockout1.
Target resources:
Under Cloud apps or actions, select All cloud apps.
Set conditions:
Under Conditions > Client apps, set Configure to Yes.
Check only the boxes for Exchange ActiveSync clients and Other clients.
Configure access controls:
Under Access controls > Grant, select Block access.
Enable policy:
Confirm your settings and set Enable policy to Report-only initially to understand the impact.
After confirming the settings using report-only mode, you can move theEnable policytoggle fromReport- onlytoOn2.

By following these steps, you will block legacy authentication protocols for all users, enhancing the security posture of your organization by requiring modern authentication methods. Remember to monitor the impact of this policy and adjust as necessary to ensure business continuity.



質問: **92**
Azure 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 Server を実行する仮想マシンが 50 台含まれています。
仮想マシンに対して Microsoft Entra ログインを有効にします。
ユーザーから、Microsoft Entra 資格情報を使用して仮想マシンにサインインできないという報告がありました。
ユーザーが仮想マシンにサインイン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.** Microsoft Entra 管理センターから、仮想マシンのデバイス登録を削除します。
**B.** OpenSSH の SSH クライアント サポートを有効にします。
**C.** 仮想マシンが https://enterpriseregistration.windows.net にアクセスできることを確認します。
**D.** プライマリ更新トークンを取り消します。
正解: **(**正解を表示します**)**

質問: **93**
Groups1、Group2、Group3 という 3 つのグループと、次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
次の設定を持つ CAT という名前の条件付きアクセス ポリシーを作成します。
* ユーザー
* 含む
#ユーザーとグループ: グループ1
o 除外
#ユーザーとグループ: グループ2
#ディレクトリの役割: グローバル管理者
o ターゲットリソース
#含める: すべてのクラウドアプリ
アクセス制御
#Grant: 多要素認証を要求する

次の設定を持つ CA2 という名前の条件付きアクセス ポリシーを作成します。
* ユーザー
* 含む
#ユーザーとグループ: グループ2
o 除外
#ユーザーとグループ: グループ3
o ターゲットリソース
#含める: すべてのクラウドアプリ
アクセス制御
#許可: アクセスをブロック
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:

質問: **94**
次の表に示すユーザーを含む Azure AD テナントがあります。
各ユーザーのロール権限を比較する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。
何を使えばいいのでしょうか？
**A.** Microsoft Purview コンプライアンス ポータル
**B.** Microsoft 365 管理センター
**C.** Microsoft 365 Defender ポータル
**D.** Microsoft Entra 管理センター
正解: **B (**コメントを発表する**)**

質問: **95**
Microsoft Office 365 Enterprise E3 ライセンスが割り当てられたユーザーが 2,500 人います。ライセンスは個々のユーザーに割り当てられています。
Azure Active Directory 管理センターの [グループ] ブレードから、ユーザーに Microsoft 365 Enterprise E5 ライセンスを割り当てます。
最小限の管理労力で、ユーザーから Office 365 Enterprise E3 ライセンスを削除する必要があります。
何を使うべきでしょうか?
**A.** Set -KindohsProductKcy コマンド
**B.** Update-MgGroup コマンドレット
**C.** Set-HgUserLicense コマンドレット
**D.** Update-MgUser コマンドレット
正解: **(**正解を表示します**)**

Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

質問: **96**
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。一連の問題にはそれぞれ、定めら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、複数の正解が存在する場合もあれば、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した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 テナントがあります。10 の部門に分かれて
100 人の IT 管理者がいます。
図に示すアクセス レビューを作成します。(図タブをクリックします。)
すべてのアクセス レビュー リクエストは Megan Bowen によって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取れるようにする必要があります。
解決策: ロールごとに個別のアクセス レビューを作成します。
これは目標を満たしていますか?
**A.** はい
**B.** 番号 D18912E1457D5D1DDCBD40AB3BF70D5D
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

質問: **97**
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。
ユーザーには、次の表に示すロールが割り当てられます。
User1 と User4 はどのユーザーのパスワードをリセットできますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:

質問: **98**
ゲストユーザーの招待に関する問題を解決する必要があります。Azure AD テナントではどのような対応が必要ですか？
**A.** アクセスレビューの設定を構成します。
**B.** 条件付きアクセス ポリシーを構成します。
**C.** 外部コラボレーション設定を変更します。

**D.** 継続的なアクセス評価設定を構成します。
正解: **(**正解を表示します**)**

質問: **99**
次のオブジェクトを含むAzureActive Directory (Azure AD)テナントがあります。
Device1という名前のデバイス
User1、User2、User3、User4、およびUser5という名前のユーザー
Group1、Group2、Group3、Group4、およびGroup5という名前のグループ
グループは、次の表に示すように構成されます。
Microsoft Office 365 Enterprise E5ライセンスを直接割り当てることができるグループはどれですか？
**A.** Group1およびGroup4のみ
**B.** Group1、Group2、Group3、Group4、およびGroup5
**C.** Group1およびGroup2のみ
**D.** グループ1のみ
**E.** Group1、Group2、Group4、およびGroup5のみ
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

質問: **100**
User1 というユーザーを含む Azure サブスクリプションがあります。Microsoft Entra Permissions Management を導入します。以下のタスクを実行する必要があります。
* グローバル管理者ロールが永続的に割り当てられているすべてのアカウントを識別します。
* User1 の Permission Creep Index (PCI) を確認します。
各タスクには権限管理のどのタブを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:
A white background with black text AI-generated content may be incorrect.

