

Microsoft.SC-300J.v2026-10-14.q217

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：	217
バージョン：	v2026-10-14
ページの閲覧量：	102
問題集の閲覧量：	2275
https://www.jpnsshiken.com/shiken/Microsoft.SC-300J.v2026-10-14.q217.html	

質問: 1

Azure Active Directory (Azure AD) テナントをお持ちです。
セルフサービスパスワードリセット(SSPR)は、以下の設定を使用して構成します。
- ログイン時にユーザー登録を必須にする :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. 組織外のアドレスへのメール
- B. スマートカード
- C. FID02セキュリティトークン
- D. Microsoft Teams チャット

正解: ([正解を表示します](#))
The following authentication methods are available for SSPR (self-service password reset)
- app notification
- Mobile app code
- Email
- Mobile phone
- Office phone (available only for tenants with paid subscriptions)
- Security questions
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

質問: 2

ホットスポットに関する質問
Azure ADテナントをお持ちです。
以下の外部ID機能を設定する必要があります。
- B2Bコラボレーション
月間アクティブユーザー数(MAU)に基づく料金設定
どの2つの設定を構成すべきですか？回答するには、回答欄で該当する設定を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area



External Identities

Contoso Ltd - Azure Active Directory

Search

«

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

User flows

Subscriptions

Microsoft

Linked subscriptions

Lifecycle management

Terms of use

Access reviews

正解:

Answer Area

External Identities

Contoso Ltd - Azure Active Directory

Search

<<

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

User flows

Subscriptions

Linked subscriptions

Lifecycle management

Terms of use

Access reviews

Microsoft

質問: 3

ホットスポットに関する質問

お客様は、次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントをお持ちです。

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

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:
- ユーザー: グループ1
- ユーザーリスク: 低以上

- コントロール:
- 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、以下の設定を含むサインインリスクポリシーを構成します。

- * 課題:
- ユーザー: グループ2
- サインインリスク: 低以上
- * コントロール:
- アクセス: 多要素認証を必須とする
- * ポリシーの適用: オン

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

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
User1 can sign in from an anonymous IP address.	☐	☐
User2 can sign in from an anonymous IP address.	☐	☐
User3 can sign in from an anonymous IP address.	☐	☐

正解:

Statements	Yes	No
User1 can sign in from an anonymous IP address.	☒	☐
User2 can sign in from an anonymous IP address.	☐	☒
User3 can sign in from an anonymous IP address.	☒	☐

Explanation:

Sign-in from an anonymous IP address falls into Sign-in risk. This means only members of Group 2 will be affected by Identity Protection.

Box 1: Yes

User1 can log in from any IP as user's IP is not scrutinized. The user is not in scope of Sign-In policy.

Box 2: No

User2 cannot login. This user is in scope of the Sign-In policy and will be challenged to perform MFA. Since MFA is disabled, MFA challenge will be unsuccessful - login fails.

Box 3: Yes

User3 can log in. This is user is also in scope of the Sign-In policy, but since user's MFA is working (hence assuming a successful MFA challenge) the user will be granted access.

Reference:

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

質問: 4

ホットスポットに関する質問

お客様は、以下の仮想マシンを含む Azure サブスクリプションをお持ちです。

- 名前: V1
- Azure リージョン : 米国東部
- システム割り当て管理ID: 無効

次の表に示すマネージドIDを作成します。

Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

あなたは以下の操作を実行します。
Managed1をV1に割り当てます。
- 米国西部地域にRG1という名前のリソースグループを作成します。
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	☐	☐
You can assign Managed3 to V1.	☐	☐
You can assign VM1 the Owner role for RG1.	☐	☐

正解:

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	☒	☐
You can assign Managed3 to V1.	☒	☐
You can assign VM1 the Owner role for RG1.	☐	☒

Explanation:
You can use user assigned managed identities in more than one Azure region.
<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-faq#can-the-same-managed-identity-be-used-across-multiple-regions>

質問: 5

ホットスポットに関する質問

お客様は、以下の表に示すリソースを含む Azure サブスクリプションをお持ちです。

Name	Type
VM1	Virtual machine
App1	Azure App Service web app
Managed1	Managed identity
Managed2	Managed identity

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、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

VM1:

User1 only
Managed2 only
Managed1 and Managed2 only
Managed2 and User1 only
Managed1, Managed2, and User1

App1:

User1 only
Managed2 only
Managed2 and User1 only
A system-assigned managed identity only
A system-assigned managed identity and Managed2 only
A system-assigned managed identity, Managed2, and User1

正解:

Answer Area

VM1:

User1 only
Managed2 only
Managed1 and Managed2 only
Managed2 and User1 only
Managed1, Managed2, and User1

App1:

User1 only
Managed2 only
Managed2 and User1 only
A system-assigned managed identity only
A system-assigned managed identity and Managed2 only
A system-assigned managed identity, Managed2, and User1

質問: 6

事例研究2 - Litware, Inc.

概要

Litware, Inc.は、Fabrikam, Inc.という子会社を持つ製薬会社です。
Litwareはボストンとシアトルにオフィスを構えているが、従業員は全米各地に分散している。
従業員はVPN接続を利用して、どちらのオフィスにもリモートで接続します。

既存環境。環境を特定する

このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect はパ
ススルー認証を使用しており、パスワードハッシュの同期は無効になっています。

Litware.comには、すべてのアプリケーション開発を監督するUser1というユーザーが存在します。

LitwareはAzure ADアプリケーションプロキシを実装しています。

Fabrikam社は、fabrikam.comという名前のAzure ADテナントを所有しています。Fabrikam社のユーザーは、litware.comテナント内のゲストアカウントを使用して、litware.comのリソースにアクセスします。

既存環境。クラウド環境

Litwareの全ユーザーはMicrosoft 365 Enterprise E5ライセンスを保有しています。Microsoft Cloud App Securityに組み込まれている異常検知ポリシーはすべて有効になっています。

Litwareは、litware.com Azure ADテナントに関連付けられたAzureサブスクリプションを保有しています。このサブスクリプションには、Azure Active DirectoryコネクタとOffice 365コネクタを使用するAzure Sentinelイン
スタンスが含まれています。Azure Sentinelは現在、Azure ADのサインインログと監査ログを収集しています。

既存環境。オンプレミス環境

オンプレミスネットワークには、次の表に示すサーバーが含まれています。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litwareの2つのオフィスはどちらもインターネットに直接接続されています。両オフィスとも、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのドメインコ
ントローラーはすべてインターネットへのアクセスが制限されています。

要件。委任要件

Litwareは、以下の委任要件を特定しています。

- * Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
- * litware.com Azure AD テナントに、権限のないユーザーがアプリケーションを登録できないようにします。
- * アイデンティティガバナンスには、カスタムカタログとカスタムプログラムを使用する。
- * User1がAzure ADでエンタープライズアプリケーションを作成できることを確認します。

最小権限の原則を適用する。

要件。ライセンス要件

Litwareは最近、litware.com Active DirectoryフォレストにLWLicensesという名前のカスタムユーザー属性を追加しました。Litwareは、LWLicenses属性の値を変更することでAzure ADライセンスの割り当てを管理したい
と考えています。LWLicensesに適切な値を持つユーザーは、適切なライセンスが割り当てられているMicrosoft 365グループに自動的に追加される必要があります。

要件。管理要件

Litwareは、LWGroup1という名前のグループを作成したいと考えています。このグループには、LitwareのすべてのAzure ADユーザーアカウントが含まれますが、すべてのAzure ADゲストアカウントは除外されます。

要件。認証要件

Litwareは、以下の認証要件を定めています。

- * すべてのLitwareユーザーに対して多要素認証(MFA)を実装する。
- * LitwareのボストンオフィスからAzure ADへの認証を行う際に、ユーザーがMFAを使用する必要がないようにする。
- * litware.com フォレストに対して、禁止パスワードリストを実装する。

オンプレミスアプリケーションへのアクセス時に多要素認証(MFA)を強制する。

- * 外部に漏洩した認証情報を自動的に検出し、修復します。

要件。アクセス要件

Litwareは、以下のアクセス要件を定めています。

条件付きアクセス ポリシーを使用して、すべての Azure リソースおよび Azure AD アプリケーションへのアクセスを制御します。

- * Microsoft SharePoint Online のセッション制御を含む条件付きアクセス ポリシーを実装します。

- * Azure AD のアクセス レビューを使用して、アプリケーションへの特権アクセスを制御します。

要件。監視要件

Litware社は、Azure SentinelのFusionルールを使用して、疑わしいAzure ADサインインとその後の異常なMicrosoft Office 365アクティビティの組み合わせを含む、複数段階の攻撃を検出したいと考えています。

ホットスポットに関する質問

オンプレミスアプリケーションへのアクセスはどのように設定すべきでしょうか？

回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2

正解:

Configure the Azure AD Password Protection proxy service on:

▼

DC1
SERVER1
SERVER2

Configure the password list:

▼

In Azure AD
On DC1
On SERVER1
On SERVER2

Explanation:

The password protection proxy is installed on a member server. You enable the banned password list in Azure AD, the proxy downloads it and passes it to the DCs in the domain.
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

質問: 7

シミュレーション

必要に応じて、以下のログイン情報を使用してください。

ユーザー名を入力するには、サインインボックスにカーソルを置き、下のユーザー名をクリックしてください。

パスワードを入力するには、カーソルを「パスワードを入力」ボックスに置いて、下のパスワードをクリックしてください。

Microsoft 365 ユーザー名: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365ポータルがブラウザに正常に読み込まれない場合は、Ctrl+Kキーを押して新しいブラウザタブでポータルを再読み込みしてください。

以下の情報は、技術サポートのみを目的としています。

ラボインスタンス: 99999999

Microsoft Entra Identity Protectionを以下の要件を満たすように構成する必要があります。

・リスクレベルが高い場合、すべてのサインインに多要素認証(MFA)を必須とする。

- Mod管理者を除くすべてのユーザーにこの設定を適用します。
このタスクを完了するには、該当する管理センターにサインインしてください。
正解:

Microsoft Entra Identity Protection multi-factor authentication (MFA) for any sign-ins at the high risk level

Enable sign-in risk policy for MFA

Most users have a normal behavior that can be tracked. When they fall outside of this norm, it could be risky to allow them to successfully sign in. Instead, you might want to block that user, or ask them to perform a multifactor authentication. If the user successfully completes the MFA challenge, you can consider it a valid sign-in attempt and grant access to the application or service.

To enable this policy, complete the following steps:

Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access.

Step 3: Select New policy.

Step 4: Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Step 5: Under Assignments, select Users or workload identities

Step 5a: Under Include, select All users.

Step 5b: Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts.

[Select Mod Administrator]

Step 6: Under Cloud apps or actions > Include, select All cloud apps.

Step 7: Under Conditions > Sign-in risk, set Configure to Yes. Under Select the sign-in risk level this policy will apply to.

a. Select High.

b. Select Done.

Step 8: Under Access controls > Grant.

a. Select Grant access, Require multifactor authentication.

b. Select Select.

Step 9: Under Session. [Skip, do not need to specify sign-in frequency]

Step 10: Confirm your settings and set Enable policy to On.

Step 11: Select Create to create to enable your policy.

Note: Use risk detections for user sign-ins to trigger Microsoft Entra multifactor authentication or password changes

To protect your users, you can configure risk-based Microsoft Entra Conditional Access policies that automatically respond to risky behaviors. These policies can automatically block a sign-in attempt or require extra action, such as require a secure password change or prompting for Microsoft Entra multifactor authentication. These policies work with existing Microsoft Entra Conditional Access policies as an extra layer of protection for your organization. Users might never trigger a risky behavior in one of these policies, but your organization is protected if an attempt to compromise your security is made.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-risk-based-sspr-mfa>

質問: 8

事例研究2 - Litware, Inc.

概要

Litware, Inc.は、Fabrikam, Inc.という子会社を持つ製薬会社です。

Litwareはボストンとシアトルにオフィスを構えているが、従業員は全米各地に分散している。

従業員はVPN接続を利用して、どちらのオフィスにもリモートで接続します。

既存環境。環境を特定する

このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect はパ
ススルー認証を使用しており、パスワードハッシュの同期は無効になっています。

Litware.comには、すべてのアプリケーション開発を監督するUser1というユーザーが存在します。

LitwareはAzure ADアプリケーションプロキシを実装しています。

Fabrikam社は、fabrikam.comという名前のAzure ADテナントを所有しています。Fabrikam社のユーザーは、litware.comテナント内のゲストアカウントを使用して、litware.comのリソースにアクセスします。

既存環境。クラウド環境

Litwareの全ユーザーはMicrosoft 365 Enterprise E5ライセンスを保有しています。Microsoft Cloud App Securityに組み込まれている異常検知ポリシーはすべて有効になっています。

Litwareは、litware.com Azure ADテナントに関連付けられたAzureサブスクリプションを保有しています。このサブスクリプションには、Azure Active DirectoryコネクタとOffice 365コネクタを使用するAzure Sentinelイン
スタンスが含まれています。Azure Sentinelは現在、Azure ADのサインインログと監査ログを収集しています。

既存環境。オンプレミス環境

オンプレミスネットワークには、次の表に示すサーバーが含まれています。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litwareの2つのオフィスはどちらもインターネットに直接接続されています。両オフィスとも、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのドメインコントローラーはすべてインターネットへのアクセスが制限されています。

要件。委任要件

Litwareは、以下の委任要件を特定しています。

- * Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
- * litware.com Azure AD テナントに、権限のないユーザーがアプリケーションを登録できないようにします。
- * アイデンティティガバナンスには、カスタムカタログとカスタムプログラムを使用する。
- * User1がAzure ADでエンタープライズアプリケーションを作成できることを確認します。

最小権限の原則を適用する。

要件。ライセンス要件

Litwareは最近、litware.com Active DirectoryフォレストにLWLicensesという名前のカスタムユーザー属性を追加しました。Litwareは、LWLicenses属性の値を変更することでAzure ADライセンスの割り当てを管理したいと考えています。LWLicensesに適切な値を持つユーザーは、適切なライセンスが割り当てられているMicrosoft 365グループに自動的に追加される必要があります。

要件。管理要件

Litwareは、Litware.com Group1という名前のグループを作成したいと考えています。このグループには、LitwareのすべてのAzure ADユーザーアカウントが含まれますが、すべてのAzure ADゲストアカウントは除外されます。

Litwareは、以下の認証要件を定めています。

- * すべてのLitwareユーザーに対して多要素認証(MFA)を実装する。
- * LitwareのボストンオフィスからAzure ADへの認証を行う際に、ユーザーがMFAを使用する必要がないようにする。
- * litware.com フォレストに対して、禁止パスワードリストを実装する。

オンプレミスアプリケーションへのアクセス時に多要素認証(MFA)を強制する。

- * 外部に漏洩した認証情報を自動的に検出し、修復します。

要件。アクセス要件

Litwareは、以下のアクセス要件を定めています。

条件付きアクセス ポリシーを使用して、すべての Azure リソースおよび Azure AD アプリケーションへのアクセスを制御します。

- * Microsoft SharePoint Online のセッション制御を含む条件付きアクセス ポリシーを実装します。
- * Azure AD のアクセス レビューを使用して、アプリケーションへの特権アクセスを制御します。

要件。監視要件

Litware社は、Azure SentinelのFusionルールを使用して、疑わしいAzure ADサインインとその後の異常なMicrosoft Office 365アクティビティの組み合わせを含む、複数段階の攻撃を検出したいと考えています。

ホットスポットに関する質問

LitwareユーザーへのAzure ADライセンスの割り当てを設定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。

どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Azure AD Connect settings to modify:

Directory Extensions
Domain Filtering
Optional Features

Assign Azure AD licenses to:

An Azure Active Directory group that has only nested groups
An Azure Active Directory group that has the Assigned membership type
An Azure Active Directory group that has the Dynamic User membership type

正解:

Answer Area

Azure AD Connect Settings to modify:

Directory Extensions
Domain Filtering
Optional Features

Assign Azure AD licenses to:

An Azure Active Directory group that has only nested groups
An Azure Active Directory group that has the Assigned membership type
An Azure Active Directory group that has the Dynamic User membership type

Explanation:

Box 1: Directory Extensions

You can use directory extensions to extend the schema in Azure Active Directory (Azure AD) with your own attributes from on-premises Active Directory.

Box 2: And AAD Group that has Dynamic User Membership Type

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 a Microsoft 365 group that has the appropriate licenses assigned.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-directory-extensions>

質問: 9

お客様は、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を所有しています。

ユーザーがサイト1から1分間に50個以上の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 では、どのタイプのポリシーを作成する必要がありますか？

A. セッションポリシー

B. 活動方針

C. ファイルポリシー

D. アプリ発見ポリシー

正解: B (コメントを发表する)

You should create an activity policy in the Microsoft Defender for Cloud Apps portal to be notified if a user downloads more than 50 files in one minute from Site1.

Activity policies allow you to monitor specific user activities, including high rates of certain actions such as file downloads, and trigger alerts based on those activities. This fits the requirement to detect and notify on a user

downloading more than 50 files within a short time frame.

質問: 10

あなたはMicrosoft 365の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セキュリティプロファイルを使用する条件付きアクセスポリシーを作成する必要があります。このソリューションでは、URLに「ギャンブル」という単語が含まれるウェブサイトへのユーザーのアクセスを阻止する必要があります。

まず最初に何をすべきでしょうか？

- A. ウェブコンテンツフィルタリングポリシーを作成します。
- B. 名前付きの場所を作成します。
- C. アダプティブアクセス設定を構成します。
- D. ネットワークセキュリティグループ(NSG)を作成します。

正解: [\(正解を表示します\)](#)

Configure Global Secure Access web content filtering

Web content filtering empowers you to implement granular Internet access controls for your organization based on website categorization.

Microsoft Entra Internet Access's first Secure Web Gateway (SWG) features include web content filtering based on domain names. Microsoft integrates granular filtering policies with Microsoft Entra ID and Microsoft Entra Conditional Access, which results in filtering policies that are user-aware, context-aware, and easy to manage.

Reference:

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-web-content-filtering>

質問: 11

クラウドベースのエンタープライズアプリを含むAzureActive Directory (Azure AD)テナントがあります。

My Appsポータルで、関連するアプリをカテゴリにグループ化する必要があります。

何を作成する必要がありますか？

- A. タグ
- B. コレクション
- C. 命名ポリシー
- D. 動的グループ

正解: [\(正解を表示します\)](#)

On the My Apps portal, applications appear in default collections and your custom app collections. The Apps collection in My Apps is a default collection that contains all the applications that have been assigned to you, sorted alphabetically.

<https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps-portal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d>

質問: 12

ホットスポットに関する質問

お客様は、以下の表に示すリソースを含む Azure サブスクリプションをお持ちです。

Name	Type	Name	Type
VM1	Virtual machine	VM1	Virtual machine
App1	Azure App Service web app	App1	Azure App Service web app
Managed1	Managed identity	Managed1	Managed identity
Managed2	Managed identity	Not applicable	Not applicable

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、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

VM1:

User1 only

Managed2 only

Managed1 and Managed2 only

Managed2 and User1 only

Managed1, Managed2, and User1

App1:

User1 only

Managed2 only

Managed2 and User1 only

A system-assigned managed identity only

A system-assigned managed identity and Managed2 only

A system-assigned managed identity, Managed2, and User1

正解:

Answer Area

VM1:

User1 only

Managed2 only

Managed1 and Managed2 only

Managed2 and User1 only

Managed1, Managed2, and User1

App1:

User1 only

Managed2 only

Managed2 and User1 only

A system-assigned managed identity only

A system-assigned managed identity and Managed2 only

A system-assigned managed identity, Managed2, and User1

質問: 13

お客様は、以下の内容を含む Microsoft 365 サブスクリプションをお持ちです。

- * Azure Active Directory Premium P2 ライセンスを持つ Azure Active Directory (Azure AD) テナント
- * Site1という名前のMicrosoft SharePoint Onlineサイト
- * Team1という名前のMicrosoft Teamsチーム

Site1とTeam1を管理するには、権限管理ワークフローを作成する必要があります。

まず最初に何をすべきでしょうか？

- A.** アプリ登録を設定します。
- B.** 管理単位を作成します。
- C.** アクセスパッケージを作成します。
- D.** カタログを作成します。

正解: **C** ([コメントを発表する](#))

All access packages must be put in a container called a catalog. A catalog defines what resources you can add to your access package. If you don't specify a catalog, your access package will be put into the general catalog.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

質問: 14

contoso.com という名前の Azure Active Directory (Azure AD) テナントをお持ちです。

Azure AD 外部 ID の料金体系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すか？

- A.** ユーザーフロー
- B.** 利用規約
- C.** 連携購読
- D.** アクセスレビュー

正解: **C** ([コメントを発表する](#))

To take advantage of MAU billing, your Azure AD tenant must be linked to an Azure subscription.

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing#what-do-i-need-to-do>

質問: 15

あなたはPass4test Inc.のクラウド管理者であり、すべてのユーザーに対して多要素認証を実装するよう指示されています。その準備として、すべてのユーザーが多要素認証に正しく登録されていることを確認する必要があります。以下の選択肢のうち、認証方法として使用できないものはどれですか？

- A.** Microsoft Authenticator アプリ
- B.** セキュリティ質問
- C.** FIDO2セキュリティキー
- D.** SMS
- E.** 音声通話

正解: ([正解を表示します](#))

Security questions cannot be used as a valid authentication method for multi-factor authentication. The Microsoft Authenticator App, FIDO2 Security Key, SMS, and Voice Call are all valid authentication methods for multi-factor authentication.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods#:~:text=How%20each%20authentication%20method%20works%20%20%20,%20%20M FA%20%204%20more%20rows%20>

質問: 16

貴社は、contosri.com という名前の Azure Active Directory (Azure AD) テナントを所有しています。貴社には、以下の表に示すビジネスパートナーがいます。

Name	Description
Fabrikam, Inc.	An Azure AD tenant that has two verified domains named fabrikam.com and adatum.com
Litware, Inc.	A third-party identity provider that uses the domain names of litwareinc.com and contoso.com

ユーザーはパッケージ1を使用してアクセスをリクエストできます。

FabrikamとLitwareのユーザーは、それぞれのドメイン名をメールアドレスとして使用します。

あなたは、FabrikamとLitwareのユーザーのみがアクセスできる「package1」という名前のアクセスパッケージを作成する予定です。

Fabrikamとlitwareの接続組織を設定することで、それらの組織のユーザーがpackage1を使用してアクセスを要求できるようにする必要があります。

最低限構築すべき連携組織とはどのようなものでしょうか？

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

正解: (正解を表示します)

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 385問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 17
ホットスポットに関する質問

お客様は、AU1とAU2という名前の2つの管理ユニットを含むMicrosoft 365 E5サブスクリプションを所有しています。

次の表に示すように、5人のユーザーを作成します。

Name	Administrative unit	Role	Role scope
User1	AU2	Global Administrator	None
User2	AU2	Helpdesk Administrator	AU1
User3	AU1	Privileged Authentication Administrator	AU2
User4	AU1	Helpdesk Administrator	AU1
User5	AU1	None	None

User2とUser3は、どのユーザーのパスワードをリセットできますか？回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

User2 can reset password for:

▼
User1 and User4 only
User1, User3, User4, and User5
User3 only
User4 only
User5 only

User3 can reset password for:

▼
User1 only
User1 and User2 only
User1, User2, and User4
User2 and User4 only
User 5 only



正解:

Answer Area

User2 can reset password for:

▼
User1 and User4 only
User1, User3, User4, and User5
User3 only
User4 only
User5 only

User3 can reset password for:

▼
User1 only
User1 and User2 only
User1, User2, and User4
User2 and User4 only
User 5 only

質問: 18

あなたはMicrosoft 365テナントをお持ちです。
全てのユーザーは携帯電話とWindows 10搭載のノートパソコンを所有している。
ユーザーは、Wi-Fiや携帯電話の接続環境がない遠隔地で作業することがよくあります。そのような遠隔地で作業する際、ユーザーはノートパソコンをインターネット接続可能な有線ネットワークに接続します。
あなたは多要素認証(MFA)を導入する予定です。
ユーザーはリモート環境からどのMFA認証方法を利用できますか？

- A. セキュリティに関する質問
- B. Microsoft Authenticatorアプリを通じた通知
- C. アプリのパスワード
- D. Windows Hello for Business

正解: ([正解を表示します](#))

質問: 19

お客様は、1,000人のユーザーを含むMicrosoft Entraテナントを所有しています。これらのユーザーには、Microsoft Entra Suiteライセンスが割り当てられています。グローバルセキュアアクセスを導入しています。グローバルセキュアアクセスによってwww.microsoft.comへの接続がバイパスされるようにする必要があります。どのプロファイルを更新すべきですか？

- A. インターネットアクセスプロファイルのみ
- B. Microsoftトラフィックプロファイルのみ
- C. Microsoftトラフィックプロファイルとインターネットアクセスプロファイルのみ
- D. Microsoftトラフィックプロファイル、プライベートアクセスプロファイル、インターネットアクセスプロファイル

正解: ([正解を表示します](#))

Global Secure Access, How to manage the Internet Access traffic forwarding profile The Internet Access traffic forwarding profile routes internet traffic through the Global Secure Access client. Enabling this traffic forwarding profile allows remote workers to connect to the internet in a controlled and secure way. With the features of Microsoft Entra Internet Access, you can control which internet sites can be accessed. You can also configure which traffic to exclude from Global Secure Access based on IP addresses, IP address ranges, IP subnets, and Fully Qualified Domain Names (FQDNs).

Reference:

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-manage-internet-access-profile>

質問: 20

お客様はMicrosoft Entraテナントをお持ちです。リスク検出レポートを開きます。どのリスク検出タイプがユーザーリスクに分類されますか？

- A. 見慣れないサインインプロパティ
- B. 匿名IPアドレス
- C. パスワードスプレー
- D. Microsoft Entra脅威インテリジェンス

正解: ([正解を表示します](#))

質問: 21

Microsoft 365 E5 サブスクリプションがあります。ユーザーは、サードパーティのクラウド アプリが自分のデータにアクセスすることを承認します。アプリが高い権限を必要とし、20 人を超えるユーザーによって承認されている場合にトリガーされるアラートを構成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どれですか？

- A. 異常検出ポリシー
- B. OAuth アプリ ポリシー
- C. アクセス ポリシー
- D. 活動方針

正解: **B** ([コメントを発表する](#))

In addition to the existing investigation of OAuth apps connected to your environment, you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria. For example, you can automatically be alerted when there are apps that require a high permission level and were authorized by more than 50 users.

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

質問: **22**

Azure AD テナントと App1 という名前の .NET Web アプリがあります。

Azure AD 認証用に App1 を登録する必要があります。

App1 には何を設定する必要がありますか？

A. 実行可能ファイルの名前

B. リダイレクト URI

C. パッケージ名

D. バンドル ID

正解: **B** ([コメントを発表する](#))

質問: **23**

あなたはMicrosoft 365テナントをお持ちです。

全ての利用者は携帯電話とノートパソコンを所有している。

ユーザーは、Wi-Fiや携帯電話の接続環境がない遠隔地で作業することがよくあります。そのような遠隔地で作業する際、ユーザーはノートパソコンをインターネット接続可能な有線ネットワークに接続します。

あなたは多要素認証(MFA)を導入する予定です。

ユーザーはリモート環境からどのMFA認証方法を利用できますか？

A. Microsoft Authenticatorアプリからの認証コード

B. セキュリティに関する質問

C. 音声

D. SMS

正解: ([正解を表示します](#))

The Authenticator app can be used as a software token to generate an OATH verification code.

After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

B: Security questions are not used as an authentication method but can be used during the self- service password reset (SSPR) process.

C, D: An automated voice call and an SMS requires mobile connectivity.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

質問: **24**

RG1 という名前のリソース グループと、User1、User2、User3、および User4 という名前の 4 人のユーザーを含む Azure サブスクリプションがあります。ユーザーに RG1 の次のロールを割り当てることを計画しています。

* ユーザー 1: 読者

* User2: 投稿者

* User3: ストレージ BLOB データ リーダー

* User4: 仮想マシンの貢献者

属性ベースのアクセス制御 (ABAC) の使用を評価しています。ABAC の使用をサポートするユーザーの役割はどれですか？

- A. ユーザー 1
- B. ユーザー 2
- C. ユーザー 3
- D. ユーザー 4

正解: ([正解を表示します](#))

<https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview>

質問: 25

新しい Azure AD テナントをデプロイする予定です。

テナントに対してデフォルトでどの多要素認証 (MFA) 方法が有効になりますか？

- A. Microsoft Authenticator
- B. SMS
- C. 音声通話
- D. 電子メール OTP

正解: ([正解を表示します](#))

Security defaults users are required to register for and use multifactor authentication using the Microsoft Authenticator app using notifications. Users might use verification codes from the Microsoft Authenticator app but can only register using the notification option. Users can also use any third party application using OATH TOTP to generate codes.

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#authentication-methods>

質問: 26

contoso.com という名前の Microsoft Entra ID P2 テナントがあり、その中に App1 という名前の登録済みアプリが含まれています。

1月1日にApp1は削除されました。

App1を復元する必要があります。

App1を復元できる最終日はいつですか？

- A. 1月14日
- B. 1月30日
- C. 3月30日
- 【日付】 6月30日

正解: B ([コメントを發表する](#))

A deleted Microsoft Entra ID P2 app can be restored within the first 30 days after its deletion.

After this 30-day window, the application is permanently deleted and cannot be restored.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/restore-application>

質問: 27

ホットスポットに関する質問

Microsoft Entraテナントには、User1という名前のユーザーが含まれています。

管理者がユーザー1を削除します。

以下の項目を特定する必要があります。

- 最大何日間までオプションを利用できますか？

User1アカウントを復元しますか？
- 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？
回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Number of days:

▼

15

30

90

180

Role:

▼

User Administrator

Network Administrator

Helpdesk Administrator

Domain Name Administrator

正解:

Answer Area

Number of days:

▼

15

30

90

180

Role:

▼

User Administrator

Network Administrator

Helpdesk Administrator

Domain Name Administrator

Explanation:
Box 1: 30
In Microsoft Entra ID (formerly Azure AD), deleted users can be restored within a period of 30 days. After this 30-day period, the account is permanently deleted and cannot be recovered.
Box 2: User Administrator
The User Administrator role is the least privileged role that has the permissions required to restore deleted user accounts in Microsoft Entra ID. Other roles, like Network Administrator or Domain Name Administrator, do not have the necessary permissions to manage user accounts.

質問: 28

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

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

Azure Monitor は、Azure Active Directory (Azure AD) のアクティビティ ログを分析するために使用します。

Azure AI のユーザーサインイン試行を監視した結果、毎日 100 件以上のメールアラートが届きます。

あなたではなく、新しいセキュリティ管理者がアラートを受信するように設定する必要があります。

解決策 :Azure Monitor からアクション グループを変更します。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解: ([正解を表示します](#))

Yes, you modify the action group from Azure Monitor.

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#configure-notifications>

質問: 29

Azure AD Privileged Identity Management (PIM) を使用する Azure サブスクリプションがあります。

クラウド アプリケーション管理者ロールに適切なユーザーを特定する必要があります。

Privileged Identity Management 設定のどのブレードを使用する必要がありますか？

A. Azure resources

B. Review access

C. Azure AD roles

D. Privileged access groups

正解: ([正解を表示します](#))

質問: 30

お客様のMicrosoft Entraテナントには、以下の表に示すIDが含まれています。

Name	Description
User1	User account
Group1	Security group
Group2	Microsoft 365 group
SP1	Service principal

テナントにApp1という名前のアプリを登録します。

App1のオーナーロールは、どのIDに割り当てることができますか？

A. ユーザー1のみ

B. ユーザー1とグループ1のみ

C. ユーザー1とSP1のみ

D. ユーザー1、グループ1、グループ2のみ

E. User1、Group1、およびSP1のみ

F. ユーザー1、グループ1、グループ2、およびSP1

正解: (正解を表示します)

In Microsoft Entra ID, the Owner role for a registered application can be assigned to users [User1] and service principals [SP1]. Groups cannot be assigned as owners of enterprise applications. A user is automatically added as an owner when they register an application, unless they have administrator roles. Service principals, which represent applications, hosted services, or automated tools, can also be owners.

Reference:

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

質問: 31

2,500人のユーザーにMicrosoft Office 365 Enterprise E3ライセンスが割り当てられています。ライセンスは個々のユーザーに割り当てられています。

Microsoft Entra 管理センターの [グループ] ブレードから、すべてのユーザーを含むグループに Microsoft Office 365 Enterprise E5 ライセンスを割り当てます。

最小限の管理作業で、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-WindowsProductKey コマンドレット

B. Update-MgGroup コマンドレット

C. Set-MgUserLicense 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)

To remove the Office 365 Enterprise E3 licenses from the users who are now part of a group with Office 365 Enterprise E5 licenses assigned, you should use the Set-MgUserLicense cmdlet. This cmdlet allows you to modify the licenses assigned to a user. By using this cmdlet, you can remove the Office 365 Enterprise E3 licenses from all users who are part of the group where you assigned the Office 365 Enterprise E5 licenses.

有効的な**SC-300J**問題集はJPNTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-300J**試験問題集を提供します。JPNTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> **385**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 32

ホットスポットに関する質問

お客様は、Microsoft EntraテナントにリンクされたAzureサブスクリプションを所有しています。このテナントには、User1、User2、User3という名前の3人のユーザーが登録されています。

お客様は以下の表に示す機器をお持ちです。

Name	Platform	Description
Device1	Windows 11	Microsoft Entra joined
Device2	Windows 11	None
Device3	Android	Microsoft Entra registered

次のような構成の仮想マシンをデプロイします。

- 名前: VM1

- リソースグループ: RG1

- オペレーティングシステム: Windows Server

- Microsoft Entra IDでログイン：有効

以下の表に示すAzureロールの割り当てがあります。

User	Role	Scope
User1	Virtual Machie Local User Login	RG1
User2	Virtual Machie User Login	RG1
User3	Virtual Machie Administrator Login	Sub1

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can sign in to VM1 from Device1 by using their Microsoft Entra credentials.	☐	☐
User2 can sign in to VM1 from Device2 by using their Microsoft Entra credentials.	☐	☐
User3 can sign in to VM1 from Device3 by using their Microsoft Entra credentials.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 can sign in to VM1 from Device1 by using their Microsoft Entra credentials.	☐	☒
User2 can sign in to VM1 from Device2 by using their Microsoft Entra credentials.	☒	☐
User3 can sign in to VM1 from Device3 by using their Microsoft Entra credentials.	☐	☒

Explanation:

- Box 1: No
User1 has the Virtual Machine Local User login role with scope RG1.
The role is not correct.
The Virtual Machine User Login role would be OK.
- Box 2: Yes
User2 has a correct role: The Virtual Machine User Login role.
The Device is Windows 11, which is fine.
The Device does not have to been Entra joined or Entra registered.

Box 3: No
Not possible from an Android device.

Note:
Enable Microsoft Entra login for a Windows VM in Azure
To use Microsoft Entra login for a Windows VM in Azure, you must:
1. Enable the Microsoft Entra login option for the VM. [we can assume this has been configured]
2. Configure Azure role assignments for users who are authorized to sign in to the VM.