質問: **101**
タスク6
Sg-Executiveのメンバーが会社のアプリにアクセスする前に、追加のセキュリティチェックを実施する必要があります。メンバーは、以下のいずれかの条件を満たす必要があります。
* Microsoft Intune によって準拠としてマークされているデバイスを使用して接続します。
* アプリ保護ポリシーによって保護されているクライアント アプリを使用して接続します。
正解:

See the Explanation for the complete step by step solution.
Explanation:
To implement additional security checks for the Sg-Executive group members before they canaccess any company apps, you can use Conditional Access policies in Microsoft Entra. Here's a step-by-step guide:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Security Administrator.
Navigate to Conditional Access:
Go to Security > Conditional Access.
Create a new policy:
Select + New policy.
Name the policy appropriately, such as "Sg-Executive Security Checks".
Assign the policy to the Sg-Executive group:
Under Assignments, select Users and groups.
Choose Select users and groups and then Groups.
Search for and select the Sg-Executive group.
Define the application control conditions:
Under Cloud apps or actions, select All cloud apps to apply the policy to any company app.
Set the device compliance requirement:
Under Conditions > Device state, configure the policy to include devices marked as compliant by Microsoft Intune.
Set the app protection policy requirement:
Under Conditions > Client apps, configure the policy to include client apps that are protected by app protection policies.
Configure the access controls:
Under Access controls > Grant, select Grant access.
Choose Require device to be marked as compliant and Require approved client app.
Ensure that the option Require one of the selected controls is enabled.
Enable the policy:
Set Enable policy to On.
Review and save the policy:
Review all settings to ensure they meet the requirements.
Click Create to save and implement the policy.
By following these steps, you will ensure that the Sg-Executive group members can only access company apps if they meet one of the specified conditions, either by using a compliant device or a protected client app.
This enhances the security posture of your organization by enforcing stricter access controls for executive- level users.

**質問: 102**

多要素認証 (MFA) が適用され、セルフサービス パスワード リセット (SSPR) が有効になっている Azure AD テナントがあります。
割り込みモードで複合登録を有効にします。
User1 という名前の新しいユーザーを作成します。
User1 が複合登録プロセスを完了するために使用できる 2 つの認証方法はどれですか。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.** Windows Hello for Business
**B.** ハードウェアトークン
**C.** Microsoft Authenticator アプリ
**D.** ワンタイムパスコードメール
**E.** FID02 セキュリティキー
正解**: (**正解を表示します**)**

質問**: 103**
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。
tenan1 から、グループの命名ポリシーを構成します。
命名ポリシーの影響を受けるユーザーは誰ですか?
**A.** ユーザー3のみ
**B.** ユーザー1、ユーザー2、ユーザー3のみ
**C.** ユーザー2のみ
**D.** ユーザー2とユーザー3のみ
**E.** ユーザー1、ユーザー2、ユーザー3、ユーザー4
**F.** ユーザー3とユーザー4のみ
正解**: (**正解を表示します**)**

質問**: 104**
ネットワークには、contoso.com というオンプレミスの Active Directory ドメインが含まれています。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。
Azure AD Connect をインストールします。「ドメインと OU のフィルタリング」の図に示すように、ドメインと OU のフィルタリング設定を構成します。( 「ドメインと OU のフィルタリング」タブをクリックします。)
「ユーザーとデバイスのフィルター」設定は、「ユーザーとデバイスのフィルター」の図に示すように構成します。( 「ユーザーとデバイスのフィルター」タブをクリックします。)
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
正解**:**
Explanation:

Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

質問: **105**
営業部門のユーザーの問題を解決する必要があります。Azure ADテナントにどのような設定を行う必要がありますか？
**A.** アクセスレビューの設定
**B.** セキュリティのデフォルト
**C.** ユーザー設定
**D.** デバイス設定
正解: **(**正解を表示します**)**

質問: **106**
VM1 という名前の仮想マシンが含まれる Sub1 という名前の Azure サブスクリプションがあります。
VM1 に対して Microsoft Entra ログインを有効にし、Sub1 のリソースにアクセスできるように VM1 を構成する必要があります。
VM1 に割り当てるべき ID の種類はどれですか?
**A.** Microsoft Entra ユーザー アカウント
**B.** システム割り当てマネージドID
**C.** ユーザー割り当てマネージド ID
**D.** Azure Automation アカウント
正解: **(**正解を表示します**)**



質問: **107**
漏洩した資格情報に対する認証要件を満たす必要があります。
何をすべきでしょうか?
**A.** Azure AD Connect で PingFederate とのフェデレーションを有効にします。
**B.** Azure AD パスワード保護を構成します。
**C.** Azure AD Connect でパスワード ハッシュ同期を有効にします。

**D.** Azure AD で認証方法ポリシーを構成します。
正解**: C (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

質問**: 108**
contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
Fabrikam, Inc. という会社のユーザーにリソース アクセスを提供するために、権限管理を実装します。Fabrikam は fabrikam.com というドメインを使用します。
アクセスが不要になった場合、Fabrikam ユーザーはテナントから自動的に削除される必要があります。
次の設定を構成する必要があります。
外部ユーザーがこのディレクトリにサインインすることをブロックする: いいえ
外部ユーザーの削除: はい
このディレクトリから外部ユーザーを削除するまでの日数: 90
Identity Governance ブレードでは何を構成する必要がありますか?
**A.** アクセスパッケージ
**B.** 権限管理設定
**C.** 利用規約
**D.** アクセスレビュー設定
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

質問**: 109**
次の表に示すユーザーを含む Azure AD テナントがあります。
次の表に示す Azure AD Identity Protection ポリシーがあります。
危険なユーザー レポートと危険なサインイン レポートを確認し、次の表に示すように各ユーザーに対してアクションを実行します。
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 110**
次の表に示す ID を含む Microsoft Entra テナントがあります。
グループ1には次の構成があります。
* 所有者: ユーザー1、ユーザー4

* メンバー: User1、Managed2、Gioup2
次の設定を持つアクセス レビューを作成します。
* 名前: レビュー1
* レビュー範囲: チーム + グループを選択
* グループ: グループ1
* 対象: すべてのユーザー
* レビュー担当者を選択: グループ所有者
フォールバックレビュー担当者: 設定が構成されていません。
正解**:**
Explanation:

質問**: 111**
タスク2
Salesforce アプリへのアクセス権を持つゲストユーザーをレビューするプロセスを実装する必要があります。レビューは、以下の要件を満たす必要があります。
* レビューは毎月行う必要があります。
* 各ゲストユーザーの管理者はアクセスを確認する必要があります。
* 5 日以内にレビューが完了しない場合は、アクセスを削除する必要があります。
* ゲスト ユーザーにマネージャーがいない場合は、Megan Bowen がアクセスを確認する必要があります。
正解**:**
See the Explanation for the complete step by step solution.
Explanation:
To implement a process for reviewing guest users' access to the Salesforce app with the specified requirements, you can use Microsoft Entra's Identity Governance access reviews feature. Here's a step-by- step guide:
Assign the appropriate role:
Ensure you have one of the following roles: Global Administrator, User Administrator, or Identity Governance Administrator1.
Navigate to Identity Governance:
Sign in to the Microsoft Entra admin center.
Go toIdentity governance>Access reviews1.
Create a new access review:
Select New access review.
Choose the Salesforce app to review guest user access1.
Configure the review settings:
Set the frequency of the review to monthly.
Define thedurationof the review period to5 days1.
Determine the reviewers:
Assign the manager of each guest user as the reviewer.

If a guest user does not have a manager, assignMegan Bowenas the reviewer1.
Automate the removal process:
Configure settings toautomatically remove accessif the review is not completed within the specified time frame1.
Monitor and enforce compliance:
Regularly check the access review results to ensure compliance with the review policy1.
Communicate the process:
Inform all stakeholders about the new review process and provide guidance on how to complete the reviews.
By following these steps, you can ensure that guest users' access to the Salesforce app is reviewed monthly, with managers being responsible for the review, and access is removed if the review is not completed in time.

質問**: 112**
Microsoft365テナントがあります。
サインインアクティビティレポートは、外部の請負業者がExchange管理センターにサインインしたことを示しています。
月末にExchange管理センターへのアクセスを確認し、必要に応じてサインインをブロックする必要があります。
何を作成する必要がありますか？
**A.** ディレクトリ外のユーザーを対象とするアクセスパッケージ
**B.** ディレクトリ内のユーザーを対象とするアクセスパッケージ
**C.** ゲストユーザーを対象としたグループベースのアクセスレビュー
**D.** ゲストユーザーを対象としたアプリケーションベースのアクセスレビュー
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

質問**: 113**
Admin1 という名前のユーザーを含む Azure AD テナントがあります。
Admin1 は、高リスク ユーザーのパスワード変更を要求するポリシー テンプレートを使用して、新しい条件付きアクセス ポリシーを作成します。
ポリシー割り当てにおいて、デフォルトで誰に含まれ、誰に除外されるのでしょうか？ 適切なオプションを正しい対象にドラッグしてください。各オプションは、1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問: **114**
You have a Microsoft Entra tenant that contains the groups shown in the following table.
グループに対して特権 ID 管理 (PIM) を実装する必要があります。
PIM を使用して管理できるグループはどれですか?
**A.** グループ1とグループ3のみ
**B.** グループ1とグループ2のみ
**C.** グループ1のみ
**D.** グループ3とグループ4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**)**

質問: **115**
User1 という名前のユーザーと App1 という名前の登録済みアプリを含む Azure AD テナントがあります。
User1 は、Appl のアプリ登録を削除します。
アプリの登録を復元する必要があります。
アプリの登録を削除してから復元できる最大日数は何ですか?
**A.** 180
**B.** 14
**C.** 30
**D.** 60
正解: **C (**コメントを発表する**)**

質問: **116**
次の表に示すユーザーを含むAzureActive Directory（Azure AD）テナントがあります。
User1はGroup1の所有者です。
次の設定を持つアクセスレビューを作成します。
レビューするユーザー :グループのメンバー
範囲：全員
グループ :グループ1
レビュアー :メンバー（自己）
User3のアクセスレビューを実行できるユーザーはどれですか？
**A.** User1とUser2のみ
**B.** User1のみ
**C.** User1、User2、およびUser3
**D.** User3のみ
正解: **(**正解を表示します**)**

質問: **117**

Azure Monitor を使用して、Azure Active Directory (Azure AD) アクティビティ ログを分析します。
追跡された Azure Al) ユーザーのサインイン試行に関する電子メール アラートを毎日 100 件以上受信します。
新しいセキュリティ管理者があなたに代わってアラートを受信するようにする必要があります。
解決策: Azure モニターからアクション グループを変更します。
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**: 118**
Microsoft Entra ID P1 ライセンスを持つ Microsoft Entra テナントがあります。
過去に発生したサインインを調査するには、Microsoft Entra ID サインイン ログを確認する必要があります。
Microsoft Entra ID はサインイン ログにイベントをどのくらいの期間保存しますか?
**A.** 14日間
**B.** 30日間
**C.** 90日間
**D.** 365日
正解**: (**正解を表示します**)**
Let's break this down step by step based on Microsoft Entra's sign-in log retention policies as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Microsoft Entra Sign-In Logs and Licensing:
Microsoft Entra ID (formerly Azure Active Directory) provides sign-in logs as part of its auditing and reporting capabilities. These logs track user and application sign-in activities, which are critical for security monitoring and compliance.
The question specifies that the tenant has a Microsoft Entra ID P1 license. Licensing is a key factor in determining the retention period for sign-in logs in Microsoft Entra.
Retention Period Based on License Tier:
Microsoft Entra ID has different editions: Free, P1, and P2. Each edition offers different capabilities and retention periods for audit and sign-in logs.
Free Tier:The Free edition of Microsoft Entra ID retains sign-in logs for7 days.
P1 Tier:With a Microsoft Entra ID P1 license (as mentioned in the question), sign-in logs are retained for30 days. This is a standard feature of the P1 license, which provides enhanced security and monitoring capabilities compared to the Free tier.
P2 Tier:The P2 license also retains sign-in logs for30 days, but it includes additional features like risk-based conditional access and identity protection, which are not relevant to the retention period.
Analysis of the Options:

A). 14 days:This is incorrect. Microsoft Entra ID does not have a 14-day retention period for sign-in logs under any license tier. This might be confused with other types of logs or services, but it does not apply here.
B). 30 days:This is correct. As stated, with a P1 license, Microsoft Entra retains sign-in logs for 30 days.
C). 90 days:This is incorrect. Microsoft Entra ID does not retain sign-in logs for 90 days, even with a P1 or P2 license. To retain logs for longer periods (e.g., 90 days or more), you would need to export the logs to a storage solution like Azure Monitor Logs or a SIEM system (e.g., Microsoft Sentinel), which allows for custom retention periods.
D). 365 days:This is incorrect for the same reason as option C. Microsoft Entra ID's default retention for sign- in logs is 30 days with a P1 or P2 license. Achieving a 365-day retention would require exporting logs to an external storage solution.
Additional Considerations:
If the tenant integrates Microsoft Entra logs with Azure Monitor or Microsoft Sentinel, the retention period can be extended based on the configuration of those services. However, the question specifically asks about Microsoft Entra's default retention, not an extended retention through integration.
The retention period for audit logs (which track changes to the directory, like user or group modifications) also follows the same pattern: 7 days for Free, 30 days for P1/P2. However, this question is about sign-in logs, not audit logs.
Conclusion:Given that the tenant has a Microsoft Entra ID P1 license, the sign-in logs are retained for 30 days. Therefore, the correct answer isB.
References:
Microsoft Entra ID documentation: "Audit and sign-in logs retention"
(Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-sign-in-logs#how-long-are-logs-retained)
Microsoft Entra ID P1 and P2 feature comparison: "Editions of Microsoft Entra ID"
(Microsoft Learn: https://learn.microsoft.com/en-us/entra/fundamentals/licensing)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers monitoring and reporting capabilities, including log retention periods.

質問**: 119**
Group3 というグループと Department1 という管理単位を含む Microsoft Entra テナントがあります。
部門には、「ユーザー」展示に示されているユーザーがいます。（「ユーザー」タブをクリックします。）
Department1 には、[グループ] 展示に表示されるグループがあります ([グループ] タブをクリックします)。
ユーザー管理者ロールの割り当ては、[割り当て] 展示に表示されます。([割り当て] タブをクリックします。)

Group2 のメンバーは、Group2 展示に表示されます。(Group2 タブをクリックします。)
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:

質問: **120**
Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という名前の 3 人のユーザーが含まれています。
次の表に示すアクティブ化設定を持つ 2 つの Azure AD ロールがあります。
Azure AD ロールには、次の表に示す割り当て設定があります。
Azure AD ロールには、次の表に示す対象ユーザーがいます。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:

質問: **121**
Microsoft 365 E5 サブスクリプションをご利用で、Microsoft Defender for Cloud Apps と条件付きアクセス ポリシーをご利用の場合、ユーザーが高リスクと評価された際にクラウド アプリへのアクセスをブロックする必要があります。
Microsoft Defender for Cloud Apps ではどのような種類のポリシーを作成する必要がありますか?
**A.** 異常検出ポリオ
**B.** アクティビティポリシー
**C.** OAuth アプリポリシー
**D.** アクセスポリシー
正解: **D** (コメントを発表する)



質問: **122**

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。
ユーザーがサイトへのアクセスを要求できるようにする必要があります。ソリューションは次の要件を満たしている必要があります。
* グループのメンバーシップに基づいてユーザーからのリクエストを自動的に承認します。
* 30日後に自動的にアクセスが削除されます
何をすべきでしょうか?
**A.** アクセス パッケージを作成します。
**B.** 条件付きアクセス ポリシーを作成します。
**C.** Azure AD Privileged Identity Management でロール設定を構成します。
**D.** Microsoft Defender for Cloud Apps アクセス ポリシーを作成します。
正解: **(**正解を表示します**)**

質問: **123**
会社には、User 1 という名前のユーザーを含む Microsoft Entra テナントがあります。
同社にはマーケティングと財務という2つの部門があります。
マーケティング部門のユーザーのみを管理するには、User1 に権限を付与する必要があります。
最初に何を作成すればよいですか?
**A.** Microsoft 365 グループ
**B.** 管理グループ
**C.** リソースグループ
**D.** 行政単位
正解: **(**正解を表示します**)**