Reference:
https://learn.microsoft.com/en-us/entra/identity/devices/howto-vm-sign-in-azure-ad-windows
https://learn.microsoft.com/en-us/azure/virtual-desktop/azure-ad-joined-session-hosts

質問: 33
お客様は、以下の表に示すオブジェクトを含む Azure Active Directory (Azure AD) テナントをお持ちです。

Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Azure AD ロールの対象となるオブジェクトとして、Azure AD 特権 ID 管理 (PIM) に追加できるのはどれですか？

- A. ユーザー1、ゲスト1、およびID1
- B. ユーザー1とゲスト1のみ
- C. ユーザー1のみ
- D. ユーザー1とID1のみ

正解: (正解を表示します)
You cannot assign service principals as eligible to Azure AD roles, Azure roles, and Privileged Access groups but you can grant a time limited active assignment to all three.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

質問: 34
事例研究1 - Contoso, Ltd
概要

Contoso, Ltd.は、モントリオールに本社を置き、ロンドンとシアトルに支店を持つコンサルティング会社です。
ContosoはFabrikam, Inc.という会社と提携関係にある。Fabrikamはfabrikam.comという名前のAzure Active Directory(Azure AD)テナントを所有している。
既存環境。既存環境

Contosoのオンプレミスネットワークには、contoso.comという名前のActive Directoryドメインが含まれています。
このドメインには、Contoso_Resources という名前の組織単位 (OU) が含まれています。Contoso_Resources OU には、すべてのユーザーとコンピューターが含まれています。
contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

既存環境 :Microsoft 365/Azure環境

Contosoはcontoso.comという名前のAzure ADテナントを所有しており、それには以下のライセンスが関連付けられています。

- * Microsoft Office 365 Enterprise E5
- * エンタープライズモビリティ+セキュリティ
- * Windows 10 Enterprise E3
- * プロジェクト計画3

Azure AD Connectは、Azure ADとActive Directoryドメインサービス(AD DS)の間で構成されています。同期されるのはContoso_Resources OUのみです。

ヘルプデスク管理者は、ユーザー設定を管理するために日常的にMicrosoft 365管理センターを使用します。

現在、ユーザー管理者はMicrosoft 365管理センターを使用してライセンスを手動で割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。

- * ロンドンオフィスのユーザーは、Microsoft 365 Phone Systemのライセンスが未割り当ての状態です。

シアトルオフィスのユーザーは、Yammer Enterpriseライセンスを未割り当ての状態です。

contoso.com では、セキュリティのデフォルト設定が無効になっています。

Contosoは、管理者ロールを保護するためにAzure ADの特権ID管理(PIM)を使用しています。

既存環境。問題点

コントソ氏は以下の問題点を指摘している。

- * 現在、すべてのヘルプデスク管理者は、Microsoft 365テナント全体にわたるユーザーライセンスを管理できます。
 - * ユーザー管理者からは、Contosoの各オフィスごとに異なるライセンス要件を手動で設定するのは面倒だという報告が寄せられています。
- ヘルプデスク管理者は、必要なMicrosoft 365サービスおよびアプリへの内部アクセスとゲストアクセスをプロビジョニングするのに時間をかけすぎている。
- * 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
 - * Azure AD で [ログ] ノードを選択すると、Log Analytics の統合が有効になっていないことを示すエラーメッセージが表示されます。

要件。計画されている変更

コントソ氏は以下の変更を実施する予定です。

- * セルフサービスパスワードリセット(SSPR)を実装する。
- * Azure Monitorを使用して、Azure監査アクティビティログを分析します。
- * テナントに追加された新規ユーザーに対するライセンス割り当てを簡素化します。
- * Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施する。
- * ユーザー管理者ロールを設定し、有効化する際に正当性の説明と承認が必要となるようにします。
- * App1という名前の、業務専用のカスタムAzure Webアプリを実装します。App1はインターネットからアクセス可能で、Azure ADアカウントを使用して認証されます。
- * マーケティング部門の新規ユーザー向けに、Microsoft SharePoint Onlineのサイト、グループ、およびアプリへのアクセス権限を付与するための自動承認ワークフローを実装します。

Contoso社はAdatum Corporationという会社を買収する予定です。Adatumという名前のActive Directory組織単位(OU)内に、新たに100人のAdatumユーザーが作成されます。これらのユーザーはロンドンとシアトルに拠点を置く予定です。

要件。技術要件

Contoso社は、以下の技術要件を特定しました。

- * すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期されている必要があります。
- * App1 には、https://contoso.com/auth-response を指すリダイレクト URI が必要です。
- * 新規ユーザーへのライセンス割り当ては、ユーザーの所在地に基づいて自動的に行われる必要があります。
- * Fabrikamのユーザーは、マーケティング部門のSharePointサイトに最大90日間アクセスできる必要があります。
- * Azure AD で実行される管理操作は監査対象とする必要があります。監査ログは 1 年間保持する必要があります。
- * ヘルプデスク管理者は、それぞれのオフィスに所属するユーザーのライセンスのみを管理する必要があります。
- * ユーザーの身元が侵害された可能性がある場合、ユーザーにはパスワードの変更を強制しなければならない。

ホットスポットに関する質問

マーケティング部門の計画された変更点と技術要件を実施する必要があります。
どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Microsoft

To configure user access:

An access package

An access review

A conditional access policy

To enable collaboration with fabrikam.com:

An accepted domain

A connected organization

A custom domain name

正解:

Answer Area

Microsoft

To configure user access:

An access package

An access review

A conditional access policy

To enable collaboration with fabrikam.com:

An accepted domain

A connected organization

A custom domain name

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>

質問: 35

ホットスポットに関する質問

お客様のオンプレミスネットワークには、Active Directory ドメインサービス(AD DS)ドメインが含まれています。このドメインには、Windows 11を実行しているコンピューターが含まれています。
あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

ハイブリッド参加を有効にして、コンピューターをMicrosoft Intuneに登録する予定です。

ドメインに展開すべきソフトウェアと、Intuneで実行すべきアクションを推奨する必要があります。

推奨状には何を含めるべきでしょうか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。



Domain:

Intune:

正解:

Answer Area

Domain:

Intune:

Explanation:

Box 1: The Intune Connector for Active Directory

Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot Intune connector server requirements

- * The Intune Connector for Active Directory must be installed on a computer that's running Windows Server 2016 or later with .NET Framework version 4.7.2 or later.
- * The server hosting the Intune Connector must have access to the Internet and Active Directory.

Box 2: Modify the mobile device management (MDM) User scope

Set up Windows automatic MDM enrollment

1. Sign in to the Azure portal and select Microsoft Entra ID.
2. In the left hand pane, select Manage | Mobility (MDM and WIP) > Microsoft Intune.
3. Make sure users who deploy Microsoft Entra joined devices by using Intune and Windows are members of a group included in MDM User scope.
4. Use the default values in the MDM Terms of use URL, MDM Discovery URL, and MDM Compliance URL boxes, and then select Save.

Reference:

<https://learn.microsoft.com/en-us/autopilot/windows-autopilot-hybrid>

質問: 36

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。)

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *

Admin review

Description ⓘ

Start date *

12/18/2020

Frequency

Monthly

Duration (in days) ⓘ

14

End ⓘ

Never

End by

Occurrences

Number of times

End date

01/17/2021

Users Scope

Everyone

Review role membership (permanent and eligible) *

Application Administrator and 72 others

Reviewers

Reviewers

(Preview) Manager

(Preview) Fallback reviewers ⓘ

Megan Bowen

Upon completion settings

Start

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)

Modify the properties of the IT administrator user accounts is not like to modify admin review to assign a manager, so, Because admin review is not modified, Megan Brow as Fallback Reviewer will still receiving reviews, no manager has been assigned to admin review.

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

質問: 37

あなたはcontoso.comというSMTPアドレス空間を使用するMicrosoft Exchange組織を持っています。

複数のユーザーが、Microsoft Entraへのセルフサービス登録にcontoso.comの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contoso.comのMicrosoft Entraテナントで、Microsoft 365サービスへのセルフサービスサインアップ用の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べきですか？

- A. Update-MgPolicyAuthorizationPolicy
- B. Update-MgDomain
- C. Update-MgPolicyPermissionGrantPolicyExclude
- D. Update-MgDomainFederationConfiguration

正解: A (コメントを発表する)

Use the "Update-MgPolicyAuthorizationPolicy" cmdlet with the "AllowedToSignUpEmailBasedSubscriptions" parameter set to False.

<https://learn.microsoft.com/en-us/entra/identity/users/directory-self-service-signup>

質問: 38

ホットスポットに関する質問

お客様は、以下の表に示すキーコンテナーを含む Azure サブスクリプションをお持ちです。

Name	In resource group	Number of days to retain deleted key vaults	Purge protection
KeyVault1	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

このサブスクリプションには、以下の表に示すユーザーが含まれています。

Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

6月1日、Admin4は以下の操作を実行します。

- KeyVault1 から Certificate1 という名前の証明書を削除します
- KeyVault2からSecret1という名前のシークレットを削除します

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Microsoft

Statements

Admin1 can recover Secret1 on June 7.

Admin2 can purge Certificate1 on June 12.

Admin3 can purge Certificate1 on June 14.

Yes

No

正解:

Answer Area

Microsoft

Statements

	Yes	No
Admin1 can recover Secret1 on June 7.	☒	☐
Admin2 can purge Certificate1 on June 12.	☐	☒
Admin3 can purge Certificate1 on June 14.	☐	☒

Explanation:

Box 1: Yes

Key Vault Administrator can perform all data plane operations on a key vault.

And purge protection is disabled for KeyVault2.

NB: Purge protection is an optional Key Vault behavior and is not enabled by default.

Do not mismatch with soft-delete

Box 2: No

We are still in the Purge protection remaining period.

NB: Also the Key Vault contributor role doesn't allow to get access to certificate Box 3: No We are still in the Purge protection remaining period.

Even if the Certificate Officer role allow to get access to certificate

質問: 39

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テナントをお持ちです。

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。

ユーザー1が統合登録プロセスを完了するために使用できる認証方法は、次のうちどれですか？正解はそれぞれ完全な解決策を示しています。

注：正解ごとに1ポイントが加算されます。

- A. FIDO2セキュリティキー
- B. ハードウェアトークン
- C. ワンタイムパスコードメール
- D. Windows Hello for Business
- E. Microsoft Authenticator アプリ

正解: (正解を表示します)

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

- Hardware token is not an option to register.
- a one-time passcode email is not even listed.

- Windows Hello for Bussines is not even listed.

質問: 40

シミュレーション

全従業員」グループのメンバーが、Microsoft Authenticator アプリを使用してパスワードなしでサインインできるようにする必要があります。

正解:

To enable passwordless sign-in via the Microsoft Authenticator app for a specific group in Microsoft Entra ID, you must enable the Microsoft Authenticator policy, target your specific group, and configure the authentication mode to passwordless.

Step 1: Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.

Navigate to Authentication Methods

Step 2: Expand the Protection menu on the left navigation bar.

Step 3: Click on Security.

Step 4: Click on Authentication methods.

Step 5: Under the Policies tab, select Microsoft Authenticator from the list of methods.

Enable Microsoft Authenticator Policy

Step 6: Change the Enable toggle to Yes.

Step 7: Under the Target tab, choose Select groups (instead of "All users").

Target Your Specific Group

Step 8: Click Add groups.

Step 9: Search for and select your specific group from the directory list. [Select All Employees] Step 10: Next to your added group, click the three dots (...) or select Configure.

Configure Passwordless Mode

Step 11: Change the Authentication mode drop-down menu from Any or Push to Passwordless.

Step 12: Click Done.

Step 13: Click the Save button at the bottom of the screen to apply the policy changes Save the Policy Reference:

<https://huntertech.ca/blog/passwordless-authentication-microsoft-365/>

質問: 41

ホットスポットに関する質問

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

サブスクリプションのアプリ同意を設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。

- アプリに対するユーザーの同意を無効にする。

- アプリの管理者同意ワークフローを設定します。

各要件に対して、どのポータルを使用すべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area



Disable user consent to apps:

	▼
Microsoft 365 admin center	
Microsoft 365 Apps admin center	
Microsoft 365 Defender portal	
Microsoft Purview compliance portal	

Configure admin consent workflow for apps:

	▼
Microsoft Entra admin center	
Microsoft 365 admin center	
Microsoft 365 Defender portal	
Microsoft Purview compliance portal	

正解:

Answer Area



Disable user consent to apps:

	▼
Microsoft 365 admin center	
Microsoft 365 Apps admin center	
Microsoft 365 Defender portal	
Microsoft Purview compliance portal	

Configure admin consent workflow for apps:

	▼
Microsoft Entra admin center	
Microsoft 365 admin center	
Microsoft 365 Defender portal	
Microsoft Purview compliance portal	

質問: 42

Sub1という名前のAzureサブスクリプションがあり、その中にVM1という名前の仮想マシンが含まれています。VM1に対してMicrosoft Entraログインを有効にし、VM1がSub1内のリソースにアクセスできるように構成する必要があります。VM1にはどのタイプのIDを割り当てるべきですか？

- A. Microsoft Entraユーザーアカウント
- B. ユーザーが割り当てた管理ID
- C. Azure Automationアカウント
- D. システム割り当て管理ID

正解: **D** ([コメントを发表する](#))

System-assigned managed identity: This type of managed identity is enabled directly on an Azure resource. In this case, enabling a system-assigned managed identity on VM1 would allow VM1 to authenticate with other Azure resources within Sub1, using the identity associated with VM1.

質問: **43**

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

Review1 という名前のアクセス レビューを作成します。Review1 では、6 か月ごとに Microsoft が

365グループのオーナーは、ゲストユーザーによるグループへのアクセス権限を審査します。

グループオーナーがReview1のメンバーシップを確認できなかった場合、ゲストユーザーが自動的に削除されるようにする必要があります。

Review1では、どの設定を構成すればよいですか？

A. レビューアー

B. 一般

C. 詳細設定

D. 設定完了後

正解: **D** ([コメントを发表する](#))

* When completed

* Upon completion settings

Incorrect:

* Advanced settings

* General

* Reviewers

* Scheduling

Note: See step 5 below.

Ask guests to review their need for access, in general

In some organizations, guests might not be aware of their group memberships.

1. Create a security group in Microsoft Entra ID with the guests as members, if a suitable group doesn't already exist.

2. To create a' access review for that group, select the reviewers to be the members themselves.

3. Ask each guest to review their own membership. By default, each guest who accepted an invitation receives an email from Microsoft Entra ID with a link to the access review in your organization's access panel.

4. After the reviewers give input, stop the access review.

5. You can automatically delete the guest users Microsoft Entra B2B accounts as part of an access review when you're configuring an Access review for Select Team + Groups. This option isn't available for All Microsoft 365 groups with guest users.

New access review ...



* Review type * Reviews Settings * Review + Create

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource ⓘ

If reviewers don't respond ⓘ

Remove access

Action to apply on denied guest users ⓘ

Block user from signing-in for 30 ...

At end of review, send notification to

Remove user's membership from the resource

Block user from signing-in for 30 days, then remove user from the tenant

To do so, select Auto apply results to resource as this will automatically remove the user from the resource. If reviewer don't respond should be set to Remove access and Action to apply on denied guest users should also be set to Block from signing in for 30 days then remove user from the tenant.

Reference:

<https://learn.microsoft.com/en-us/entra/id-governance/manage-guest-access-with-access-reviews>

質問: 44

あなたはMicrosoft 365のサブスクリプションをお持ちです。

ユーザーがエンタープライズアプリケーションにプロファイルへのアクセス権限を付与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User.Read権限とプロファイル委任権限のみに同意できるようにする必要があります。

最初に何を設定すべきですか？

- A. ID保護設定
- B. 許可の分類
- C. 管理者同意設定
- D. セキュリティのデフォルト設定

正解: C (コメントを发表する)

In Microsoft 365 you may need to configure Admin consent settings to control whether users can grant enterprise applications access to their profiles. By default, users can consent to applications for permissions that don't

require administrator approval. However, you can restrict this and require administrator consent for certain permissions or for all applications.

* User Consent:

By default, users can consent to applications for permissions that don't require admin approval.

This means they can grant apps access to their profile information or other resources that don't require elevated permissions.

* Admin Consent:

For certain permissions, such as those requiring access to all files in the organization or other sensitive data, admin consent is required. This means that an administrator must approve the application's access to these resources.

Reference:

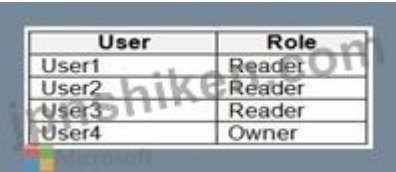
<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/user-admin-consent-overview>

質問: 45

ホットスポットに関する質問

Azure サブスクリプションには、RG1 と RG2 という名前の 2 つのリソース グループと、storage1 という名前のストレージ アカウントが含まれています。

サブスクリプションには、以下の表に示すように役割を割り当てます。



User	Role
User1	Reader
User2	Reader
User3	Reader
User4	Owner

RG1には、以下の表に示すように役割を割り当てます。

User	Role
User1	Reader and Data Access
User2	Contributor

以下の図に示すように、storage1 に役割を割り当てます。

```

1 [
2   {
3     "RoleAssignmentId": "9dea588b-7569-4cfb-b92b-92748cdc550b",
4     "Scope": "/subscriptions/7fe6d66e-8694-4b54-beae-17fd819d4873/resourceGroups/RG2/providers/Microsoft.Storage/storageAccounts/storage1",
5     "DisplayName": "User3",
6     "SignInName": "User3@contoso.com",
7     "RoleDefinitionName": "User Access Administrator",
8     "RoleDefinitionId": "/subscriptions/7fe6d66e-8694-4b54-beae-17fd819d4873/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
9     "ObjectId": "919948b2-bc93-41a0-9562-9399576cc8f0",
10    "ObjectType": "User",
11    "RoleAssignmentDescription": "",
12    "ConditionVersion": "",
13    "Condition": ""
14  }
15 ]

```

他のAzureリソースにはロールは割り当てられません。

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

注：正解ごとに1ポイントが加算されます。

Answer Area		
Statements	Yes	No
User1 can read the data stored in storage1.	☐	☐
User2 can create a virtual network in RG2.	☐	☐
User3 can assign roles for storage1.	☐	☐

正解:

Answer Area		
Statements	Yes	No
User1 can read the data stored in storage1.	☒	☐
User2 can create a virtual network in RG2.	☐	☒
User3 can assign roles for storage1.	☒	☐

Explanation:

Box 1: Yes

User1 has the Reader role in the subscription.

The subscription includes the storage account.

User1 will have read access to the storage account.
(For RG1 User1 has the Reader and Data Access role.
User1 has no role at the storage account scope level.)
Note:
The Azure Reader role is a built-in role that grants users read-only access to view Azure resources. This means they can see information about resources, their properties, and configurations, but they cannot make any changes or modifications to those resources.
Box 2: No
User2
User2 has the Contributor role for RG1 only, but not for RG2.
User2 has the Reader role in the subscription.
User2 will not be able to create a virtual network in RG2.
Box 3: Yes
User3 has the User Access Administrator role for the storage1storage account.
The User Access Administrator role can assign roles. This role is specifically designed to manage access to Azure resources, including assigning roles to other users, groups, or service principals.
Reference:
<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

質問: 46

Azure AD Identity Protectionを使用するAzure Active Directory(Azure AD)テナントがあり、次の表に示すリソースが含まれています。

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	Not applicable

Azure 多要素認証 (MFA) は、すべてのユーザーに対して有効になっています。
ユーザー1が、追加調査が必要な中程度の深刻度のアラートをトリガーしました。
ユーザー1が次回ログインする際に、パスワードをリセットするように強制する必要があります。解決策は、管理者の手間を最小限に抑えるものでなければなりません。
あなたはどうすべきでしょうか？
A. ユーザーリスクを再設定し、ポリシーが中程度または低程度の深刻度でトリガーされるようにします。
B. ユーザー1を侵害されたユーザーとしてマークする。
C. User1 の Azure MIFA 登録をリセットします。
D. サインインリスクポリシーを設定します。

正解: (正解を表示します)

Scenario: User compromised (True positive)

'Risky users' report shows an at-risk user [Risk state = At risk] with low risk [Risk level = Low] and that user was indeed compromised.

Feedback: Select the user and click on 'Confirm user compromised'.

What happens under the hood? Azure AD will move the user risk to High [Risk state = Confirmed compromised; Risk level = High] and will add a new detection

'Admin confirmed user compromised'.

Notes: Currently, the 'Confirm user compromised' option is only available in 'Risky users' report.

The detection 'Admin confirmed user compromised' is shown in the tab 'Risk detections not linked to a sign-in' in the 'Risky users' report.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback

有効的な**SC-300J**問題集はJPNTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-300J**試験問題集を提供します。JPNTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 885問、30%**ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 47

ホットスポットに関する質問

Sub1 という名前の Azure サブスクリプションがあり、その中に storage1 という名前のストレージ アカウントが含まれています。

App1とApp2という名前の2つのアプリをデプロイする必要があります。それぞれのアプリには以下の設定が必要です。

- App1はSub1に登録済みアプリとしてデプロイされます。
- App1はMicrosoft Entra認証を使用してstorage1にアクセスします。
- App2は、単一のMicrosoft Entra IDを使用してstorage1にアクセスします。
- App2は、VM1とVM2という名前の2つの新しい仮想マシン上でホストされます。

解決策は、管理上の負担を最小限に抑えるものでなければならない。

各アプリはストレージ1にアクセスするために、どのタイプのIDを使用しますか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

App1:

User-assigned managed identity

Microsoft Entra group account

Microsoft Entra user account

Service principal

System-assigned managed identity

App2:

User-assigned managed identity

Microsoft Entra group account

Microsoft Entra user account

Service principal

System-assigned managed identity

正解:



App1:

▼

User-assigned managed identity

Microsoft Entra group account

Microsoft Entra user account

Service principal

System-assigned managed identity

App2:

▼

User-assigned managed identity

Microsoft Entra group account

Microsoft Entra user account

Service principal

System-assigned managed identity

質問: 48

ホットスポットに関する質問

お客様はcontoso.comという名前のMicrosoft 365テナントをお持ちです。

ゲストユーザーによるアクセスが有効になっています。

以下の表に示すように、ユーザーはcontoso.comと連携して活動することができます。

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

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 ロラボレーションの制限」設定を構成します。

Collaboration restrictions

☐ Allow invitations to be sent to any domain (most inclusive)

☐ Deny invitations to the specified domains

☒ Allow invitations only to the specified domains (most restrictive)

Delete

☒ TARGET DOMAINS

☐ Outlook.com

Microsoft SharePoint Online サイトから、ユーザーが user3@adatum.com をサイトに招待します。

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements

Yes

No

User1 can accept the invitation and gain access to the enterprise application.	☐	☐
User2 can access the enterprise application.	☐	☐
User3 can accept the invitation and gain access to the SharePoint site.	☐	☐

正解:

Answer Area

Statements

Yes

No

User1 can accept the invitation and gain access to the enterprise application.	☒	☐
User2 can access the enterprise application.	☒	☐
User3 can accept the invitation and gain access to the SharePoint site.	☐	☒

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: 49
ホットスポットに関する質問

Sub1とSub2という名前の2つのAzureサブスクリプションがあり、これらはMicrosoft Entraテナントにリンクされています。このテナントには、Group1、Group2、Group3という名前の3つのグループが含まれています。購読プランには、以下の表に示すリソースが含まれています。

Name	Type	Subscription
VM1	Virtual machine	Sub1
VM2	Virtual machine	Sub2
Automation1	Azure Automation account	Sub2

テナントには、以下の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group2, Group3
User3	Group3

サブスクリプションの管理には、Microsoft Entra Permissions Management を使用します。Permissions Management は、次の表に示すように構成されます。

Name	Roles	Authorization System Name	Requestor for Other Identities
Group1	Viewer	Sub1	None
Group2	Controller	Sub2	User1
Group3	Approver	All Current and Future	None

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements

User1 can request access to VM2 by using Permissions Management.

User2 can create an access request to Automation1 on behalf of User1.

User3 can approve access requests for VM2.

Yes

No

正解:

Answer Area

Statements

User1 can request access to VM2 by using Permissions Management.

Yes

☐

No

☒

User2 can create an access request to Automation1 on behalf of User1.

☐☒

User3 can approve access requests for VM2.

☒☐

Explanation:

No - User1 is part of the group that can request access to sub1, not sub2 No - User1 can request access to Sub1 on behalf of other identities, not user2 Yes - User3's group can approve access requests for all subscriptions

質問: 50

お客様は、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をお持ちです。
あなたは、複数の仮想マシン上でホストされるApp1という名前のアプリをデプロイする予定です。これらの仮想マシンは、シークレットを使用してサードパーティのAPIに対して認証を行います。
仮想マシン向けの認証ソリューションを推奨する必要があります。そのソリューションは、以下の要件を満たす必要があります。
機密情報を安全に保管する。

- 認証情報をApp1のコードに保存する必要がないことを確認してください。
- 仮想マシンが Azure リソースにアクセスできることを確認するには、

Microsoft Entra認証

管理業務の手間を最小限に抑える。

推薦状には何を含めるべきでしょうか？

- A. ユーザーアカウントとストレージサービスの暗号化
- B. ユーザーが割り当てたマネージド ID と Azure Key Vault
- C. ユーザーアカウントとAzure Key Vault
- D. システム割り当て管理IDおよびストレージサービス暗号化

正解: (正解を表示します)

Azure Key Vault for the 3rd party API creds, and a user assigned managed identity for the MULTIPLE VMs to access "Azure resources by using Entra authentication".

質問: 51

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

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

あなたはMicrosoft 365テナントをお持ちです。

Microsoft 365 サービスにアクセスする際は、すべてのユーザーが Microsoft Authenticator アプリを使用して多要素認証 (MFA) を行う必要があります。

一部のユーザーから、サインイン要求を開始していないにもかかわらず、Microsoft Authenticatorアプリで多要素認証(MFA)のプロンプトが表示されたとの報告があった。

ユーザーが自ら開始していない多要素認証要求を報告した場合、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。

これは目標を達成していると言えるでしょうか？

- A. はい
- B. いいえ

正解: (正解を表示します)

You need to configure the fraud alert settings.

Fraud alert setting literally has an option to configure it to automatically block.

To enable and configure fraud alerts, complete the following steps:

1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>

質問: 52

Microsoft Entraテナントには、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が含まれています。Package1は、次の図に示すように構成されています。

The screenshot displays the configuration page for an Access Package in Microsoft Entra. The page is divided into two main sections: Expiration and Access Reviews. In the Expiration section, 'Access package assignments expire' is set to 'Number of days' with a value of 365. 'Users can request specific timeline' is set to 'Yes'. In the Access Reviews section, 'Require access reviews' is set to 'Yes', 'Starting on' is set to 25/01/2024, 'Review frequency' is set to 'Bi-annually', 'Duration (in days)' is set to 90 (with a maximum of 175), and 'Reviewers' is set to 'Self-review'.

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。解決策は最小権限の原則に基づいている必要があります。

User1にはどの役割を割り当てるべきですか？

A. 特権ロール管理者

- B. 外部IDプロバイダー管理者
- C. アイデンティティガバナンス管理者
- D. セキュリティ管理者

正解: ([正解を表示します](#))

Correct:

* Identity Governance Administrator

* User administrator

Check catalog for resources

If you need to add resources to an access package, you should check whether the resources you need are available in the access package's catalog. If you're an access package manager, you can't add resources to a catalog, even if you own them. You're restricted to using the resources available in the catalog.

Prerequisite role: Global administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager.

In the Azure portal, select Azure Active Directory and then select Identity Governance.

In the left menu, select Catalog and then open the catalog.

In the left menu, select Resources to see the list of resources in this catalog.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources>

質問: 53

User1 という名前のユーザーが Microsoft Defender for Cloud Apps ポータルにアクセスしようとする、エラー メッセージが表示されます。

エラーの原因を特定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。

何をすればいいのでしょうか？

- A. プロビジョニングログ
- B. ログ分析
- 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: 54

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

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

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

User1という名前のユーザーを作成します。

ユーザー1がIDセキュリティスコア改善アクションのステータスを更新できるようにする必要があります。

解決策 :ユーザー1にセキュリティオペレーターの役割を割り当てます。

これは目標を達成していると言えるでしょうか？

- A. はい
- B. いいえ

正解: ([正解を表示します](#))

With read and write access, you can make changes and directly interact with identity secure score.

Global administrator

Security administrator
Exchange administrator
SharePoint administrator
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score>

質問: 55
事例研究1 - Contoso, Ltd
概要

Contoso, Ltd.は、モントリオールに本社を置き、ロンドンとシアトルに支店を持つコンサルティング会社です。
ContosoはFabrikam, Inc.という会社と提携関係にある。Fabrikamはfabrikam.comという名前のAzure Active Directory(Azure AD)テナントを所有している。

既存環境。既存環境
Contosoのオンプレミスネットワークには、contoso.comという名前のActive Directoryドメインが含まれています。
このドメインには、Contoso_Resources という名前の組織単位 (OU) が含まれています。Contoso_Resources OU には、すべてのユーザーとコンピューターが含まれています。
contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

既存環境 :Microsoft 365/Azure環境
Contosoはcontoso.comという名前のAzure ADテナントを所有しており、それには以下のライセンスが関連付けられています。
* Microsoft Office 365 Enterprise E5
* エンタープライズモビリティ+セキュリティ
* Windows 10 Enterprise E3
* プロジェクト計画3

Azure AD Connectは、Azure ADとActive Directoryドメインサービス(AD DS)の間で構成されています。同期されるのはContoso_Resources OUのみです。
ヘルプデスク管理者は、ユーザー設定を管理するために日常的にMicrosoft 365管理センターを使用します。
現在、ユーザー管理者はMicrosoft 365管理センターを使用してライセンスを手動で割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。
* ロンドンオフィスのユーザーは、Microsoft 365 Phone Systemのライセンスが未割り当ての状態です。
シアトルオフィスのユーザーは、Yammer Enterpriseライセンスを未割り当ての状態です。

contoso.com では、セキュリティのデフォルト設定が無効になっています。
Contosoは、管理者ロールを保護するためにAzure ADの特権ID管理(PIM)を使用しています。

既存環境。問題点

コントソ氏は以下の問題点を指摘している。

* 現在、すべてのヘルプデスク管理者は、Microsoft 365テナント全体にわたるユーザーライセンスを管理できます。

* ユーザー管理者からは、Contosoの各オフィスごとに異なるライセンス要件を手動で設定するのは面倒だという報告が寄せられています。

ヘルプデスク管理者は、必要なMicrosoft 365サービスおよびアプリへの内部アクセスとゲストアクセスをプロビジョニングするのに時間をかけすぎている。

* 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。

* Azure AD で [ログ] ノードを選択すると、Log Analytics の統合が有効になっていないことを示すエラーメッセージが表示されます。

要件。計画されている変更

コントソ氏は以下の変更を実施する予定です。

* セルフサービスパスワードリセット(SSPR)を実装する。

* Azure Monitorを使用して、Azure監査アクティビティログを分析します。

* テナントに追加された新規ユーザーに対するライセンス割り当てを簡素化します。

* Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施する。

* ユーザー管理者ロールを設定し、有効化する際に正当性の説明と承認が必要となるようにします。

* App1という名前の、業務専用のカスタムAzure Webアプリを実装します。App1はインターネットからアクセス可能で、Azure ADアカウントを使用して認証されます。

* マーケティング部門の新規ユーザー向けに、Microsoft SharePoint Onlineのサイト、グループ、およびアプリへのアクセス権限を付与するための自動承認ワークフローを実装します。

Contoso社はAdatum Corporationという会社を買収する予定です。Adatumという名前のActive Directory組織単位(OU)内に、新たに100人のAdatumユーザーが作成されます。これらのユーザーはロンドンとシアトルに拠点を置く予定です。

要件。技術要件

Contoso社は、以下の技術要件を特定しました。

* すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期されている必要があります。

* App1 には、https://contoso.com/auth-response を指すリダイレクト URI が必要です。

* 新規ユーザーへのライセンス割り当ては、ユーザーの所在地に基づいて自動的に行われる必要があります。

* Fabrikamのユーザーは、マーケティング部門のSharePointサイトに最大90日間アクセスできる必要があります。

* Azure AD で実行される管理操作は監査対象とする必要があります。監査ログは 1 年間保持する必要があります。

* ヘルプデスク管理者は、それぞれのオフィスに所属するユーザーのライセンスのみを管理できる必要があります。

* ユーザーの身元が侵害された可能性がある場合、ユーザーにはパスワードの変更を強制しなければならない。

質問

技術要件を満たすためには、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。

その役割を担う上で、実行すべき2つの行動はどれですか？それぞれの正解は、解決策の一部を示しています。

注：正解ごとに1ポイントが加算されます。

A. 有効化時に正当化を要求するを選択します。

B. 有効化時にチケット情報を要求するを選択します。

C. 設定後に期限切れ対象割り当てを変更します。

D. すべての割り当てを適格に設定します。

E. すべての割り当てをアクティブに設定します。

正解: ([正解を表示します](#))

Scenario: Configure the User administrator role to require justification and approval to activate.

Require justification.

You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the Require justification on activation box.

To require justification need assignment to be Eligible instead of Active.

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

質問: 56

ユーザー「User1」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にはどの役割を割り当てるべきですか？

- A. ヘルプデスク管理者
- B. 請求管理者
- C. ライセンス管理者
- D. ユーザー管理者

正解: (正解を表示します)
Only User Access Admin fits in both the requirement : manage license assignments and reset user passwords.

質問: 57

あなたはMicrosoft 365のサブスクリプションをお持ちです。
ユーザーがMicrosoft EdgeからMicrosoft 365ポータルにアクセスし、ブラウザの言語設定がスペイン語になっている場合、スペイン語のサインインフォームが表示されるようにする必要があります。
Microsoft Entraの管理センターでは、どのような操作を行うべきですか？

- A. ユーザー設定から、使用場所設定を構成します。
- B. グローバルセキュアアクセスから、セッション管理設定を構成します。
- C. 会社のブランディング設定を構成します。
- D. 条件付きアクセスポリシー.mdletを作成します。

正解: (正解を表示します)
Configure your company branding
Language customization
Customize the sign-in experience based on browser language when users authenticate into your corporate intranet or web-based applications.
Customize the sign-in experience by browser language
You can create a personalized sign-in experience for users who sign in using a specific browser language by customizing the branding elements for that browser language. This customization overrides any configurations made to the default branding. If you don't make any changes to the elements, the default elements are displayed.
1. Sign in to the Microsoft Entra admin center as an Organizational Branding Administrator.
2. Browse to Identity > User experiences > Company branding.
3. Select Add browser language.

Reference:
<https://learn.microsoft.com/en-us/entra/fundamentals/how-to-customize-branding>

質問: 58

ホットスポットに関する質問
お客様は、Set1とSet2という名前の2つの属性セットを含むMicrosoft 365 E5サブスクリプションを所有しています。
このサブスクリプションには、以下の表に示すユーザーが含まれています。

Name	Microsoft Role
User1	Global Administrator
User2	Global Administrator
User3	Attribute Assignment Administrator

以下の表に示すカスタムセキュリティ属性が利用可能です。

Name	Attribute set
Secure1	Set1
Secure2	Set1
Secure3	Set2

あなたはUser2にSet1の属性定義管理者ロールを割り当てます。
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can modify the configuration of Secure1.	☐	☐
User2 can view the value of Secure2 for all users.	☐	☐
User3 can view the value of Secure3 for all users.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 can modify the configuration of Secure1.	☐	☒
User2 can view the value of Secure2 for all users.	☐	☒
User3 can view the value of Secure3 for all users.	☒	☐

Explanation:
Box 1: No
User1 is Global Administrator.
By default, Global Administrator and other administrator roles do not have permissions to read, define, or assign custom security attributes.
Note: The roles that apply to configuration sets are:

Attribute Definition Administrator
Attribute Assignment Administrator
Attribute Definition Reader
Attribute Assignment Reader

Box 2: No

User2 is Attribute Definition Administrator.

Attribute Definition Administrator

Users with this role can define a valid set of custom security attributes that can be assigned to supported Microsoft Entra objects. This role can also activate and deactivate custom security attributes.

Box 3: Yes

User3 is Attribute assignment Administrator.