質問: **124**
A Datum から新規ユーザーにライセンスを割り当てる必要があります。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。
どのようなタイプのオブジェクトを作成する必要がありますか?
**A.** 配布グループ
**B.** 動的ユーザーセキュリティグループ
**C.** 行政単位
**D.** あなたの中に
正解: **C (**コメントを発表する**)**
Topic 1, Contoso, Ltd
Overview
Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc Fabcricam has an Azure Active Diretory (Azure AD) tenant named fabrikam.com.
Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contos.com.
The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resoureces OU contains all users and computers.
The Contoso.com Active Directory domain contains the users shown in the following table.
Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named Contoso.com that has the following associated licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security
Windows 10 Enterprise E5
Project Plan 3
Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (AD DS). Only the Contoso Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses, All user have all licenses assigned besides following exception:
The users in the London office have the Microsoft 365 admin center to manually assign licenses.
All user have licenses assigned besides the following exceptions:
The users in the London office have the Microsoft 365 Phone System License unassigned.
The users in the Seattle office have the Yammer Enterprise License unassigned.
Security defaults are disabled for Contoso.com.
Contoso uses Azure AD Privileged identity Management (PIM) to project administrator roles.
Problem Statements
Contoso identifies the following issues:
* Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
* The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
* The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
* Currently, the helpdesk administrators can perform tasks by using the: User administrator role without justification or approval.
* When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.
Planned Changes
Contoso plans to implement the following changes.
Implement self-service password reset (SSPR). Analyze Azure audit activity logs by using Azure Monitor- Simplify license allocation for new users added to the tenant. Collaborate with the users at Fabrikam on a joint marketing campaign. Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named Corporation. One hundred new A Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Technical Requirements
Contoso identifies the following technical requirements:
* AH users must be synced from AD DS to the contoso.com Azure AD tenant.
* App1 must have a redirect URI pointed tohttps://contoso.com/auth-response.
* License allocation for new users must be assigned automatically based on the location of the user.
* Fabrikam users must have access to the marketing department's SharePoint site for a maximumof 90 days.
* Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
* The helpdesk administrators must be able to manage licenses for only the users in their respective office.
* Users must be forced to change their password if there is a probability that the users' identity was compromised.

質問**: 125**
オンプレミスの Linux デバイスがあります。
Microsoft 365 E5 サブスクリプションをお持ちです。
グローバル セキュア アクセス インターネット アクセスを構成する予定です。
デバイスが Global Secure Access に接続できることを確認する必要があります。
何をすべきでしょうか?
**A.** プライベート ネットワーク コネクタをデプロイします。
**B.** Adaptive Access 設定を構成します。
**C.** デバイスに Azure Connected Machine エージェントをインストールします。
**D.** リモート ネットワークを作成します。
正解**: A (**コメントを発表する**)**

質問**: 126**
contoso.comのSMTPのアドレス空間を使用するMicrosoftExchange組織があります。
何人かのユーザーは、自分のcontoso.com電子メールアドレスを使用して、Azure Active Directory（Azure AD）へのセルフサービスサインアップを行います。
自己署名ユーザーを含むAzureADテナントに対するグローバル管理者特権を取得します。
Microsoft 365サービスへのセルフサービスサインアップのために、ユーザーがcontoso.com AzureADテナントでユーザーアカウントを作成できないようにする必要があります。
どのPowerShellコマンドレットを実行する必要がありますか？

**A.** Set-MsolCompanySettings
**B.** Set-MsolDomainFederationSettings
**C.** 更新-MsolfederatedDomain
**D.** Set-MsolDomain
正解: **C** (コメントを発表する)
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

質問: **127**
ネットワークには、Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory ドメインが含まれています。テナントには、次の表に示すものが含まれています。
すべてのユーザーはリモートで作業します。
Azure AD Connect は、次の図に示すように Azure で構成されます。
オンプレミス ドメインからインターネットへの接続が失われます。
どのユーザーが Azure AD にサインインできますか?
**A.** ユーザー1とユーザー3のみ
**B.** ユーザー1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、ユーザー3
正解: **A** (コメントを発表する)

質問: **128**
次の表に示すユーザーを含む Azure AD テナントがあります。
App1 という名前のエンタープライズ アプリケーションを Azure AD に追加し、User1 を App1 の所有者として設定して、アプリを使用する前に Azure AD にアクセスするための管理者の同意が必要になります。
次の図に示すように、管理者の同意リクエストを強力に構成します。
管理者の同意リクエスト。
**A.** Admln1、Admin2、およびUser1のみ
**B.** Admm1のみ
**C.** Admm1、Admm2、Admm3、およびUser1
**D.** Admm1とAdmin2のみ
**E.** Admm1、Admm2、Admin3のみ
正解: **D** (コメントを発表する)

質問: **129**
条件付きアクセス ポリシーを使用する Azure Active Directory (Azure AD) テナントがあります。
条件付きアクセスの使用状況を分析するために、サードパーティのセキュリティ情報およびイベント管理 (SIEM) を使用する予定です。
条件付きアクセス ポリシー データを含む Azure AD ログをダウンロードする必要があります。

Azure AD から何をエクスポートする必要がありますか?
**A.** JSON形式のサインイン
**B.** CSV形式のサインイン
**C.** JSON形式の監査ログ
**D.** CSV形式の監査ログ
正解**: C (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

質問**: 130**
Microsoft 365 E5 サブスクリプションをお持ちです。
App1 という名前のサードパーティの SaaS (Software as a Service) アプリを展開する予定です。
App1 を Microsoft Defender for Cloud Apps にオンボードする必要があります。このソリューションでは、セッション制御ポリシーを実装できる必要があります。
まず何をすべきでしょうか?
**A.** Microsoft Defender ポータルから、OAuth アプリ ポリシーを作成します。
**B.** Microsoft Entra 管理センターから、トラフィック転送プロファイルを構成します。
**C.** Microsoft Entra 管理センターから、App1 のシングル サインオン (SSO) を構成します。
**D.** Microsoft Defender ポータルから、クラウド検出を構成します。
正解**: D (**コメントを発表する**)**

質問**: 131**
Litware ユーザーへの Azure AD ライセンスの割り当てを構成する必要があります。ソリューションはライセンス要件を満たしている必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。
正解**:**
Explanation:
Litware recently added a custom user attribute namedLWLicensesto the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure AD licenses by modifying the value of theLWLicensesattribute. Users who have the appropriate value forLWLicensesmust be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.
Topic 3, A Datum CorpOverview
A Datum Corporation is a consulting company in Montreal.
A Datum recently acquired a Vancouver-based company named Litware, Inc.
A Datum Environment
The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect A Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Problem Statements

A Datum identifies the following issues:

* Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
* A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address,
* When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
* Anyone in the organization can invite guest users, including other guests and non-administrators.
* The helpdesk spends too much time resetting user passwords.
* Users currently use only passwords for authentication.

Requirements

A Datum plans to implement the following changes;

* Configure self-service password reset {SSPR}.
* Configure multi-factor authentication (MFA) for all users.
* Configure an access review for an access package named Package1.
* Require admin approval for application access to organizational data.
* Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
* Ensure that only users that are assigned specific admin roles can invite guest users.
* Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Technical Requirements

A Datum identifies the following technical requirements:

* Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
* Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
* Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

* Email
* Phone
* Security questions
* The Microsoft Authenticator app
* Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.

* The principle of least privilege must be used.

質問: **132**
次の表に示すグループを含むAzureActive Directory (Azure AD)テナントがあります。
どのグループに対してアクセスレビューを作成できますか？
**A.** グループ1のみ
**B.** Group1およびGroup4のみ
**C.** Group1およびGroup2のみ
**D.** Group1、Group2、Group4、およびGroup5のみ
**E.** Group1、Group2、Group3、Group4、Group5
正解: **(正解を表示します)**
You cannot create access reviews for device groups.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

質問: **133**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。
次の設定を持つユーザー リスク ポリシーがあります。
* 課題:
o 含める: グループ 1
o 除外: グループ2
* サインインリスク 中以上
* アクセス制御:
o アクセスを許可する: パスワードの変更を要求する
ユーザーがサインインしようとすると、次の表に示すようにユーザーのリスク レベルが検出されます。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
正解:
Explanation:

質問: **134**
Microsoft 36S テナントがあります。
高リスク国のリストを含む、HighRiskCountries という名前の名前付き場所を作成します。
高リスクの国から接続する場合、ユーザーが認証されたままでいられる時間を制限する必要があります。
条件付きアクセス ポリシーでは何を構成する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

質問: **135**
Sub1 という名前の Azure サブスクリプションがあります。
Microsoft Entra Permissions Management を展開する予定です。
権限管理がSub1にアクセスできることを確認する必要があります。ソリューションは最小権限の原則に従う必要があります。
PowerShell コマンドをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解:
Explanation:

質問: **136**
次の図に示すように、ユーザー管理者ロールの Azure AD Privileged Identity Management (PIM) ロール設定を含む Azure Active Directory (Azure AD) テナントがあります。
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た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 ポイントが加算されます。
正解:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan



質問: **137**

Microsoft Enta ID P2 ライセンスを持つ Microsoft Entra テナントがあり、Log Analytics ワークスペースを作成します。
Azure Monitor を使用して Microsoft Entra ID 監査ログ情報を表示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.** update-Mgorganization コマンドレットを実行します。
**B.** Microsoft Entra ID の診断設定を変更します。
**C.** update-ngoomain コマンドレットを実行します。
**D.** Microsoft Entra ID ブックを作成します。
正解: **(**正解を表示します**)**

質問: **138**
技術要件を満たすために、ユーザー管理者ロールの設定を変更する必要があります。このロールに対して実行すべき2つのアクションはどれですか？ 正解はそれぞれ解答の一部です。注：正解は1つにつき1ポイントです。
**A.** すべての割り当てをアクティブに設定する
**B.** 有効な割り当ての有効期限の設定を変更します。
**C.** アクティベーション時にチケット情報を要求するを選択します。
**D.** アクティベーション時に正当化を要求するを選択
**E.** すべての割り当てを 適格」に設定する
正解: **B,E (**コメントを発表する**)**

質問: **139**
Azure サブスクリプション、Google Cloud Platform (GCP) アカウント、Amazon Web Services (AWS) アカウントがあります。
すべてのプラットフォームにわたる権限割り当てに関連するリスクを評価するためのソリューションを推奨する必要があります。ソリューションは管理作業を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.** マイクロソフト センチネル
**B.** Microsoft のアクセス許可管理
**C.** Microsoft Entra ID 保護
**D.** クラウド アプリ向け Microsoft Defender
正解: **B (**コメントを発表する**)**

質問: **140**
storage1 という名前のストレージ アカウントを含む Azure サブスクリプションがあります。
複数の仮想マシンでホストされるApp1というアプリを展開する予定です。仮想マシンはシークレットを使用してサードパーティAPIに認証します。仮想マシン用の認証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。
* 秘密を安全に保管します。

* 資格情報を App1 コードに保存する必要がないことを確認します。
* Microsoft Entra 認証を使用して、仮想マシンが Azure リソースにアクセスできることを確認します。
* 管理上の労力を最小限に抑えます。
推薦書には何を含めるべきでしょうか?
**A.** システム割り当てマネージド ID とストレージ サービス暗号化
**B.** ユーザー アカウントと Azure Key Vault
**C.** ユーザーアカウントとストレージサービス暗号化
**D.** ユーザー割り当てマネージド ID と Azure Key Vault
正解: **(**正解を表示します**)**

質問: **141**
Azure Monitor を使用して、Azure Active Directory (Azure AD) アクティビティ ログを分析します。
追跡された Azure Al) ユーザーのサインイン試行に関する電子メール アラートを毎日 100 件以上受信します。
新しいセキュリティ管理者があなたに代わってアラートを受信するようにする必要があります。
解決策: Azure AD から、Insights at 管理者ロールの割り当てを作成します。
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: **142**
Microsoft Defender for Cloud Apps を使用する Microsoft 365 E5 サブスクリプションがあります。
サブスクリプションのアプリのセキュリティを強化する予定です。
ユーザー認証を必要としないアプリを特定する必要がある
Microsoft 365 Defender ポータルでは何をすべきでしょうか?
**A.** クラウド アプリ カタログを確認します。
**B.** スナップショット Cloud Discovery レポートを作成します。
**C.** OAuth ポリシーを作成し、アラートを確認します。
**D.** 検出されたアプリのクエリを作成します。
正解: **D (**コメントを発表する**)**