Attribute Assignment Administrator

Users with this role can assign and remove custom security attribute keys and values for supported Microsoft Entra objects such as users, service principals, and devices.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

質問: 59

ホットスポットに関する質問

Sub1という名前のAzureサブスクリプションをお持ちです。

Sub1の管理には、Microsoft Entra Permissions Managementを使用する予定です。

権限管理が以下のタスクを実行できることを確認する必要があります。

- アプリケーションに割り当てられ、管理されている未使用の権限を特定します。

アイデンティティ。

- ユーザーに、削除すべき権限に関する推奨事項を提供する。

未使用の権限を削除します。

解決策は最小権限の原則に従わなければならない。

権限管理のサービスプリンシパルにはどの役割を割り当て、推奨事項を提供したり、使用されていない権限を削除したりするには何を使用すべきでしょうか？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：正解ごとに1ポイントが加算されます。

Answer Area

Role:

▼

Access Review Operator Service Role

Owner

Reader

User Access Administrator

Use:

▼

A custom report

A role template

An audit query

An Autopilot rule

正解:

Answer Area



Role:

Access Review Operator Service Role

Owner

Reader

User Access Administrator

Use:

A custom report

A role template

An audit query

An Autopilot rule

質問: 60

ホットスポットに関する質問

Sub1 という名前の Azure サブスクリプションがあり、その中に storage1 と storage2 という名前の 2 つのストレージ アカウントと、次の表に示す BLOB コンテナが含まれています。

Name	In storage account	Contains blob named
cont1	storage1	blob1
cont2	storage1	blob2
cont1	storage2	blob3

Sub1には、以下の表に示すユーザーが含まれています。

Name	Role	Scope	Role assignment condition
User1	Reader	Sub1	Not applicable
	Storage Blob Data Reader	Sub1	Condition1
User2	Reader	Sub1	Not applicable
	Storage Blob Data Owner	storage1	Condition2

Condition1の定義は以下のとおりです。

```

(
  (
    !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'})
  )
  OR
  (
    @Resource[Microsoft.Storage/storageAccounts/blobServices/containers:name] StringEquals 'cont1'
  )
)

```

Condition2 has the following definition:

```

(
  (
    !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write'})
  )
  OR
  (
    @Resource[Microsoft.Storage/storageAccounts/blobServices/containers/blobs:path] StringLike '*2*'
  )
)

```

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements

Yes

No

User1 can read the contents of blob2.

☐
☐

User1 can read the contents of blob3.

☐
☐

User2 can read the contents of blob1.

☐
☐

正解:

Answer Area

Statements

YesNo

User1 can read the contents of blob2.

☐☒

User1 can read the contents of blob3.

☒☐

User2 can read the contents of blob1.

☒☐

Explanation:
Box 1: No
User1 has the Reader role. Does not apply to the blob container.
User1 also has the Storage Blob Data Reader with Condition1.
Blob2 is in Cont2.
Condition1 will be false:
The action is ..blob/reads
Resource name is cont2 not cont1
Note: Storage Blob Data Reader
Read and list Azure Storage containers and blobs.
Box 2: Yes
Blob3 is in cont1. Condition1 will be true.
Box 3: Yes
User2 has the Reader role. Does not apply to the blob container.
User2 also has the Storage Blob Data Owner Role with Condition2.
blob1 is in cont1
Condition2 will be true, as the action is read, not a write.

質問: 61
事例研究2 - Litware, Inc.
概要

Litware, Inc.は、Fabrikam, Inc.という子会社を持つ製薬会社です。
Litwareはボストンとシアトルにオフィスを構えているが、従業員は全米各地に分散している。
従業員はVPN接続を利用して、どちらのオフィスにもリモートで接続します。
既存環境。環境を特定する
このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect はパ
ススルー認証を使用しており、パスワードハッシュの同期は無効になっています。

Litware.comには、すべてのアプリケーション開発を監督するUser1というユーザーが存在します。

LitwareはAzure ADアプリケーションプロキシを実装しています。

Fabrikam社は、fabrikam.comという名前のAzure ADテナントを所有しています。Fabrikam社のユーザーは、litware.comテナント内のゲストアカウントを使用して、litware.comのリソースにアクセスします。

既存環境。クラウド環境

Litwareの全ユーザーはMicrosoft 365 Enterprise E5ライセンスを保有しています。Microsoft Cloud App Securityに組み込まれている異常検知ポリシーはすべて有効になっています。

Litwareは、litware.com Azure ADテナントに関連付けられたAzureサブスクリプションを保有しています。このサブスクリプションには、Azure Active DirectoryコネクタとOffice 365コネクタを使用するAzure Sentinelインスタンスが含まれています。Azure Sentinelは現在、Azure ADのサインインログと監査ログを収集しています。

既存環境。オンプレミス環境

オンプレミスネットワークには、次の表に示すサーバーが含まれています。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litwareの2つのオフィスはどちらもインターネットに直接接続されています。両オフィスとも、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのドメインコントローラーはすべてインターネットへのアクセスが制限されています。

要件。委任要件

Litwareは、以下の委任要件を特定しています。

- * Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
- * litware.com Azure AD テナントに、権限のないユーザーがアプリケーションを登録できないようにします。
- * アイデンティティガバナンスには、カスタムカタログとカスタムプログラムを使用する。
- * User1がAzure ADでエンタープライズアプリケーションを作成できることを確認します。

最小権限の原則を適用する。

要件。ライセンス要件

Litwareは最近、litware.com Active DirectoryフォレストにLWLicensesという名前のカスタムユーザー属性を追加しました。Litwareは、LWLicenses属性の値を変更することでAzure ADライセンスの割り当てを管理したいと考えています。LWLicensesに適切な値を持つユーザーは、適切なライセンスが割り当てられているMicrosoft 365グループに自動的に追加される必要があります。

要件。管理要件

Litwareは、LWGroup1という名前のグループを作成したいと考えています。このグループには、LitwareのすべてのAzure ADユーザーアカウントが含まれますが、すべてのAzure ADゲストアカウントは除外されます。

要件。認証要件

Litwareは、以下の認証要件を定めています。

- * すべてのLitwareユーザーに対して多要素認証(MFA)を実装する。
- * LitwareのボストンオフィスからAzure ADへの認証を行う際に、ユーザーがMFAを使用する必要があるようにする。
- * litware.com フォレストに対して、禁止パスワードリストを実装する。

オンプレミスアプリケーションへのアクセス時に多要素認証(MFA)を強制する。

- * 外部に漏洩した認証情報を自動的に検出し、修復します。

要件。アクセス要件

Litwareは、以下のアクセス要件を定めています。

条件付きアクセス ポリシーを使用して、すべての Azure リソースおよび Azure AD アプリケーションへのアクセスを制御します。

- * Microsoft SharePoint Online のセッション制御を含む条件付きアクセス ポリシーを実装します。

* Azure AD のアクセス レビューを使用して、アプリケーションへの特権アクセスを制御します。

要件。監視要件

Litware社は、Azure SentinelのFusionルールを使用して、疑わしいAzure ADサインインとその後の異常なMicrosoft Office 365アクティビティの組み合わせを含む、複数段階の攻撃を検出したいと考えています。

ホットスポットに関する質問

認証要件を満たすためには、パスワード制限を実装する必要があります。

DC1にAzure ADパスワード保護DCエージェントをインストールします。

次に何をすべきでしょうか？回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Configure the Azure AD Password Protection proxy service on:

DC1
SERVER1
SERVER2

Configure the password list:

In Azure AD
On DC1
On SERVER1
On SERVER2

正解:

Configure the Azure AD Password Protection proxy service on:

▼

DC1
SERVER1
SERVER2

Configure the password list:

▼

In Azure AD
On DC1
On SERVER1
On SERVER2

Explanation:

Box 1: Server 2

Box 2: In Azure AD

The password protection proxy is installed on a member server. You enable the banned p/w list in Azure AD, the proxy downloads it and passes it to the DCs in the domain.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 385問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 62

お客様は、以下の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントをお持ちです。

Name	Member of
User1	Group1
User2	Group2
User3	Group3

テナントは、以下の表に示す認証方法を使用できます。

Method	Target	Enabled
FIDO2	Group2	Yes
Microsoft Authenticator app	Group1	Yes
SMS	Group3	Yes

どのユーザーが、アプリに表示される番号と自分の携帯電話に表示される番号を照合することで、クラウドアプリにサインインするのでしょうか？

- A. ユーザー1のみ
- B. ユーザー2のみ
- C. ユーザー3のみ
- D. ユーザー1とユーザー2のみ
- E. ユーザー2とユーザー3のみ

正解: [\(正解を表示します\)](#)

Microsoft Authenticator

You can also allow your employee's phone to become a passwordless authentication method.

You may already be using the Authenticator app as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.

The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.

Users can sign in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.

FIDO2 security keys

The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.

FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources without a username or password using an external security key or a platform key built into a device.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

質問: 63

VM1 という名前の仮想マシンと 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。VM1 には、システムによって割り当てられたマネージド ID があります。VM1 が Vault 1 に保存されているシークレットの値を取得できることを確認する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。まず何をすべきでしょうか？

- A. Vault1 のリソース アクセス設定を構成します。
- B. Azure ロールを VM1 に割り当てます。
- C. Vault1 の権限モデルを構成します
- D. ユーザー割り当てのマネージド ID を VM1 に追加します。

正解: [\(正解を表示します\)](#)

質問: 64

シミュレーション

アクセスパッケージの割り当てを通じてテナントに追加された外部ユーザーのセキュリティを設定しています。

アクセス パッケージの割り当てを使用して外部ユーザーがテナントに追加された場合、アクセス パッケージがユーザーから解除されてから 15 日後に、そのユーザーがテナントから自動的に削除されるようにする必要があります。

正解:

To automatically delete external guest users 15 days after they lose their last access package assignment, you need to configure the global entitlement management settings in the admin portal.

Follow these steps using the Microsoft Entra admin center:

Step 1: Sign in and Navigate: Log in to the Microsoft Entra admin center as at least an Identity Governance Administrator.

Step 2: Access Governance Settings: In the left navigation menu, expand Identity Governance, then expand Entitlement management, and select Settings (or Control configurations depending on your portal theme updates).

Step 3: Locate Lifecycle Settings: Look for the Lifecycle of external users card and click Edit (or View settings).

Step 4: Configure Account Removal: Locate the Remove external user setting and set it to Yes.

Step 5: Set the Retention Period: In the field labeled Number of days before removing external user from this directory, enter 15.

Step 6: Save Changes: Click Save at the bottom of the page to apply the policy.

Reference:

[https://microsoftlearning.github.io/SC-300-Identity-and-Access-Administrator/Instructions/Labs/Lab_24_ManageTheLifecycleOfExternalUsersInAADIdentityGove rnanceSettings%20.html](https://microsoftlearning.github.io/SC-300-Identity-and-Access-Administrator/Instructions/Labs/Lab_24_ManageTheLifecycleOfExternalUsersInAADIdentityGovernanceSettings%20.html)

質問: 65

ユーザー「User1」と、リソースグループ「RG1」および「RG2」を含むAzureサブスクリプションをお持ちです。

User1が以下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てください。

- RG1領域のみに仮想マシンを作成する。
- RG1にのみストレージアカウントを作成してください。

ロールベースアクセス制御(RBAC)において、最低限必要なロール割り当て数はいくつですか？

- A. 1
 - B. 2
 - C. 3
 - D. 4
- 正解: (正解を表示します)
- Assign User1 the "Reader" role at the subscription level to view all resources.
- Assign User1 the "Virtual Machine Contributor" role at the RG1 level to restart virtual machines and create virtual machines in RG1 only.
- Assign User1 the "Storage Account Contributor" role at the RG1 level to create storage accounts in RG1 only.

質問: 66

事例研究2 - Litware, Inc.

概要

Litware, Inc.は、Fabrikam, Inc.という子会社を持つ製薬会社です。

Litwareはボストンとシアトルにオフィスを構えているが、従業員は全米各地に分散している。

従業員はVPN接続を利用して、どちらのオフィスにもリモートで接続します。

既存環境。環境を特定する

このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect はパ
ススルー認証を使用しており、パスワードハッシュの同期は無効になっています。

Litware.comには、すべてのアプリケーション開発を監督するUser1というユーザーが存在します。

LitwareはAzure ADアプリケーションプロキシを実装しています。

Fabrikam社は、fabrikam.comという名前のAzure ADテナントを所有しています。Fabrikam社のユーザーは、litware.comテナント内のゲストアカウントを使用して、litware.comのリソースにアクセスします。

既存環境。クラウド環境

Litwareの全ユーザーはMicrosoft 365 Enterprise E5ライセンスを保有しています。Microsoft Cloud App Securityに組み込まれている異常検知ポリシーはすべて有効になっています。

Litwareは、litware.com Azure ADテナントに関連付けられたAzureサブスクリプションを保有しています。このサブスクリプションには、Azure Active DirectoryコネクタとOffice 365コネクタを使用するAzure Sentinelイン
スタンスが含まれています。Azure Sentinelは現在、Azure ADのサインインログと監査ログを収集しています。

既存環境。オンプレミス環境

オンプレミスネットワークには、次の表に示すサーバーが含まれています。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litwareの2つのオフィスはどちらもインターネットに直接接続されています。両オフィスとも、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのドメインコ
ントローラーはすべてインターネットへのアクセスが制限されています。

要件。委任要件

Litwareは、以下の委任要件を特定しています。

- * Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
- * litware.com Azure AD テナントに、権限のないユーザーがアプリケーションを登録できないようにします。
- * アイデンティティガバナンスには、カスタムカタログとカスタムプログラムを使用する。
- * User1がAzure ADでエンタープライズアプリケーションを作成できることを確認します。

最小権限の原則を適用する。

要件。ライセンス要件

Litwareは最近、litware.com Active DirectoryフォレストにLWLicensesという名前のカスタムユーザー属性を追加しました。Litwareは、LWLicenses属性の値を変更することでAzure ADライセンスの割り当てを管理したい
と考えています。LWLicensesに適切な値を持つユーザーは、適切なライセンスが割り当てられているMicrosoft 365グループに自動的に追加される必要があります。

要件。管理要件

Litwareは、LWGroup1という名前のグループを作成したいと考えています。このグループには、LitwareのすべてのAzure ADユーザーアカウントが含まれますが、すべてのAzure ADゲストアカウントは除外されます。

要件。認証要件

Litwareは、以下の認証要件を定めています。

- * すべてのLitwareユーザーに対して多要素認証(MFA)を実装する。
- * LitwareのボストンオフィスからAzure ADへの認証を行う際に、ユーザーがMFAを使用する必要があるようにする。
- * litware.com フォレストに対して、禁止パスワードリストを実装する。

オンプレミスアプリケーションへのアクセス時に多要素認証(MFA)を強制する。

- * 外部に漏洩した認証情報を自動的に検出し、修復します。

要件。アクセス要件

Litwareは、以下のアクセス要件を定めています。

条件付きアクセス ポリシーを使用して、すべての Azure リソースおよび Azure AD アプリケーションへのアクセスを制御します。

* Microsoft SharePoint Online のセッション制御を含む条件付きアクセス ポリシーを実装します。

* Azure AD のアクセス レビューを使用して、アプリケーションへの特権アクセスを制御します。

要件。監視要件

Litware社は、Azure SentinelのFusionルールを使用して、疑わしいAzure ADサインインとその後の異常なMicrosoft Office 365アクティビティの組み合わせを含む、複数段階の攻撃を検出したいと考えています。

ホットスポットに関する質問

管理要件を満たすためには、LWGroup1グループを作成する必要があります。

動的メンバーシップルールはどのように設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

(user.objectId -ne

"Guest"
"Member"
Null

) and (user.userType - eq

"Guest"
"Member"
Null

)

正解:

Answer Area

(user.objectId -ne

"Guest"
Member
Null

) and (user.userType - eq

"Guest"
"Member"
Null

)

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups#creating-a-group-of-members-only>

質問: 67

ドラッグアンドドロップ問題

あなたは、User1とUser2という名前の2人のユーザーを含むMicrosoft 365 E5サブスクリプションを所有しています。

ユーザー1がグループのアクセスレビューを作成できること、およびユーザー2が完了したすべてのアクセスレビューの履歴レポートを確認できることを保証する必要があります。このソリューションは、最小権限の原則に基づいている必要があります。

各ユーザーにどの役割を割り当てるべきでしょうか？回答するには、適切な役割を正しいユーザーにドラッグしてください。各役割は、1回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注：正解ごとに1ポイントが加算されます。

Roles

Global administrator

Global reader

Reports reader

Security operator

Security reader

User administrator

Answer Area

User1:

Role

User2:



正解:

Roles

Global administrator

Global reader

Reports reader

Security operator

Answer Area

User1:

User administrator

User2:

Security reader



Explanation:

User 1: User Administrator

Create, update, or delete access review of a group or of an app User Administrator.

User 2: Security Reader

Read access review of an Azure AD role Security Reader.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews#what-resource-types-can-be-reviewed>

質問: 68

ホットスポットに関する質問

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、その中に All Company という名前のグループがあり、以下の ID ガバナンス設定が適用されています。

- 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: はい

- 外部ユーザーを削除します。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: 30
- 2022年3月11日に、以下の設定を持つPackage1という名前のアクセスパッケージを作成します。
- リソースルール
1. 名称 : 全企業
 2. タイプ :グループとチーム
 3. 役割 :メンバー
- ライフサイクル
1. アクセスパッケージの割り当て期限 : 日付
 2. 課題提出期限 2022年4月1日
- 2022年3月1日、あなたは以下の表に示すゲストユーザーにPackage1を割り当てます。

Name	Email address
Guest1	guest1@outlook.com
Guest2	guest2@outlook.com

2022年3月2日、あなたはGuest1にレポート閲覧者の役割を割り当てます。

2022年4月1日、あなたはGuest3という名前のゲストユーザーをcontoso.comに招待します。

2022年4月4日に、Guest3を全社グループに追加します。

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

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	☐	☐
On May 5, 2022, the Guest2 account is in contoso.com.	☐	☐
On May 5, 2022, the Guest3 account is in contoso.com.	☐	☐

正解:

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	☐	☒
On May 5, 2022, the Guest2 account is in contoso.com.	☐	☒
On May 5, 2022, the Guest3 account is in contoso.com.	☒	☐

Explanation:

Box 1: No

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 2: No

On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 3: Yes

Note: Lifecycle

On the Lifecycle tab, you specify when a user's assignment to the access package expires. You can also specify whether users can extend their assignments.

In the Expiration section, set Access package assignments expires to On date, Number of days, Number of hours, or Never.

For On date, select an expiration date in the future.

For Number of days, specify a number between 0 and 3660 days.

For Number of hours, specify a number of hours.

Based on your selection, a user's assignment to the access package expires on a certain date, a certain number of days after they are approved, or never.

Note 2: By default, when an external user no longer has any access package assignments, they are blocked from signing in to your directory. After 30 days, their guest user account is removed from your directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-lifecycle-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

質問: 69

お客様は、Microsoft Entra Permissions Management にオンボーディングされた Microsoft 365 サブスクリプションをお持ちです。

権限が割り当てられている管理対象IDを特定し、90日間使用されていない権限を削除する必要があります。このソリューションは、管理作業を最小限に抑えるものでなければなりません。

Entraの権限管理ポータルでは、どのような操作を行うべきですか？

- A. オートパイロットルールを設定します。
- B. 権限分析レポートをスケジュールします。
- C. Microsoft Entra Insights から、特権ロールが割り当てられているサービス プリンシパルを確認します。
- D. 監査クエリを実行します。

正解: A (コメントを發表する)

Microsoft Entra Permissions Management includes an Autopilot feature that allows you to create prebuilt or custom rules to automatically remediate permissions based on usage patterns, including removing unused

permissions after a specified period such as 90 days.

The Remediation tab in the Permissions Management portal supports Autopilot rules to automate right-sizing of permissions, reducing manual effort.

質問: 70

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

Name	Role
Admin1	Global Administrator
Admin2	Conditional Access Administrator
Admin3	Authentication Policy Administrator
Admin4	Global Administrator

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. Admin1、Admin2、Admin3のみ
- B. Admin2とAdmin3のみ
- C. Admin1とAdmin4のみ
- D. 管理者1、管理者2、管理者3、および管理者4

正解: D (コメントを發表する)

質問: 71

シミュレーション

Microsoft Entraテナントには、fabrikam.comドメインのユーザーのみが招待されるように設定する必要があります。

- 正解:
- To restrict external invitations to a specific domain, you must configure the Collaboration restrictions allowlist within the Microsoft Entra admin center.
- Step 1: Sign in to the Microsoft Entra admin center using an account with at least Global Administrator privileges.
- Step 2: Navigate through the left-hand sidebar menu: Identity > External Identities > External collaboration settings.
- Step 3: Scroll down to locate the Collaboration restrictions section near the bottom of the page.
- Step 4: Select the radio button labeled "Allow invitations only to the specified domains (most restrictive)".
- Step 5: Target the domain: Under the Target domains input field, type the exact domain name you want to allow. [Enter fabrikam.com] Note: If you need to include multiple domains, type each one on a new line.
- Step 6: Apply changes by clicking the Save button at either the top or bottom of the page.

Reference:

<https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list>

質問: 72

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

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

あなたはMicrosoft 365テナントをお持ちです。

Microsoft 365 サービスにアクセスする際は、すべてのユーザーが Microsoft Authenticator アプリを使用して多要素認証 (MFA) を行う必要があります。

一部のユーザーから、サインイン要求を開始していないにもかかわらず、Microsoft Authenticatorアプリで多要素認証(MFA)のプロンプトが表示されたとの報告があった。

ユーザーが自ら開始していない多要素認証要求を報告した場合、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。

これは目標を達成していると言えるでしょうか？

- A. はい
- B. いいえ

正解: ([正解を表示します](#))

You need to configure the fraud alert settings.

Fraud alert setting literally has an option to configure it to automatically block.

To enable and configure fraud alerts, complete the following steps:

1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>

質問: 73

Microsoft Entraテナントをお持ちです。このテナントにFacebookソーシャルIDプロバイダーを追加する必要があります。最初に何をすべきですか？

- A. カスタムドメインを追加する
- B. WS-Fed IDプロバイダーを追加します。
- C. SAML IDプロバイダーを追加します。
- D. ユーザーフローによるゲストセルフサービスサインアップを有効にする設定を 「はい」に設定します。

正解: ([正解を表示します](#))

Add Facebook as an identity provider for External ID

You can add Facebook to your self-service sign-up user flows so that users can sign in to your applications using their own Facebook accounts. To allow users to sign in using Facebook, you first need to enable self-service sign-up for your tenant. After you add Facebook as an identity provider, set up a user flow for the application and select Facebook as one of the sign-in options.

After you add Facebook as one of your application's sign-in options, on the Sign in page, a user can enter the email they use to sign in to Facebook, or they can select Sign-in options and choose Sign in with Facebook. In either case, they're redirected to the Facebook sign in page for authentication.



Reference:

<https://learn.microsoft.com/en-us/entra/external-id/facebook-federation>

質問: 74

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、Microsoft Azure 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](#))

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

質問: 75
ホットスポットに関する質問

お客様のAzure ADテナントには、以下の表に示すユーザーが含まれています。

Name	User risk level
User1	Low
User2	Medium
User3	High

以下の表に示すAzure AD ID保護ポリシーが適用されます。

Type	Users	User risk	Sign-in risk	Controls
User risk policy	All users	Low and above	Unconfigured	Block access
Sign-in risk policy	All users	Unconfigured	High	Block access

RiskyユーザーレポートとRisky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。

User	Action
User1	Confirm user compromised
User2	Confirm sign-in safe
User3	Dismiss user risk
User2	Confirm user compromised

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

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	☐	☐
User2 can sign in by using multi-factor authentication (MFA).	☐	☐
User3 can sign in from an anonymous IP address.	☐	☐

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	☐	☒
User2 can sign in by using multi-factor authentication (MFA).	☐	☒
User3 can sign in from an anonymous IP address.	☒	☐

Explanation:

Box 1: No

Blocked access prevents self-remediation through password resets & Azure AD MFA.

Box 3: No

Blocked access prevents self-remediation through password resets & Azure AD MFA Box 3: Yes Anonymous IP address sign-in risk is Medium.

質問: 76

ホットスポットに関する質問

お客様のMicrosoft Entraテナントには、以下の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

お客様のユーザーリスクポリシーには、以下の設定が含まれています。

- * 課題:
 - o 含める: グループ1
 - 除外対象: グループ2
- * ログインリスク：中程度以上
- * 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

ユーザーがログインしようとする、以下の表に示すように、ユーザーのリスクレベルが検出されます。

User	Risk level
User1	High
User2	Medium
User3	High

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	☐	☐
User2 must change their password during sign in.	☐	☐
User3 must change their password during sign in.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	☒	☐
User2 must change their password during sign in.	☐	☒
User3 must change their password during sign in.	☐	☒

有効的な**SC-300J**問題集はJPNTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-300J**試験問題集を提供します。JPNTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> **385**問、**30%ディスカウント**、特別な割引コード：**JPNshiken**」

質問: 77

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

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

あなたはMicrosoft 365テナントをお持ちです。

Microsoft 365 サービスにアクセスする際は、すべてのユーザーが Microsoft Authenticator アプリを使用して多要素認証 (MFA) を行う必要があります。

一部のユーザーから、サインイン要求を開始していないにもかかわらず、Microsoft Authenticatorアプリで多要素認証(MFA)のプロンプトが表示されたとの報告があった。

ユーザーが自ら開始していない多要素認証要求を報告した場合、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 Active Directory 管理センターから、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。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解: **B** ([コメントを发表する](#))

Report suspicious activity and the legacy Fraud Alert implementation can operate in parallel. You can keep your tenant-wide Fraud Alert functionality in place while you start to use Report suspicious activity with a targeted test group.

If Fraud Alert is enabled with Automatic Blocking, and Report suspicious activity is enabled, the user will be added to the blocklist and set as high-risk and in-scope for any other policies configured. These users will need to be removed from the blocklist and have their risk remediated to enable them to sign in with MFA.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#report-suspicious-activity-and-fraud-alert>

質問: 78

ホットスポットに関する質問

お客様は、以下の表に示すユーザーを含むハイブリッド型の Microsoft 365 サブスクリプションをご利用になっています。

Name	Role
Admin1	Global Administrator
Admin2	Application Administrator
Admin3	Cloud Application Administrator
Admin4	Application Developer
User1	None  Microsoft

App1という名前のオンプレミスアプリをデプロイする予定です。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は、最小権限の原則に従う必要があります。

どのユーザーがインストールを実行すべきか、また、User1にはどの役割を割り当てるべきか。回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

User that should perform the installation:

Admin1

Admin2

Admin3

Admin4

 Microsoft

Assign User1 the role of:

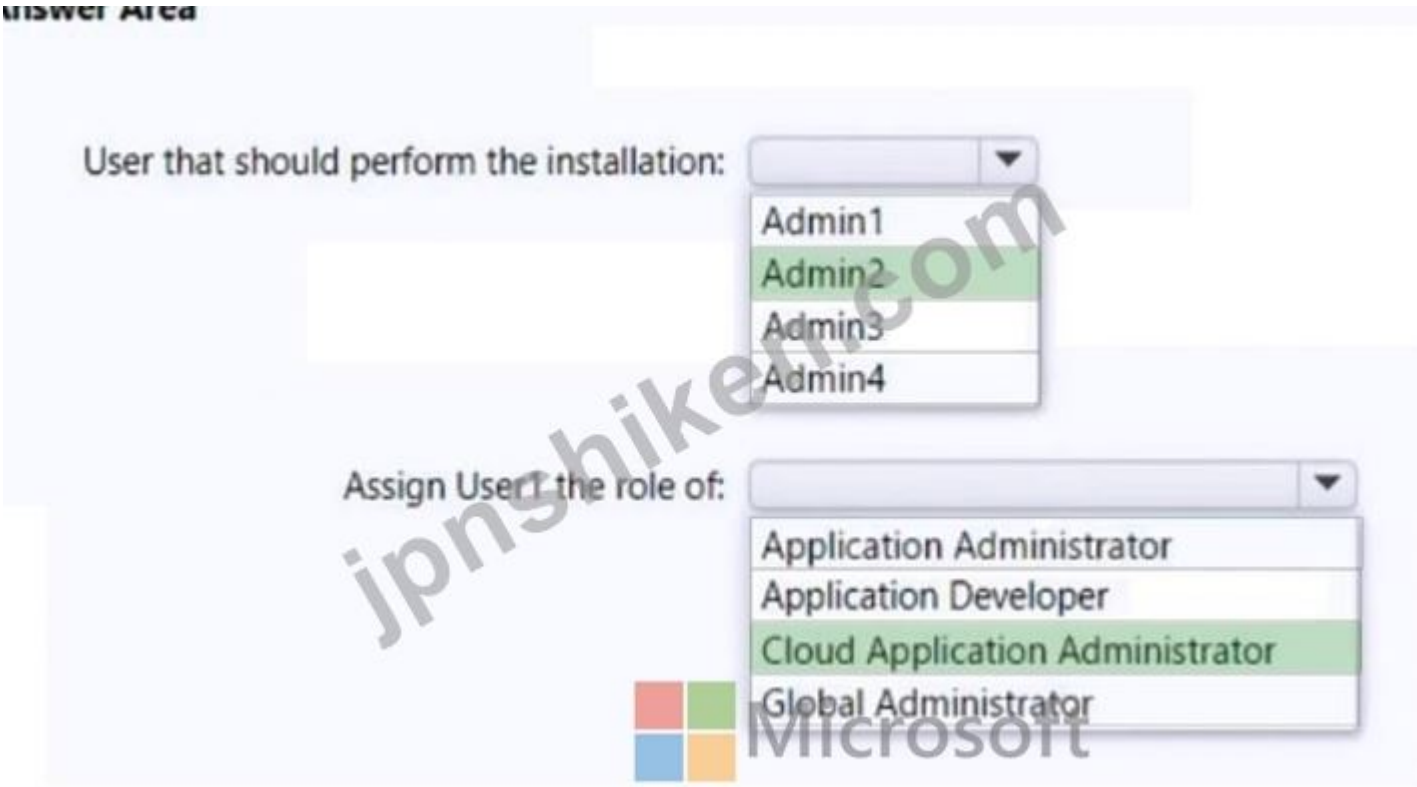
Application Administrator

Application Developer

Cloud Application Administrator

Global Administrator

正解:



質問: 79

ホットスポットに関する質問

お客様は、以下の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントをお持ちです。

Name	User type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

Azure AD で「職位」プロパティと「使用場所」プロパティを設定できるユーザーはどれですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Job title property:

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

Usage location property:

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

正解:

Job title property:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Usage location property:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Explanation:

Box 1: User2 and User3 only

Job title property for directory synched users cannot be updated from Azure AD.

Box 2: User1, User2, and User3

Invite users with Azure Active Directory B2B collaboration, Update user's name and usage location.

To assign a license, the invited user's Usage location must be specified. Admins can update the invited user's profile on the Azure portal.

- 1. Go to Azure Active Directory > Users and groups > All users. If you don't see the newly created user, refresh the page.
- 2. Click on the invited user, and then click Profile.
- 3. Update First name, Last name, and Usage location.
- 4. Click Save, and then close the Profile blade.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal>

質問: 80

ホットスポットに関する質問

contoso.com という名前の Microsoft Entra テナントがあり、その中に Group1 という名前のグループがあります。

グループ1には、貴社のIT部門のユーザー50名と、経理部門のユーザー50名が含まれています。

貴社には、fabrikam.com という名前の Microsoft Entra テナントを持つパートナー企業があります。

contoso.comとfabrikam.comの間で、テナント間の同期を設定します。

Group1のメンバーをfabrikam.comに同期する必要があります。ソリューションは以下の要件を満たす必要があります。

- IT部門のユーザーのみがfabrikam.comと同期するようにしてください。

管理業務の手間を最小限に抑える。

テナント間同期の設定では、どのような操作を行うべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

For the configuration object:

From Expression builder, build an expression.
From Provision on demand, add Group1.
From Users and groups, add Group1.
From Users and groups, add the IT department users

For the configuration object from Settings:

Add a scoping filter
Add new attribute mappings
Modify the attribute mappings

正解:

Answer Area

For the configuration object:

 Microsoft

From Expression builder, build an expression.
From Provision on demand, add Group1.
From Users and groups, add Group1.
From Users and groups, add the IT department users

For the configuration object from Settings:

Add a scoping filter
Add new attribute mappings
Modify the attribute mappings

質問: 81

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。テナントには、App1 という名前の登録済みアプリが含まれています。Microsoft Entra テナントを持つパートナー組織があります。テナントには、App2 という名前の登録済みアプリが含まれています。App1 が App2 にアクセスできることを確認する必要があります。

App1 が使用できる資格情報は 2 種類あります。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. マネージド ID
- B. ユーザーアカウント
- C. ワンタイムパスワード
- D. 証明書
- E. 秘密

正解: ([正解を表示します](#))

質問: 82

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: C ([コメントを發表する](#))

You can target a group with a conditional policy to detect and remediate the login at the end of each month.

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

質問: 83

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

ユーザーは、サードパーティのクラウドアプリが自身のデータにアクセスすることを承認します。

アプリが高い権限を必要とし、かつ20人以上のユーザーによって承認されている場合にトリガーされるアラートを設定する必要があります。

Microsoft Defender for Cloud Appsでは、どのタイプのポリシーを作成すべきですか？

- A. アプリ発見ポリシー
- B. アクセスポリシー
- C. OAuthアプリポリシー
- D. 活動方針

正解: ([正解を表示します](#))

Correct:

* OAuth app policy

You can create an OAuth app policy in the Microsoft Defender for Cloud Apps portal (now part of App Governance within Defender XDR) to generate alerts when an app requests high permissions and is authorized by a specified number of users, such as over 20, helping you detect potentially risky, overprivileged apps. These policies allow you to monitor, block, or flag apps based on permission levels (high, medium, low), publisher status, and user authorization count, enabling proactive security management.

Incorrect:

* access policy

* activity policy

* anomaly detection policy

* app discovery policy

Reference:
<https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

質問: 84

ホットスポットに関する質問

Azure サブスクリプションには、Group1 という名前のグループと、User1 および User2 という名前の 2 人のユーザーが含まれています。User1 は Group1 のメンバーです。
App1という名前のエンタープライズアプリケーションを登録します。

App1のセルフサービスアプリケーションアクセスを有効にし、以下の設定を構成します。

- ユーザーがこのアプリケーションへのアクセスを要求することを許可する: はい
- 割り当てられたユーザーをどのグループに追加しますか: グループ1
- このアプリケーションへのアクセスを許可する前に承認を要求する :はい
- このアプリケーションへのアクセスを承認できるのは誰ですか: User2

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements

Yes No

User1 must request access to App1 before they can use the app.

☐ ☐

If User2 requests access to App1, they will be added to Group1 automatically.

☐ ☐

User2 can approve App1 requests by using the Microsoft Entra admin center.

☐ ☐

正解:

Answer Area

Statements

Yes No

User1 must request access to App1 before they can use the app.

☒ ☐

If User2 requests access to App1, they will be added to Group1 automatically.

☐ ☒

User2 can approve App1 requests by using the Microsoft Entra admin center.

☒ ☐

Explanation:

Box 1: Yes

Box 2: No

Being allowed to approve access to an application in Azure self-service application access does not automatically assign you to the application's group. While you can configure an application to have a specific group assigned to it upon approval, the approver themselves is not automatically added to that group.

Box 3: Yes

For self-service application access in Azure, approvers utilize the Microsoft Entra admin center to review and make decisions on access requests. Specifically, approvers can access the "My Access" portal within the Microsoft Entra admin center to view pending requests and either approve or deny them.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-self-service-access>

質問: 85

ホットスポットに関する質問

あなたは、Group1とGroup2という名前の2つのグループを含むMicrosoft 365 E5サブスクリプションを所有しています。このサブスクリプションには、以下の表に示すユーザーが含まれています。

Name	Member of	Role
User1	Group1	None
User2	Group2	Global Administrator
User3	Group1, Group2	None

以下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

除外対象: グループ2

対象リソース:

o 含まれるもの: すべてのクラウドアプリ

付与 :

o アクセスを許可する: 多要素認証を要求する

セッション :

o ブラウザセッションの永続性: 永続化しない

名前: ポリシー2

ユーザー:

o 含める:

- ディレクトリの役割: グローバル管理者

- ユーザーとグループ: User3

除外対象: グループ2

対象リソース:

o 含まれるもの: すべてのクラウドアプリ

セッション :

o ログイン頻度 :

定期認証 2時間ごと

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Microsoft

Statements

User1 will be prompted for the Stay signed in option when they sign in to the Microsoft 365 portal.