質問: **143**
Microsoft 365 テナントがあります。
条件付きアクセス ポリシーの図に示されているように、条件付きアクセス ポリシーを構成します ([条件付きアクセス ポリシー] タブをクリックします)。

ユーザー管理者ロールの設定は、「ロール設定の詳細」の図のように表示されます。( 「ロール設定の詳細」タブをクリックします。)
「ロールの割り当て」展示に示されているように、ユーザー管理者ロールの割り当てを表示します。( 「ロールの割り当て」ラボをクリックします。)
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:
Yes
Yes
No

質問**: 144**
Microsoft Entra テナントがあります。
セルフサービス パスワード リセット (SSPR) は、次の設定で構成します。
サインイン時にユーザー登録を要求する: はい
リセットに必要なメソッドの数: 1
ユーザーが利用できる有効な認証方法は何ですか?
**A.** スマートカード
**B.** モバイルアプリのコード
**C.** FIDO2セキュリティトークン
**D.** Windows Hello PIN
正解**: (**正解を表示します**)**
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Entra ID self-service password reset (SSPR) settings and the available authentication methods, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Self-Service Password Reset (SSPR) in Microsoft Entra ID:
Self-service password reset (SSPR) allows users to reset their passwords without administrator intervention, improving security and reducing helpdesk workload.
The settings provided are:
Require users to register when signing in: Yes- Users must register their authentication methods (e.g., phone number, email, security questions) the first time they sign in. This ensures they have methods available for SSPR.
Number of methods required to reset: 1- Users must verify their identity using one authentication method to reset their password. This is the minimum number of methods required, meaning users must have at least one method registered, and they will use one method during the reset process.
Available Authentication Methods for SSPR:

Microsoft Entra ID SSPR supports a specific set of authentication methods that users can use to verify their identity during a password reset. These methods are configured by the administrator in the Microsoft Entra admin center under "Password reset" settings.
The default authentication methods available for SSPR include:
Email:Users receive a code sent to an alternate email address.
Mobile phone (SMS):Users receive a code via SMS to their registered mobile phone.
Mobile app code:Users use a code generated by the Microsoft Authenticator app (or another compatible authenticator app).
Mobile app notification:Users receive a push notification in the Microsoft Authenticator app to approve the reset.
Security questions:Users answer predefined security questions they set up during registration.
Important Note:Methods like smartcards, FIDO2 security tokens, and Windows Hello are not supported for SSPR. These methods are typically used for authentication during sign-in (e.g., MFA or passwordless sign- in), not for the SSPR process.
Analysis of the Options:
A). A smartcard:
Smartcards are a form of certificate-based authentication often used for sign-in to Windows devices or VPNs.
They require a physical card and a reader, and they are typically used for primary authentication, not for SSPR.
Microsoft Entra ID SSPR does not support smartcards as an authentication method for password reset.
Smartcards are not listed as an available method in the SSPR configuration settings.
Conclusion:This is incorrect.
B). A mobile app code:
A mobile app code refers to a time-based one-time password (TOTP) generated by an authenticator app, such as the Microsoft Authenticator app.
This is a supported method for SSPR in Microsoft Entra ID. Users can register the Microsoft Authenticator app (or another compatible app) and use the generated code to verify their identity during a password reset.
Since the setting "Number of methods required to reset: 1" means only one method is needed, a mobile app code is a valid option if the user has registered it.
Conclusion:This is correct.
C). An FIDO2 security token:
FIDO2 security tokens (e.g., YubiKey) are hardware-based security keys that support passwordless authentication in Microsoft Entra ID. They are part of Microsoft's passwordless authentication strategy and can be used for sign-in.
However, FIDO2 security tokens are not supported for SSPR. The SSPR process does not allow users to verify their identity using a FIDO2 security key because the reset process is designed to work with simpler, more accessible methods like email, SMS, or app-based codes.
Conclusion:This is incorrect.

D). A Windows Hello PIN:
Windows Hello PIN is a device-specific authentication method used to sign in to Windows devices. It is part of Windows Hello, which also includes biometric authentication (e.g., facial recognition, fingerprint).
Windows Hello PIN is not supported for SSPR in Microsoft Entra ID. The SSPR process occurs in a web- based portal (e.g., aka.ms/sspr) and does not integrate with device-specific authentication methods like Windows Hello. Additionally, Windows Hello PIN is tied to a specific device, whereas SSPR is designed to be device-agnostic.
Conclusion:This is incorrect.
Additional Considerations:
The setting "Require users to register when signing in: Yes" ensures that users have at least one authentication method registered. However, the question does not specify which methods are enabled by the administrator.
In Microsoft Entra ID, the default enabled methods for SSPR typically include email, mobile phone (SMS), mobile app code, and mobile app notification. Security questions may also be enabled but are less common due to security concerns.
If the administrator has disabled certain methods (e.g., mobile app code), the answer could change. However, the question does not indicate any such restrictions, so we assume the default methods are available.
The "Number of methods required to reset: 1" setting means users only need to use one method to reset their password, but they may have multiple methods registered. The question asks for a "valid authentication method available to users," so we need to identify a method that SSPR supports.
Conclusion:Based on the SSPR settings and the supported authentication methods in Microsoft Entra ID:
A mobile app code (option B) is a valid authentication method for SSPR, as it is supported by default and aligns with the configuration.
Smartcards, FIDO2 security tokens, and Windows Hello PIN are not supported for SSPR.Therefore, the correct answer isB.
References:
Microsoft Entra ID documentation: "Self-service password reset authentication methods" (Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#authentication- methods) Microsoft Entra ID documentation: "Configure self-service password reset" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers SSPR configuration and supported authentication methods.