User2 must reauthenticate to Microsoft 365 Apps every two hours.

User3 must reauthenticate to Microsoft 365 Apps every two hours.

Yes

No

☐

☐

☐

☐

☐

☐

正解:

Answer Area

Microsoft

Statements

User1 will be prompted for the Stay signed in option when they sign in to the Microsoft 365 portal.

User2 must reauthenticate to Microsoft 365 Apps every two hours.

User3 must reauthenticate to Microsoft 365 Apps every two hours.

Yes

No

☒

☐

☐

☒

☐

☒

質問: 86

ホットスポットに関する質問

Microsoft Entraテナントには、RemoteNetwork1とRemoteNetwork2という名前の2つのリモートネットワークと、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group1
User3	Group2

お客様は以下の表に示す機器をお持ちです。

Name	Global Secure Access client	User	Connected to
Device1	Deployed	User1	RemoteNetwork1
Device2	Not deployed	User2	RemoteNetwork1
Device3	Deployed	User3	RemoteNetwork2

条件付きアクセス ポリシーに以下の設定があります。

* 名前: CAPolicy1

* 課題

- ユーザー: グループ1、グループ2

- 対象リソース: Global Secure が有効なすべてのインターネットリソース

アクセス

* アクセス制御

- 許可：多要素認証を要求する

* ポリシーを有効にする: オン

グローバルセキュアアクセス(GSAA)のトラフィック転送は、以下の図に示すように構成されます。

...

Remote network

Traffic forwarding

...

Traffic forwarding

...

Refresh

Got feedback?

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward users running the Global Secure Access client. For cli

Learn more

One or more profiles are configured and ready to

Microsoft traffic profile

Enabled

Last modified on 01/09/2025, 03:54 PM

Applies to

Internet traffic to Microsoft services

Microsoft traffic policies

4 policies

View

Linked Conditional Access policies

1 policy

View

User and group assignments

0 users, 1 groups assigned

View

Remote network assignments

1 assigned remote networks

Edit

Edit an assignment (Microsoft traffic profile)

Traffic profile

Add assignments

Name	Assignment type
RemoteNetwork1	Remote networks

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
When User1 signs in to Microsoft Exchange Online, the user will be prompted for multifactor authentication (MFA).	☐	☐
When User2 signs in to Microsoft SharePoint Online, the user will be prompted for multifactor authentication (MFA).	☐	☐
When User3 signs in to Microsoft Exchange Online, the user will be prompted for multifactor authentication (MFA).	☐	☐

正解:

Answer Area



Microsoft

Yes

No

When User1 signs in to Microsoft Exchange Online, the user will be prompted for multifactor authentication (MFA).

☒☐

When User2 signs in to Microsoft SharePoint Online, the user will be prompted for multifactor authentication (MFA).

☒☐

When User3 signs in to Microsoft Exchange Online, the user will be prompted for multifactor authentication (MFA).

☐☒

質問: 87

ホットスポットに関する質問

お客様は、以下の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントをお持ちです。

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

以下の表に示す場所が利用可能です。

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

テナントには、以下の構成を持つ名前付きロケーションが含まれています。

* 名前: 場所1

* 信頼できる場所としてマーク: 有効

IPv4範囲: 10.10.0.0/16 -

MFAの信頼できるIPアドレス範囲は193.17.17.0/24です。

* 名前: CAPolicy1

* 課題

- ユーザーまたはワークロードの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

- 付与

- アクセスを許可する: 多要素認証を要求する

- セッション: 0個のコントロールが選択されました

* ポリシーを有効にする: オン

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

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	☐	☐
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	☐	☐
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	☐	☐

正解:

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	☐	☒
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	☒	☐
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	☐	☒

Explanation:

Box 1: No

User1 will not be prompted for MFA because user not in CA scope and MFA is disabled.

Box 2: Yes

User2's source IP is 10.10.1.160, the public IP of which is in the range of 20.93.15.0/24, which isn't a trusted MFA range. Besides, User2 is a per-user MFA-enforced user. Therefore, User2 will be prompted for MFA.

Box 3: No

The public IP address of 192.168.1.20 is in the space of 193.17.17.0/24, which is an MFA-trusted IP range. Although user2 is a per-user MFA-enforced user, it won't be prompted for MFA.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

質問: 88

展示に示されているように、Azure Active Directory (Azure AD) パスワード保護を構成します。 [展示] タブをクリックします。)

Custom smart lockout

Lockout threshold ⓘ

5

✓

Lockout duration in seconds ⓘ

3600

✓

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

Contoso

Litware

Tailwind project

Zettabyte

MainStreet

✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Microsoft

Enforced

Audit

次のパスワードを評価しています。

Pr0jectlitw @ re
T @ ilw1nd
C0nt0s0

どのパスワードがブロックされますか？

A. Pr0jectlitw @reおよびT @ ilw1ndのみ
B. C0nt0s0のみ
C. C0nt0s0、Pr0jectlitw @ re、およびT @ ilw1nd
D. C0nt0s0およびT @ ilw1ndのみ
E. C0nt0s0およびPr0jectlitw @reのみ

正解: ([正解を表示します](#))

After normalization we have :

- Pr0jectlitw@re - > projectlitware = 2 points
- T@ilw1nd -> tailwind =1 point
- C0nt0s0 -> contoso = 1 point

You need 5 points therefore everything is blocked.

質問: 89

新しい Microsoft 365 E5 テナントを作成します。

ユーザーが匿名 IP アドレスから Microsoft 365 ポータルに接続するときに、多要素認証 (MFA) を使用するように求められることを確認する必要があります。

何を設定する必要がありますか？

- A. サインイン リスク ポリシー
- B. ユーザー リスク ポリシー
- C. MFA 登録ポリシー

正解: (正解を表示します)

Examples for Sign-In Risk:

- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray

質問: 90

ホットスポットに関する質問

お客様のAzure Active Directory(Azure AD)テナントには、次の表に示すユーザーが含まれています。

Name	Role
User1	None
User2	Privileged authentication administrator
User3	Global administrator

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。

 Edit

Setting	State
Activation maximum duration (hours)	1 hour(s)
vRequire justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

ユーザー1はグローバル管理者ロールの資格を有しています。
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Microsoft

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role.	☐	☐
User2 must approve all activation requests for the Global administrator role.	☐	☐
User2 and User3 can edit the Global administrator role assignment.	☐	☐

正解:

Answer Area

Microsoft

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role.	☒	☐
User2 must approve all activation requests for the Global administrator role.	☐	☒
User2 and User3 can edit the Global administrator role assignment.	☐	☒

Explanation:
Box 1: Yes
MFA is required on activation

Box 2: No

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Box 3: No

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

質問: 91

Azure ADテナントをお持ちです。

ログイン失敗回数10回をロックアウトのしきい値とするスマートロックアウト機能を実装する必要があります。

Azure AD 管理センターでは、どのような設定を行うべきですか？

A. 認証の強み

B. パスワード保護

C. ユーザーリスクポリシー

D. サインインリスクポリシー

正解: B (コメントを发表する)

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values>

有効的な**SC-300J**問題集はJPNTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-300J**試験問題集を提供します。JPNTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 385問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 92

ホットスポットに関する質問

お客様には、contoso.com と fabrikam.com という名前の 2 つの Microsoft Entra テナントがあります。

Contoso.comには、以下の表に示すユーザーが含まれています。

Name	Type
User1	Member
User2	Member
User3	Guest

Contoso.comには、以下の表に示すグループが含まれています。

Name	Membership type	Members
Group1	Assigned	User1
Group2	Assigned	Group1, User2

contoso.com から fabrikam.com へのテナント間同期を設定し、User3 と Group2 のテナント間同期を有効にします。

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

注：正解ごとに1ポイントが加算されます。

Answer Area Microsoft

Statements	Yes	No
User1 will sync to fabrikam.com.	☐	☐
User2 will sync to fabrikam.com.	☐	☐
User3 will sync to fabrikam.com.	☐	☐

正解:

Answer Area Microsoft

Statements	Yes	No
User1 will sync to fabrikam.com.	☐	☒
User2 will sync to fabrikam.com.	☒	☐
User3 will sync to fabrikam.com.	☒	☐

質問: 93

ホットスポットに関する質問

Server1という名前のオンプレミスサーバーがあり、そこでWindows Serverが稼働しています。

Microsoft Entraテナントには、App1という名前のアプリ登録が含まれています。App1には、Microsoft Graphアプリケーションのアクセス許可が付与されています。

App1をサポートするように環境を構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。

- App1は社内ネットワークからのみアクセス可能である必要があります。
- App1の認証情報は、平文で保存してはなりません。
- Server1 上の非対話型スケジュール タスクは、

App1への認証を行います。

どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area



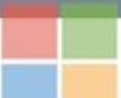
- An authentication method
- A Conditional Access policy
- A Microsoft Entra application proxy
- A permission classification

Configure scheduled tasks on Server1 to authenticate by using a:

- Certificate
- Client secret
- System-assigned managed identity
- User-assigned managed identity

正解:

Answer Area



In the tenant configure:

An authentication method

A Conditional Access policy

A Microsoft Entra application proxy

A permission classification

Configure scheduled tasks on Server1 to authenticate by using a:

Certificate

Client secret

System-assigned managed identity

User-assigned managed identity

Explanation:

Box 1: A Conditional Access policy

To restrict access to a Microsoft Entra app registration with Microsoft Graph application permissions to only the corporate network, Conditional Access policies are used. These policies allow administrators to define rules based on various conditions, including network location, to control access to resources.

Box 2: User-assigned managed identity

It is possible to use a managed identity to configure non-interactive scheduled tasks on an on- premises server to authenticate with an application that has Microsoft Graph application permissions within a Microsoft Entra tenant. This involves leveraging a user-assigned managed identity, granting it the necessary permissions to access Microsoft Graph, and then configuring the scheduled task to utilize that identity for authentication.

Reference:

<https://learn.microsoft.com/en-us/graph/migrate-azure-ad-graph-configure-permissions>

<https://docs.azure.cn/en-us/app-service/configure-authentication-provider-aad>

あなたはAzureサブスクリプションをお持ちです。
あなたは、企業向けソフトウェア・アズ・ア・サービス(SaaS)アプリケーションを評価しています。
アプリがAzure AD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べきでしょうか？

- A. OAuth 2.0
 - B. WS-Fed
 - C. SCIM 2.0
 - D. LDAP 3
- 正解: C (コメントを發表する)

https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning

質問: 95
App1という名前のオンプレミスアプリケーションがあります。
お客様はMicrosoft Entraテナントをお持ちです。
あなたはMicrosoft Entra Private Accessを使用してApp1を公開する予定です。
プライベートアクセス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. リモートネットワーク
 - B. 交通転送
 - C. セキュリティプロファイル
 - D. コネクタ
- 正解: (正解を表示します)

Enable the Private Access traffic forwarding profile
Browse to Global Secure Access > Connect > Traffic forwarding. Select the checkbox for Private Access profile.

質問: 96
ドラッグアンドドロップ問題
お客様のネットワークには、Microsoft Entra Connectを使用してMicrosoft Entra IDと同期する、contoso.comという名前のオンプレミスActive Directoryドメインが含まれています。このドメインには、次の表に示すユーザーが含まれています。

Name	User principal name (UPN)	Proxy address
User1	user1@contoso.com	smtp: user1@contoso.com smtp: sales@contoso.com
User2	user2@contoso.com	smtp: user2@contoso.com smtp: user.2@contoso.com smtp: service@contoso.com

Active Directoryユーザーとコンピューターから、次のユーザーを追加します。
- 名前: User3
- UPN: user3@contoso.com
- プロキシアドレス: smtp: user3@contoso.com、smtp: sales@contoso.com
Active Directoryユーザーとコンピューターから、次の表に示すように、各ユーザーのproxyAddresses属性を更新します。

Name	Proxy address
User1	smtp: admin@contoso.com
User2	smtp: sales@contoso.com

手動同期を実行します。

Microsoft Entra Connectの同期では、各ユーザーに対してどの同期ステータスが返されますか？回答するには、適切なステータスを正しいユーザーにドラッグしてください。各ステータスは、1回、複数回、またはまったく使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注：正解ごとに1ポイントが加算されます。

Microsoft

ipnshiken.com

Statures

AttributeValueMustBeUnique error occurs

InvalidSoftMatch error occurs.

ObjectTypeMismatch error occurs.

Successfully synced

Answer Area

User1@contoso.com

User2@contoso.com

User3@contoso.com

正解:

Statuses

ObjectTypeMismatch error occurs .



Answer Area

User1@contoso.com

Successfully synced

User2@contoso.com

AttributeValueMustBeUnique error occurs

User3@contoso.com

InvalidSoftMatch error occurs .

質問: 97

事例研究1 - Contoso, Ltd

概要

Contoso, Ltd.は、モントリオールに本社を置き、ロンドンとシアトルに支店を持つコンサルティング会社です。

ContosoはFabrikam, Inc.という会社と提携関係にある。Fabrikamはfabrikam.comという名前のAzure Active Directory(Azure AD)テナントを所有している。

既存環境。既存環境

Contosoのオンプレミスネットワークには、contoso.comという名前のActive Directoryドメインが含まれています。

このドメインには、Contoso_Resources という名前の組織単位 (OU) が含まれています。Contoso_Resources OU には、すべてのユーザーとコンピューターが含まれています。

contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

既存環境 :Microsoft 365/Azure環境

Contosoはcontoso.comという名前のAzure ADテナントを所有しており、それには以下のライセンスが関連付けられています。

* Microsoft Office 365 Enterprise E5

- * エンタープライズモビリティ+セキュリティ
- * Windows 10 Enterprise E3
- * プロジェクト計画3

Azure AD Connectは、Azure ADとActive Directoryドメインサービス(AD DS)の間で構成されています。同期されるのはContoso_Resources OUのみです。

ヘルプデスク管理者は、ユーザー設定を管理するために日常的にMicrosoft 365管理センターを使用します。

現在、ユーザー管理者はMicrosoft 365管理センターを使用してライセンスを手動で割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。

- * ロンドンオフィスのユーザーは、Microsoft 365 Phone Systemのライセンスが未割り当ての状態です。

シアトルオフィスのユーザーは、Yammer Enterpriseライセンスを未割り当ての状態です。

contoso.com では、セキュリティのデフォルト設定が無効になっています。

Contosoは、管理者ロールを保護するためにAzure ADの特権ID管理(PIM)を使用しています。

既存環境。問題点

コントソ氏は以下の問題点を指摘している。

- * 現在、すべてのヘルプデスク管理者は、Microsoft 365テナント全体にわたるユーザーライセンスを管理できます。

- * ユーザー管理者からは、Contosoの各オフィスごとに異なるライセンス要件を手動で設定するのは面倒だという報告が寄せられています。

ヘルプデスク管理者は、必要なMicrosoft 365サービスおよびアプリへの内部アクセスとゲストアクセスをプロビジョニングするのに時間をかけすぎている。

- * 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。

- * Azure AD で [ログ] ノードを選択すると、Log Analytics の統合が有効になっていないことを示すエラーメッセージが表示されます。

要件。計画されている変更

コントソ氏は以下の変更を実施する予定です。

- * セルフサービスパスワードリセット(SSPR)を実装する。

- * Azure Monitorを使用して、Azure監査アクティビティログを分析します。

- * テナントに追加された新規ユーザーに対するライセンス割り当てを簡素化します。

- * Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施する。

- * ユーザー管理者ロールを設定し、有効化する際に正当性の説明と承認が必要となるようにします。

- * App1という名前の、業務専用のカスタムAzure Webアプリを実装します。App1はインターネットからアクセス可能で、Azure ADアカウントを使用して認証されます。

- * マーケティング部門の新規ユーザー向けに、Microsoft SharePoint Onlineのサイト、グループ、およびアプリへのアクセス権限を付与するための自動承認ワークフローを実装します。

Contoso社はAdatum Corporationという会社を買収する予定です。Adatumという名前のActive Directory組織単位(OU)内に、新たに100人のAdatumユーザーが作成されます。これらのユーザーはロンドンとシアトルに拠点を置く予定です。

要件。技術要件

Contoso社は、以下の技術要件を特定しました。

- * すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期されている必要があります。

- * App1 には、https://contoso.com/auth-response を指すリダイレクト URI が必要です。

- * 新規ユーザーへのライセンス割り当ては、ユーザーの所在地に基づいて自動的に行われる必要があります。

- * Fabrikamのユーザーは、マーケティング部門のSharePointサイトに最大90日間アクセスできる必要があります。

- * Azure AD で実行される管理操作は監査対象とする必要があります。監査ログは 1 年間保持する必要があります。

- * ヘルプデスク管理者は、それぞれのオフィスに所属するユーザーのライセンスのみを管理する必要があります。

- * ユーザーの身元が侵害された可能性がある場合、ユーザーにはパスワードの変更を強制しなければならない。

質問

ホットスポットに関する質問

ヘルプデスク管理者によるライセンス管理には、技術要件を満たす必要があります。
最初に何を作成すべきか、そしてどのツールを使用すべきか？回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Object to create for each branch office:

An administrative unit

A custom role

A Dynamic User security group

An OU

Tool to use:

Azure Active Directory admin center

Active Directory Administrative Center

Active Directory module for Windows PowerShell

Microsoft 365 admin center

正解:

Answer Area

Object to create for each branch office:

An administrative unit

A custom role

A Dynamic User security group

An OU

Tool to use:

Azure Active Directory admin center

Active Directory Administrative Center

Active Directory module for Windows PowerShell

Microsoft 365 admin center

Explanation: <https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units> Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.

質問: 98

ホットスポットに関する質問

contoso.com という名前の Microsoft Entra テナントがあり、その中に AU1 という名前の管理単位と、User1 および User2 という名前の 2 人のユーザーがいます。User1 は AU1 のメンバーです。

以下の役割割り当てを実行する必要があります。

- ユーザー1: セキュリティ管理者
- ユーザー2: ユーザー管理者

各ユーザーには、どの範囲で役割を割り当てることができますか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

User1:

AU1 only

contoso.com only

AU1 and contoso.com

User2:

AU1 only

contoso.com only

AU1 and contoso.com

正解:

Answer Area

User1:

AU1 only

contoso.com only

AU1 and contoso.com

User2:

AU1 only

contoso.com only

AU1 and contoso.com

質問: 99

ホットスポットに関する質問

セキュリティの既定値が無効になっている Azure Active Directory (Azure AD) テナントをお持ちです。
次の図に示すように、条件付きアクセス ポリシーを作成します。

New

Conditional access policy

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

Name *

Policy1 ✓

Assignments

Users and groups ⓘ>

Specific users included

Cloud apps or actions ⓘ>

All cloud apps

Conditions ⓘ>

0 conditions selected

Access controls

Grant ⓘ>

0 controls selected

Session ⓘ>

0 controls selected

Enable policy

Report-only On Off

Create

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. [Learn more](#)

Include Exclude

☐ None

☐ All users

☒ Select users and groups

☐ All guest users (preview) ⓘ

☐ Directory roles (preview) ⓘ

☒ Users and groups

Select ⓘ>

1 user

US User1

user1@sk200922outlook.onm...

...

図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

Conditions settings

Enable policy setting

Grant settings

Sessions settings

Users and groups setting

正解:

Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

Conditions settings

Enable policy setting

Grant settings

Sessions settings

Users and groups setting

Explanation:

Create a Conditional Access policy

1. Under Access controls > Grant, select Grant access, Require multi-factor authentication, and select Select.
2. Confirm your settings and set Enable policy to On.
3. Select Create to create to enable your policy.

Sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

Reference:

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

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

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#sign-in-frequency>

質問: 100

ホットスポットに関する質問

お客様は、Team1 という名前の Microsoft Teams チームと、Group1 および Group2 という名前の 2 つの Microsoft 365 グループを含む Microsoft 365 E5 サブスクリプションを所有しています。このサブスクリプションには、次の表に示すユーザーが含まれています。

Name	Member of	Role
User1	Group1	None
User2	Group2	None
User3	Group1	Global Administrator

以下の設定を持つアクセスパッケージを作成します。

名前: パッケージ1

リソースの役割:

o チーム1 :オーナー

アクセスをリクエストできるユーザー: ディレクトリ内のユーザー

o 特定のユーザーとグループ: グループ1

承認が必要 :はい

o 申請者の正当性の説明を求める :いいえ

o ステージ数 :1

o 最初の承認者: チーム1、ユーザー3

承認者の正当化を求める :はい

新しいリクエストを有効にする: はい

有効期限:

アクセスパッケージの割り当ては7日間で期限切れとなります。

o ユーザーは特定のタイムラインをリクエストできます: はい

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can gain access to Team1 by requesting Package1.	☐	☐
User2 can gain access to Team1 by requesting Package1.	☐	☐
User3 can approve their own request for Package1.	☐	☐

Answer Area

Microsoft

Statements

Yes

No

User1 can gain access to Team1 by requesting Package1.

User2 can gain access to Team1 by requesting Package1.

User3 can approve their own request for Package1.

質問: 101

ホットスポットに関する質問

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、その中に User1 という名前のユーザーが存在します。
ユーザー1は、以下の表に示すデバイスを所有しています。

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

2020年11月5日、あなたはcontoso.comで以下の設定を含む利用規約を作成し、施行しました。

- 名前: 用語1
- 表示名: Contoso利用規約
- ユーザーに利用規約の展開を要求する:
- すべてのデバイスでユーザーに同意を求める: オン
- 同意の期限切れ:

有効期限開始日 2020年12月10日

頻度：月回

2020年11月15日、ユーザー1はデバイス3上で利用規約1に同意しました。

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Microsoft

Statements

Yes

No

On November 20, 2020, User1 can accept Terms1 on Device1.

On December 11, 2020, User1 can accept Terms1 on Device2.

On December 7, 2020, User1 can accept Terms1 on Device3.

正解:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	☒	☐
On December 11, 2020, User1 can accept Terms1 on Device2.	☒	☐
On December 7, 2020, User1 can accept Terms1 on Device3.	☐	☒

Explanation:

Box 1: Yes

Because User1 has not yet accepted the terms on Device1.

Box 2: Yes

Because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.

Box 3: No

Because User1 has already accepted the terms on Device3. The terms do not expire until December 10th and then monthly after that.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

質問: 102

ホットスポットに関する質問

既定のアプリ登録設定が設定された Azure Active Directory (Azure AD) テナントがあります。このテナントには、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

あなたはApp1とApp2という名前の2つのクラウドアプリを購入します。グローバル管理者はApp1をAzure ADに登録します。

ユーザーをApp1に割り当てることができるユーザーと、App2をAzure ADに登録できるユーザーを特定する必要があります。

何を特定すべきでしょうか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Can assign users to App1:

Admin1 only

Admin3 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3 only

Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

Admin1 only

Admin3 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3 only

Admin1, Admin2, Admin3, and User1

正解:

Answer Area

Can assign users to App1:

Admin1 only

Admin3 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3 only

Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

Admin1 only

Admin3 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3 only

Admin1, Admin2, Admin3, and User1

Explanation:

Only administrators (Admin1 - Application Administrator & Admin3 - Cloud application administrator) can manage/configure apps.

Name: Cloud application administrator

Description: Users in this role can add, manage, and configure enterprise applications, app registrations but will not be able to configure or manage on-premises like app proxy.

Azure AD - User settings - App registration: default is Yes (If this option is set to yes, then non- admin users may register custom-developed applications for use within this directory.)

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

Azure ADテナントをお持ちです。

ユーザーが認証済みの発行元からのアプリに同意できるように、ユーザー同意設定を構成します。

ユーザーが、影響の少ない権限を必要とするアプリにのみ同意できるようにする必要があります。

あなたはどうすべきでしょうか？

- A. エンタープライズアプリケーションコレクションを作成します。
- B. アクセスレビューを作成します。
- C. アクセスパッケージを作成します。
- D. 権限分類を設定します。

正解: D (コメントを發表する)

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-permission-classifications?pivots=portal

質問: 104

貴社は現在、業務手順全体を見直し、効率化を図る方法を模索しています。懸念事項の一つとして、ヘルプデスク管理者がユーザーの問題対応に費やす時間の長さが挙げられます。ヘルプデスク管理者への問い合わせ件数やチケット発行件数を削減するために、どのようなサービスを導入できますか？

- A. アプリケーションプロキシ
- B. 多要素認証
- C. Active Directory Connect
- D. セルフサービスパスワードリセット

正解: (正解を表示します)

Self Service Password Reset would provide users to reset their own passwords when they forget their current password or they are locked out of the system. They would no longer need to contact the Help Desk for these actions thus reducing Help Desk utilization.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

質問: 105

ホットスポットに関する質問

お客様には、contoso.com と fabrikam.com という名前の 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。

Name	Department	Job title	City	Member of
User1	IT	Support	Vancouver	Group1
User2	IT	Technician	Madrid	None
User3	HR	Consultant	Montreal	Group1

contoso.com から fabrikam.com へのテナント間同期は、以下の設定を使用して構成します。

- ユーザーとグループ: グループ1
- プロビジョニングモード：自動
- 属性マッピング
- ソースオブジェクトのスコープ: Filter1、Filter2

Filter1は、以下の表に示すように構成されています。

Source attribute	Operator	Clause value
department	EQUALS	IT
jobTitle	PRESENT	Not applicable

Filter2は、以下の表に示すように構成されています。

Source attribute	Operator	Clause value
city	INCLUDES	M

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 syncs to fabrikam.com.	☐	☐
User2 syncs to fabrikam.com.	☐	☐
User3 syncs to fabrikam.com.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 syncs to fabrikam.com.	☐	☒
User2 syncs to fabrikam.com.	☒	☐
User3 syncs to fabrikam.com.	☐	☒

Explanation:

Box 1: No

User1 is in IT department and has the job title support. Filter1 matches.

User1 is in city Vancouner, which does not have a letter M. Filter2 does not match.

User1 is not synced.

Note:

Both filter must match.

Filter1 matches if department is IT, and there is jobTitle value.

Filter2 matches any city that has the letter M in it.

In Microsoft Entra Connect Sync, the "PRESENT" operator in scoping filters specifies that the attribute must exist with any value, even if it's empty or null. This is different from EQUALS, which requires a specific value, or NOT EQUALS, which excludes a specific value. The PRESENT operator is used to ensure that an attribute exists in the object being synchronized, regardless of its actual value.

Box 2: Yes

User2 is in IT department and has the job title technician. Filter1 matches.

User2 is in city Madrid, which does not have a letter M. Filter2 matches.

User2 syncs.

Box 3: No

User3 is in HR department, so Filter1 will not match.

User3 will not sync.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering>

質問: 106

事例研究1 - Contoso, Ltd

概要

Contoso, Ltd.は、モントリオールに本社を置き、ロンドンとシアトルに支店を持つコンサルティング会社です。

ContosoはFabrikam, Inc.という会社と提携関係にある。Fabrikamはfabrikam.comという名前のAzure Active Directory(Azure AD)テナントを所有している。

既存環境。既存環境

Contosoのオンプレミスネットワークには、contoso.comという名前のActive Directoryドメインが含まれています。

このドメインには、Contoso_Resources という名前の組織単位 (OU) が含まれています。Contoso_Resources OU には、すべてのユーザーとコンピューターが含まれています。

contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

既存環境 :Microsoft 365/Azure環境

Contosoはcontoso.comという名前のAzure ADテナントを所有しており、それには以下のライセンスが関連付けられています。

- * Microsoft Office 365 Enterprise E5
- * エンタープライズモビリティ+セキュリティ
- * Windows 10 Enterprise E3
- * プロジェクト計画3

Azure AD Connectは、Azure ADとActive Directoryドメインサービス(AD DS)の間で構成されています。同期されるのはContoso_Resources OUのみです。

ヘルプデスク管理者は、ユーザー設定を管理するために日常的にMicrosoft 365管理センターを使用します。

現在、ユーザー管理者はMicrosoft 365管理センターを使用してライセンスを手動で割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。

- * ロンドンオフィスのユーザーは、Microsoft 365 Phone Systemのライセンスが未割り当ての状態です。

シアトルオフィスのユーザーは、Yammer Enterpriseライセンスを未割り当ての状態です。

contoso.com では、セキュリティのデフォルト設定が無効になっています。

Contosoは、管理者ロールを保護するためにAzure ADの特権ID管理(PIM)を使用しています。

既存環境。問題点

コントソ氏は以下の問題点を指摘している。

- * 現在、すべてのヘルプデスク管理者は、Microsoft 365テナント全体にわたるユーザーライセンスを管理できます。
 - * ユーザー管理者からは、Contosoの各オフィスごとに異なるライセンス要件を手動で設定するのは面倒だという報告が寄せられています。
- ヘルプデスク管理者は、必要なMicrosoft 365サービスおよびアプリへの内部アクセスとゲストアクセスをプロビジョニングするのに時間をかけすぎている。
- * 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。

* Azure AD で [ログ] ノードを選択すると、Log Analytics の統合が有効になっていないことを示すエラーメッセージが表示されます。

要件。計画されている変更

コントソ氏は以下の変更を実施する予定です。

* セルフサービスパスワードリセット(SSPR)を実装する。

* Azure Monitorを使用して、Azure監査アクティビティログを分析します。

* テナントに追加された新規ユーザーに対するライセンス割り当てを簡素化します。

* Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施する。

* ユーザー管理者ロールを設定し、有効化する際に正当性の説明と承認が必要となるようにします。

* App1という名前の、業務専用のカスタムAzure Webアプリを実装します。App1はインターネットからアクセス可能で、Azure ADアカウントを使用して認証されます。

* マーケティング部門の新規ユーザー向けに、Microsoft SharePoint Onlineのサイト、グループ、およびアプリへのアクセス権限を付与するための自動承認ワークフローを実装します。

Contoso社はAdatum Corporationという会社を買収する予定です。Adatumという名前のActive Directory組織単位(OU)内に、新たに100人のAdatumユーザーが作成されます。これらのユーザーはロンドンとシアトルに拠点を置く予定です。

要件。技術要件

Contoso社は、以下の技術要件を特定しました。

* すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期されている必要があります。

* App1 には、https://contoso.com/auth-response を指すリダイレクト URI が必要です。

* 新規ユーザーへのライセンス割り当ては、ユーザーの所在地に基づいて自動的に行われる必要があります。

* Fabrikamのユーザーは、マーケティング部門のSharePointサイトに最大90日間アクセスできる必要があります。

* Azure AD で実行される管理操作は監査対象とする必要があります。監査ログは 1 年間保持する必要があります。

* ヘルプデスク管理者は、それぞれのオフィスに所属するユーザーのライセンスのみを管理できる必要があります。

* ユーザーの身元が侵害された可能性がある場合、ユーザーにはパスワードの変更を強制しなければならない。

Log Analyticsワークスペースを作成します。

監査に必要な技術要件を実装する必要があります。

Azure ADでは何を構成すべきですか？

A. 企業ブランディング

B. 診断設定

C. 外部アイデンティティ

D. アプリ登録

正解: **B** ([コメントを发表する](#))

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/design-logs-deployment>

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-logging-monitoring>

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> **885**問、**3 0 %ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **107**

ホットスポットに関する質問

あなたはAzureサブスクリプションをお持ちです。

Role1とRole2という名前の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、アプリケーションセキュリティグループを管理できます。
- ロール2が割り当てられたユーザーは、Azure Firewallを管理できます。

各役割に必要なリソースプロバイダーの権限はどれですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Role1:

Microsoft.App

Microsoft.Computer

Microsoft.Network

Microsoft.Security

Role2:

Microsoft.App

Microsoft.Management

Microsoft.Network

Microsoft.Security

正解:

Answer Area

Role1:

Microsoft.App

Microsoft.Computer

Microsoft.Network

Microsoft.Security

Role2:

Microsoft.App

Microsoft.Management

Microsoft.Network

Microsoft.Security

Explanation:
<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork>

ホットスポットに関する質問

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、以下の図に示すように構成されています。

Save

Discard

Delete

Got feedback?

Enabled for users to sign-in?

Yes

No

Name

App1

Homepage URL

https://app1.m365x629615.onmicrosoft.com/

Logo

AP

User access URL

https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...

Application ID

09df58d6-d29d-40de-b0d0-321fdc63c665

Object ID

03709d22-7e61-4007-a2a0-04dbdff269cd

Terms of Service Url

Publisher did not provide this information

Privacy Statement Url

Publisher did not provide this information

Reply Url

https://contoso.com/App1/login

User assignment required?

Yes

No

Visible to users?

Yes

No

図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

[answer choice] can access App1 from the homepage URL.

All users

No one

Only users listed on the Owners blade

Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

all users

no one

only users listed on the Owners blade

only users listed on the Users and groups blade

正解:

Answer Area

[answer choice] can access App1 from the homepage URL.

All users

No one

Only users listed on the Owners blade

Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

all users

no one

only users listed on the Owners blade

only users listed on the Users and groups blade

Explanation:

Box 1: All users

"Enable for users to sign-in" is selected and "User assignment required" is set to No. Any user can login using the app url.

Box 2: Only users listed on the users and groups blade

User assignment required - This option does not affect whether or not an application appears on My Apps. To show the application there, assign an appropriate user or group to the application.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-configure>

ホットスポットに関する質問

お客様は、以下の表に示すリソースを含む Azure サブスクリプションをお持ちです。

Name	Type
User1	User
User2	User
Vault1	Azure Key Vault

Vault1へのアクセスを設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。

- User1がVault1でキーを管理および作成できることを確認します。
- User2がVault1に保存されている証明書にアクセスできることを確認してください。

最小権限の原則を適用する。

各ユーザーにどの役割を割り当てるべきですか？回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

User1:

▼

Key Vault Certificates Officer

Key Vault Crypto Officer

Key Vault Secrets Officer

User2:

▼

Key Vault Certificates Officer

Key Vault Crypto Officer

Key Vault Secrets Officer

正解:

Answer Area

User1:

▼

Key Vault Certificates Officer

Key Vault Crypto Officer

Key Vault Secrets Officer

User2:

▼

Key Vault Certificates Officer

Key Vault Crypto Officer

Key Vault Secrets Officer

Explanation:

<https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide#azure-built-in-roles-for-key-vault-data-plane-operations>

質問: 110
シミュレーション

必要に応じて、以下のログイン情報を使用してください。

ユーザー名を入力するには、サインインボックスにカーソルを置き、下のユーザー名をクリックしてください。
パスワードを入力するには、カーソルを「パスワードを入力」ボックスに置いて、下のパスワードをクリックしてください。

Microsoft 365 ユーザー名: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365ポータルがブラウザに正常に読み込まれない場合は、Ctrl+Kキーを押して新しいブラウザタブでポータルを再読み込みしてください。

以下の情報は、技術サポートのみを目的としています。

ラボインスタンス: 999999999

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している必要があります。

Microsoft Intuneによって準拠していると認定されたデバイスを使用して接続してください。

- 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。

このタスクを完了するには、該当する管理センターにサインインしてください。

正解:

Part 1: First, create a Conditional Access policy and assign your test group of users as follows:

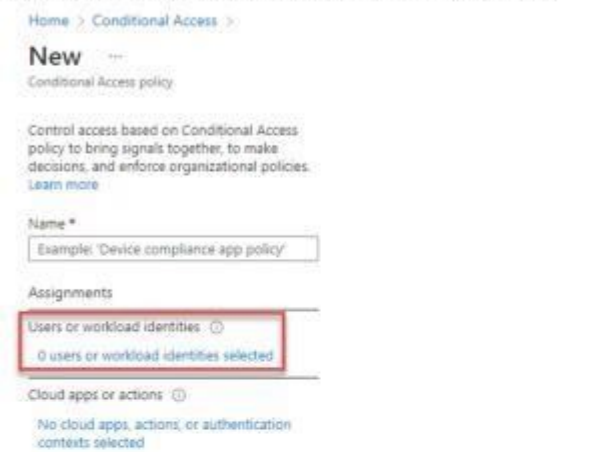
Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access, select + New policy, and then select Create new policy.



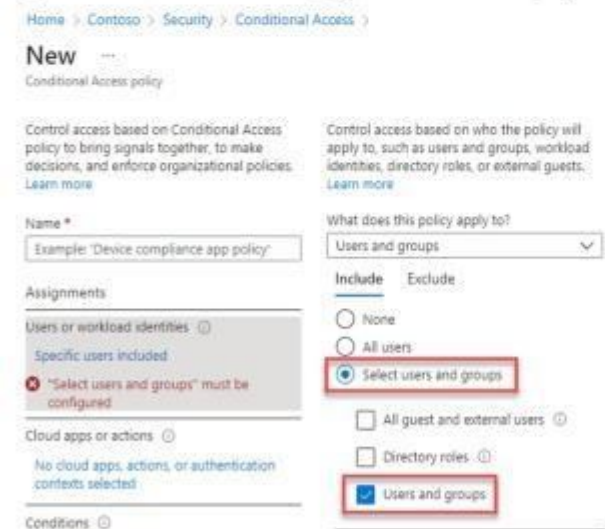
Step 3: Enter a name for the policy, such as MFA Pilot.

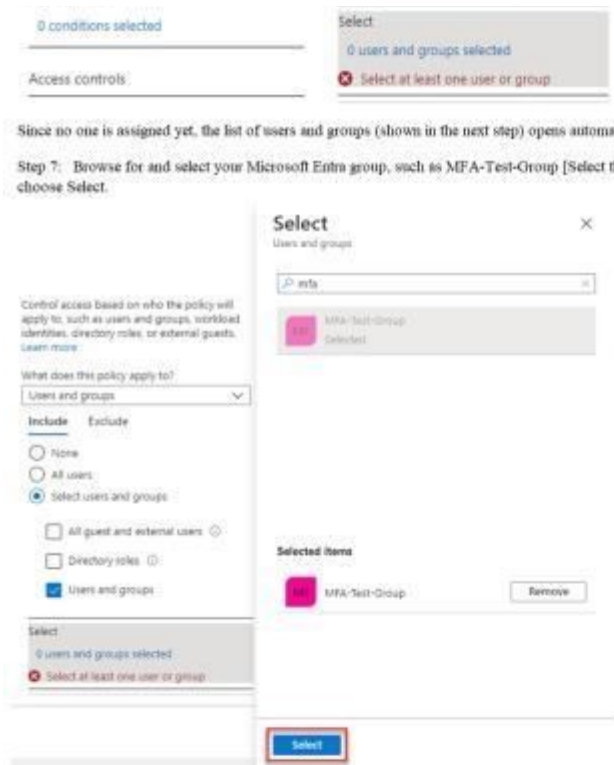
Step 4: Under Assignments, select the current value under Users or workload identities.



Step 5: Under What does this policy apply to?, verify that Users and groups is selected.

Step 6: Under Include, choose Select users and groups, and then select Users and groups.





Since no one is assigned yet, the list of users and groups (shown in the next step) opens automatically.

Step 7: Browse for and select your Microsoft Entra group, such as MFA-Test-Group [Select the sg-Executive group], then choose Select.

Part 2: Select applications

Configure the apps which require the conditions :

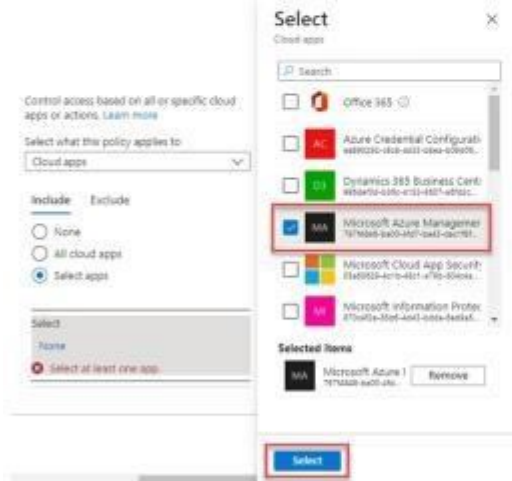
Step 8: Select the current value under Cloud apps or actions, and then under Select what this policy applies to, verify that Cloud apps is selected.

Step 9: Under Include, choose Select apps.

Since no apps are yet selected, the list of apps (shown in the next step) opens automatically.

Step 10: Browse the list of available sign-in events that can be used. Then choose Select.

Choose Select apps and select the link under Select.



Step 11: On the Select page, choose Windows Azure Service Management API, and then choose Select.

Part 3: Select Conditions

Question:

The members must meet one of the following conditions:

Connect by using a device that is marked as compliant by Microsoft Intune.

Connect by using client apps that are protected by app protection policies.

Step 12: Select Conditions > Client apps to apply the policy to apps and browsers. Select Yes, and then select the checkboxes for enable Browser and Mobile apps and desktop clients.

Step 13: Under Access controls, select Grant to apply Conditional Access based on a device compliance status. Select Grant access > Intune compliant Device, and Require app protection policy, then select Require one of the selected controls.

Step 14: For Enable policy, select On, and then select Create to save your changes. By default, Enable policy is set to Report-only.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/indepth/tutorial-enable-azure-mfa>

<https://learn.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune-create>

お客様のネットワークには、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が動作し、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。
Windows 10 コンピューターで Azure AD シームレス SSO をサポートするように構成する必要があります。
あなたはどうすべきでしょうか？

- A. 設定アプリからサインインオプションを設定します。
- B. 企業内ローミングを有効にする。
- C. イン트라ネットゾーンの設定を変更します。
- D. Azure AD Connect 認証エージェントをインストールします。

正解: **C** ([コメントを发表する](#))

You can gradually roll out Seamless SSO to your users using the instructions provided below.
You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory:

<https://autologon.microsoftazuread-ssso.com>

In addition, you need to enable an Intranet zone policy setting called Allow updates to status bar via script through Group Policy.

more information in:

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

質問: 112

あなたはMicrosoft 365テナントをお持ちです。
現在、基本認証を使用する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に接続できるのは、最新の認証プロトコルを使用するメールクライアントからのみであることを確認する必要があります。
何を実装すべきでしょうか？

- A. Microsoft Defender for Cloud Apps の OAuth ポリシー
- B. Azure Active Directory(Azure AD)の条件付きアクセス ポリシー
- C. Microsoft Endpoint Manager のコンプライアンス ポリシー
- D. Microsoft Endpoint Manager のアプリケーション制御プロファイル

正解: **B** ([コメントを发表する](#))

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

質問: 113

お客様は、Microsoft Defender for Cloud Appsおよび条件付きアクセス ポリシーを使用するMicrosoft 365 E5サブスクリプションをご利用中です。
ユーザーが高リスクと判断された場合は、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 ポータルで作成すべきポリシーの種類はどれですか？

- A. アクセスポリシー
- B. OAuthアプリポリシー
- C. 異常検知ポリシー
- D. 活動方針

Microsoft Defender for Cloud Apps access policies enable real-time monitoring and control over access to cloud apps based on user, location, device, and app.

正解: ([正解を表示します](#))

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

質問: 114

お客様はAzureサブスクリプションをお持ちです。そのサブスクリプションには、Linuxを実行するVM1という名前の仮想マシンが含まれています。VM1のセキュリティを強化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。

- ユーザーがMicrosoft Entraを使用してVM1にサインインできることを確認してください。

資格。

- ユーザーが多要素アウトオブバンド認証を使用して認証されるようにします。

- ユーザーがパスワードを使用してVM1にサインインすることを防止します。

解決策に含めることができる認証方法を2つ挙げてください。正解はそれぞれ完全な解決策を示しています。

注：正解ごとに1ポイントが加算されます。

A. FIDO2セキュリティキー

B. 一時アクセスパス

C. Windows Hello for Business

D. SMS

E. Microsoft Authenticatorアプリ

正解: ([正解を表示します](#))

質問: 115

Azure ADテナントをお持ちです。

App1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デプロイします。

ユーザーがApp1にテナントへのアクセス権を付与しようとする、その試みは失敗します。

ユーザーがApp1に対する管理者同意を要求できるように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。

まず最初に何をすべきでしょうか？

A. テナントに対する管理者同意要求を有効にします。

B. テナントの管理同意要求のレビュー担当者を指定する。

C. App1 の権限設定から、テナントに対して App1 の管理者同意を付与します。

D. App1 の条件付きアクセス ポリシーを作成します。

正解: ([正解を表示します](#))

To ensure that users can request admin consent for App1 in your Azure AD tenant, you should first enable admin consent requests for the tenant.

Enabling admin consent requests allows users to initiate the process of requesting admin consent for applications that require it. By default, users do not have the ability to grant admin consent for applications. Enabling this feature ensures that users can request admin consent for App1 without having to rely on an administrator to initiate the process.

質問: 116

事例研究2 - Litware, Inc.

概要

Litware, Inc.は、Fabrikam, Inc.という子会社を持つ製薬会社です。

Litwareはボストンとシアトルにオフィスを構えているが、従業員は全米各地に分散している。

従業員はVPN接続を利用して、どちらのオフィスにもリモートで接続します。

既存環境。環境を特定する

このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect はパ
ススルー認証を使用しており、パスワードハッシュの同期は無効になっています。

Litware.comには、すべてのアプリケーション開発を監督するUser1というユーザーが存在します。

LitwareはAzure ADアプリケーションプロキシを実装しています。

Fabrikam社は、fabrikam.comという名前のAzure ADテナントを所有しています。Fabrikam社のユーザーは、litware.comテナント内のゲストアカウントを使用して、litware.comのリソースにアクセスします。

既存環境。クラウド環境

Litwareの全ユーザーはMicrosoft 365 Enterprise E5ライセンスを保有しています。Microsoft Cloud App Securityに組み込まれている異常検知ポリシーはすべて有効になっています。

Litwareは、litware.com Azure ADテナントに関連付けられたAzureサブスクリプションを保有しています。このサブスクリプションには、Azure Active DirectoryコネクタとOffice 365コネクタを使用するAzure Sentinelインスタンスが含まれています。Azure Sentinelは現在、Azure ADのサインインログと監査ログを収集しています。

既存環境。オンプレミス環境

オンプレミスネットワークには、次の表に示すサーバーが含まれています。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litwareの2つのオフィスはどちらもインターネットに直接接続されています。両オフィスとも、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのドメインコントローラーはすべてインターネットへのアクセスが制限されています。

要件。委任要件

Litwareは、以下の委任要件を特定しています。

- * Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
- * litware.com Azure AD テナントに、権限のないユーザーがアプリケーションを登録できないようにします。
- * アイデンティティガバナンスには、カスタムカタログとカスタムプログラムを使用する。
- * User1がAzure ADでエンタープライズアプリケーションを作成できることを確認します。

最小権限の原則を適用する。

要件。ライセンス要件

Litwareは最近、litware.com Active DirectoryフォレストにLWLicensesという名前のカスタムユーザー属性を追加しました。Litwareは、LWLicenses属性の値を変更することでAzure ADライセンスの割り当てを管理したいと考えています。LWLicensesに適切な値を持つユーザーは、適切なライセンスが割り当てられているMicrosoft 365グループに自動的に追加される必要があります。

要件。管理要件

Litwareは、LWGroup1という名前のグループを作成したいと考えています。このグループには、LitwareのすべてのAzure ADユーザーアカウントが含まれますが、すべてのAzure ADゲストアカウントは除外されます。

要件。認証要件

Litwareは、以下の認証要件を定めています。

- * すべてのLitwareユーザーに対して多要素認証(MFA)を実装する。
- * LitwareのボストンオフィスからAzure ADへの認証を行う際に、ユーザーがMFAを使用する必要がないようにする。
- * litware.com フォレストに対して、禁止パスワードリストを実装する。

オンプレミスアプリケーションへのアクセス時に多要素認証(MFA)を強制する。

- * 外部に漏洩した認証情報を自動的に検出し、修復します。

要件。アクセス要件

Litwareは、以下のアクセス要件を定めています。

条件付きアクセス ポリシーを使用して、すべての Azure リソースおよび Azure AD アプリケーションへのアクセスを制御します。

- * Microsoft SharePoint Online のセッション制御を含む条件付きアクセス ポリシーを実装します。

* Azure AD のアクセス レビューを使用して、アプリケーションへの特権アクセスを制御します。

要件。監視要件

Litware社は、Azure SentinelのFusionルールを使用して、疑わしいAzure ADサインインとその後の異常なMicrosoft Office 365アクティビティの組み合わせを含む、複数段階の攻撃を検出したいと考えています。

ホットスポットに関する質問

委任要件を満たすには、Azure AD でアプリ登録を構成する必要があります。

どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Azure AD tenant-level setting to modify:

Allow users to register application

Users can consent to apps accessing company data on their behalf

Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

Application administrator

Application developer

Cloud application administrator

正解:

Answer Area

Azure AD tenant-level setting to modify:

Allow users to register application

Users can consent to apps accessing company data on their behalf

Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

Application administrator

Application developer

Cloud application administrator

Explanation:

- 1: Requirements for delegation clearly says " Prevent users to register applications"
- 2: User1 would need App Developer to register an app in tenant using "principle of least privilege"

質問: 117

事例研究2 - Litware, Inc.

概要

Litware, Inc.は、Fabrikam, Inc.という子会社を持つ製薬会社です。

Litwareはボストンとシアトルにオフィスを構えているが、従業員は全米各地に分散している。

従業員はVPN接続を利用して、どちらのオフィスにもリモートで接続します。

既存環境。環境を特定する

このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect は、パスワードハッシュの同期は無効になっています。

Litware.comには、すべてのアプリケーション開発を監督するUser1というユーザーが存在します。

LitwareはAzure ADアプリケーションプロキシを実装しています。

Fabrikam社は、fabrikam.comという名前のAzure ADテナントを所有しています。Fabrikam社のユーザーは、litware.comテナント内のゲストアカウントを使用して、litware.comのリソースにアクセスします。

既存環境。クラウド環境

Litwareの全ユーザーはMicrosoft 365 Enterprise E5ライセンスを保有しています。Microsoft Cloud App Securityに組み込まれている異常検知ポリシーはすべて有効になっています。

Litwareは、litware.com Azure ADテナントに関連付けられたAzureサブスクリプションを保有しています。このサブスクリプションには、Azure Active DirectoryコネクタとOffice 365コネクタを使用するAzure Sentinelインスタンスが含まれています。Azure Sentinelは現在、Azure ADのサインインログと監査ログを収集しています。

既存環境。オンプレミス環境

オンプレミスネットワークには、次の表に示すサーバーが含まれています。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litwareの2つのオフィスはどちらもインターネットに直接接続されています。両オフィスとも、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのドメインコントローラーはすべてインターネットへのアクセスが制限されています。

要件。委任要件

Litwareは、以下の委任要件を特定しています。

- * Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
- * litware.com Azure AD テナントに、権限のないユーザーがアプリケーションを登録できないようにします。
- * アイデンティティガバナンスには、カスタムカタログとカスタムプログラムを使用する。
- * User1がAzure ADでエンタープライズアプリケーションを作成できることを確認します。

最小権限の原則を適用する。

要件。ライセンス要件

Litwareは最近、litware.com Active DirectoryフォレストにLWLicensesという名前のカスタムユーザー属性を追加しました。Litwareは、LWLicenses属性の値を変更することでAzure ADライセンスの割り当てを管理したいと考えています。LWLicensesに適切な値を持つユーザーは、適切なライセンスが割り当てられているMicrosoft 365グループに自動的に追加される必要があります。

要件。管理要件

Litwareは、LWGroup1という名前のグループを作成したいと考えています。このグループには、LitwareのすべてのAzure ADユーザーアカウントが含まれますが、すべてのAzure ADゲストアカウントは除外されます。

要件。認証要件

Litwareは、以下の認証要件を定めています。

- * すべてのLitwareユーザーに対して多要素認証(MFA)を実装する。
- * LitwareのボストンオフィスからAzure ADへの認証を行う際に、ユーザーがMFAを使用する必要があるようにする。
- * litware.com フォレストに対して、禁止パスワードリストを実装する。

オンプレミスアプリケーションへのアクセス時に多要素認証(MFA)を強制する。

- * 外部に漏洩した認証情報を自動的に検出し、修復します。

要件。アクセス要件

Litwareは、以下のアクセス要件を定めています。

条件付きアクセス ポリシーを使用して、すべての Azure リソースおよび Azure AD アプリケーションへのアクセスを制御します。

- * Microsoft SharePoint Online のセッション制御を含む条件付きアクセス ポリシーを実装します。
- * Azure AD のアクセス レビューを使用して、アプリケーションへの特権アクセスを制御します。

要件。監視要件

Litware社は、Azure SentinelのFusionルールを使用して、疑わしいAzure ADサインインとその後の異常なMicrosoft Office 365アクティビティの組み合わせを含む、複数段階の攻撃を検出したいと考えています。

アイデンティティガバナンスを使用して、アプリケーションへのアクセス権限の割り当てを追跡する必要があります。ソリューションは委任要件を満たしている必要があります。

まず最初に何をすべきでしょうか？

- A. エンタープライズアプリケーションのユーザー同意設定を変更します。
- B. カタログを作成する。
- C. プログラムを作成します。
- D. エンタープライズアプリケーションの管理者同意要求設定を変更します。

正解: (正解を表示します)

Requirement is for program which is a part of Access Reviews. Catalog is for Access Packages.

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

質問: 118

ホットスポットに関する質問

お客様のMicrosoft Entraテナントには、以下の表に示すユーザーが含まれています。

Name	Department
User1	Marketing
User2	Marketing
User3	Engineering
User4	Engineering
User5	Finance
User6	Finance

テナントには、以下の表に示す管理部門が含まれています。

Name	Description
AU1	Contains all the users in the marketing department Contains all the resources for the marketing department Contains User1 and User2
AU2	Contains all the users in the engineering department Contains all the resources for the engineering department Contains User3 and User4
AU3	Contains Group4, User5, and User6.

テナントには、以下の表に示すグループが含まれています。

Name	Administrative unit	Members
Group1	AU1	User1, User2
Group2	AU2	User3, User4
Group3	AU3	User5, User6
Group4	AU3	User1, User2, User3, User4, User5, User6

あなたは以下の操作を実行します。

- User1にAU2のユーザー管理者ロールを割り当てます。
- User3にAU1のグループ管理者ロールを割り当てます。
- User5にAU3の認証管理者ロールを割り当てます。

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	☐	☐
User3 can add User4 to Group2.	☐	☐
User5 can configure an authentication method policy that requires all Group4 members to use passwordless sign-in.	☐	☐

正解:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	☒	☐
User3 can add User4 to Group2.	☐	☒
User5 can configure an authentication method policy that requires all Group4 members to use passwordless sign-in.	☐	☒

質問: 119

お客様は、Microsoft Defender for Cloud AppsおよびYammerを使用するMicrosoft 365 E5サブスクリプションをご利用中です。
ユーザーがリスクの高い場所からYammerにログ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、どのような操作を行うべきですか？

- A. アクセス ポリシーを作成します。
- B. 活動方針を作成する。
- C. 非制裁ヤマー。
- D. 異常検知ポリシーを作成します。

正解: (正解を表示します)

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

質問: 120

お客様は、以下の表に示すリソースを含む Azure サブスクリプションをお持ちです。

Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

どのリソースに対してアクセス審査を作成できますか？

- A. グループ1、ロール1、および貢献者のみ
- B. グループ1のみ
- C. グループ1、アプリ1、貢献者、および役割1
- D. 役割1と貢献者のみ

正解: (正解を表示します)

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/toc.json>

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

質問: 121

あなたは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、適切な規模の役割を作成および実装するには、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は、どの役割を割り当てるべきですか？

- A. オーナー
- B. ユーザーアクセス管理者
- C. 貢献者
- D. 読者

正解: ([正解を表示します](#))

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> **385**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 122

ホットスポットに関する質問

お客様は、Microsoft EntraテナントにリンクされたAzureサブスクリプションをお持ちです。このテナントには、次の表に示すIDが含まれています。

Name	Type	Role
User1	User	Helpdesk Administrator
User2	User	Conditional Access Administrator
Group1	Group	Global Administrator
Group2	Group	Exchange Administrator
App1	Registered app	Authentication Administrator

テナントは権限管理に登録されました。

次の表に示すAzureリソースを作成します。

Name	Type	Role
Managed1	Managed identity	Owner
Managed2	Managed identity	Cloud Application Administrator
SPrincipal1	Service principal	Security Operator

Microsoft Entra Insights から、特権ロールが割り当てられたアカウントにはどの ID が含まれ、特権ロールが割り当てられたサービスプリンシパルにはどの ID が含まれますか？

Answer Area

Accounts assigned to highly privileged roles:

User1

User2

Group1

Group2

Service principals with privileged role assignments:

App1

Managed1

Managed2

SPrincipal1

正解:

Answer Area

Accounts assigned to highly privileged roles:

User1

User2

Group1

Group2

Service principals with privileged role assignments:

App1

Managed1

Managed2

SPrincipal1



質問: 123

ホットスポットに関する質問

Sub1 という名前の Azure サブスクリプションがあり、その中に User1、User2、User3 という名前の 3 人のユーザーがいます。Sub1 には storage1 という名前のストレージ アカウントがあり、そこには次の表に示すリソースが含まれています。

Name	Type	Contents
cont1	Container	File1
share1	File share	File2

Sub1には、以下の表に示すユーザーが含まれています。

Name	Role	Scope
User1	Reader	Sub1
User2	Reader	Sub1
User2	Storage Blob Data Reader	storage1
User3	Storage Contributor	storage1

ファイル1を読み取れるユーザーと、ファイル2を読み取れるユーザーはそれぞれ誰ですか？回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

File1:

User2 onlyUser3 onlyUser1 and User2 onlyUser2 and User3 onlyUser1, User2, and User3

File2:

User2 onlyUser3 onlyUser1 and User2 onlyUser2 and User3 onlyUser1, User2, and User3

正解:

Answer Area

File1:

User2 onlyUser3 onlyUser1 and User2 onlyUser2 and User3 onlyUser1, User2, and User3

File2:

User2 onlyUser3 onlyUser1 and User2 onlyUser2 and User3 onlyUser1, User2, and User3

質問: 124

ドラッグアンドドロップ問題

お客様は、以下の表に示すリソースを含む Azure サブスクリプションをお持ちです。

Name	Type	Description
User1	User	Not applicable
User2	User	Not applicable
Vault1	Azure Key Vault	Contains a secret named Secret1
Vault2	Azure Key Vault	Contains a secret named Secret2
Secret1	Secret	Stored in Vault1
Secret2	Secret	Stored in Vault2

このサブスクリプションでは、特権ID管理(PIM)を使用しています。

PIMを使用して、以下のアクセス制御を設定する必要があります。

- User1がSecret1を読み取り、更新できることを確認してください。

- User2 が保存されている秘密の内容を読み取れるようにします
ヴォールト2。
解決策は最小権限の原則に従わなければならない。
各ユーザーにはどの認証方法を使用すべきでしょうか？回答するには、適切な認証方法を正しいユーザーにドラッグしてください。各認証方法は、1回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注：正解ごとに1ポイントが加算されます。

Authorization methods

The GET Secret Permissions Access Policy permission

The Key Vault Secrets Officer RBAC role

The Key Vault Reader RBAC role

The Key Vault Secrets User RBAC role

The LIST Secret Permissions Access Policy permission

The SET Secret Permissions Access Policy permission

Answer Area

User1:

User2:



正解:

Authorization methods

The GET Secret Permissions Access Policy permission

The Key Vault Reader RBAC role

The LIST Secret Permissions Access Policy permission

The SET Secret Permissions Access Policy permission

Answer Area

User1:

The Key Vault Secrets Officer RBAC role

User2:

The Key Vault Secrets User RBAC role



質問: 125
貴社は、専用のセキュリティ情報イベント管理システムとしてMicrosoft Sentinelを導入することを計画しています。Microsoft Sentinelの使用を開始する前に、以下のどれが前提条件となりますか？
A. Azure AD Premium P1 ライセンス

B. ログ分析ワークスペース

C. Azure AD Premium P2 ライセンス

D. Azure Key Vault

正解: ([正解を表示します](#))

As having a configured Log Analytics Workspace is a prerequisite before begging to ingest data into Microsoft Sentinel.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard#:~:text=%20Enable%20Azure%20Sentinel%20%201%20Sign%20in,support%20the%20moving%20of%20that%20workspace...%20See%20More>

質問: **126**

シミュレーション

プロジェクト・ファルコン・グループのメンバーは、四半期ごとにグループへの参加継続の必要性を表明する必要があります。メンバーシップが不要になった場合、またはユーザーが応答しない場合は、そのユーザーはグループから自動的に削除されます。

正解:

To automate this membership review, you must configure a Microsoft Entra ID Access Review through the Microsoft Entra admin center.

Step 1: Navigate to the Microsoft Entra admin center.

Open Access Reviews

Step 2: Expand the Identity Governance menu.

Step 3: Click on Access reviews.

Step 4: Select New access review.

Step 5: Select Teams + Groups for the review type.

Configure Scope

Step 6: Choose Select teams + groups.

Step 7: Find and select your specific group. [Select Project Falcon]

Step 8: Set scope to All users.

Step 9: Select Multi-stage review if needed, or leave it off for a standard single-stage review.

[Leave it as a standard single-stage review]

Step 10: Set quarterly Schedule

Step 11: Set the Frequency to Quarterly.

Step 12: Define a Duration (e.g., 14 days) for users to respond.

Step 13: Choose an End date or set it to Never to run indefinitely. [Choose Never] Step 14: Set the Select reviewers dropdown to Users review their own access. This forces the group members to self-attest.

Assign Reviewers

Step 15: Expand the Upon completion settings section.

Configure Automatic Removal

Step 16: Check the box for Auto apply results to resource.

Step 17: Set If reviewers don't respond to Remove access.

Step 18: Advanced settings allow you to enable Notifications and Reminders.

Finalize and Create

Step 19: Click Review + Create.

Step 20: Provide a Review name and description.

Step 21: Click Create to activate.

Reference:

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-perform-roles-and-resource-roles-review>

質問: 127

お客様は、User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションを所有しています。User1 は、アプリケーション管理者ロールの資格を有しています。

ユーザー1は、アプリケーションプロキシ用の新しいコネクタグループを設定する必要があります。

User1の役割を有効にするには、何を使用すればよいですか？

A. Microsoft 365 管理センター

B. Microsoft Intune 管理センター

C. Microsoft 365 Defender ポータル

D. Azure Active Directory 管理センター

正解: ([正解を表示します](#))

質問: 128

あなたはMicrosoft 365 E5サブスクリプションとAzureサブスクリプションをお持ちです。

Azure Monitorを使用して、Microsoft Entraのサインインログを分析する予定です。

Microsoft Entraの診断設定を構成する必要があります。

サインインログの保存先はどこに設定すればよいですか？

A. Azureイベントハブ

B. Azure SQLデータベース

C. Log Analyticsワークスペース

D. Azureストレージアカウント

正解: ([正解を表示します](#))

Integrate Microsoft Entra logs with Azure Monitor logs

A Log Analytics workspace allows you to collect data based on a variety of requirements, such as geographic location of the data, subscription boundaries, or access to resources.

Note: Use the integration of Microsoft Entra activity logs and Azure Monitor to perform the following tasks:

*-> Compare your Microsoft Entra sign-in logs against security logs published by Microsoft Defender for Cloud.

* Troubleshoot performance bottlenecks on your application's sign-in page by correlating application performance data from Azure Application Insights.

* Analyze the Identity Protection risky users and risk detections logs to detect threats in your environment.

* Identify sign-ins from applications still using the Active Directory Authentication Library (ADAL) for authentication.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-integrate-activity-logs-with-azure-monitor-logs>

質問: 129

ケーススタディ3 - A Datum Corp

概要

A Datum Corporationはモントリオールに拠点を置くコンサルティング会社です。A Datumは最近、バンクーバーに拠点を置くLitware, Inc.を買収しました。

既存の環境

データム環境

A Datumのオンプレミスネットワークには、adatum.comという名前のActive Directoryドメインサービス(AD DS)フォレストが含まれています。

Datum は Microsoft 365 E5 サブスクリプションを所有しています。このサブスクリプションには、Azure AD Connect を使用して adatum.com AD DS ドメインと同期する検証済みドメインが含まれています。Datum

は、adatum.com という名前の Azure Active Directory (Azure AD) テナントを所有しています。このテナントでは、セキュリティの既定値が無効になっています。
テナントには、以下の表に示すユーザーが含まれています。

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

テナントには、以下の表に示すグループが含まれています。

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

既存の環境

Litware環境

Litwareはlitware.comという名前のAD DSフォレストを持っています。

既存の環境

問題提起

データは、以下の問題を特定します。

営業部門の複数のユーザーが最大5台のデバイスを所有しています。営業部門のユーザーからは、デバイス数の上限に達したため、Azure ADテナントにデバイスを参加させるためにサポート部門に連絡しなければならない場合があるとの報告がありました。

最近のセキュリティインシデントにより、複数のユーザーが認証情報を漏洩し、不審なブラウザがログインに使用され、匿名のIPアドレスからリソースにアクセスされたことが明らかになった。

- デバイス管理者ロールを IT_Group1 に割り当てようとすると、そのグループが選択リストに表示されません。

組織内の誰でも、他のゲストや管理者以外のユーザーを含め、ゲストユーザーを招待できます。

ヘルプデスクはユーザーパスワードのリセットに時間をかけすぎている。

現在、ユーザーは認証にパスワードのみを使用しています。

要件

計画されている変更

A Datum社は、以下の変更を実施する予定です。

- セルフサービスパスワードリセット(SSPR)を設定します。

- すべてのユーザーに対して多要素認証(MFA)を設定します。

- Package1 という名前のアクセス パッケージのアクセス レビューを設定します。
組織データへのアプリケーションアクセスには、管理者の承認が必要となる。

- AD DSユーザーとgroupsoflitware.comをAzure ADテナントと同期します。

特定の管理者ロールが割り当てられたユーザーのみがゲストユーザーを招待できるようにします。

- Azure AD に参加または登録できるデバイスの最大数を 10 に増やします。

要件

技術要件

基準点には、以下の技術要件が規定されています。

- ユーザー管理者ロールを割り当てられたユーザーは、必要に応じて最長1年間、そのロールを使用するための許可を要求できる必要があります。

・ユーザーには多要素認証(MFA)への登録を促し、一定期間の登録をスキップできるオプションを提供する必要があります。

- ユーザーは、SSPRを使用してパスワードをリセットするために、1つの認証方法を提供する必要があります。

利用可能な方法には以下が含まれる必要があります。

- メール

- 電話

- セキュリティに関する質問

- Microsoft Authenticator アプリ

- adatum.comとlitware.comのAD DSドメイン間で信頼関係を確立してはなりません。

最小権限の原則を適用しなければならない。

ドラッグアンドドロップ問題

最近発生したセキュリティインシデントの問題を解決する必要があります。

各インシデントに対してどのような設定を行うべきでしょうか？回答するには、適切なポリシータイプを該当する問題にドラッグしてください。各ポリシータイプは、1回、複数回、または全く使用しない場合があります。

コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注：正解ごとに1ポイントが加算されます。

Policy Types

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

Answer Area

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

正解:

Policy Types

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

Answer Area

Leaked credentials:

A user risk policy

A sign-in from a suspicious browser:

A sign-in risk policy

Resources accessed from an
anonymous IP address:

A sign-in risk policy

Explanation:

Box 1: A user risk policy

User-linked detections include:

Leaked credentials: This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials.

User risk policy

Identity Protection can calculate what it believes is normal for a user's behavior and use that to base decisions for their risk. User risk is a calculation of probability that an identity has been compromised. Administrators can make a decision based on this risk score signal to enforce organizational requirements. Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

Box 2: A sign-in risk policy

Suspicious browser: Suspicious browser detection indicates anomalous behavior based on suspicious sign-in activity across multiple tenants from different countries in the same browser.

Box 3: A sign-in risk policy

A sign-in risks include activity from anonymous IP address: This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.

Note: The following three policies are available in Azure AD Identity Protection to protect users and respond to suspicious activity. You can choose to turn the policy enforcement on or off, select users or groups for the policy to apply to, and decide if you want to block access at sign-in or prompt for additional action.

* User risk policy

Identifies and responds to user accounts that may have compromised credentials. Can prompt the user to create a new password.

* Sign in risk policy

Identifies and responds to suspicious sign-in attempts. Can prompt the user to provide additional forms of verification using Azure AD Multi-Factor Authentication.

* MFA registration policy

Makes sure users are registered for Azure AD Multi-Factor Authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Azure AD Multi-Factor Authentication.

Reference:

質問: 130

ホットスポットに関する質問

お客様はMicrosoft 365テナントをお持ちです。

HighRiskCountries」という名前の場所を作成し、その中に高リスク国のリストを含めます。

リスクの高い国から接続する場合、ユーザーが認証状態を維持でき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、どのような設定を行うべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Configure HighRiskCountries by using:

A cloud app or action

A condition

A grant control

A session control

Configure Sign-in frequency by using:

A cloud app or action

A condition

A grant control

A session control

正解:

Answer Area

Configure HighRiskCountries by using:

	▼
A cloud app or action	
A condition	
A grant control	
A session control	

Configure Sign-in frequency by using:

	▼
A cloud app or action	
A condition	
A grant control	
A session control	



Microsoft

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: 131

貴社は、User1という名前のユーザーを含むAzure ADテナントを所有しています。

同社にはマーケティング部門と財務部門という2つの部門がある。

User1には、マーケティング部門のユーザーのみを管理できる権限を付与する必要があります。

この解決策では、User1が財務部門のユーザーを管理する権限を持たないようにする必要があります。

最初に何を作るべきでしょうか？

- A. 経営グループ
- B. リソースグループ
- C. Microsoft 365 グループ
- D. 行政単位

正解: [\(正解を表示します\)](#)

質問: 132

Azure Active Directory (Azure AD) テナントがあります。

リスク検出レポートを開きます。

どのリスク検出タイプがユーザーリスクとして分類されますか？

- A. 不可能な旅行
- B. 匿名IPアドレス
- C. 非定型旅行
- D. 漏洩したクレデンシャル

正解: [\(正解を表示します\)](#)

Leaked credentials indicates that the user's valid credentials have been leaked.

Note:

There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:

- password spray
- malicious IP address
- unfamiliar sign-in properties

Reference:

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

質問: 133

お客様のMicrosoft Entraテナントには、以下の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	None
User3	None

App1という名前のエンタープライズアプリケーションを追加し、以下のセルフサービス設定を構成します。

- * ユーザーがこのアプリケーションへのアクセスを要求することを許可する: はい
- * 割り当てられたユーザーをどのグループに追加しますか: グループ1
- * このアプリケーションへのアクセスを許可する前に承認が必要ですか? :はい
- * このアプリケーションへのアクセスを承認できるのは誰ですか: User2

どのユーザーがApp1へのアクセスをリクエストできるか

- A. ユーザー2とユーザー3のみ
- B. User3のみ
- C. User1、User2、およびUser3
- D. ユーザー1とユーザー3のみ

正解: ([正解を表示します](#))

質問: 134

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: ([正解を表示します](#))

Authentication administrator: can reset passwords for non-admins but can't invalidate sessions.

Helpdesk administrator: Users with this role can change passwords, invalidate refresh tokens, manage service requests, and monitor service health. Invalidating a refresh token forces the user to sign in again.

Privileged Authentication Administrator: can reset all passwords (admins & non-admins) but can't invalidate any sessions.

Security Operator: can't reset any passwords.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#authentication-administrator>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-authentication-administrator>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator>

質問: 135

ホットスポットに関する質問

ユーザー「User1」を含むAzure Active Directory(Azure AD)テナントをお持ちです。

管理者がユーザー1を削除します。

以下の項目を特定する必要があります。

ユーザー1のアカウントが削除されてから何日後に復元できますか？

アカウント？

- 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、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Number of days:

Role:

Microsoft

正解:

Answer Area

Number of days:

	▼
15	
30	
90	
180	

Role:

	▼
User administrator	
Network administrator	
Helpdesk administrator	
Domain name administrator	

質問: 136

お客様のネットワークには、Microsoft 365 E5 サブスクリプションとユーザーアカウントを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。Microsoft Entraへのサインインに、オンプレミスのアカウントロックアウトポリシーが適用され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すか？

- A. Azure Active Directoryシームレスシングルサインオン(Azure ADシームレスSSO)
- B. Microsoft Entra Cloud Sync
- C. パススルー認証
- D. パスワードハッシュ同期

正解: C (コメントを发表する)

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 385問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 137

contoso.com という名前の Microsoft Entra テナントがあり、その中に App1 という名前のエンタープライズ アプリケーションが含まれています。

請負業者はuser1@outlook.comの認証情報を使用します。

請負業者にApp1へのアクセス権を付与できることを確認してください。請負業者はuser1@outlook.comとして認証する必要があります。

あなたはどうすべきでしょうか？

- A. Microsoft Entra Connect 同期を実装します。
- B. contoso.comでゲストユーザーアカウントを作成します。
- C. 外部コラボレーション設定を構成します。
- D. New-MgUserコマンドレットを実行します。

正解: (正解を表示します)

* Create a guest user account in contoso.com.

* Run the New-AzureADMSInvitation cmdlet. [For Microsoft Active Directory]

* Run the New-MgInvitationcmdlet. [For Microsoft Entra]

Note:

* New-AzureADMSInvitation

This cmdlet is used to invite a new external user to your directory.

* New-MgInvitation

Microsoft.Graph.Identity.SignIns

Use this API to create a new invitation or reset the redemption status for a guest user who already redeemed their invitation. Invitation adds an external user to the organization Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation>

<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0>

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。)

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *

Admin review

Description ⓘ

Start date *

12/18/2020

Frequency

Monthly

Duration (in days) ⓘ

14

End ⓘ

Never

End by

Occurrences

End date

01/17/2021

Users Scope

Everyone

Review role membership (permanent and eligible) *

Application Administrator and 72 others

Reviewers

Reviewers

(Preview) Manager

(Preview) Fallback reviewers ⓘ

Megan Bowen

Upon completion settings

Start

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. はい

B. いいえ

正解: **B** ([コメントを发表する](#))

Members (self) - Use this option to have the users review their own role assignments. Groups assigned to the role will not be a part of the review when this option is selected. This option is only available if the review is scoped to Users and Groups.

Also Megan Brow still there as Fallback Reviewer so will still receiving reviews.

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

質問: **139**

あなたはMicrosoft 365のサブスクリプションをお持ちです。

Gateway1という名前のサードパーティ製Webゲートウェイをデプロイします。

Gateway1をMicrosoft Defender for Cloud Appsと統合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。

- データがDefender for Cloud Appsに自動的に送信されるようにします。

・管理業務の手間を最小限に抑える。

まず最初に何をすべきでしょうか？

A. データソースを追加します。

B. スナップショットレポートを作成します。

C. アプリ登録を作成します。

D. ログコレクターを追加します。

正解: ([正解を表示します](#))

The first action you should take is to add a data source.

Add a data source: In Microsoft Defender for Cloud Apps, before a log collector can process and format data automatically, you must define the specific third-party web gateway as a data source.

This action establishes the expected log format (such as Blue Coat, Cisco ASA, or Check Point) so the system can parse the incoming traffic automatically with low administrative overhead.

Reference:

<https://learn.microsoft.com/en-us/defender-cloud-apps/discovery-docker>

質問: **140**

事例研究1 - Contoso, Ltd

概要

Contoso, Ltd.は、モントリオールに本社を置き、ロンドンとシアトルに支店を持つコンサルティング会社です。

ContosoはFabrikam, Inc.という会社と提携関係にある。Fabrikamはfabrikam.comという名前のAzure Active Directory(Azure AD)テナントを所有している。

既存環境。既存環境

Contosoのオンプレミスネットワークには、contoso.comという名前のActive Directoryドメインが含まれています。

このドメインには、Contoso_Resources という名前の組織単位 (OU) が含まれています。Contoso_Resources OU には、すべてのユーザーとコンピューターが含まれています。

contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

既存環境 :Microsoft 365/Azure環境

Contosoはcontoso.comという名前のAzure ADテナントを所有しており、それには以下のライセンスが関連付けられています。

- * Microsoft Office 365 Enterprise E5
- * エンタープライズモビリティ+セキュリティ
- * Windows 10 Enterprise E3
- * プロジェクト計画3

Azure AD Connectは、Azure ADとActive Directoryドメインサービス(AD DS)の間で構成されています。同期されるのはContoso_Resources OUのみです。

ヘルプデスク管理者は、ユーザー設定を管理するために日常的にMicrosoft 365管理センターを使用します。

現在、ユーザー管理者はMicrosoft 365管理センターを使用してライセンスを手動で割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。

- * ロンドンオフィスのユーザーは、Microsoft 365 Phone Systemのライセンスが未割り当ての状態です。

シアトルオフィスのユーザーは、Yammer Enterpriseライセンスを未割り当ての状態です。

contoso.com では、セキュリティのデフォルト設定が無効になっています。

Contosoは、管理者ロールを保護するためにAzure ADの特権ID管理(PIM)を使用しています。

既存環境。問題点

コントソ氏は以下の問題点を指摘している。

- * 現在、すべてのヘルプデスク管理者は、Microsoft 365テナント全体にわたるユーザーライセンスを管理できます。
- * ユーザー管理者からは、Contosoの各オフィスごとに異なるライセンス要件を手動で設定するのは面倒だという報告が寄せられています。

ヘルプデスク管理者は、必要なMicrosoft 365サービスおよびアプリへの内部アクセスとゲストアクセスをプロビジョニングするのに時間をかけすぎている。

- * 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
- * Azure AD で [ログ] ノードを選択すると、Log Analytics の統合が有効になっていないことを示すエラーメッセージが表示されます。

要件。計画されている変更

コントソ氏は以下の変更を実施する予定です。

- * セルフサービスパスワードリセット(SSPR)を実装する。
- * Azure Monitorを使用して、Azure監査アクティビティログを分析します。
- * テナントに追加された新規ユーザーに対するライセンス割り当てを簡素化します。
- * Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施する。
- * ユーザー管理者ロールを設定し、有効化する際に正当性の説明と承認が必要となるようにします。
- * App1という名前の、業務専用のカスタムAzure Webアプリを実装します。App1はインターネットからアクセス可能で、Azure ADアカウントを使用して認証されます。

- * マーケティング部門の新規ユーザー向けに、Microsoft SharePoint Onlineのサイト、グループ、およびアプリへのアクセス権限を付与するための自動承認ワークフローを実装します。
- Contoso社はAdatum Corporationという会社を買収する予定です。Adatumという名前のActive Directory組織単位(OU)内に、新たに100人のAdatumユーザーが作成されます。これらのユーザーはロンドンとシアトルに拠点を置く予定です。
- 要件。技術要件
- Contoso社は、以下の技術要件を特定しました。
- * すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期されている必要があります。
 - * App1 には、https://contoso.com/auth-response を指すリダイレクト URI が必要です。
 - * 新規ユーザーへのライセンス割り当ては、ユーザーの所在地に基づいて自動的に行われる必要があります。
 - * Fabrikamのユーザーは、マーケティング部門のSharePointサイトに最大90日間アクセスできる必要があります。
 - * Azure AD で実行される管理操作は監査対象とする必要があります。監査ログは 1 年間保持する必要があります。
 - * ヘルプデスク管理者は、それぞれのオフィスに所属するユーザーのライセンスのみを管理できる必要があります。
 - * ユーザーの身元が侵害された可能性がある場合、ユーザーにはパスワードの変更を強制しなければならない。

質問

ゲストユーザー招待に関する問題を解決する必要があります。

Azure ADテナントに対しては、どのような対応が必要ですか？

- A.** 継続アクセス評価設定を構成します。
- B.** 条件付きアクセス ポリシーを設定します。
- C.** アクセスレビューの設定を行います。
- D.** 外部コラボレーション設定を変更します。

正解: ([正解を表示します](#))

You can add enable 'Guest Inviter' role. But you cannot enable self-service role for 'Office 365' apps. So far, that is only available for apps you build.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-in-the-portal>

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-user-flow#enable-self-service-sign-up-for-your-tenant>

質問: 141

Azure ADテナントをお持ちです。

テナントに多数の新しいアプリが追加されていることに気づく。

新規企業アプリケーションには承認プロセスを導入する必要があります。

あなたはどうすべきでしょうか？

- A.** Microsoft Entra 管理センターから、管理者の同意設定を構成します。
- B.** Microsoft Defender for Cloud Apps ポータルから、クラウド検出異常検出ポリシーを作成します。
- C.** Microsoft Defender for Cloud Apps ポータルから、アプリ コネクタを構成します。
- D.** Microsoft Entra 管理センターから、アクセス レビューを設定します。

正解: ([正解を表示します](#))

質問: 142

シミュレーション

必要に応じて、以下のログイン情報を使用してください。

ユーザー名を入力するには、サインインボックスにカーソルを置き、下のユーザー名をクリックしてください。

パスワードを入力するには、カーソルを「パスワードを入力」ボックスに置いて、下のパスワードをクリックしてください。

Microsoft 365 ユーザー名: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365ポータルがブラウザに正常に読み込まれない場合は、Ctrl+Kキーを押して新しいブラウザタブでポータルを再読み込みしてください。

以下の情報は、技術サポートのみを目的としています。

ラボインスタンス: 99999999

Microsoft 365 サブスクリプション内のデータへのアクセスを必要とするアプリケーションに対して、同意を設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。

ユーザーがアプリケーションへの同意を提供できない場合、ユーザーは管理者に同意要求を審査するよう要求できる必要があります。

アラン・デヤングは、ユーザーからの同意要求を審査できる必要があります。

このタスクを完了するには、該当する管理センターにサインインしてください。

正解:

Microsoft Entra ID, Enterprise applications, Configure how users consent to applications

Before an application can access your organization's data, a user must grant the application permissions to do so.

Part 1: If a user cannot provide consent to an application, the user must be able to request that an administrator review the consents requests.

Configure user consent settings

Step 1: Sign in to the Microsoft Entra admin center as a Global Administrator.

Step 2: Browse to Identity > Applications > Enterprise applications > Consent and permissions > User consent settings.

Step 3: Under User consent for applications, select which consent setting you want to configure for all users. [Here: Do not allow user consent]

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data.

☐ Do not allow user consent
An administrator will be required for all apps.

☒ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

 7 permissions classified as low impact

☐ Allow user consent for apps
All users can consent for any app to access the organization's data.

Step 4: Select Save to save your settings.

Part 2: Allan Deyoung must be able to review the consent requests of the users.

Configure the admin consent workflow to enable users to request access to applications that require admin consent. You enable the ability to make requests by using an admin consent workflow.

Enable the admin consent workflow

To enable the admin consent workflow and choose reviewers:

- Step 1: Sign in to the Microsoft Entra admin center as as a Global Administrator.
- Step 2: Browse to Identity > Applications > Enterprise applications > Consent and permissions > Admin consent settings.
- Step 3: Under Admin consent requests, select Yes for Users can request admin consent to apps they are unable to consent to

Save Discard

Admin consent requests

Users can request admin consent to apps they are unable to consent to ⓘ

Yes No

Who can review admin consent requests ⓘ

Reviewer type	Reviewers
Users	5 users selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests ⓘ

Yes No

Selected users will receive request expiration reminders ⓘ

Yes No

Consent request expires after (days) ⓘ

30

Step 4: Configure the following settings:

Who can review admin consent requests

Step 4a: Specify Allan Deyoung

Step 5: Select Save. It can take up to an hour for the workflow to become enabled.

Reference:

- <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent>
- <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-admin-consent-workflow>

お客様は、Group1とGroup2という名前の2つのグループと、以下の表に示すユーザーを含むMicrosoft 365 E5サブスクリプションを所有しています。

Name	Member of	Role
User1	Group1	None
User2	Group1, Group2	None
User3	Group2	Global Administrator

このサブスクリプションには、以下の設定を持つ条件付きアクセス ポリシーが含まれています。

- 名前: ポリシー1
- 課題
 - o 含める
 - ユーザーとグループ: グループ1
 - ディレクトリの役割: グローバル管理者
- 除外する
 - ユーザーとグループ: グループ2
- o 対象リソース
 - 含む
 - すべてのクラウドアプリ
 - アクセス制御
- 付与
- 多要素認証を必須とする

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements

User1 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps.

☐☐

User2 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps.

☐☐

User3 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps.

☐☐

Answer Area		
Statements	Yes	No
User1 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps.	☒	☐
User2 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps.	☐	☒
User3 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps.	☐	☒

質問: 144

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として認証する必要があります。あなたは何をすべきか？

- 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)

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

質問: 145

あなたはMicrosoft 365のサブスクリプションをお持ちです。あなたは、以下の構成を持つApp1という名前のアプリをデプロイする予定です。

- Microsoft Entraに登録されます
- サインインしているユーザーの Microsoft Outlook カレンダーにアクセスします

Microsoft Graph API

App1がMicrosoft Graphにアクセスできることを確認する必要があります。何をすべきでしょうか？

- A. アプリケーション権限
- B. 委任された権限
- C. カスタムロールベースアクセス制御(RBAC)ロール
- D. 組み込みのロールベースアクセス制御(RBAC)ロール

正解: (正解を表示します)

Delegated permissions are used when your app needs to act on behalf of the signed-in user, and they require consent from the user.

質問: 146

貴社は、Microsoft 365 E5 の新しいサブスクリプションと、App1 という名前のアプリを購入しました。

App1 用に 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。

まず最初に何をすべきでしょうか？

A. 条件付きアクセス アプリケーション制御を使用するように条件付きアクセス ポリシーを設定します。

B. App1 のトークン設定を構成します。

C. App1 の API 権限を追加します。

D. アプリによる制限を適用するには、条件付きアクセス ポリシーを設定します。

正解: (正解を表示します)

質問: 147

お客様は、fabrikam.comというドメイン名を使用するMicrosoft 365テナントをお持ちです。

外部コラボレーションの設定は、コラボレーション図に示されているとおりに構成されています。(「コラボレーション」タブをクリックしてください。)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

☐

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

☒

Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

☐

Only users assigned to specific admin roles can invite guest users

☐

No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

Learn more

Yes

No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

Learn more

Yes

No

Collaboration restrictions

⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. [Learn more.](#)

☒

Allow invitations to be sent to any domain (most inclusive)

☐

Deny invitations to the specified domains

☐

Allow invitations only to the specified domains (most restrictive)

テナントに対して、ゲスト用のメールによるワンタイムパスコード設定が有効になっています。

bsmith@fabrikam.com というユーザーが、Microsoft SharePoint Online のドキュメントライブラリを、次の表に示すユーザーと共有しています。

Name	Email	Description
User1	User1@contoso.com	An existing guest user in fabrikam.com
User2	User2@tailsphoto.com	A guest user who has never accessed resources in fabrikam.com
User3	User3@fabrikam.com	A user in fabrikam.com

どのユーザーにパスワードがメールで送信されますか？

- A. ユーザー2のみ
- B. ユーザー1、ユーザー2、ユーザー3
- C. ユーザー1とユーザー2のみ
- D. ユーザー1のみ

正解: C (コメントを发表する)

質問: 148

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: (正解を表示します)

Self-service sign-up: Method by which a user signs up for a cloud service and has an identity automatically created for them in Azure AD based on their email domain.

Azure AD cmdlet Set-MsolCompanySettings could help you to prevent creating user accounts with parameters:

AllowEmailVerifiedUsers (users can join the tenant by email validation)-->when is TRUE.

AllowAdHocSubscriptions (controls the ability for users to perform self-service sign-up) e.g. Set-MsolCompanySettings -AllowEmailVerifiedUsers \$false -AllowAdHocSubscriptions \$false Reference:

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

質問: 149

次の表に示すユーザーを含む Azure AD テナントがあります。

Name	Role
User1	User Administrator
User2	Password Administrator
User3	Security Reader
User4	User

すべてのユーザーに対してセルフサービス パスワード リセット (SSPR) を有効にし、唯一の認証方法としてセキュリティの質問を要求するように SSPR を構成します。

パスワードをリセットするときに秘密の質問を使用する必要があるのはどのユーザーですか？

- A. User4 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 4 のみ
- D. User1、User3、User4 のみ
- E. ユーザー 1、ユーザー 2、ユーザー 3。とユーザー4

正解: (正解を表示します)

Basically, some administrative roles, by design can only use strong, two-gate password reset policy, regardless of SSPR settings. User Administrator and Password Administrator will be always forced to use two methods and cannot use security questions. Securiry Reader and User will use whatever is set under SSPR, so security questions in this case.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

質問: 150

ホットスポットに関する質問

お客様は、Site1 という名前の Microsoft SharePoint Online サイトと、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を所有しています。

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

ユーザーが所有するデバイスは以下の表に示すとおりです。

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Azure AD joined
Device3	Android	Azure AD registered

次の2つの条件付きアクセス ポリシーを作成します。

- 名前: CAPolicy1
- 課題
 - o ユーザーまたはワークロードのID: グループ1
 - o クラウド アプリまたはアクション: Office 365 SharePoint Online

条件

デバイスのフィルタリング: ポリシーからフィルタリングされたデバイスを除外します

ルール構文: device.displayName -startsWith Device?

- o アクセス制御
- 許可: アクセスをブロックする
- セッション: 0個のコントロールが選択されました
- o ポリシーを有効にする: オン

- 名前: CAPolicy2

- 課題

- o ユーザーまたはワークロードのID: グループ2
- o クラウド アプリまたはアクション: Office 365 SharePoint Online
- o 条件: 0 個の条件が選択されました

- アクセス制御

- o 許可: アクセスを許可する

多要素認証を必須とする

- セッション: 0個のコントロールが選択されました
- ポリシーを有効にする: オン

すべてのユーザーは、多要素認証(MFA)を使用して正常に認証できることを確認しています。

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

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
User1 can access Site1 from Device1.	☐	☐
User2 can access Site1 from Device2.	☐	☐
User3 can access Site1 from Device3.	☐	☐

正解:

Statements	Yes	No
User1 can access Site1 from Device1.	☐	☒
User2 can access Site1 from Device2.	☒	☐
User3 can access Site1 from Device3.	☐	☒

質問: 151

お客様は、Microsoft Entra ID Premium ライセンスを使用する Microsoft Entra テナントをお持ちです。テナント向けに利用規約(ToU)を設定する予定です。利用規約(ToU)文書をアップロードする必要があります。文書にはどの形式を使用すべきですか？

- A. HTML
- B. RTF

C. PDF 最も投票された

D. DOCX

正解: C (コメントを発表する)

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/terms-of-use>

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 385問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 152

シミュレーション

必要に応じて、以下のログイン情報を使用してください。

ユーザー名を入力するには、サインインボックスにカーソルを置き、下のユーザー名をクリックしてください。

パスワードを入力するには、カーソルを「パスワードを入力」ボックスに置いて、下のパスワードをクリックしてください。

Microsoft 365 ユーザー名: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365ポータルがブラウザに正常に読み込まれない場合は、Ctrl+Kキーを押して新しいブラウザタブでポータルを再読み込みしてください。

以下の情報は、技術サポートのみを目的としています。

ラボインスタンス: 99999999

sg-Legalグループのユーザーがテナントによって管理されているクラウドアプリにアクセスする際には、12時間ごとに再認証を行う必要があることを確認してください。

このタスクを完了するには、該当する管理センターにサインインしてください。

正解:

Microsoft Entra, Microsoft Entra ID, Conditional Access, Configure adaptive session lifetime policies

Sign-in frequency control

Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access.

Step 3: Select Create new policy.

Step 4: Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Step 5: Choose all required conditions for customer’s environment, including the target cloud apps.

Step 6: Under Access controls > Session.

Step 6a: Select Sign-in frequency.

Step 6b: Choose Periodic reauthentication and enter a value of hours or days [Specify 12 hours: 12 + Hours as Unit] or select Every time.

Home > Control > Security > Security > Conditional Access > Conditional Access > Policies > Create new policy

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name *

Sign-in frequency



Assignments

Users or workload identities ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[1 app included](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

[0 controls selected](#)

Session ⓘ

[0 controls selected](#)

Session



Control access based on session controls to enable limited experiences within specific cloud applications.

[Learn more](#)

☐ Use app enforced restrictions ⓘ

☐ Use Conditional Access App Control ⓘ

☒ Sign-in frequency ⓘ

☒ Periodic reauthentication

0

Select units



☐ Every time



Some of the applications currently selected are not compatible with the "Sign-in frequency" option of "Every time"

☐ Persistent browser session ⓘ

☐ Customize continuous access evaluation ⓘ

Enable policy

Report-only

On

Off

Create

☐ Disable resilience defaults ⓘ

Select

Step 6c: For Assignments, User or workload identities, specify the sg-Legal group

Step 6d: For Cloud apps or actions, specify any/all cloud apps.

Step 7: Click Create, and save your policy.

Reference:
<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-session-lifetime>

質問: 153

Azure Active Directory (Azure AD) 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、AzureAD サインインログを確認する必要があります。
Azure AD はどのくらいの期間イベントをサインインログに保存しますか？

- A. 14 日
- B. 30 日
- C. 90 日
- D. 365 日

正解: B (コメントを发表する)
<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention#how-long-does-azure-ad-store-the-data>

質問: 154

あなたは、Automation1 という名前の Azure Automation アカウントを含む Azure サブスクリプションを持っています。
Automation1 に Azure リソースへのアクセス権を付与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 に付与された権限が削除されていることを確認してください。
アカウントは削除されました。
管理業務の手間を最小限に抑える。

- 何をすべきでしょうか？
- A. ユーザーが割り当てた管理 ID
 - B. システムによって割り当てられた管理 ID
 - C. 証明書

D. クライアントの秘密

正解: [\(正解を表示します\)](#)

質問: 155

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

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

Azure Monitor は、Azure Active Directory (Azure AD) のアクティビティ ログを分析するために使用します。

Azure AI のユーザーサインイン試行を監視した結果、毎日 100 件以上のメールアラートが届きます。

あなたではなく、新しいセキュリティ管理者がアラートを受信するように設定する必要があります。

解決策 :Azure AD から、Insights の管理者ロールの割り当てを作成します。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解: [\(正解を表示します\)](#)

質問: 156

必要に応じて、以下のログイン情報を使用してください。

ユーザー名を入力するには、サインインボックスにカーソルを置き、下のユーザー名をクリックしてください。

パスワードを入力するには、カーソルを「パスワードを入力」ボックスに置いて、下のパスワードをクリックしてください。

Microsoft 365 ユーザー名: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365ポータルがブラウザに正常に読み込まれない場合は、Ctrl+Kキーを押して新しいブラウザタブでポータルを再読み込みしてください。

以下の情報は、技術サポートのみを目的としています。

ラボインスタンス: 99999999

多要素認証(MFA)を導入する必要があります。導入するソリューションは、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のみ、MFA登録を義務付ける。

- デブラ ッバーガーをMFA(美術学修士)課程への登録義務から除外する。

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する。

このタスクを完了するには、該当する管理センターにサインインしてください。

正解:

Configure the Microsoft Entra multifactor authentication registration policy

Policy configuration

Step 1: Sign in to the Microsoft Entra admin center as at least a Security Administrator

Step 2: Browse to Protection > Identity Protection > MFA registration policy.

Step 3: Under Assignments > Users

Step 4: Under Include, select All users or Select individuals and groups if limiting your rollout.
[Select sg-Finance group]

Step 5: Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts. [Select Debra Berger]

Step 6: Enforce Policy - On

Step 7: Save

Reference:

<https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-mfa-policy>

質問: 157

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

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

あなたはMicrosoft 365テナントをお持ちです。

貴社には100名のIT管理者がおり、10の部署に組織されています。

展示資料に示されているアクセス審査を作成します。(展示資料」タブをクリックしてください。)

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Admin review ✓

Description ⓘ

Start date * 12/18/2020 📅

Frequency Monthly ▾

Duration (in days) ⓘ 14

End ⓘ **Never** End by Occurrences

Number of times ⓘ

End date 01/17/2021 📅

Users Scope ☒ Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers
Reviewers (Preview) Manager ▾

(Preview) Fallback reviewers ⓘ
Megan Bowen

▾ Upon completion settings

Start

アクセス審査の依頼はすべてメガン・ボーエンが受け取っていることが分かります。

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受け取れるようにする必要があります。

解決策：各役割ごとに個別のアクセス審査を作成します。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解: (正解を表示します)

Each access review would still send review approval to Megan as no manager has been set for the user accounts under review.

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

質問: 158

ドラッグアンドドロップ問題

お客様のネットワークには、contoso.com という名前の Active Directory フォレストが含まれており、Azure AD Connect を使用して、contoso.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。

Attire AD Connectは、Server1という名前のサーバーにインストールされています。

Windows Server 2019を実行するServer1という名前の新しいサーバーをデプロイします。

Azure AD Connect のフェールオーバー サーバーを実装する必要があります。このソリューションは、Server1 が故障した場合にフェールオーバーにかかる時間を最小限に抑える必要があります。

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

Actions

On Server1, run export for all connectors.

On Server2, run export for all connectors.

On Server2, run full import for all connectors.

On Server2, run delta synchronization for all connectors.

On Server2, install Azure AD Connect.

On Server1, configure the staging mode.

Answer Area

正解:

Actions

On Server2, run full import for all connectors.

On Server2, install Azure AD Connect.

On Server1, configure the staging mode.

Answer Area

On Server2, run export for all connectors.

On Server2, run delta synchronization for all connectors.

On Server1, run export for all connectors.

質問: 159

ケーススタディ3 - A Datum Corp

概要

A Datum Corporationはモントリオールに拠点を置くコンサルティング会社です。A Datumは最近、バンクーバーに拠点を置くLitware, Inc.を買収しました。

既存の環境

データム環境

A Datumのオンプレミスネットワークには、adatum.comという名前のActive Directory ドメインサービス(AD DS)フォレストが含まれています。

Datum は Microsoft 365 E5 サブスクリプションを所有しています。このサブスクリプションには、Azure AD Connect を使用して adatum.com AD DS ドメインと同期する検証済みドメインが含まれています。Datum

は、adatum.com という名前の Azure Active Directory (Azure AD) テナントを所有しています。このテナントでは、セキュリティの既定値が無効になっています。
テナントには、以下の表に示すユーザーが含まれています。

Name	Role
User1	None
User2	None
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

テナントには、以下の表に示すグループが含まれています。

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	None	All users in the IT department
AdatumUsers	Security	Assigned	None	User1, User2

既存の環境

Litware環境

Litwareはlitware.comという名前のAD DSフォレストを持っています。

既存の環境

問題提起

データは、以下の問題を特定します。

営業部門の複数のユーザーが最大5台のデバイスを所有しています。営業部門のユーザーからは、デバイス数の上限に達したため、Azure ADテナントにデバイスを参加させるためにサポート部門に連絡しなければならない場合があるとの報告がありました。

最近のセキュリティインシデントにより、複数のユーザーが認証情報を漏洩し、不審なブラウザがログインに使用され、匿名のIPアドレスからリソースにアクセスされたことが明らかになった。

- デバイス管理者ロールを IT_Group1 に割り当てようとすると、そのグループが選択リストに表示されません。

組織内の誰でも、他のゲストや管理者以外のユーザーを含め、ゲストユーザーを招待できます。

ヘルプデスクはユーザーパスワードのリセットに時間をかけすぎている。

現在、ユーザーは認証にパスワードのみを使用しています。

要件

計画されている変更

A Datum社は、以下の変更を実施する予定です。

- セルフサービスパスワードリセット(SSPR)を設定します。

- すべてのユーザーに対して多要素認証(MFA)を設定します。

- Package1 という名前のアクセス パッケージのアクセス レビューを設定します。

組織データへのアプリケーションアクセスには、管理者の承認が必要となる。

- AD DSユーザーとgroupsoflitware.comをAzure ADテナントと同期します。

特定の管理者ロールが割り当てられたユーザーのみがゲストユーザーを招待できるようにします。

- Azure AD に参加または登録できるデバイスの最大数を 10 に増やします。

要件

技術要件

基準点には、以下の技術要件が規定されています。

- ユーザー管理者ロールを割り当てられたユーザーは、必要に応じて最長1年間、そのロールを使用するための許可を要求できる必要があります。

- ユーザーには多要素認証(MFA)への登録を促し、一定期間の登録をスキップできるオプションを提供する必要があります。

- ユーザーは、SSPRを使用してパスワードをリセットするために、1つの認証方法を提供する必要があります。

利用可能な方法には以下が含まれる必要があります。

- メール

- 電話

- セキュリティに関する質問

- Microsoft Authenticator アプリ

- adatum.comとlitware.comのAD DSドメイン間で信頼関係を確立してはなりません。

最小権限の原則を適用しなければならない。

IT_Group1の問題を解決する必要があります。

まず最初に何をすべきでしょうか？

A. IT_Group1 のメンバーシップタイプを動的ユーザーに変更します。

B. IT_Group1グループを再作成します。

C. ITグループ1のメンバーシップタイプを動的デバイスに変更します。

D. IT_Group1にオーナーを追加します。

正解: **B** ([コメントを發表する](#))

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

質問: **160**

あなたはcontoso.comというSMTPアドレス空間を使用するMicrosoft Exchange組織を持っています。

複数のユーザーが、Azure ADへのセルフサービス登録にcontoso.comの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 Azure AD テナントに対するグローバル管理者権限が付与されます。

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のために、contoso.comのAzure AD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べきですか？

A. Update-MgOrganization

B. Update-MgPolicyPermissionGrantPolicyExclude

C. Update-MgDomain

D. Update-MgDomainFederationConfiguration

正解: ([正解を表示します](#))

The Update-MgPolicyPermissionGrantPolicyExclude cmdlet is used to exclude a policy from being applied to a specific set of users. In this case, you can use the cmdlet to exclude the self- service sign-up policy from being applied to users with the contoso.com SMTP address space.

質問: **161**

新しい Microsoft 365 テナントを構成して、既定のドメイン名として contoso.com を使用します。

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ようにする必要があります。

まず最初に何をすべきでしょうか？

- A. セキュリティのデフォルト設定を無効にします。
- B. ユーザー同意設定を無効にします。
- C. 多要素認証(MFA)登録ポリシーを設定します。
- D. Azure AD テナントのパスワード保護を設定します。

正解: ([正解を表示します](#))

質問: 162

お客様はMicrosoft Entraテナントをお持ちです。

テナントへの管理者アクセスを管理するには、条件付きアクセス ポリシーを作成する必要があります。

このソリューションは、フィッシング対策に優れた多要素認証(MFA)方式を用いて、管理者が認証されることを保証する必要がある。

解決策に含めるべき認証方法はどれですか？正解はそれぞれ完全な解決策を示しています。

- A. 証明書ベース認証(シングルファクター)
- B. 音声通話
- C. マイクロソフト認証システム
- D. 証明書ベース認証(多要素認証)
- E. メールOTP
- F. Windows Hello for Business
- G. FIDO2セキュリティキー
- H. SMS

正解: ([正解を表示します](#))

質問: 163

あなたはMicrosoft 365のサブスクリプションをお持ちです。

あなたは、App1 という名前の Azure App Service Web アプリを含む Azure サブスクリプションを所有しています。

お使いのデバイスは複数台あり、いずれもWindowsを搭載し、Microsoft Intuneに登録されています。

Intuneを使用して、グローバルセキュアアクセスクライアントをデバイスに展開します。

App1へのプライベートアクセスを設定する必要があります。

次に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. トラフィック転送プロファイルを設定します。
- C. リモートネットワークを作成します。
- D. アプリケーションセキュリティグループを作成します。

正解: ([正解を表示します](#))

質問: 164

事例研究1 - Contoso, Ltd

概要

Contoso, Ltd.は、モントリオールに本社を置き、ロンドンとシアトルに支店を持つコンサルティング会社です。

ContosoはFabrikam, Inc.という会社と提携関係にある。Fabrikamはfabrikam.comという名前のAzure Active Directory(Azure AD)テナントを所有している。

既存環境。既存環境

Contosoのオンプレミスネットワークには、contoso.comという名前のActive Directoryドメインが含まれています。

このドメインには、Contoso_Resources という名前の組織単位 (OU) が含まれています。Contoso_Resources OU には、すべてのユーザーとコンピューターが含まれています。

contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

既存環境 :Microsoft 365/Azure環境

Contosoはcontoso.comという名前のAzure ADテナントを所有しており、それには以下のライセンスが関連付けられています。

- * Microsoft Office 365 Enterprise E5
- * エンタープライズモビリティ+セキュリティ
- * Windows 10 Enterprise E3
- * プロジェクト計画3

Azure AD Connectは、Azure ADとActive Directoryドメインサービス(AD DS)の間で構成されています。同期されるのはContoso_Resources OUのみです。

ヘルプデスク管理者は、ユーザー設定を管理するために日常的にMicrosoft 365管理センターを使用します。

現在、ユーザー管理者はMicrosoft 365管理センターを使用してライセンスを手動で割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。

- * ロンドンオフィスのユーザーは、Microsoft 365 Phone Systemのライセンスが未割り当ての状態です。

シアトルオフィスのユーザーは、Yammer Enterpriseライセンスを未割り当ての状態です。

contoso.com では、セキュリティのデフォルト設定が無効になっています。

Contosoは、管理者ロールを保護するためにAzure ADの特権ID管理(PIM)を使用しています。

既存環境。問題点

コントソ氏は以下の問題点を指摘している。

- * 現在、すべてのヘルプデスク管理者は、Microsoft 365テナント全体にわたるユーザーライセンスを管理できます。
- * ユーザー管理者からは、Contosoの各オフィスごとに異なるライセンス要件を手動で設定するのは面倒だという報告が寄せられています。

ヘルプデスク管理者は、必要なMicrosoft 365サービスおよびアプリへの内部アクセスとゲストアクセスをプロビジョニングするのに時間をかけすぎている。

- * 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
- * Azure AD で [ログ] ノードを選択すると、Log Analytics の統合が有効になっていないことを示すエラーメッセージが表示されます。

要件。計画されている変更

コントソ氏は以下の変更を実施する予定です。

- * セルフサービスパスワードリセット(SSPR)を実装する。
- * Azure Monitorを使用して、Azure監査アクティビティログを分析します。

- * テナントに追加された新規ユーザーに対するライセンス割り当てを簡素化します。
- * Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施する。
- * ユーザー管理者ロールを設定し、有効化する際に正当性の説明と承認が必要となるようにします。
- * App1という名前の、業務専用のカスタムAzure Webアプリを実装します。App1はインターネットからアクセス可能で、Azure ADアカウントを使用して認証されます。
- * マーケティング部門の新規ユーザー向けに、Microsoft SharePoint Onlineのサイト、グループ、およびアプリへのアクセス権限を付与するための自動承認ワークフローを実装します。

Contoso社はAdatum Corporationという会社を買収する予定です。Adatumという名前のActive Directory組織単位(OU)内に、新たに100人のAdatumユーザーが作成されます。これらのユーザーはロンドンとシアトルに拠点を置く予定です。

要件。技術要件

Contoso社は、以下の技術要件を特定しました。

- * すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期されている必要があります。
- * App1 には、https://contoso.com/auth-response を指すリダイレクト URI が必要です。
- * 新規ユーザーへのライセンス割り当ては、ユーザーの所在地に基づいて自動的に行われる必要があります。
- * Fabrikamのユーザーは、マーケティング部門のSharePointサイトに最大90日間アクセスできる必要があります。
- * Azure AD で実行される管理操作は監査対象とする必要があります。監査ログは 1 年間保持する必要があります。
- * ヘルプデスク管理者は、それぞれのオフィスに所属するユーザーのライセンスのみを管理できる必要があります。
- * ユーザーの身元が侵害された可能性がある場合、ユーザーにはパスワードの変更を強制しなければならない。

ホットスポットに関する質問

ユーザーの身元情報が侵害された可能性に関する技術的な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、設定すべき項目は何でしょうか？回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

The users must first:

Provide consent for any app to access the data of Contoso.

Register for multi-factor authentication (MFA).

Register for self-service password reset (SSPR).

You must configure:

A sign-in risk policy

A user risk policy

An Azure AD Password Protection policy

正解:

Answer Area



The users must first:

Provide consent for any app to access the data of Contoso.

Register for multi-factor authentication (MFA).

Register for self-service password reset (SSPR).

You must configure:

A sign-in risk policy

A user risk policy

An Azure AD Password Protection policy

Explanation:

User risk is a calculation of probability that an "identity" has been compromised. Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset. <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

質問: 165

ホットスポットに関する質問

お客様のネットワークには、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、以下の表に示すグループが含まれています。

Name	Source	Member of
Group1	Cloud	Group3
Group2	Active Directory domain	None
Group3	Cloud	None

テナントには、以下の表に示すユーザーが含まれています。

Name	Directory-synced	Member of
User1	No	Group1
User2	No	Group2
User3	Yes	Group3

以下の表に示すように、アクセス審査を作成します。

Setting	Value
Review type	Teams + Groups
Review scope	All users
Group	Group2, Group3
Reviewers	Users review own access
If reviewers don't respond	Remove access

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 will be removed automatically from Group 1 if the user does not respond to the review request.	☐	☐
User 2 will be removed automatically from Group 3 if the user does not respond to the review request.	☐	☐
User 3 will be removed automatically from Group 2 if the user does not respond to the review request.	☐	☐

正解:

Answer Area

Statements

Yes

No

User1 will be removed automatically from Group 1 if the user does not respond to the review request.

☐☒

User 2 will be removed automatically from Group 3 if the user does not respond to the review request.

☐☒

User 3 will be removed automatically from Group 2 if the user does not respond to the review

☐☒

Explanation:

Box 1: No

User1 is member of Group1. Group1 is in the cloud. Group1 is member of Group3. Group3 is in the cloud.
The access review applies to Group3, but not to Group1. The access review is setup to remove access if reviewers don't respond.

Box 2: No

User2's membership cannot be managed since he is a part of Group2 which is an AD group (not AAD).

Box 3: No

User3 is member of Group3, not of Group2.

Reference:

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

質問: 166

ホットスポットに関する質問

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。

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

次の表に示すように、グループ1のアクセス審査を作成します。

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

次の表に示すように、グループ2のアクセス審査を作成します。

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

各グループに必要な Azure Active Directory Premium P2 ライセンスの最小メンバー数はいくつですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Group1:

1

500

525

Group2:

1

100

295

395

正解:

Group1: ▼

1
500
525

Group2: ▼

1
100
295
395



Explanation:

Box 1: 500

Scenario = An administrator creates an access review of Group C with 50 member users and 25 guest users. Makes it a self-review.

Calculation = 50 licenses for each user as self-reviewers.*

Number of licenses = 50

* Azure AD External Identities (guest user) pricing is based on monthly active users (MAU), which is the count of unique users with authentication activity within a calendar month. This model replaces the 1:5 ratio billing model, which allowed up to five guest users for each Azure AD Premium license in your tenant.

Box 2: 1

For Group2:

Review scope: Guest users only. Reviewers: Group Owner.

Reference:

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

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 385問、30%ディスカウント、特別な割引コード: **JPNshiken**」

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. はい

B. いいえ

正解: B (コメントを发表する)

Adding the GitHub app connector to Microsoft Defender for Cloud Apps will allow you to monitor OAuth authentication requests from GitHub to Microsoft 365. However, it will not allow you to monitor OAuth authentication requests to your AWS account, Google Workspace subscription, or Azure subscription.

質問: 168

ホットスポットに関する質問

お客様は、Microsoft Entra Permissions Management を使用する Azure サブスクリプションをお持ちです。

あなたはAmazon Web Services(AWS)のアカウントをお持ちです。

あなたは権限管理をAWSに接続する予定です。

Azureでアクセス許可管理アプリを作成する必要があります。

PowerShellコマンドをどのように実行すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

New-AzureADApplication

New-AzureADApplicationExtensionProperty

New-AzureADApplicationKeyCredential

-DisplayName "mciem-aws-oidc-connector"

-GroupMembershipClaims

-IdentifierUrls

-InformationalUrls

-KeyCredentials

"api://mciem-aws-oidc-app"

正解:

Answer Area

New-AzureADApplication

New-AzureADApplicationExtensionProperty

New-AzureADApplicationKeyCredential

-DisplayName "mciem-aws-oidc-connector"

-GroupMembershipClaims

-IdentifierUrls

-InformationalUrls

-KeyCredentials

"api://mciem-aws-oidc-app"

質問: 169

シミュレーション

必要に応じて、以下のログイン情報を使用してください。

ユーザー名を入力するには、サインインボックスにカーソルを置き、下のユーザー名をクリックしてください。

パスワードを入力するには、カーソルを「パスワードを入力」ボックスに置いて、下のパスワードをクリックしてください。

Microsoft 365 ユーザー名: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365ポータルがブラウザに正常に読み込まれない場合は、Ctrl+Kキーを押して新しいブラウザタブでポータルを再読み込みしてください。

以下の情報は、技術サポートのみを目的としています。

ラボインスタンス: 99999999

あなたの会社は、App1という名前の新しいカスタムWebアプリを開発しています。

App1をMicrosoft Entra IDに登録する必要があります。認証済みのユーザーは、URI https://app1.contoso.com にリダイレクトされる必要があります。

このタスクを完了するには、該当する管理センターにサインインしてください。

正解:

Register an application with the Microsoft identity platform

Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around. Once created, the application object can't be moved between different tenants.

Specify who can use the application in the Supported account types section.

Step 1: Sign in to the Microsoft Entra admin center.

Step 2: If you have access to multiple tenants, use the Settings icon in the top menu to switch to the tenant in which you want to register the application from the Directories + subscriptions menu.

Step 3: Browse to Identity > Applications > App registrations and select New registration.

Step 4: Enter a display Name for your application. [Here: App1]

Step 5: Specify who can use the application in the Supported account types section.

Step 6: Redirect URI (optional). [Here: https://app1.contoso.com]

Step 7: Select Register to complete the initial app registration.

Home > Contoso AD (dev) >

Register an application

 Microsoft

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

 Accounts in this organizational directory only (Contoso AD (dev) only - Single tenant)

Accounts in the organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Register

Reference:

<https://learn.microsoft.com/en-us/graph/auth-register-app-v2>

質問: 170

お客様はMicrosoft Entraテナントをお持ちです。
アプリへのサインインに対する継続的なアクセス評価を設定し、その設定をアプリケーション管理者ロールが割り当てられているユーザーに割り当てる必要があります。
何を設定すればよいですか？
A. アクセスレビュー
B. サインインリスクポリシー
C. 条件付きアクセスポリシー
D. 管理者同意設定
正解: (正解を表示します)

質問: 171

ドラッグアンドドロップ問題
あなたは、User1、User2、User3という名前の3人のユーザーを含むMicrosoft 365 E5サブスクリプションを所有しています。
以下の表に示すように、ユーザーを設定する必要があります。

User	Configuration
User1	• User administrator role • Device Administrators role • Identity Governance Administrator role
User2	• Records Management role • Quarantine Administrator role group
User3	• Endpoint Security Manager role • Intune Role Administrator role

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？回答するには、適切なポータルを正しい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、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

Portals

Azure Active Directory admin center

Exchange admin center

Microsoft 365 compliance center

Microsoft Endpoint Manager admin center

SharePoint admin center

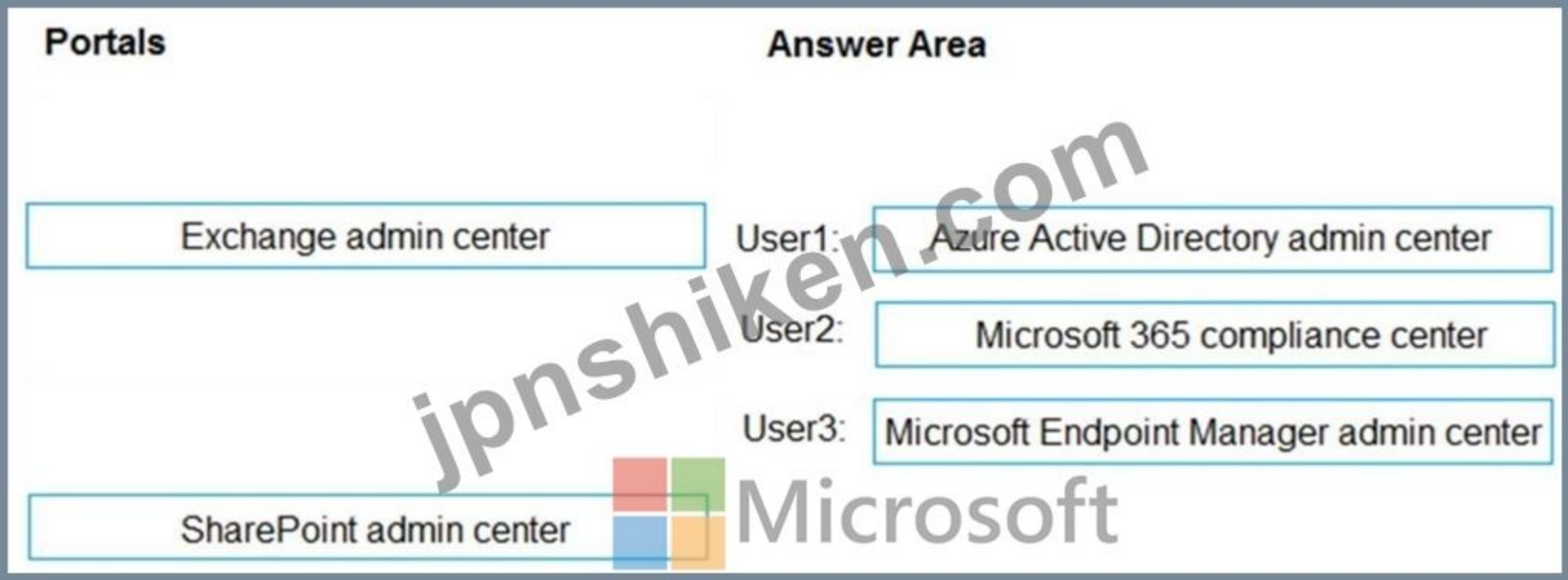
Answer Area

User1:

User2:

User3:

正解:



Explanation:

User 1: Azure Active Directory Admin Center

User 2: Microsoft Purview admin center (legacy Microsoft Compliance Admin center) These roles came from Exchange, Microsoft is not enforcing the roles permission from Exchange, Microsoft is recommending using Microsoft Purview Admin center. I believe this answer is too old.
it could be true years ago, however, Microsoft today is with MS purview to assign these roles.
Record management and Quarantine role are known as SCC (security and compliance center) SCC roles have evolved from Exchange role groups design to MS Purview.

User 3: Microsoft Endpoint Manager Admin Center

You will see these two roles in the endpoint admin center.

質問: 172

Sub1 という名前の Azure サブスクリプションがあり、その中に RG1 という名前のリソース グループが含まれています。RG1 には、DB1 という名前の Azure Cosmos DB データベースと、AKS1 という名前の Azure Kubernetes Service (AKS) クラスタが含まれています。AKS1 はマネージド ID を使用しています。

AKS1がDB1にアクセスできることを確認する必要があります。ソリューションは以下の要件を満たす必要があります。

- AKS1がマネージドIDを使用してDB1にアクセスするようにしてください。

最小権限の原則に従うこと。

AKS1のマネージドIDには、どの役割を割り当てるべきですか？

A. Sub1 にオーナーの役割を割り当てます。

B. DB1 に対して、Azure Cosmos DB アカウントの閲覧者ロールを割り当てます。

C. RG1 に閲覧者の役割を割り当てます。

D. RG1 に対して、Azure Cosmos DB データ リーダー ロールを割り当てます。

正解: (正解を表示します)

質問: 173

貴社では、ユーザーが社内アプリケーションにアクセスする前に、アクセス許可を申請することを義務付けています。

Azure Active Directory (Azure AD) に 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登録し、MyApp1 のシングル サインオン (SSO) を構成します。

MyApp1では、次にどの設定を構成すればよいでしょうか？

- A. セルフサービス
- B. プロビジョニング
- C. アプリケーションプロキシ
- D. 役割と管理者

正解: ([正解を表示します](#))

Users can self discover apps, users can request access for app, can configure list of individuals to approve or require business approval before granting access to application.

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

質問: 174

ActiveDirectoryドメインに同期するAzureActive Directory (Azure AD)テナントがあります。

オンプレミスネットワークには、オンプレミスActiveDirectoryドメインに対して認証を行うVPNサーバーが含まれています。VPNサーバーは、Azure Multi-Factor Authentication (MFA)をサポートしていません。

VPN接続にAzureMFAを提供するソリューションを推奨する必要があります。

推奨事項には何を含める必要がありますか？

- A. AzureADアプリケーションプロキシ
- B. AzureADパスワード保護プロキシ
- C. ネットワークポリシーサーバー (NPS)
- D. パススルー認証プロキシ

正解: ([正解を表示します](#))

NPS (Network Policy and Access Service) is like a middle man between the VPN client and Azure MFA. The NPS role is installed on a domain-joined server or the domain controller and is configured to authenticate and authorize RADIUS requests from the VPN client.

The VPN should be configured to use RADIUS authentication and point to the NPS server.

The MFA NPS extension is installed anywhere but the VPN server. When a user/VPN client attempts to authenticate, it sends a RADIUS request to the NPS server through the VPN which performs the primary authentication and then triggers the NPS Extension for secondary authentication.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn>

質問: 175

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

ユーザーがサブスクリプションにログインする際に、カスタマイズされた利用規約(ToU)に同意するよう促されるようにする必要があります。

何を設定すればよいですか？

- A. アクセスパッケージ
- B. 条件付きアクセスポリシー
- C. ライフサイクルワークフロー
- D. 認証方法

正解: ([正解を表示します](#))

Organizations can use terms of use along with Conditional Access policies to require employees or guests to accept your terms of use policy before getting access.

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/terms-of-use#add-terms-of-use>

質問: 176

お客様はAzure AD Premium P2テナントをお持ちです。

Log Analyticsワークスペースを作成します。

Azure Monitorを使用してAzure ADの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。

まず最初に何をすべきでしょうか？

- A. Azure AD ワークブックを作成します。
- B. Azure AD の診断設定を変更します。
- C. Update-MgOrganization コマンドレットを実行します。
- D. Update-MgDomain コマンドレットを実行します。

正解: B (コメントを发表する)

質問: 177

Sub1という名前のAzureサブスクリプションがあり、その中にUser1という名前のユーザーがいます。

User1がSub1向けにMicrosoft Entra Permissions Managementライセンスを購入できるように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。

User1にはどの役割を割り当てるべきですか？

- A. 権限管理管理者
- B. グローバル管理者
- C. ユーザーアクセス管理者
- D. 請求管理者

正解: (正解を表示します)

質問: 178

ユーザー「User1」を含むAzureサブスクリプションをお持ちです。

Azure ADテナントのアプリ登録設定は、次の図に示すように構成されます。



User1はApp1という名前のASP.NET Webアプリケーションを構築します。

User1がApp1を登録できるようにする必要があります。解決策は最小権限の原則に従う必要があります。

User1にはどの役割を割り当てるべきですか？

- A. アプリケーション開発者
- B. クラウドアプリセキュリティ管理者
- C. クラウドアプリケーション管理者
- D. アプリケーション管理者

正解: (正解を表示します)

Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf

when the Users can consent to apps accessing company data on their behalf setting is set to No.
<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability-is-disabled>

質問: 179

Microsoft365テナントがあります。
Azure Active Directory (Azure AD) テナントは、オンプレミスのActiveDirectoryドメインに同期します。
Emergency1という名前の緊急アクセス管理アカウントを作成する予定です。Emergency1には、AzureADのグローバル管理者の役割が割り当てられます。Emergency1は、AzureAD機能の障害およびオンプレミスインフラストラクチャの障害が発生した場合に使用されます。
緊急時にEmergency1がサインインできなくなる可能性を減らす必要があります。
あなたは何をすべきか？

- A. Emergency1が変更された場合、またはサインインした場合にアラートを生成するようにAzureMonitorを構成します。
- B. Emergency1のグローバル管理者ロールのAzure AD特権ID管理 (PIM) アクティベーションが必要です。
- C. Emergency1のサインイン場所を企業ネットワークのみに制限する条件付きアクセスポリシーを構成します。
- D. Emergency1に多要素認証 (MFA) を要求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: (正解を表示します)
Monitor sign-in and audit logs
Organizations should monitor sign-in and audit log activity from the emergency accounts and trigger notifications to other administrators.
When you monitor the activity on break glass accounts, you can verify these accounts are only used for testing or actual emergencies.
You can use Azure Log Analytics to monitor the sign-in logs and trigger email and SMS alerts to your admins whenever break glass accounts sign in.

質問: 180

ホットスポットに関する質問
貴社は、Microsoft Entra IDを使用して、Microsoft 365サービスへのユーザーおよびゲストのアクセスを管理しています。
お客様が最近、ゲストアクセスを有効にしたことで、ユーザーが他社とプロジェクトで共同作業できるようになりました。現在のユーザー設定構成は、以下の3つの図に示されています。



Administration center

[Learn more](#)

Restrict access to Microsoft Entra admin center ☒ No

LinkedIn account connections

[Learn more](#)

Allow users to connect their work or school account with LinkedIn ☐ Yes ☒ Selected group ☐ No

Allow users to connect their work or school account with LinkedIn * AWS-WS [Edit](#)

[Home](#) > [IamITGeek](#) | [User settings](#)

User features

[Save](#) [Discard](#)

Starting Sept. 30th, 2022 Combined registration experiences for multifactor authentication and SSPR will be enabled for all tenants.

Users can use preview features for My Apps ☐ None ☒ Selected ☐ All

Users can use the combined security information registration experience ☐ None ☒ Selected ☐ All

Select a group

AWS-WS

Administrators can access My Staff ☐ None ☒ Selected ☐ All

Select a group

AVD-Users

新たに協力する必要があるプロジェクトチームの一つは、以下の要件を満たしています。

Username	Group Association	Requirements
User-GU-A	None	Requires same access as UserC
UserA	AVD-Users, AWS-WS	- Should not be able to access preview features for My Apps - Needs to access LinkedIn with Microsoft Entra ID account
UserB	AVD Users	- Requires access to My Staff - Needs to be able to use the combined security information registration experience
UserC	AWS-WS	Needs to access LinkedIn with the Microsoft Entra ID account
UserD	AVD-Users	- Should not be able to access preview features for My Apps - Needs to access LinkedIn with the Microsoft Entra ID account

一部のユーザーから次のような報告がありました。

- User-GU-A (ゲストユーザー) は、現在以下の UserCと同じアクセス権限。
- UserBは、統合されたセキュリティ情報を使用できないと報告しています。登録手続きの手順。
- UserDは、MicrosoftアカウントでLinkedInにアクセスできないと報告している。Entra IDアカウント。

ユーザーの要件を満たすために、Microsoft Entra のユーザー設定を更新する必要があります。以下の各項目について、該当する場合は 「はい」を選択してください。該当しない場合は 「いいえ」を選択してください。

Statement	Yes	No
You should change Guest User access to be more inclusive to allow User-GU-A to have the same access as UserC.	☐	☐
You need to add UserB to the AWS-WS group to allow them access to My Staff.	☐	☐
Only UserA and UserD can access the Combined Security Information Registration Experience.	☐	☐

正解:

Statement	Yes	No
You should change Guest User access to be more inclusive to allow User-GU-A to have the same access as UserC.	☒	☐
You need to add UserB to the AWS-WS group to allow them access to My Staff.	☐	☒
Only UserA and UserD can access the Combined Security Information Registration Experience.	☐	☒

Explanation:

You should change Guest user access to be more inclusive to allow User-GU-A to have the same access as UserC. With the current configuration of the User Settings and User Features, as shown in the three exhibits, Guest user access is set to limit access to properties and memberships of directory objects. To allow User-GU-A to have the same access as UserC, this setting would need to change to the most inclusive setting, which is Guest users have the same access as members.

You do not need to add UserB to the AWS-WS group to allow them access to My Staff. With the current configuration of the User Settings and User Features, as shown in the three exhibits, we can see that only the AVD-Users group have been added to the setting Administrator can access My Staff option. As UserB is already a member of this group, they already have the access they need to access My Staff, and you do not need to add them to the AWS-WS group.

Not only UserA and UserD can access the Combined Security Information Registration Experience. With the current configuration of the User Settings and User Features, as shown in the three exhibit images, we can see that the AVD-Users group is selected under the Users can use the combined security information registration experience setting. In this scenario, UserA, UserB, and UserD are all in the AVD-User group.

質問: 181

ホットスポットに関する質問

Microsoft Entraテナントには、Group1とGroup2という名前の2つのグループと、次の表に示すユーザーが含まれています。

Name	Type	Member of	Description
User1	Member	Group1	None
User2	Guest	Group1	None
User3	Member	None	Assigned the Owner role for Group1
User4	Member	Group2	Assigned the Owner role for Group2
User5	Guest	Group2	None

グループ2はグループ1のメンバーである。

以下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: チームとグループを選択
- グループ: グループ1
- 対象 :ゲストユーザーのみ
- レビュー担当者の選択 :グループオーナー

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

注：正解ごとに1ポイントが加算されます。

Answer Area Microsoft

Statements	Yes	No
User3 can perform an access review of User1.	☐	☐
User3 can perform an access review of User4.	☐	☐
User3 can perform an access review of User5.	☐	☐

正解:

Answer Area Microsoft

Statements	Yes	No
User3 can perform an access review of User1.	☐	☒
User3 can perform an access review of User4.	☐	☒
User3 can perform an access review of User5.	☒	☐

有効的な**SC-300J**問題集はJPNTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-300J**試験問題集を提供します。JPNTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> 885問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 182

contoso.com という名前の Azure AD テナントがあり、そこには次の表に示すリソースが含まれています。

Name	Description
Au1	Administrative unit
CAPolicy1	Conditional Access policy
Package1	Access package

Admin1という名前のユーザーを作成します。

Admin1がcontoso.comのセキュリティデフォルト設定を有効にできることを確認する必要があります。

まず最初に何をすべきでしょうか？

- A. パッケージ1を削除します。
- B. CAPolicy1を削除します。
- C. Admin1 に Au1 の認証管理者ロールを割り当てます。
- D. アイデンティティガバナンスを設定します。

正解: B (コメントを发表する)

To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator. Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults. (Imply that Conditional Access policies has conflict with security defaults)

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

質問: 183

ユーザーが重大なサインインアラートをトリガーした場合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。

以下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ログインしました。
- ユーザーがサインインリスクを引き起こした。

テストを完了するには何を使えばよいですか？

- A. 条件付きアクセスのWhat Ifツール
- B. Azure Active Directory(Azure AD)のサインインログ
- C. Microsoft Defender for Cloud Apps のアクティビティ ログ
- D. Azure Active Directory(Azure AD)でのアクセスレビュー

正解: (正解を表示します)

The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.

Reference:

<https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available>

質問: 184

2,500人のユーザーにMicrosoft Office 365 Enterprise E3ライセンスが割り当てられています。ライセンスは個々のユーザーに割り当てられています。

Microsoft Entra 管理センターの [グループ] ブレードから、すべてのユーザーを含むグループに Microsoft Office 365 Enterprise E5 ライセンスを割り当てます。

最小限の管理作業で、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. Microsoft Entra管理センターのライセンスブレード
- B. Microsoft Entra管理センターの 管理ユニット」ブレード
- C. Microsoft Entra管理センターのIDガバナンスブレード
- D. Update-MgUser コマンドレット

正解: (正解を表示します)

To remove the Office 365 Enterprise E3 licenses from the users who are now part of a group with Office 365 Enterprise E5 licenses assigned, you should use the "Licenses" blade in the Microsoft Entra admin center. This allows you to manage license assignments at a group level, making it easier to apply and remove licenses for multiple users simultaneously.

質問: 185

ホットスポットに関する質問

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあり、ゲスト用のメールによるワンタイムパスコードが 「はい」に設定されています。

次の表に示されているゲストユーザーを招待します。

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

どのユーザーにワンタイムパスコードが発行され、そのパスコードの有効期間はどのくらいですか？回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Users:

Microsoft

Guest1 only

Guest2 only

Guest3 only

Guest1 and Guest2 only

Guest2 and Guest3 only

Guest1, Guest2, and Guest3

Valid for:

30 minutes

60 minutes

24 hours

48 hours

正解:

Users:

Microsoft

Guest1 only

Guest2 only

Guest3 only

Guest1 and Guest2 only

Guest2 and Guest3 only

Guest1, Guest2, and Guest3

Valid for:

30 minutes

60 minutes

24 hours

48 hours

Explanation:

Box 1: Guest3 only

When does a guest user get a one-time passcode?

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account

They don't have a Microsoft account

The inviting tenant didn't set up federation with social (like Google) or other identity providers.

Box 2: 30 minutes

One-time passcodes are valid for 30 minutes. After 30 minutes, that specific one-time passcode is no longer valid, and the user must request a new one. User sessions expire after 24 hours.

After that time, the guest user receives a new passcode when they access the resource. Session expiration provides added security, especially when a guest user leaves their company or no longer needs access.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

質問: 186

Microsoft365テナントがあります。

すべてのユーザーは携帯電話とラップトップを持っています。

ユーザーは、Wi-Fiアクセスや携帯電話接続がない遠隔地から頻繁に作業します。ユーザーは、離れた場所から作業しているときに、ラップトップをインターネットにアクセスできる有線ネットワークに接続します。

多要素認証 (MFA) を実装することを計画しています。

ユーザーがリモートロケーションから使用できるMFA認証方法はどれですか？

A. MicrosoftAuthenticatorアプリを介した通知

B. メール

C. セキュリティの質問

D. MicrosoftAuthenticatorアプリからの確認コード

正解: ([正解を表示します](#))

The Authenticator app can be used as a software token to generate an OATH verification code.

After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon.

B: An email requires network connectivity.

C: Security questions are not used as an authentication method but can be used during the self- service password reset (SSPR) process.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app>

質問: 187

お客様は、Site1 という名前の Microsoft SharePoint Online サイトと Team1 という名前の Microsoft Teams チームを含む Microsoft 365 E5 サブスクリプションを所有しています。このサブスクリプションに

は、Group1、Group2、Group3、Group4、Group5 という名前の 5 つのセキュリティ グループが含まれています。

Site1とTeam1へのアクセスパッケージを実装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。

グループ3のメンバーは、サイト1へのアクセスのみを要求できる必要があります。

グループ1のメンバーは、サイト1およびチーム1へのアクセスを要求できる必要があります。

グループ4のメンバーは、サイト1およびチーム1へのアクセスを要求できる必要があります。

- アクセスパッケージを承認できるのはグループ2のメンバーのみである

グループ1メンバーからのリクエスト。

- グループのメンバーのみがアクセスパッケージを承認できる必要があります
グループ3およびグループ4のメンバーからの要望。
作成すべきアクセスパッケージの最小数はいくつですか？

- A. 2
- B. 3
- C. 4
- D. 5

正解: (正解を表示します)

Three access packages needed.

- * Members of Group3 must be able to request access to Site1 only. [One access package for Site1 named X1]
- * Members of Group1 must be able to request access to Site1 and Team1. [One access package for Site1 and Team1 named X2]
- * Members of Group4 must be able to request access to Site1 and Team1. [One access package for Site1 and Team1 named X3]
- * Only members of Group2 must be able to approve access package requests from Group1 members. [Add Group2 as approver for X2]
- * Only members of Group5 must be able to approve access package requests from Group3 and Group4 members. [Add Group5 as approver for X1 and for X3] Reference:
<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-first>

質問: 188

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

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

Azure Monitor は、Azure Active Directory (Azure AD) のアクティビティ ログを分析するために使用します。

Azure AI のユーザーサインイン試行を監視した結果、毎日 100 件以上のメールアラートが届きます。

あなたではなく、新しいセキュリティ管理者がアラートを受信するように設定する必要があります。

解決策 :Azure Monitor からデータ収集ルールを作成します。

これは目標を達成していると言えるでしょうか？

- A. はい
- B. いいえ

正解: (正解を表示します)

Data Collection Rules (DCRs) define the data collection process in Azure Monitor. DCRs specify what data should be collected, how to transform that data, and where to send that data. Some DCRs will be created and managed by Azure Monitor to collect a specific set of data to enable insights and visualizations.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview>>

質問: 189

ホットスポットに関する質問

お客様のMicrosoft Entraテナントには、以下の表に示すユーザーが含まれています。

Microsoft	
Name	Microsoft Entra role
User1	Global Administrator
User2	Attribute Definition Administrator
User3	Security Administrator

テナントには、以下の表に示すIDが含まれています。

Name	Type
Group1	Security group
Service1	Service principal
MI1	Managed identity

どのユーザーがカスタムセキュリティ属性を作成でき、どのIDにその属性を割り当てることができますか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Can create custom security attributes:

User1 only

User2 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Custom security attributes can be assigned to:

Group1 only

Group1 and MI1 only

Group1 and Service1 only

Group1, MI1, and Service1 MI1 only

MI1 and Service1 only

Service1 only

正解:
Answer Area

Can create custom security attributes:

User1 only

User2 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Custom security attributes can be assigned to:

Group1 only

Group1 and MI1 only

Group1 and Service1 only

Group1, MI1, and Service1 MI1 only

MI1 and Service1 only

Service1 only

貴社はMicrosoft 365テナントを所有しています。

すべてのユーザーは、Windows 10 を実行し、Azure Active Directory (Azure AD) テナントに参加しているコンピューターを使用しています。

同社はService1というサードパーティのクラウドサービスを利用している。Service1はOAuthに基づくAzure AD認証および認可をサポートしている。Service1はAzure ADギャラリーに公開されている。

ユーザーが認証を求められることなくService1に接続できるような解決策を提案してください。この解決策は、ユーザーがAzure ADに参加済みのコンピューターからのみService1にアクセスできるようにする必要があります。また、管理作業を最小限に抑える必要があります。

それぞれの要件に対して、どのような推奨事項を提示すべきでしょうか？回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Ensure that the users can connect to Service1 without being prompted for authentication:

An app registration in Azure AD

Azure AD Application Proxy

An enterprise application in Azure AD

A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

Azure AD Application Proxy

A compliance policy

A conditional access policy

An OAuth policy

正解:
Answer Area

Ensure that the users can connect to Service1 without being prompted for authentication:

An app registration in Azure AD

Azure AD Application Proxy

An enterprise application in Azure AD

A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

Azure AD Application Proxy

A compliance policy

A conditional access policy

An OAuth policy

Explanation:

Service1 support OAuth for Authentication & authorization, however Service1 is published in Azure AD gallery, hence we will use An enterprise application in Azure AD blade to register for SSO.

Conditional access policy - to ensure users access from Azure AD joined computers.

質問: 191

2,500人のユーザーにMicrosoft Office 365 Enterprise E3ライセンスが割り当てられています。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、Microsoft Office を割り当てます。
365 Enterprise E5ライセンスを、すべてのユーザーを含むグループに付与します。
最小限の管理作業で、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. Update-MgGroup コマンドレット
- B. Azure Active Directory 管理センターのライセンスブレード
- C. Azure Active Directory 管理センターの「管理ユニット」ブレード
- D. Set-WindowsProductKey コマンドレット

正解: [\(正解を表示します\)](#)

質問: 192

お客様は、User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションを所有しています。User1 はアプリケーション管理者ロールの資格を有しています。
ユーザー1は、アプリケーションプロキシ用の新しいコネクタグループを設定する必要があります。
User1の役割を有効にするには、何を使用すればよいですか？

- A. Microsoft 365 Defender ポータル
- B. Microsoft Defender for Cloud Apps ポータル
- C. Azure Active Directory 管理センター
- D. Microsoft 365 管理センター

正解: [\(正解を表示します\)](#)

質問: 193

ホットスポットに関する質問

お客様は、以下の表に示すグループを含む Microsoft 365 E5 サブスクリプションをお持ちです。

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

あなたはグループのライフサイクルを管理する計画を立てています。
どのグループに有効期限を設定できますか？また、設定できる最短のグループ有効期間はどれくらいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Can expire:

▼

Group1 only

Group2 only

Group1 and Group3 only

Group3 and Group4 only

Group2, Group3, and Group4 only

Shortest lifetime:

▼

3 days

7 days

14 days

30 days

45 days

正解:

Answer Area

Can expire:

▼

Group1 only

Group2 only

Group1 and Group3 only

Group3 and Group4 only

Group2, Group3, and Group4 only

Shortest lifetime:

▼

3 days

7 days

14 days

30 days

45 days

Explanation:
Box 1: Group2 only
* Group2 - Yes
Microsoft 365 group expiration policy
You can set an expiration policy only for Microsoft 365 groups in Microsoft Entra ID. Administrators can specify an expiration period and any inactive group that reaches the end of that period, and isn't renewed, will be deleted.
Box 2: 30 days
The group lifetime is specified in days and can be set to 180, 365 or to a custom value that you specify. The custom value has to be at least 30 days.
Reference:
<https://learn.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-groups-expiration-policy>

ホットスポットに関する質問

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

Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

Azure AD Connect をインストールします。ドメインと OU のフィルタリング設定を、ドメインと OU のフィルタリングの図に示すように構成します。(ドメインと OU のフィルタリング」タブをクリックします。)

Welcome

Tasks

Connected to Azure AD

Sync

Connect Directories

Domain/OU Filtering

Filtering

Optional Features

Configure

Domain and OU filtering

If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.

Directory: contoso.com

Refresh Ou/Domain

☐ Sync all domains and OUs

☒ Sync selected domains and OUs

contoso.com

☐ Builtin

☐ Computers

☐ Domain Controllers

☐ ForeignSecurityPrincipals

☐ Infrastructure

☐ LostAndFound

☐ Managed Service Accounts

☒ OU1

☒ OU2

☐ Program Data

☐ System

☐ Users

Previous

Next

「ユーザーとデバイスのフィルタリング」の設定は、「ユーザーとデバイスのフィルタリング」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リング」タブをクリックしてください。)



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

Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	☐	☐
User2 syncs to Azure AD.	☐	☐
Group2 syncs to Azure AD.	☐	☐

正解:

Statements	Yes	No
User1 syncs to Azure AD.	☒	☐
User2 syncs to Azure AD.	☐	☒
Group2 syncs to Azure AD.	☒	☐

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: 195

シミュレーション

必要に応じて、以下のログイン情報を使用してください。

ユーザー名を入力するには、サインインボックスにカーソルを置き、下のユーザー名をクリックしてください。

パスワードを入力するには、カーソルを「パスワードを入力」ボックスに置いて、下のパスワードをクリックしてください。

Microsoft 365 ユーザー名: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365ポータルがブラウザに正常に読み込まれない場合は、Ctrl+Kキーを押して新しいブラウザタブでポータルを再読み込みしてください。

以下の情報は、技術サポートのみを目的としています。

ラボインスタンス: 999999999

グループ管理者ロールを以下の要件を満たすように構成する必要があります。

- アラン・デヤングが、この役割を有効化するためのリクエストを承認および拒否できることを確認してください。

- クリスティ・クラインが役割の有効化を要求できることを確認してください。

最小権限の原則を適用する。

このタスクを完了するには、該当する管理センターにサインインしてください。

A. 特権ID管理(PIM)において：

クリスティ・クラインに、グループ管理者として適格な職務を割り当ててください。

グループ管理者の役割設定を開き、承認ワークフローを有効にして、Allan Deyoung を指定承認者として追加します。

B. Entra ID ロール内:

クリスティ・クラインにグループ管理者権限を永続的に付与する。

アクティベーションリクエストを承認できるように、アラン・デヤングをグローバル管理者ロールに追加してください。

C. Microsoft 365 管理センター > グループ:

クリスティ・クラインをグループオーナーとして追加する。

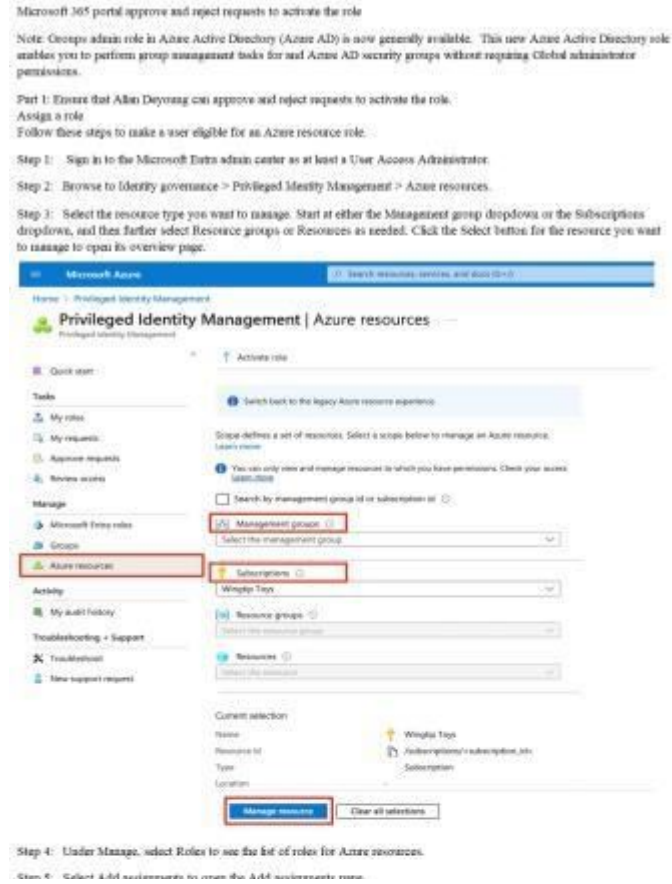
ロールリクエストを管理するユーザー管理者ロールをアラン・デヤングに割り当ててください。

D. Exchange 管理センターで:

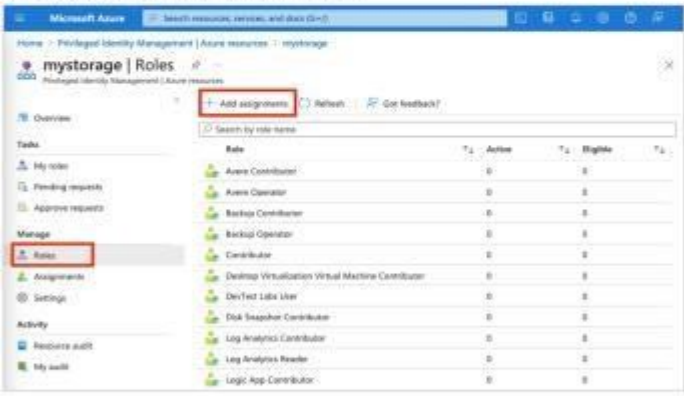
Christieグループに管理権限を付与する役割割り当てポリシーを作成します。

アクセス要求を承認する権限をアランに付与し、コンプライアンス管理の役割を割り当ててください。

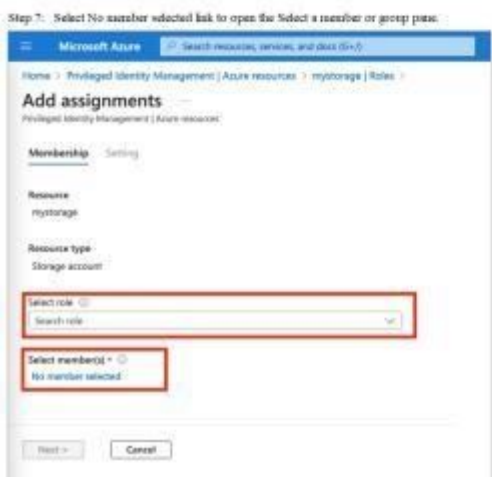
正解: **A** (コメントを发表する)



Step 6: Select the role you want to assign. [Here: Select the Group Administrator role]



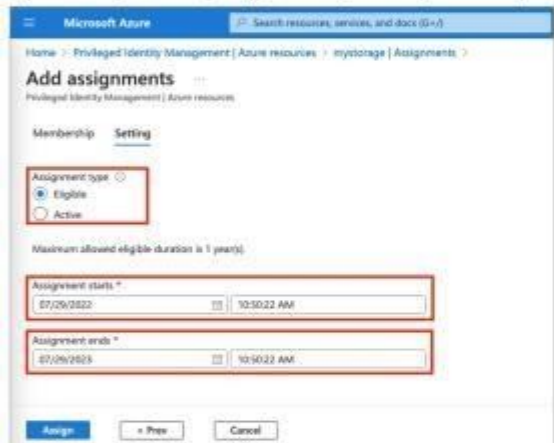
Step 7: Select No number selected link to open the Select a member or group page.



Step 8: Select a number or group you want to assign to the role and then choose Select. [Here: select Alim.Deycong]



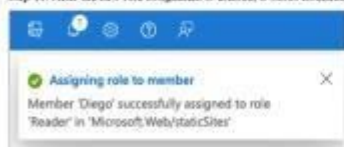
Step 9: On the Settings tab, in the Assignment type list, select Eligible or Active. [Here: Select Active]



Active assignments don't require the member to activate the role before usage. Members assigned as active have the privileges assigned ready to use. This type of assignment is also available to customers that don't use Microsoft Entra PIM.

Step 10: When finished, select Assign.

Step 11: After the new role assignment is created, a status notification is displayed.



Part 2: Ensure that Christie Clark can request activation of the role.

Repeat steps 1-7 above.

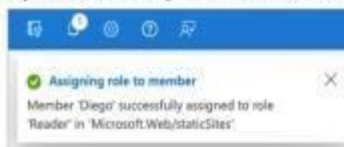
Step 8: Select a member or group you want to assign to the role and then choose Select. [Here: select Christie Clark]

Step 9: On the Settings tab, in the Assignment type list, select Eligible or Active. [Here: Select Eligible]

Eligible assignments require the member to activate the role before using it. Administrator may require role member to perform certain actions before role activation, which might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

Step 10: When finished, select Assign.

Step 11: After the new role assignment is created, a status notification is displayed.



Reference:

<https://techcommunity.microsoft.com/t5/microsoft-365-groups/creating-the-group-admin-role-to-p478985>

<https://docs.microsoft.com/en-us/azure/active-directory/permissions/role-assignments-overview#role-assignment>

質問: 196

ホットスポットに関する質問

お客様のMicrosoft 365テナントには、以下の表に示す管理単位が含まれています。

Name	Membership type	Restricted management	Dynamic membership rule
AU1	Dynamic user	Disabled	(user.department –eq “Department1”)
AU2	Dynamic user	Disabled	(user.department –eq “Department2”)

このサブスクリプションには、以下の表に示す管理者が含まれています。

Name	Role	Role assignment scope
Admin1	Password Administrator	AU1
Admin2	Password Administrator	AU2
Admin3	Password Administrator	Global

このサブスクリプションには、以下の表に示すユーザーが含まれています。

Name	Department
User1	Department1
User2	Department1
User3	Department2

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

注：正解ごとに1ポイントが加算されます。

Answer Area

Microsoft

Statements	Yes	No
Admin1 can reset the password of User1.	☐	☐
Admin2 can reset the password of User2.	☐	☐
Admin3 can reset the password of User3.	☐	☐

正解:

Answer Area

Microsoft

Statements	Yes	No
Admin1 can reset the password of User1.	☒	☐
Admin2 can reset the password of User2.	☐	☒
Admin3 can reset the password of User3.	☒	☐

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> **385**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 197

ドラッグアンドドロップ問題

お客様のオンプレミスネットワークには、Active Directoryドメインサービス(AD DS)ドメインが含まれています。このドメインには、Windows Serverを実行し、Share1という名前の共有フォルダをホストするServer1という名前のサーバーが含まれています。また、このドメインには、Windows 11を実行するデバイスが500台含まれています。

お客様は、ドメインと同期するMicrosoft 365 E5サブスクリプションをご利用中です。

グローバルセキュアアクセスから、プライベートアクセスプロファイルを有効にし、グローバルセキュアアクセスクライアントをすべてのデバイスに展開します。

グローバルセキュアアクセスを使用して、デバイスがShare1にリモート接続できることを確認する必要があります。

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

Actions

Answer Area

Create an enterprise application.

Create an application segment.

Allow internet inbound traffic on TCP 443 to Server1.

Install a connector on Server1.

Create an app protection policy.

1

2

3

Microsoft

正解:

Actions

Allow internet inbound traffic on TCP 443 to Server1.

Create an app protection policy.

Answer Area

1 Install a connector on Server1.

2 Create an enterprise application.

3 Create an application segment.



質問: 198

ドラッグアンドドロップ問題

お客様はMicrosoft Entraテナントをお持ちです。

保護されたアクションを実装する必要があります。

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

注：正解の選択肢は複数あります。どの正解の選択肢を選んでも点数が加算されます。

Actions

Create a custom Microsoft Entra role.

Create an access package.

Create a Conditional Access policy.

Create an authentication strength.

Add the protected actions.

Create an authentication context.

Answer Area



正解:

Actions

Create a custom Microsoft Entra role.

Create an access package.

Create an authentication strength.

Answer Area

Create an authentication context.

Create a Conditional Access policy.

Add the protected actions.

Explanation:

To implement Microsoft Entra protected actions, you need to configure Conditional Access policies and authentication contexts, then link those to specific permissions within Microsoft Entra ID. This allows you to enforce additional security requirements, like multi-factor authentication or compliance checks, before certain actions can be performed.

Step 1: Create an authentication context

Create a new authentication context: In the Microsoft Entra admin center, navigate to Entra ID > Protection > Conditional Access > Authentication contexts and create a new authentication context with a unique name and description.

Define authentication requirements: Specify the required authentication methods (e.g., multi- factor authentication, compliant device) for this context.

Publish the context: Make sure the context is enabled for use in Conditional Access policies.

Step 2: Create a Conditional Access policy

Create a new policy: In the Microsoft Entra admin center, navigate to Entra ID > Protection > Conditional Access > Policies and create a new policy.

Define policy scope: Specify which users, groups, or applications the policy applies to.

Choose the authentication context: Select the authentication context you configured in step 1.

Enable the policy: Set the policy to "On" or "Report-only" for testing.

Step 3: Add the protected actions:

Navigate to Protected Actions:

In the Microsoft Entra admin center, navigate to Entra ID > Roles & admins > Protected actions.

Add a new protected action:

Click "Add protected actions" and select the authentication context you configured in step 1.

Select permissions:

Choose the specific permissions you want to protect with the Conditional Access policy.

Save the protected action:

Click "Save" to link the authentication context and permissions.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/protected-actions-overview>

質問: 199

以下の表に示すAzureリソースが利用可能です。

Name	Description
User1	User account
Group1	Security group that uses the Dynamic user membership type
VM1	Virtual machine with a system-assigned managed identity
App1	Enterprise application
RG1	Resource group

RG1の「貢献者」ロールは、どのIDに割り当てることができますか？

- A. ユーザー1、グループ1、VM1、およびアプリ1
- B. ユーザー1とVM1のみ
- C. ユーザー1のみ
- D. ユーザー1とグループ1のみ
- E. User1、VM1、およびApp1のみ

正解: [\(正解を表示します\)](#)

質問: 200

次の表に示すユーザーを含む Azure AD テナントがあります。

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Application Administrator

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。

何をえばいいのでしょうか？

- A. Microsoft 365 Defender ポータル
- B. Microsoft 365 管理センター
- C. Microsoft Entra 管理センター
- D. Microsoft Purview コンプライアンス ポータル

正解: [\(正解を表示します\)](#)

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/admin-roles-page#compare-roles>

質問: 201

Microsoft Entraテナントには、User1という名前のユーザーが含まれており、特権ID管理(PIM)を使用しています。

火曜日の午前8時、ユーザー1は承認が必要なMicrosoft Entraロールの有効化を要求しました。

承認者が応答しない場合に、リクエストが自動的に削除されるタイミングを特定する必要があります。

何を特定すべきでしょうか？

- A. 日曜日の午前8時
- B. 木曜日の午前8時

C. 水曜日 8:00

D. 火曜日の20:00

正解: (正解を表示します)

The request will be deleted automatically at 08:00 on Wednesday (exactly 24 hours after the submission).

Key PIM Expiration Mechanics

Fixed Time Window: Delegated approvers have a strict 24-hour window to respond to a pending Microsoft Entra role activation request.

Non-Configurable: The 24-hour approval timeout is a built-in system constraint and cannot be changed or extended by administrators.

Resolution: If no action is taken within this timeframe, the request automatically expires and is deleted from the pending queue, requiring the eligible user to resubmit a brand-new request.

Reference:

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-approval-workflow>

質問: **202**

ユーザー「User1」を含むAzureサブスクリプションをお持ちです。

以下の要件を満たす必要があります。

- User1が新規登録アプリの所有者として追加されないようにする。

- User1がアプリケーションのプロキシ設定を管理できることを確認してください。

- User1がアプリを登録できることを確認してください。

最小権限の原則を適用する。

User1にはどの役割を割り当てべきですか？

A. アプリケーション開発者

B. クラウドアプリケーション管理者

C. サービスサポート管理者

D. アプリケーション管理者

正解: **D** (コメントを発表する)

Application Administrator = Can create and manage all aspects of app registrations and enterprise apps.

Cloud Application Administrator = Can create and manage all aspects of app registrations and enterprise apps ***except App Proxy***.

Service Support Administrator = Can read service health information and manage support tickets.

Application Developer = Can create application registrations independent of the 'Users can register applications' setting.

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

質問: **203**

シミュレーション

「Bellevue」という名前のグループを作成し、そのグループには「City」プロパティが「Bellevue」に設定されているすべてのユーザーを含める必要があります。

正解:

To create a group that automatically includes users based on a specific property value, you need to create a Dynamic User Group.

Step 1: Sign in to the Microsoft Entra admin center.

Access the Portal

Step 2: Expand the Identity menu on the left.

Step 3: Click on Groups and then select All groups.

Step 4: Click New group at the top of the page.

Initiate New Group

Step 5: Group type: Select Security (or Microsoft 365, depending on your needs).

Configure Basic Settings

Step 6: Group name: Enter a descriptive name. [Enter Bellevue]

Step 7: Membership type: Change this from Assigned to Dynamic User.

Step 8: Click Add dynamic query under the Dynamic user members section.

Build the Membership Rule

Step 9: Choose a Property from the dropdown (e.g., department, country, jobTitle). [Choose City] Step 10: Choose an Operator. [Choose Equals] Step 11: Enter your specific value in the Value field. [Enter Bellevue] Step

12: Click Save at the top of the rule builder page Reference:

<https://www.manageengine.com/microsoft-365-management-reporting/kb/how-to-add-group-members-in-entra-id.html>

質問: 204

Azure Active Directory (Azure AD) テナントをお持ちです。

HR Appsという名前のエンタープライズアプリケーションコレクションを作成し、以下の設定を行います。

- アプリケーション: App1、App2、App3

- 所有者: Admin1

- ユーザーとグループ: HRUsers

3つのアプリすべてに、以下のプロパティ設定があります。

- ユーザーがサインインできるように有効 :はい

- ユーザー割り当てが必要: はい

- ユーザーに表示される :はい

ユーザーからは、「マイアプリ」ポータルにアクセスしても、App1とApp2しか表示されないという報告が寄せられています。

ユーザーがApp3も閲覧できるようにする必要があります。

App3では何をすべきですか？

A. ユーザーとグループから、HRUsersを追加します。

B. シングルサインオンから、サインオン方法を設定します。

C. プロパティから、ユーザー割り当てを「いいえ」に変更します。

D. 権限から、ユーザー同意権限を確認します。

正解: (正解を表示します)

User assignment and Visible to Users goes hand in hand for this.

If Visible to Users is set to Yes then this is the explanation from the 'i' next to it:

If this option is set to yes, then assigned users will see the application on My Apps and O365 app launcher. If this option is set to no, then no users will see this application on their My Apps and O365 launcher. Assigned User is the key here.

Unless the users are assigned to the app, then No one will see the application on their MyApps or O365 Launcher.

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

<https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces>

質問: 205

Microsoft Entra Permissions Management を使用する Sub1 という名前の Azure サブスクリプションがあります。Sub1 には User1 という名前のユーザーが含まれています。User1 には Sub1 全体にわたる複数のアクセス許可が付与されています。

User1に付与されているすべての権限を読み取り専用権限に置き換える必要があります。解決策は、管理作業を最小限に抑えるものでなければなりません。

権限管理の「修復」タブでは、どのような操作を行うべきですか？

- A. [役割/ポリシー テンプレート] サブタブからテンプレートを作成します。
- B. [マイリクエスト]サブタブから、新しいリクエストを作成します。
- C. [役割/ポリシー] サブタブから役割を作成します。
- D. [権限] サブタブからクイックアクションを使用します。

正解: (正解を表示します)

There are four quick actions that can be used to manage users:

Revoke Unused Tasks

Revoke High-Risk Tasks

Revoke Delete Tasks

Assign Read-Only Status

<https://learn.microsoft.com/en-us/training/permissions-management/explore-features-of-permissions-management/9-act-on-your-findings-with-remediation-tab>

質問: 206

ユーザー「User1」と「Vault1」という名前のAzureキーコンテナを含むAzureサブスクリプションをお持ちです。

User1がVault1に保存されている証明書、鍵、および秘密情報のメタデータを読み取れるように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。

User1にはどの役割を割り当てるべきですか？

- A. キー保管庫の秘密ユーザー
- B. キーボールド暗号ユーザー
- C. キーボールドリーダー
- D. キーボールド暗号担当官

正解: (正解を表示します)

The Key Vault Reader role is the minimum user role required to read the metadata of certificates, keys, and secrets stored in an Azure Key Vault. This role allows users to view the properties and attributes of these objects, but not to access their actual contents.

Reference:

<https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide>

質問: 207

ドラッグアンドドロップ問題

お客様はMicrosoft 365 E5サブスクリプションをご利用中です。このサブスクリプションには、Windowsを実行するデバイスが500台含まれています。

グローバルセキュアアクセスクライアントをデバイスに展開します。

ユーザーがデバイスから<https://contoso.com>にアクセスできないようにする必要があります。

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

Actions

Create an app protection policy.

Create a Conditional Access policy.

Create a remote network.

Configure a security profile.

Create a web content filtering policy.

Answer Area

正解:

Actions

Create an app protection policy.

Create a remote network.

Answer Area

Create a web content filtering policy.

Configure a security profile.

Create a Conditional Access policy.

質問: 208

条件付きアクセス ポリシーを使用する Azure Active Directory (Azure AD) テナントをお持ちです。
条件付きアクセスの使用状況を分析するために、サードパーティ製のセキュリティ情報およびイベント管理(SIEM)ツールを使用する予定です。
管理ポータルを使用してAzure ADログをダウンロードする必要があります。ログファイルには、条件付きアクセス ポリシーの変更内容が含まれている必要があります。
Azure ADから何をエクスポートすべきですか？

- A. 監査ログはCSV形式で提供されます。
- B. CSV形式のサインインデータ
- C. JSON形式の監査ログ
- D. サインインはJSON形式で行います

正解: (正解を表示します)

You can also choose to download the filtered data, up to 250,000 records, by selecting the Download button. You can download the logs in either CSV or JSON format.
You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column.

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

質問: 209

お客様は、Microsoft Defender for Cloud Appsを使用するMicrosoft 365 E5サブスクリプションをご利用中です。

どのユーザーがどのデバイスやブラウザからFacebookにアクセスしているかを特定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ものでなければなりません。

まず最初に何をすべきでしょうか？

- A. 条件付きアクセス ポリシーを作成します。
- B. Microsoft Intune でアプリ構成ポリシーを作成します。
- C. Defender for Cloud Appsのアクセス ポリシーを作成します。
- D. Microsoft 365 Defender ポータルから、Facebook の制裁を解除します。

正解: (正解を表示します)

質問: 210

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: B (コメントを発表する)

You need to use "Use app enforced restrictions" from the "Session" control of the CA.

<https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

質問: 211

ドラッグアンドドロップ問題

お客様はMicrosoft 365 E5テナントをご利用中です。

あなたはApp1という名前のクラウドアプリを購入します。

Microsoft Cloud App Securityを使用して、App1のリアルタイムセッションレベル監視を有効にする必要があります。

どのような順序で操作を実行すればよいでしょうか？回答するには、操作リストから適切な操作を回答欄に移動させ、正しい順序に並べ替えてください。

Actions

From Microsoft Cloud App Security, create a session policy.

Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.

Answer Area

⬅

➡

⬆

⬆

正解:

Actions

Answer Area

Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.

From Microsoft Cloud App Security, create a session policy.

⬆

⬆

⬆

⬆

質問: 212

Microsoft Entraテナントには、User1、User2、User3という名前の3人のユーザーが含まれています。

特権ID管理(PIM)を使用して、管理者ロールへのジャストインタイム(JIT)アクセスを構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。

- User1 がユーザー管理者ロールを使用できることを確認します。

承認。

- User3がユーザー管理者ロールを使用できるようになったら、User2もユーザー管理者ロールを使用できることを確認してください。

User2の役割要求を承認しました。

最初に何を作るべきでしょうか？

A. 役割分担

B. 行政単位

C. セキュリティグループ

D. 条件付きアクセスポリシー

正解: (正解を表示します)

To achieve your goal, first, create Privileged Access Groups (PAGs) for the User Administrator role, assign eligible members (User1, User2) to these groups, and then configure separate PIM Role Settings for each: one with no approval (automatic activation) for User1, and another with a custom approval workflow requiring User3's approval for User2. You'll create two separate PIM Role Assignments for the User Administrator role, one linked to each PAG, managing member settings to define activation requirements.

Here's the step-by-step creation process:

1. Create Privileged Access Groups (PAGs)

2. Assign Users to Groups

3. Configure PIM Role Settings

Go to Identity Governance > Privileged Identity Management > Microsoft Entra roles > Roles, then select the User Administrator role.

For User (Auto Activation):

*-> Select Add assignments, choose the PIM-UserAdmin-Auto group, set Assignment type to Eligible, and click Next.

In Membership settings, select Edit. Set Activation settings to require MFA (recommended) but NO approval (or disable approval settings).

For User2 (Approval Required):

*-> Select Add assignments, choose the PIM-UserAdmin-Approval group, set Assignment type to Eligible, and click Next.

In Membership settings, select Edit. Set Activation settings to require MFA and enable Require approval, specifying User 3 as the delegated approver.

4. Activate PIM for the User Administrator Role

Reference:

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure>

質問: 213

ホットスポットに関する質問

Microsoft Entraテナントには、User1という名前のユーザーが含まれています。

Sub1という名前のAzureサブスクリプションがあります。User1にはSub1の所有者ロールが割り当てられています。

User1がSub1を権限管理にオンボーディングできるように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。テナントにおいて、Sub1にはどの役割を割り当て、User1にはどの役割を割り当てるべきでしょうか？

回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Sub1:

Tenant:

正解:

Answer Area

Sub1:

Tenant:

質問: 214

ドラッグアンドドロップ問題

貴社は、Azureリソースへの管理者アクセス権を付与するために、特権ID管理(PIM)の利用を計画しています。
PIMを初めてセットアップし、最初のユーザーがPIMを使用できることを確認するためのワークフローを確立します。
最小権限の原則に従いながら、以下の操作にはどの役割を使用すべきでしょうか？回答するには、適切な役割を各操作にドラッグしてください。役割は、1回だけ使用することも、複数回使用することも、まったく使用しないこともできます。

To determine the users and roles to be managed using PIM

Microsoft

To assign users as eligible admins

To request the activation of eligible admin roles

To view and approve activation requests

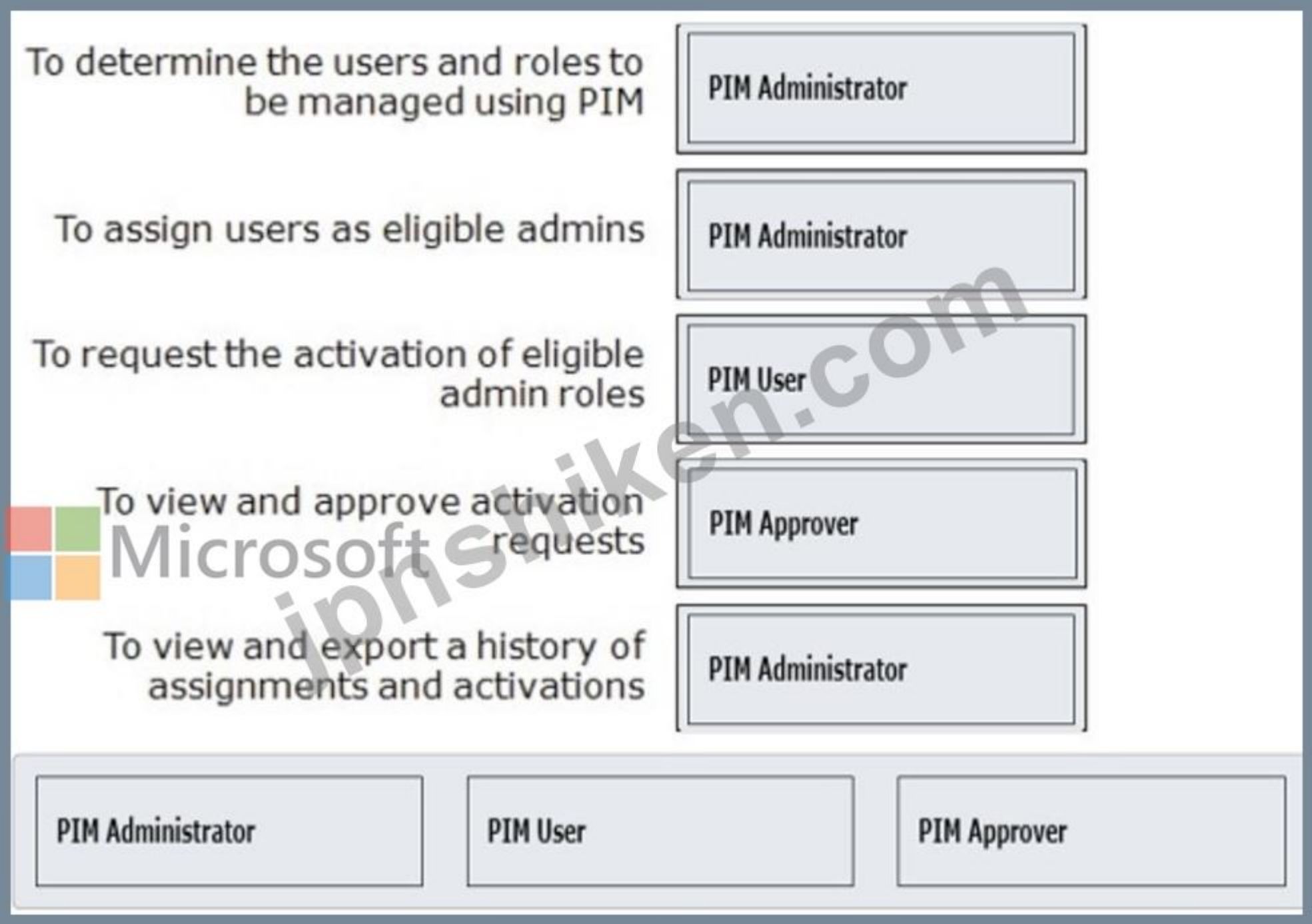
To view and export a history of assignments and activations

PIM Administrator

PIM User

PIM Approver

正解:



Explanation:

You should use the Privileged Identity Management (PIM) Administrator role to determine the users and roles to be managed using PIM. The PIM Administrator will be the person performing the initial setup of PIM and will therefore need to collect the requirements for the implementation.

You should use the PIM Administrator role to assign users as eligible admins. The PIM Administrator will determine and configure which users will have which rights within the environment. As this is an administrative task, the PIM Administrator role will be required for this.

You should use the PIM User role to request the activation of eligible admin roles. When users require elevated rights for their account, they can create a PIM activation request to be granted the requested permissions.

You should use the PIM Approver role to view and approve activation requests. When PIM requests are created, the PIM Approver will approve or deny the request for the elevated permissions.

You should use the PIM Administrator role to view and export a history of assignments and activations. The PIM Administrator can access the history to make sure compliance requirements are met.

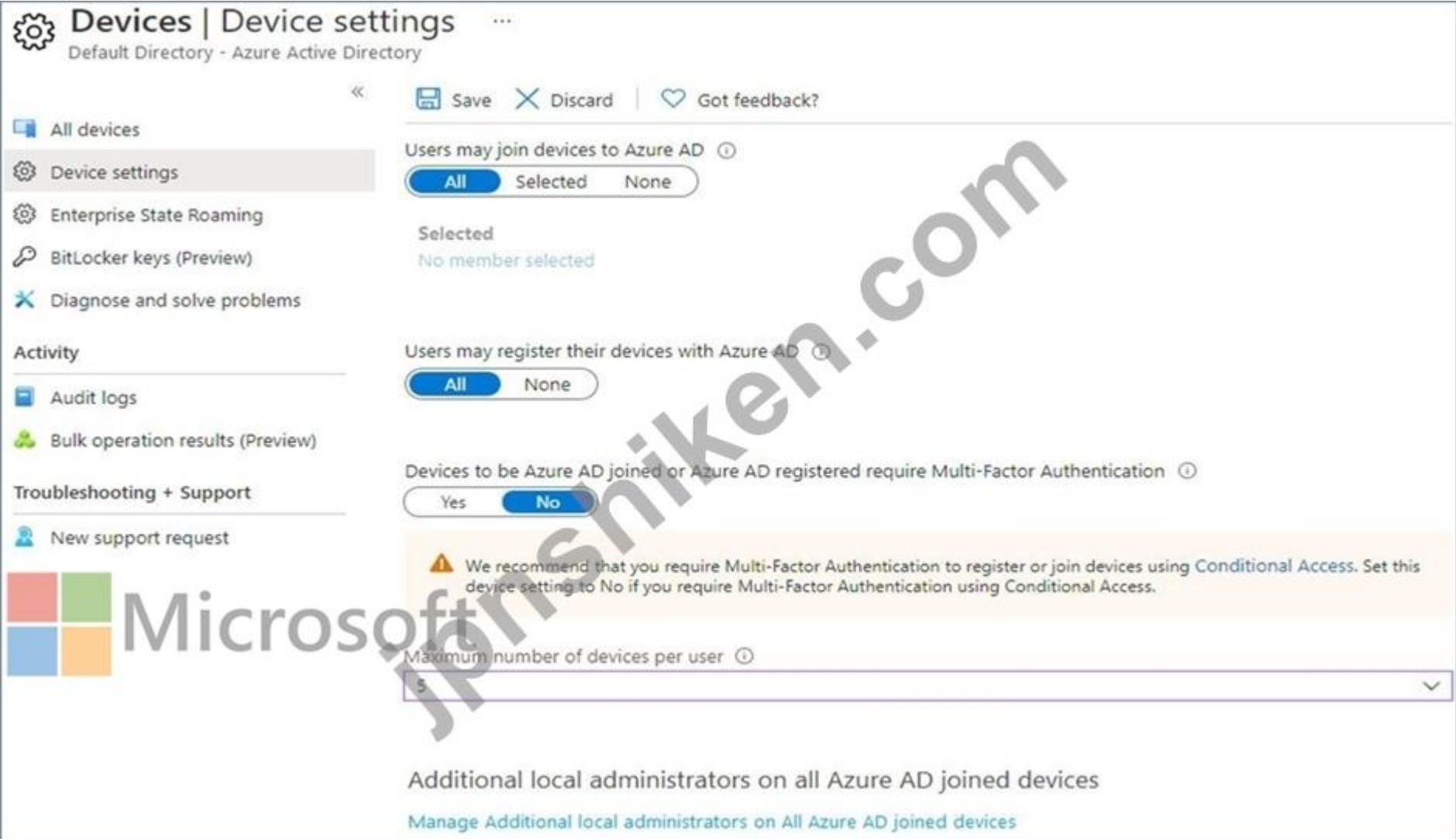
質問: 215

ホットスポットに関する質問

お客様は、Azure Active Directory Premium Plan 2 ライセンスを持つ Azure Active Directory (Azure AD) テナントを所有しています。このテナントには、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	None

デバイス設定は、以下の図に示すとおりです。



ユーザー1は、以下の表に示すデバイスを所有しています。

Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

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

注：正解ごとに1ポイントが加算されます。

Answer Area		Microsoft	Statements	Yes	No
			User1 can join four additional Windows 10 devices to Azure AD.	☐	☐
			Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to Yes .	☐	☐
			Admin2 is a local administrator on Device3.	☐	☐

正解:

Answer Area		Microsoft	Statements	Yes	No
			User1 can join four additional Windows 10 devices to Azure AD.	☐	☒
			Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to Yes .	☒	☐
			Admin2 is a local administrator on Device3.	☐	☒

Explanation:

Box 1: No

Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD.

Box 2: Yes

You must be assigned one of the following roles to view or manage device settings in the Azure portal:

- * Global Administrator
- * Cloud Device Administrator
- * Global Reader
- * Directory Reader

Box 3: No

Additional local administrators on Azure AD joined devices (Device is Registered not Joined) Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

質問: 216

ホットスポットに関する質問

多要素認証(MFA)が有効になっているAzure Active Directory(Azure AD)テナントをお持ちです。

アカウントロックアウトの設定は、以下の図に示すように構成されています。

Account lockout

Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.

Number of MFA denials to trigger account lockout *

3 ✓

Minutes until account lockout counter is reset *

60 ✓

Minutes until account is automatically unblocked *

30 ✓

図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

A user account will be locked out if the user enters the wrong [answer choice] three times.

If a user account is locked, the user can sign in again successfully after [answer choice] minutes.

email address
Microsoft Authenticator app code
password

30
60
90

正解:

Answer Area

A user account will be locked out if the user enters the wrong [answer choice] three times.

If a user account is locked, the user can sign in again successfully after [answer choice] minutes.

email address
Microsoft Authenticator app code
password

30
60
90

質問: 217

あなたはContoso, Ltd.という会社に勤務しており、その会社はcontoso.comという名前のMicrosoft Entraテナントを所有しています。

Contosoは、以下の2つのパートナー企業と共同でプロジェクトに取り組んでいます。

- Microsoft Entra を持つ A Datum Corporation という会社

テナント名はadatum.comです。

- Microsoft Entraテナントを持つFabrikam, Inc.という会社

fabrikam.comという名前です。

adatum.com から contoso.com に新しいゲストユーザーを招待しようとする、エラーメッセージが表示されます。

fabnkam.com から contoso.com へ新しいゲストユーザーを正常に招待できます。

adatum.com から contoso.com に新しいゲストユーザーを招待できるようにする必要があります。

何を設定すればよいですか？

A. ゲスト招待設定

B. 検証可能な資格情報

C. 名称付き場所

D. コラボレーション制限

正解: D (コメントを发表する)

You need to add adatum.com to the list of domains on External Identities >> External Collab Settings >> Collaboration Restrictions >> Allow invitations only to the specified domains.

有効的な**SC-300J**問題集はJPNTTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-300J**試験問題集を提供します。JPNTTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-300J-mondaishu> **385**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」