**質問: 145**

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。一連の問題にはそれぞれ、定めら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、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションで質問に回答した後は、そのセクションに戻ることはできず、その結果、これらの質問はレビュー画面に表示されなくなります。
Microsoft 365 ES 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を作成します。
User1 が ID セキュア スコアの改善アクションのステータスを更新できることを確認する必要があります。
解決策: Exchange 管理者の役割を User1 に割り当てます。
**A.** はい
**B.** いいえ
正解**: A (**コメントを発表する**)**

質問**: 146**
Azure Active Directory (Azure AD) テナントがあります。
テナントの場合、ユーザーはアプリケーションを登録できますが、[いいえ] に設定されています。
Admin1 という名前のユーザーは、App1 という名前の新しいクラウド アプリをデプロイする必要があります。
Admin1 が App1 を Azure AD に登録できることを確認する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
Admin1 に割り当てるべきロールはどれですか?
**A.** Azure AD のアプリケーション開発者
**B.** サブスクリプション1のアプリ構成データ所有者
**C.** サブスクリプション1の管理対象アプリケーション共同作成者
**D.** Azure AD のクラウド アプリケーション管理者
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

質問**: 147**
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。
アマゾン ウェブ サービス (AWS) アカウント、Google Workspace サブスクリプション、および GitHub アカウントをお持ちです。
Azure サブスクリプションをデプロイし、Microsoft 365 Defender を有効にします。

Microsoft Defender for Cloud Apps を使用して OAuth 認証要求を監視できることを確認する必要があります。
解決策: Microsoft 365 Defender ポータルから、アマゾン ウェブ サービス アプリ コネクタを追加します。
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**)**

質問**: 148**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryフォレストに同期するAzureActive Directory (Azure AD)テナントがあります。
Active Directoryでユーザーアカウントが無効になっている場合でも、無効になっているユーザーは最大30分間AzureADに対して認証できることがわかります。
Active Directoryでユーザーアカウントが無効になっている場合、そのユーザーアカウントがAzureADへの認証をすぐに阻止されるようにする必要があります。
解決策：条件付きアクセスポリシーを構成します。
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**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

質問**: 149**
User1 という名前のユーザーを含む Azure AD テナントがあります。User1 には、ユーザー管理者ロールが割り当てられています。
次の要件を満たすように、テナントの外部コラボレーション設定を構成する必要があります。|
*ゲスト ユーザーがスタッフの電子メール アドレスを照会できないようにする必要があります。
*ゲスト ユーザーは、User1 によって招待された場合にのみテナントにアクセスできる必要があります。
どの 3 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てください。
正解**:**
Explanation:

Box1 = User access is restricted to properties and memberships of their own directory objects (most restrictive). This setting ensures that guest users are prevented from querying staff email addresses and can access the tenant only if they are invited by User1.
Box2 =Only users assigned to specific admin roles can invite guest users. This setting ensures that guest users can access the tenant only if they are invited by User1.
Box3 = This setting enables guest users to sign up for the tenant only if they are invited by User1.

質問**: 150**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。
ユーザー管理者ロールに次の割り当てを追加します。
* スコープの種類: 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
* 課題開始は2022年8月15日
* 任務終了日: 2022年12月15日
Exchange 管理者の役割に次の割り当てを追加します。
* スコープの種類: 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
* 課題開始日: 2022年10月15日
* 任務終了日: 2023年1月15日
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
正解**:**
Explanation:

質問**: 151**
会社では、ユーザーが企業のアプリケーションにアクセスする前にアクセスを要求する必要があります。
MyApp1 という名前の新しいエンタープライズ アプリケーションを Azure Active Directory (Azure AD) に登録し、MyApp1 のシングル サインオン (SSO) を構成します。
MyApp1 に対して次にどの設定を構成する必要がありますか?
**A.** セルフサービス
**B.** プロビジョニング
**C.** 役割と管理者
**D.** アプリケーションプロキシ
正解**: A (**コメントを発表する**)**
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access



質問: **152**
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。一連の問題にはそれぞれ、定めら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、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションで質問に回答した後は、そのセクションに戻ることはできず、その結果、これらの質問はレビュー画面に表示されなくなります。
Microsoft 365 ES 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を作成します。
User1 が ID セキュア スコア改善アクションのステータスを更新できることを確認する必要があります。
解決策: セキュリティ オペレーター ロール User1 を割り当てます。
これは目標を満たしていますか?
**A.** いいえ
**B.** はい
正解: **(**正解を表示します**)**

質問: **153**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryフォレストに同期するAzureActive Directory (Azure AD)テナントがあります。
Active Directoryでユーザーアカウントが無効になっている場合でも、無効になっているユーザーは最大30分間AzureADに対して認証できることがわかります。
Active Directoryでユーザーアカウントが無効になっている場合、そのユーザーアカウントがAzureADへの認証をすぐに阻止されるようにする必要があります。
解決策 :パススルー認証を構成します。

これは目標を達成していますか？
**A.** はい
**B.** いいえ
正解: **A** (コメントを発表する)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

質問: **154**
次の表に示すリソースを含む Azure サブスクリプションがあります。
User1 という名前の Microsoft Entra ユーザーを作成します。
VM1 と App1 に追加できる ID 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。
注意: 正解ごとに 1 ポイントが付与されます。
正解:
Explanation: