Microsoft.SC-300J.v2026-09-22.q168

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：	168
バージョン：	v2026-09-22
ページの閲覧量：	107
問題集の閲覧量：	1683

https://www.jpnshiken.com/shiken/Microsoft.SC-300J.v2026-09-22.q168.html

質問: **1**

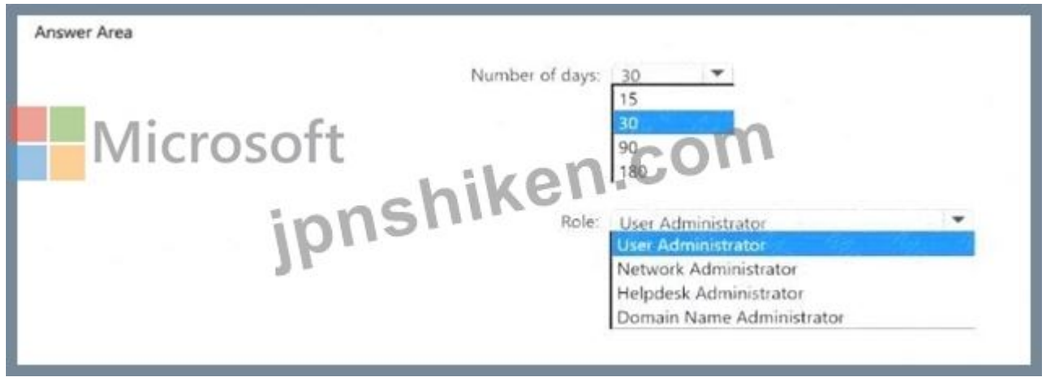
User1 という名前のユーザーを含む Microsoft Entra テナントがあります。

管理者がUser1を削除します。以下の点を確認する必要があります。

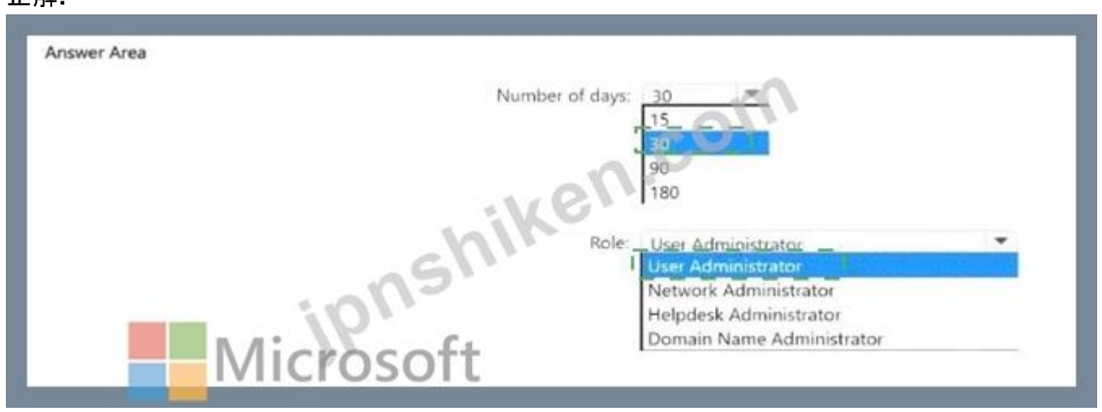
* User1 アカウントを復元できるオプションがある最大日数は何ですか?

* User1 を復元するために使用できる最も権限の低いロールはどれですか?

回答するには、回答エリアで適切な選択肢を選択してください。注: 正解ごとに1ポイント加算されます。



正解:



Explanation:



According to the Microsoft SC-300 Study Guide and the official Microsoft Learn module: "Manage user accounts in Microsoft Entra ID" , when a user account is deleted from Microsoft Entra ID (formerly Azure AD), the deleted user object is soft-deleted and retained in the Deleted Users container for 30 days.
During this retention period, the user can be restored with all associated attributes, such as group memberships and licenses, unless a permanent (hard) delete is performed before the 30-day period ends. After the 30-day soft-delete retention period expires, the user object and all related data are permanently removed from the tenant and cannot be recovered.
Microsoft documentation states:
"When a user is deleted, the account is retained in a soft-deleted state for 30 days. During that time, an administrator can restore the user from the Azure portal or by using PowerShell." To perform the restoration, the least privileged role that has this permission is the User Administrator.
The User Administrator can:
* Restore deleted users.
* Reset passwords for non-admin users.
* Create, edit, and delete standard user accounts.
Higher-level roles (e.g., Global Administrator or Privileged Role Administrator) also have this ability but are not required - thus, User Administrator is the least privileged appropriate role.

質問: 2

Azure Active Directory (Azure AD) テナントに、User1、User2、User3 という 3 人のユーザーが含まれています。Group1 というグループを作成します。User2 と User3 を Group1 に追加します。
アプリケーション管理者の図に示されているように、Azure AD Privileged Identity Management (PIM) でロールを構成します (アプリケーションの [管理者] タブをクリックします)。



Group1 は、アプリケーション管理者ロールの承認者として構成されています。
User2 をアプリケーション管理者ロールの資格を持つように構成します。

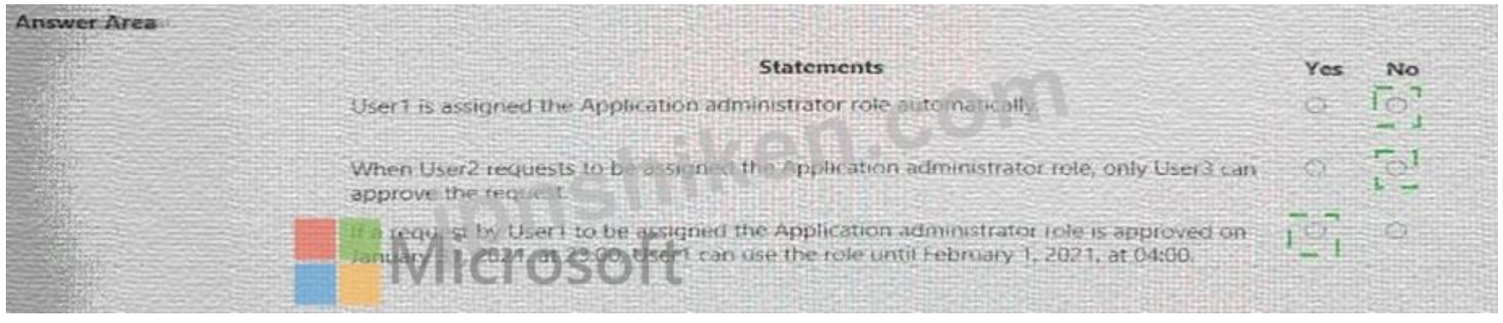
User1 の場合、割り当ての図に示すように、アプリケーション管理者ロールに割り当てを追加します。
[割り当て]タブをクリック）



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



正解:



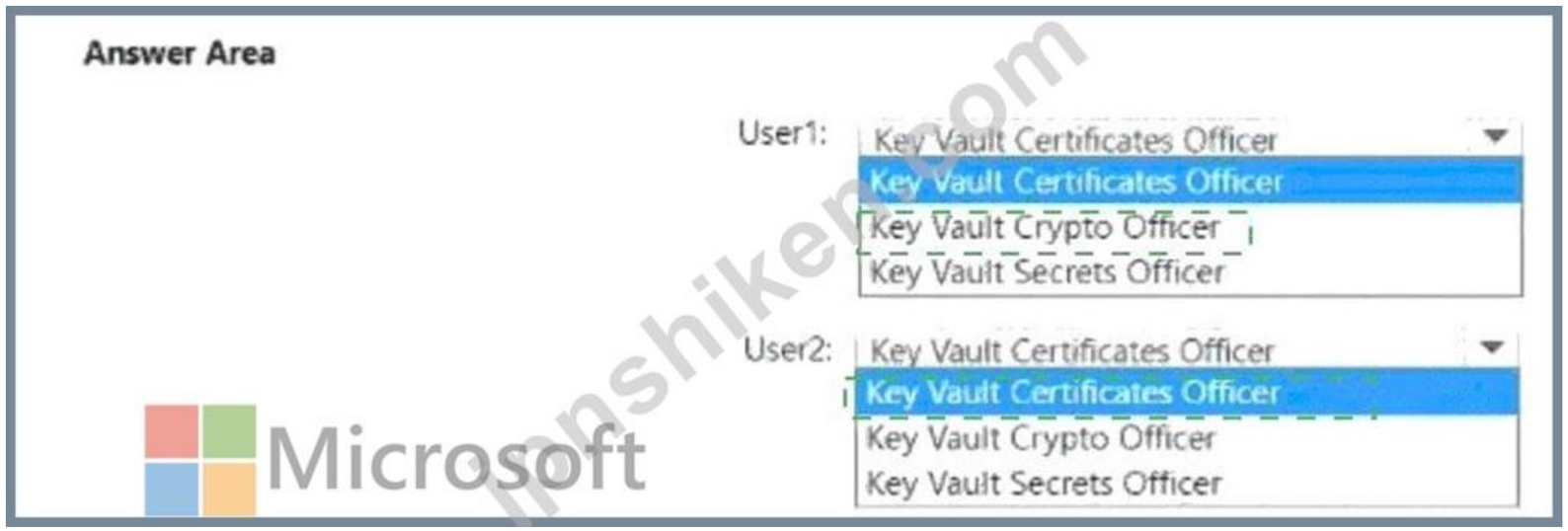
Explanation:
< Statement 1 # No
Statement 2 # No
Statement 3 # Yes
According to the Microsoft SC-300: Microsoft Identity and Access Administrator study guide and Azure AD Privileged Identity Management (PIM) documentation, roles in PIM can be configured for eligible or active assignments.

* User1 is assigned automatically - No The "Add assignments" screen shows User1's assignment type as Eligible, not Active. Eligible assignments mean the user is not automatically granted the role; they must activate it manually when needed. Therefore, User1 is not assigned automatically to the Application Administrator role.
* When User2 requests role assignment, only User3 can approve - No The Role setting details show that approval is required to activate and that the approver is listed as Group1. Because both User2 and User3 are members of Group1, any member of the group can approve the request, not only User3. Hence, the statement that only User3 can approve is incorrect.
* User1's approval on January 31, 2021, at 23:00 - Yes The configuration shows an activation maximum duration of 5 hours. Therefore, if User1's request is approved at 23:00 on January 31, the role remains active for 5 hours - until 04:00 on February 1, 2021. This aligns precisely with the parameters displayed in the exhibit.
As confirmed in Microsoft documentation ("Configure role settings in Azure AD PIM"), activation settings define how long a user can remain active after approval, and group approvers allow any member of that group to approve activations.

質問**: 3**
次の表に示すリソースを含む Azure サブスクリプションがあります。
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している必要があります。
* 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ます。
* 最小権限の原則を使用します。
各ユーザーにはどのような役割を割り当てる必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:

User1: Key Vault Crypto Officer

User2: Key Vault Certificates Officer

As detailed in Microsoft documentation and the Exam Ref SC-300: Microsoft Identity and Access Administrator, Azure Key Vault provides role-based access control (RBAC) to manage keys, secrets, and certificates independently. The built-in roles are designed with the principle of least privilege - granting users only the permissions necessary to perform their tasks.

According to the Microsoft Learn module "Manage access to Key Vault using Azure RBAC", the relevant built-in roles are:

* Key Vault Crypto Officer - This role allows users to manage cryptographic keys in a key vault.

Specifically, the Crypto Officer can create, import, delete, and manage keys, as well as perform cryptographic operations such as encrypt, decrypt, sign, and verify. This aligns perfectly with the requirement that User1 must manage and create keys in Vault1.

* Key Vault Certificates Officer - This role allows a user to manage and retrieve certificates within a key vault. It provides access to read, import, and delete certificates but not to manage or create keys or secrets. This satisfies the requirement that User2 must access a certificate stored in Vault1.

The Exam Ref SC-300 emphasizes that the least privilege principle requires assigning users the lowest possible role that meets their operational needs. Therefore, assigning Key Vault Crypto Officer to User1 and Key Vault Certificates Officer to User2 ensures compliance, minimal access exposure, and operational

質問**: 4**

ネットワークには、contoso.com というオンプレミスの Active Directory ドメインがあり、Microsoft Entra Connect を使用して Microsoft Entra テナントと同期しています。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: ユーザー3

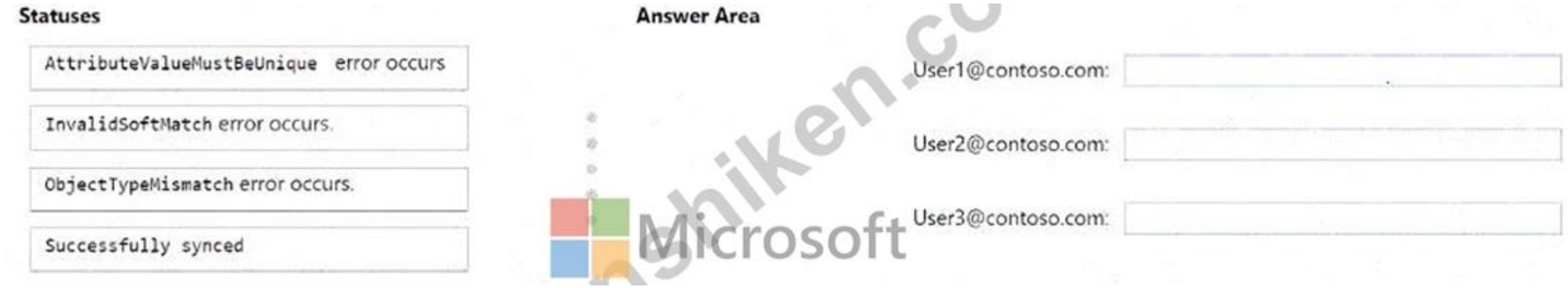
* UPN: user3@contoso.com

* プロキシアドレス: smtp: user3@contoso.com、smtp: sales@contoso.com

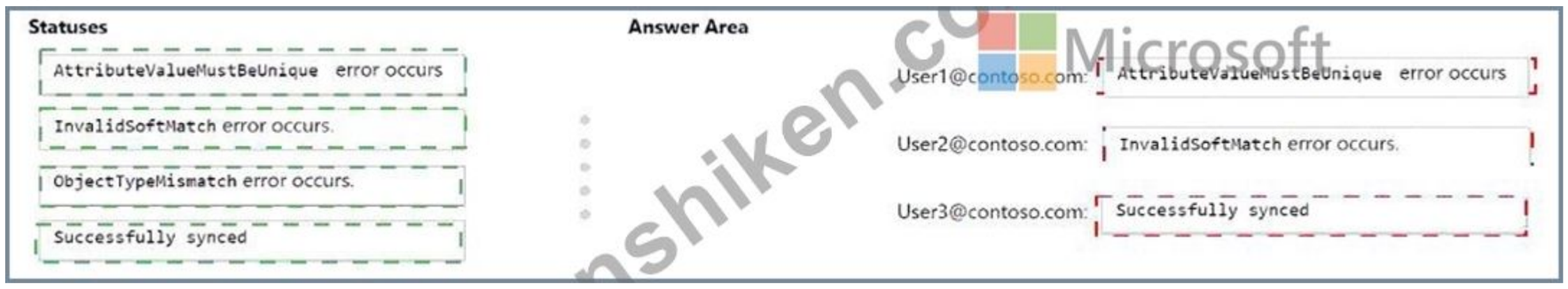
Active Directory ユーザーとコンピューターから、次の表に示すように各ユーザーの proxyAddresses 属性を更新します。

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

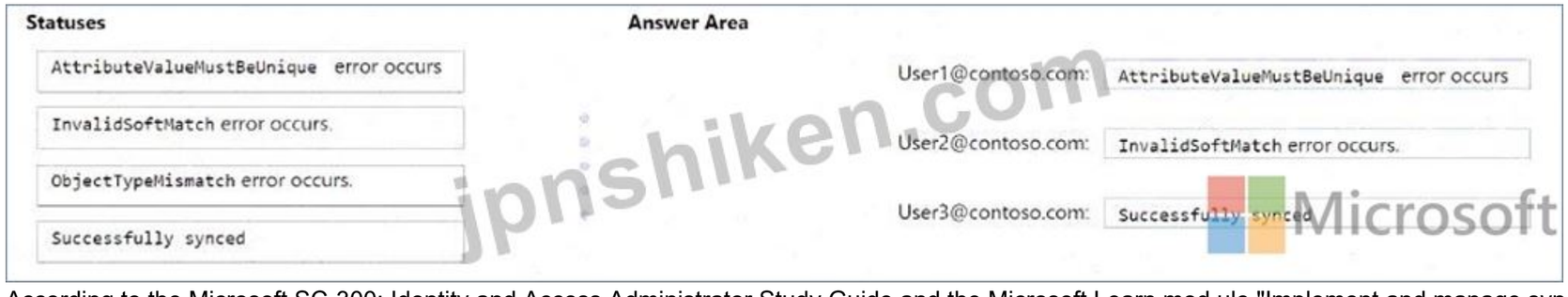
手動で同期を開始します。
Microsoft Entra Connect Sync は各ユーザーに対してどの同期ステータスを返しますか？ 適切なステータスを適切なユーザーにドラッグしてください。各ステータスは、1 回だけ、複数回、またはまったく使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn mod ule "Implement and manage synchronization with Microsoft Entra Connect" , when Microsoft Entra Connect synchronizes user objects between on-premises Active Directory (AD) and Microsoft Entra ID (formerly Azure AD), each user must have unique proxyAddresses attributes across the directory.
The proxyAddresses attribute represents all the email aliases (SMTP addresses) associated with a user. The synchronization process verifies these values to ensure they are not duplicated among multiple user objects. If two or more objects in AD share the same SMTP address, the synchronization process generates an error, typically reported as a "Duplicate Attribute" conflict.
In the provided scenario:

* User1 (proxyAddresses: user1@contoso.com, sales@contoso.com)
* User2 (proxyAddresses: user2@contoso.com, user.2@contoso.com, service@contoso.com)
* User3 (proxyAddresses: user3@contoso.com, sales@contoso.com)
After updating the proxy addresses:
* User1 # admin@contoso.com
* User2 # sales@contoso.com
Because sales@contoso.com is now used by both User2 and User3, the sync process detects a duplicate SMTP address. This causes synchronization errors for User2 and User1 if any other duplicates exist.
User3, with unique attributes, synchronizes successfully.
The SC-300 reference under "Manage s ynchronization errors using Microsoft Entra Connect Health" confirms:
"If two or more objects contain the same value for attributes marked as unique (such as proxyAddresses or userPrincipalName), Microsoft Entra Connect synchronization fails for those obje cts until the conflict is resolved."

質問**: 5**
Microsoft 365 E5 サブスクリプションがあり、そこには User1 と User2 という 2 人のユーザーが含まれています。
ユーザー1がグループのアクセスレビューを作成でき、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確認する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
各ユーザーにどのロールを割り当てるべきですか？ 回答するには、適切なロールを正しいユーザーにドラッグしてください。各ロールは1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。注：正解ごとに1ポイント獲得できます。



正解:



Explanation:
< User1: User administrator
User2: Reports reader
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Exam Ref SC-300: Microsoft Identity and Access Administrator , Azure AD includes several predefined roles that control delegated administrative permissions in the directory. Access reviews in Azure AD (part of Identity Governance) can be created and managed by specific roles, depending on their intended task.
The User administrator role is designed for managing users and groups. It allows the user to create and manage access reviews for groups and applications within the organization. This includes the ability to start new reviews, modify existing ones, and manage reviewers. Therefore, User1 , who must create access reviews, requires this role.
On the other hand, the Reports reader role is a read-only administrative role that allows viewing of all audit logs, sign-in logs, and reports, including access review history reports . This role cannot create or modify reviews but can access and review the outcomes of completed reviews. Therefore, User2 , who needs to review historical access review reports, should be assigned the Reports reader role.
Microsoft Learn's "Manage access reviews in Azure AD Identity Governance" module and the SC-300 Learning Path confirm:
"User administrators can create and manage access reviews for users, groups, and applications. Reports readers can view the access review results and history reports but cannot create or modify them

質問: 6
次の表に示すユーザーを含む Microsoft 365 サブスクリプションがあります。

Name	Role
User1	Global Administrator
User2	User Administrator
User3	Groups Administrator
User4	None

tenan1 から、グループの命名ポリシーを構成します。
命名ポリシーの影響を受けるユーザーは誰ですか?
A. ユーザー2のみ
B. ユーザー3のみ
C. ユーザー2とユーザー3のみ
D. ユーザー3とユーザー4のみ
E. ユーザー1、ユーザー2、ユーザー3のみ
F. ユーザー1、ユーザー2、ユーザー3、ユーザー4
正解: **D (**コメントを発表する**)**
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and the Microsoft Learn - "Manage Microsoft 365 Groups naming policies" documentation, group naming policies in Azure Active Directory (now Microsoft Entra ID) apply to end users who create Microsoft 365 groups, but do not apply to administrators who have roles that allow them to override naming restrictions.
The policy defines conventions such as prefixes, suffixes, blocked words, and enforced naming rules.
However, certain administrative roles are exempt from this policy to allow organizational management and automation processes. The exempt roles are:
* Global Administrator
* User Administrator
These two roles can create Microsoft 365 groups without the naming policy constraints. Other users - including Groups Administrator and users without administrative roles - are subject to the naming policy when creating groups.
From the official documentation:
"Naming policies apply to all users who create groups, except for global administrators and user administrators. These roles can create groups that bypass the naming policy restrictions." Applying this rule:
* User1 (Global Administrator) - exempt

* User2 (User Administrator) - exempt
* User3 (Groups Administrator) - affected by the policy
* User4 (no role) - affected by the policy

質問: **7**
User1 と User2 という 2 人のユーザーを含む Azure AD テナントがあり、以下のアクションを実行する予定です。
* 「グループ 1」という名前のグループを作成します。
* User1 と User2 を Group1 に追加します。
* Group1 に Azure AD ロールを割り当てます。
Group1を作成する必要があります。
どの2つの設定を使用できますか？ それぞれの正解は完全な解決策を示します。注：正解の選択は1ポイントです
A. グループの種類: Microsoft 365 メンバーシップの種類: 動的ユーザー
B. グループの種類: セキュリティ メンバーシップの種類: 動的デバイス
C. グループタイプ セキュリティ メンバーシップタイプ: 動的ユーザー
D. グループタイプ セキュリティ メンバーシップタイプ: 割り当て済み
E. グループの種類: Microsoft 365 メンバーシップの種類: 割り当て済み
正解: **(**正解を表示します**)**
In Azure AD, assigning directory roles to a group requires creating a role-assignable group. The SC-300 study materials and the official exam reference emphasize that the group must be a Security group and created with the isAssignableToRole capability. Microsoft's guidance states: "Only security groups can be assigned Azure AD roles. Microsoft 365 groups are not supported." It also clarifies membership constraints: "Dynamic membership is not supported for role-assignable groups." Because you intend to assign Azure AD roles to Group1 and also add User1 and User2 directly, the acceptable configuration is a Security group with Assigned membership. This allows you to explicitly add the two users and later attach an Azure AD role to the group via PIM or standard role assignment. Options using Microsoft 365 groups (A, E) are invalid for role assignment, and options using Dynamic membership (A, B, C) are not permitted for role-assignable groups.
Therefore, the only configuration that satisfies both adding the users and assigning Azure AD roles is Security
+ Assigned (Option D).

質問: **8**
タスク3
LinkedInアプリケーションをSales and Marketingアクセスパッケージのリソースとして追加する必要があります。このソリューションでは、アクセスパッケージから他のリソースを削除しないでください。
正解:
See the Explanation for the complete step by step solution.
Explanation:
To add the LinkedIn application as a resource to the Sales and Marketing access package without removing any other resources, you can follow these steps:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Identity Governance Administrator.
Navigate to Entitlement Management:
Go to Identity governance > Entitlement management > Access packages1.
Select the Sales and Marketing access package:
Find and select the Sales and Marketing access package to modify it.
Add a new resource:

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

質問: 9
タスク8
Microsoft Entra ID への認証時に、すべてのユーザーが従来の認証プロトコルを使用しないようにする必要があります。
正解:
See the Explanation for the complete step by step solution.
Explanation:
To prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID, you can create a Conditional Access policy that blocks legacy authentication. Here's how to do it:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Conditional Access Administrator.
Navigate to Conditional Access:
Go to Security > Conditional Access.
Create a new policy:
Select + New policy.
Give your policy a name that reflects its purpose, like "Block Legacy Auth".
Set users and groups:
Under Assignments, select Users or workload identities.
Under Include, select All users.
Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication.It's recommended to exclude at least one account to prevent lockout1.
Target resources:
Under Cloud apps or actions, select All cloud apps.
Set conditions:
Under Conditions > Client apps, set Configure to Yes.
Check only the boxes for Exchange ActiveSync clients and Other clients.
Configure access controls:
Under Access controls > Grant, select Block access.
Enable policy:
Confirm your settings and set Enable policy to Report-only initially to understand the impact.

After confirming the settings using report-only mode, you can move theEnable policytoggle fromReport- onlytoOn2.
By following these steps, you will block legacy authentication protocols for all users, enhancing the security posture of your organization by requiring modern authentication methods. Remember to monitor the impact of this policy and adjust as necessary to ensure business continuity.

質問**: 10**
注: この問題は、同じシナリオを提示する一連の問題の一部です。一連の問題にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションで質問に回答した後は、そのセクションに戻ることはできず、その結果、これらの質問はレビュー画面に表示されなくなります。
Microsoft 365 ES サブスクリプションをお持ちです。
User1 という名前のユーザーを作成します。
User1 が ID セキュア スコアの改善アクションのステータスを更新できることを確認する必要があります。
解決策: Exchange 管理者の役割を User1 に割り当てます。
A. はい
B. いいえ
正解**: (**正解を表示します**)**
The Exchange Administrator role provides permissions to manage mailboxes, Exchange policies, and email configurations but does not include permissions to access or update Microsoft Secure Score.
Secure Score is a Microsoft 365 security and compliance feature managed primarily through the Microsoft
365 Security Center or Microsoft Defender portal, and it is only editable by users who have security-specific administrative roles.
Thus, Exchange Administrators can manage mail flow and Exchange Online Protection but cannot update or change Secure Score recommendations.

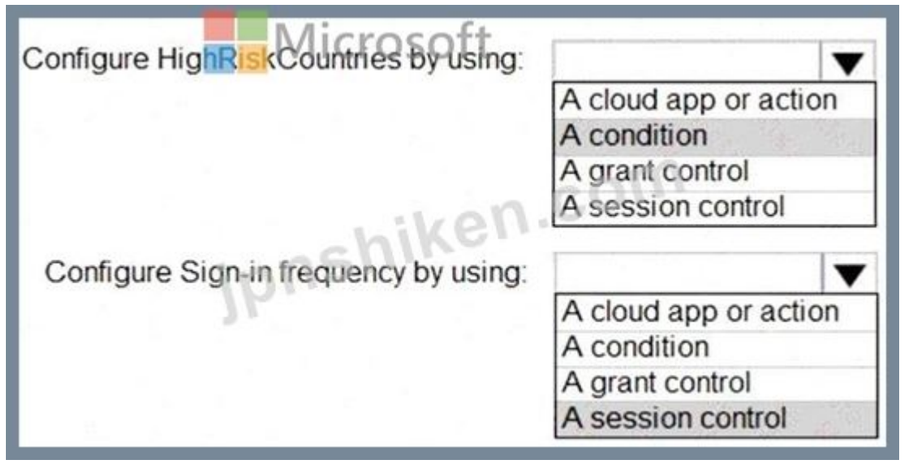
質問**: 11**
Microsoft 36S テナントがあります。
高リスク国のリストを含む、HighRiskCountries という名前の名前付き場所を作成します。
高リスクの国から接続する場合、ユーザーが認証されたままでいられる時間を制限する必要があります。
条件付きアクセス ポリシーでは何を構成する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解**:**



Explanation:



According to the Microsoft SC-300: Identi ty and Access Administrator Study Guide and the Microsoft Learn module "Implement Conditional Access Policies," the Azure AD Conditional Access engine uses a structured framework that consists of conditions, grant controls, and session controls.

1# # Configure HighRiskCountries by using A condition In Conditional Access, conditions define the circumstances under which a policy applies. Named locations (such as HighRiskCountries) are part of the Locations condition. When configuring a Conditional Access policy, administrators can include or exclude sign-ins based on IP address ranges, country/region, or named locations.

Microsoft documentation states: "You can define named locations to specify IP ranges or countries/regions and use them as conditions in your C onditional Access policies." Thus, HighRiskCountries should be configured as a condition within the policy to target sign-ins from those regions.

2# # Configure Sign-in frequency by using A session control Session controls in Conditional Access determine how sessions behave after a user successfully signs in. The Sign-in frequency setting controls how often users must reauthenticate, effectively limiting the duration of their authentication session.

Microsoft Learn reference: "Session controls, such as sig n-in frequency and persistent browser session, enable administrators to enforce how often users must reauthenticate." Therefore, to restrict how long a user can remain authenticated when signing in from high-risk countries, you configure Sign-in frequency as a session control.

Final Correct Answers:

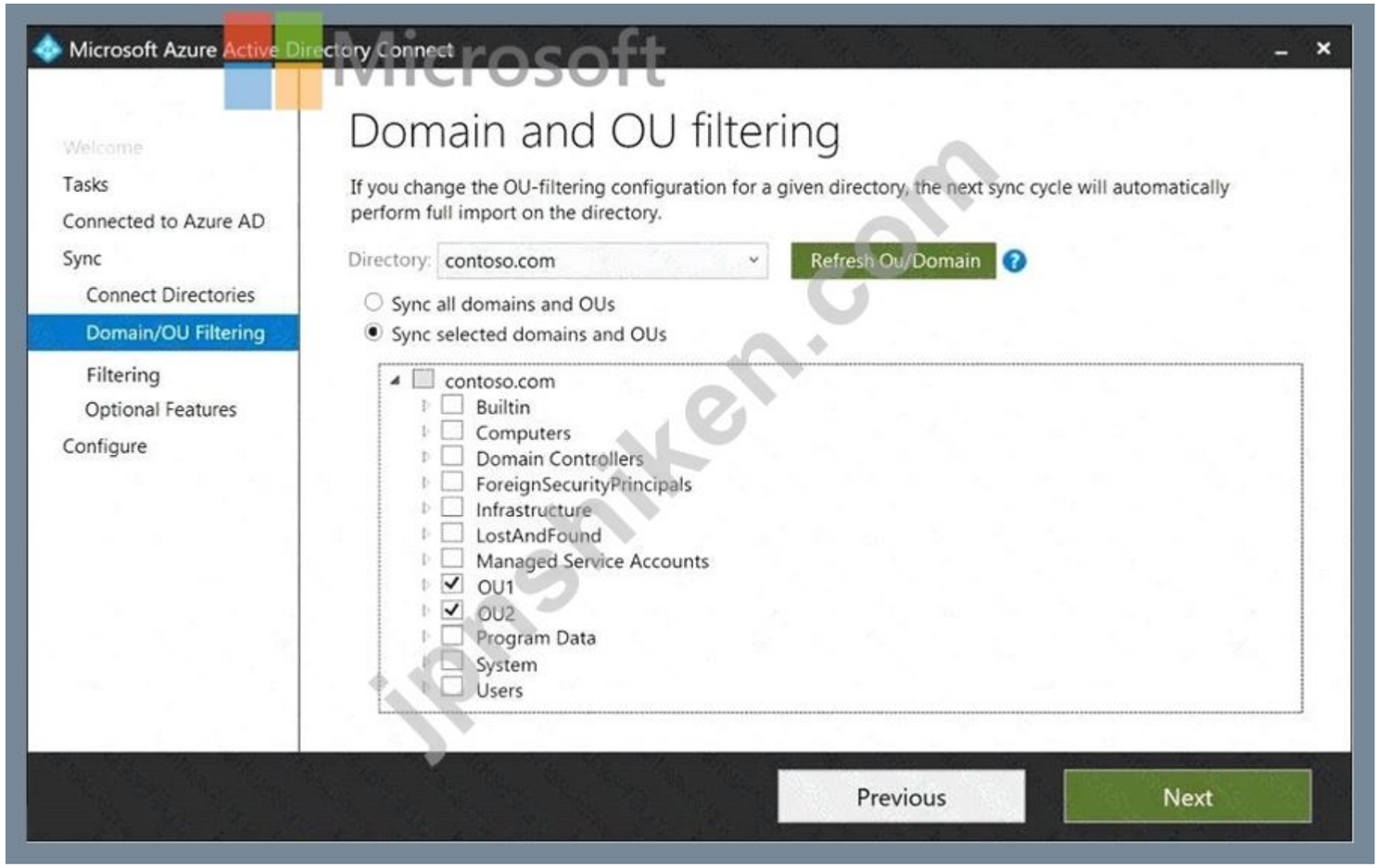
* HighRiskCountries: A condition
* Sign-in frequency: A session control

質問**: 12**

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

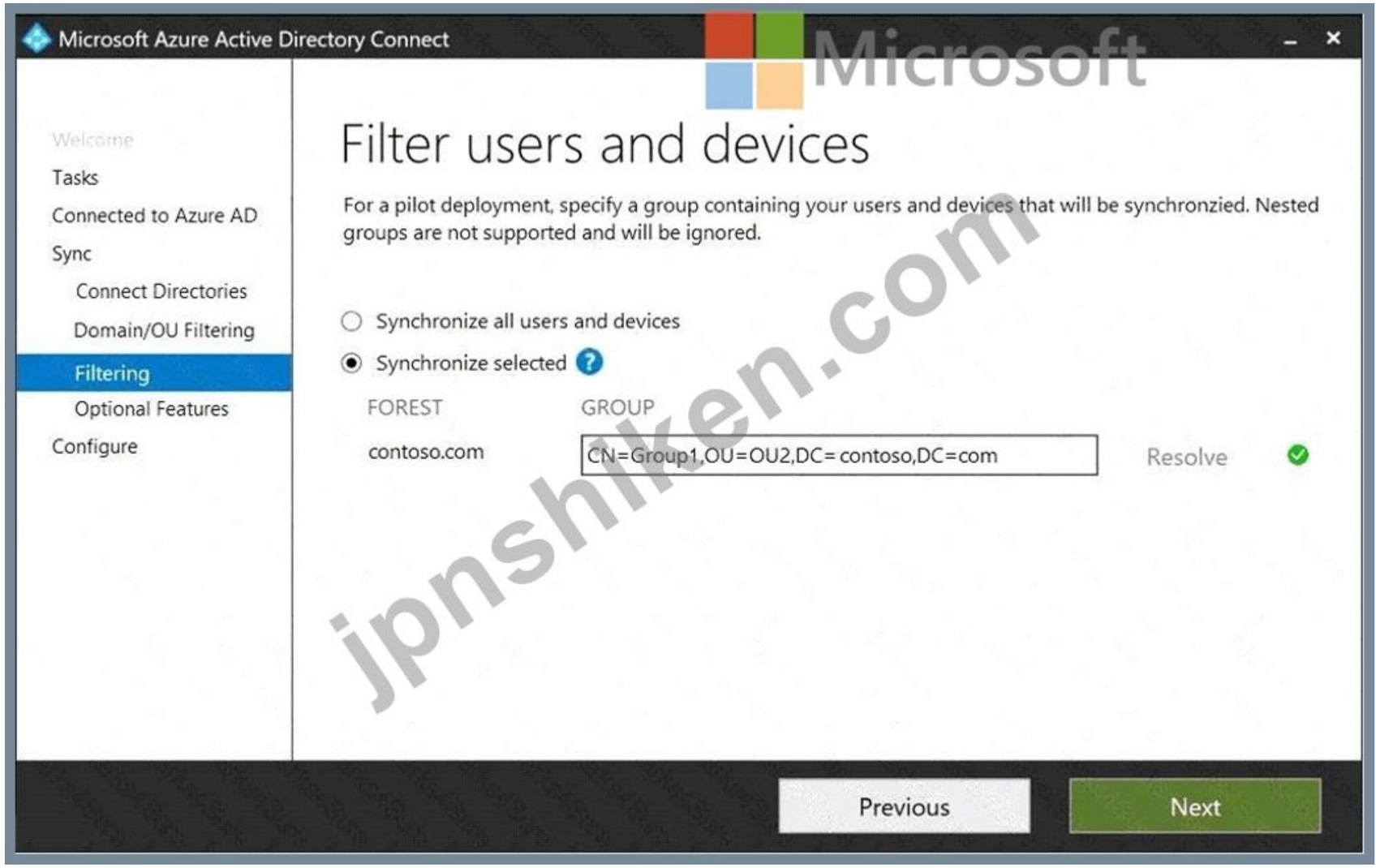
Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

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」の図に示すように、ドメインと OU のフィルタリング設定を構成します。(「ドメインと OU のフィルタリング」タブをクリックします。)



jnpshiken.com

ﾑユーザーとデバイスのフィルター」設定は、ﾑユーザーとデバイスのフィルター」の図に示すように構成します。(ﾑユーザーとデバイスのフィルター」タブをクリックします。)



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

正解:

jpnshiken.com



jpnshiken.com

Explanation:

User1 syncs to Azure AD: # Yes

* User2 syncs to Azure AD: # No

* Group2 syncs to Azure AD: # No

This scenario is directly covered in the Microsoft SC-300: Identity and Access Administrator exam section "Implement Azure AD Connect synchronization" and detailed in Microsoft documentation: "Azure AD Connect: Configure filtering" .

Azure AD Connect supports multiple filtering mechanisms:

* Domain and Organizational Unit (OU) filtering - only objects in selected OUs are synchronized.

* Group-based filtering (Pilot sync) - when enabled, only members of the specified security group (and required dependency objects) are synchronized. Nested groups are not supported.

* OU Filtering:

* Both OU1 and OU2 are selected.

* Therefore, objects in both OUs are eligible for synchronization (if other filters allow).

* Group-based filtering:

* The selected filter group is Group1, located in OU2.

* Azure AD Connect synchronizes only direct members of Group1 (users, groups, or devices).

* Nested groups are ignored - their members are not recursively synchronized .

* User1:

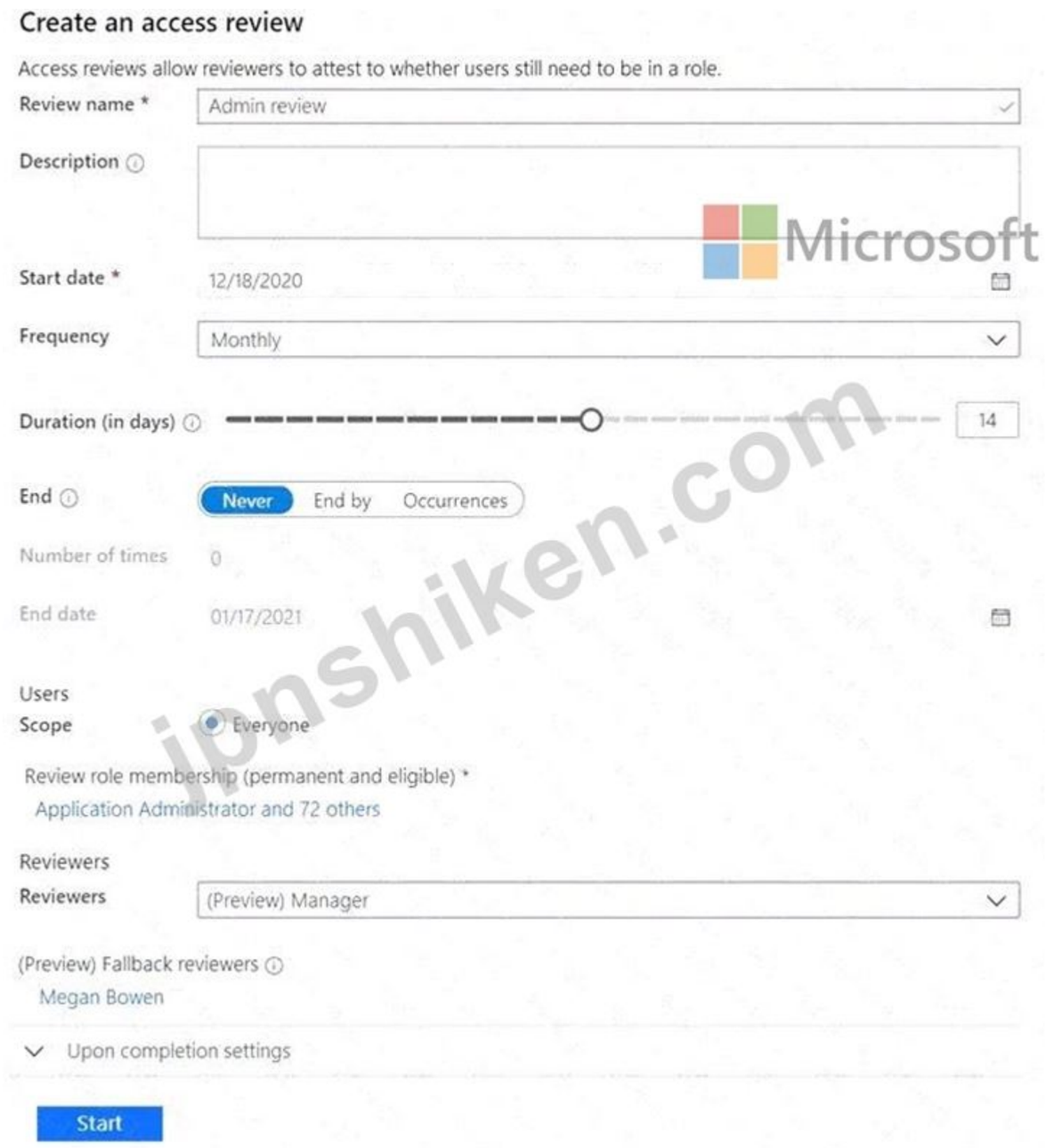
* Is a direct member of Group1 (in OU1).
* Since User1 is directly in Group1, and OU1 is included, User1 will sync to Azure AD. # User1 syncs to Azure AD = Yes
* User2:
* Is not a member of any group.
* The Group1-based filtering excludes non-members, even though OU1 is selected. # User2 syncs to Azure AD = No
* Group2:
* Is a member of Group1, but nested groups are ignored in Azure AD Connect group-based filtering.
* Thus, Group2 itself and its members will not be synchronized. # Group2 syncs to Azure AD = No Based on the exhibits: Evaluating Each Object: Supporting Microsoft Documentation (from SC-300 material):
"When you use group-based filtering, only objects that are direct members of the specified group are synchronized. Nested group memberships are ignored."
"If you select specific OUs for synchronization, objects must meet both the OU filtering and the group filtering criteria to be included in the sync."

質問**: 13**
Microsoft 365 E5 サブスクリプションがあり、その中に Site1 という Microsoft SharePoint Online サイトが含まれています。ユーザーが Site1 から 1 分間に 50 件を超えるファイルをダウンロードした場合に通知を受け取る必要があります。
Microsoft Defender for Cloud Apps ポータルで作成する必要があるポリシーの種類は何ですか?
A. セッションポリシー
B. 異常検出ポリシー
C. アクティビティポリシー
D. ファイルポリシー
正解**: (**正解を表示します**)**
To detect and get alerts when a user downloads a large number of files in a short period of time (for example, more than 50 files within one minute) in Microsoft SharePoint Online , you must configure an Activity policy in Microsoft Defender for Cloud Apps (MCAS) .
* Activity policies monitor specific user actions (upload, download, delete, share, etc.) and can trigger alerts based on thresholds or frequency.
* Anomaly detection policies detect behavioral anomalies automatically (not threshold-based).
* Session policies apply real-time controls during sessions (e.g., block download).
* File policies monitor or classify files at rest.
From Microsoft's documentation:
"Activity policies let you monitor specific activities in your cloud apps and define actions or alerts when certain criteria are met, such as excessive downloads or mass deletions." Thus, for detecting a user who downloads more than 50 files in one minute - an Activity polic y is required.

質問**: 14**
contoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
Azure ADに登録されているアプリケーションを実行するすべてのユーザーには、条件付きアクセスポリシーが適用されます。
ユーザーがレガシー認証を使用できないようにする必要があります。
従来の認証の試行を除外するために、条件付きアクセスポリシーに何を含める必要がありますか？
A. クラウドアプリまたはアクションの条件
B. ユーザーのリスク条件
C. クライアントアプリの状態
D. サインインのリスク条件

正解: **(**正解を表示します**)**
Reference:
The Conditional Access chapter of SC-300 states that administrators block legacy protocols by targeting them with the Client apps condition. The guide notes: "Client apps lets you target policy by application type such as browser, modern authentication clients, and legacy authentication clients." It gives the prescriptive action:
"To block legacy authentication, configure a policy with Client apps set to 'Other clients' (legacy) and grant control = Block." In contrast, Cloud apps or actions chooses the service (e.g., Office 365), User risk and Sign- in risk apply risk-based controls, not protocol filtering. Therefore, to filter out and prevent legacy authentication attempts, you must configure Conditional Access with the client apps condition targeting legacy
/other clients and block them, exactly as taught in the SC-300 objectives "Configure and manage Conditional Access."

質問: **15**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Microsoft365テナントがあります。
10の部門に編成された100人のIT管理者がいます。
展示に表示されるアクセスレビューを作成します。 [展示]タブをクリックします。）



すべてのアクセスレビューリクエストがMeganBowenによって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取るようにする必要があります。
解決策 :レビュー担当者をメンバー（自己）に設定します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**

In Azure AD access reviews, the Reviewer type determines who gets the review tasks. The SC-300 materials explain that selecting "Members (self)" triggers self-attestation, meaning each user only reviews their own access . The guidance states that when you use Members (self), "each user reviews only their own access," and owners or other people do not receive tasks for others. Your goal is for each department's manager to review their staff's access. For that, the documented reviewer choice is Manager (leveraging the user's manager attribute) and, optionally, fallback reviewers to catch users without a manager value. The exhibits show all requests going to Megan Bowen, which typically occurs when Manager is selected but many users lack a populated manager attribute-thus the tasks fall back to the specified fallback reviewer. Changing the reviewer to Members (self) would not route tasks to managers; it would simply ask every user to attest to their own access, failing the goal of manager-based attestation by department. Therefore, the proposed solution does not meet the requirement.

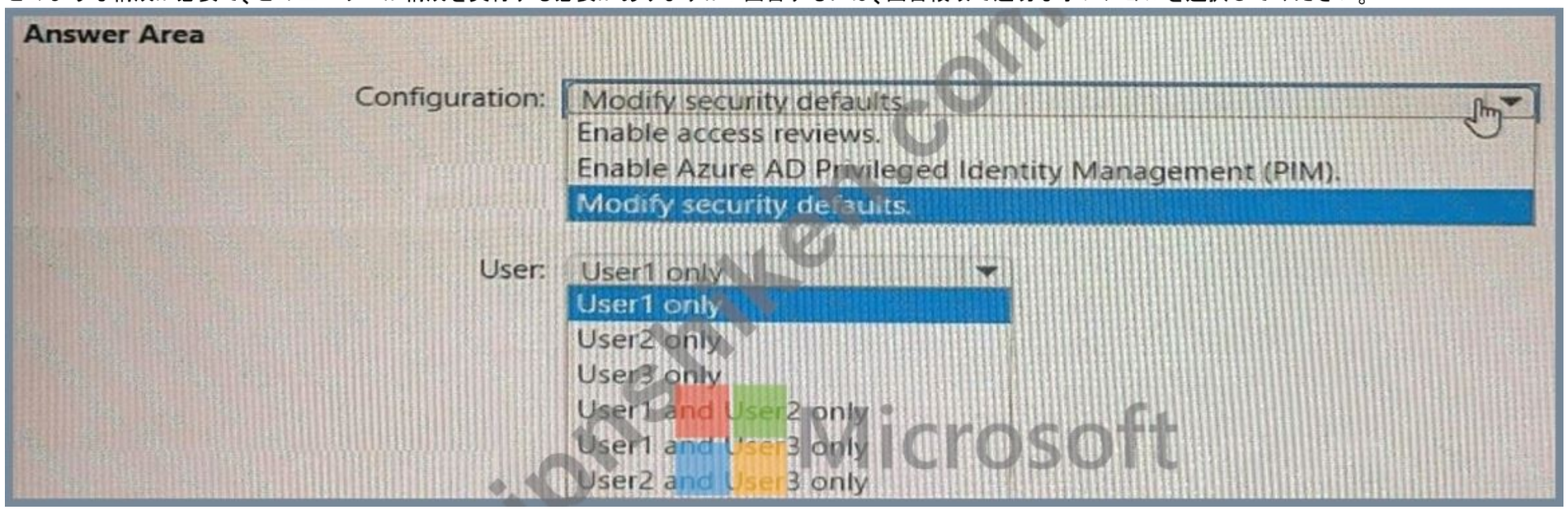
質問: **16**
Azure ADテナントをお持ちの場合
ユーザーの同意設定を構成して、確認済みの発行元からのアプリに対してユーザーが同意できるようにします。
ユーザーが、影響の少ない権限を必要とするアプリにのみ同意できるようにする必要があります。
何をすべきでしょうか?
A. アクセス パッケージを作成します。
B. 権限の分類を構成します。
C. エンタープライズ アプリケーション コレクションを作成します。
D. アクセスレビューを作成します。
正解: **(**正解を表示します**)**
When configuring user consent settings in Az ure AD, administrators can allow users to consent to third- party or verified publisher apps. However, to control which apps users can consent to based on their permission levels (for example, only "low impact" permissions), Microsoft provides enterprise ap plication collections .
An enterprise application collection lets administrators group apps and assign consent policies that define what permissions apps can request and what level of user consent is allowed.
From Microsoft documentation:
"You can use enterprise application collections to group apps and assign user consent policies that restrict the permissions users can grant to apps. For instance, you can ensure users can only grant low-impact permissions, even when the app comes from a verified publi sher." Other options explained:
* Access package : Used for entitlement management, not app consent.
* Permission classifications : Used to label permissions for administrators' understanding, not enforce user consent behavior.
* Access review : Used for periodic e valuation of access, not consent management.

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**」

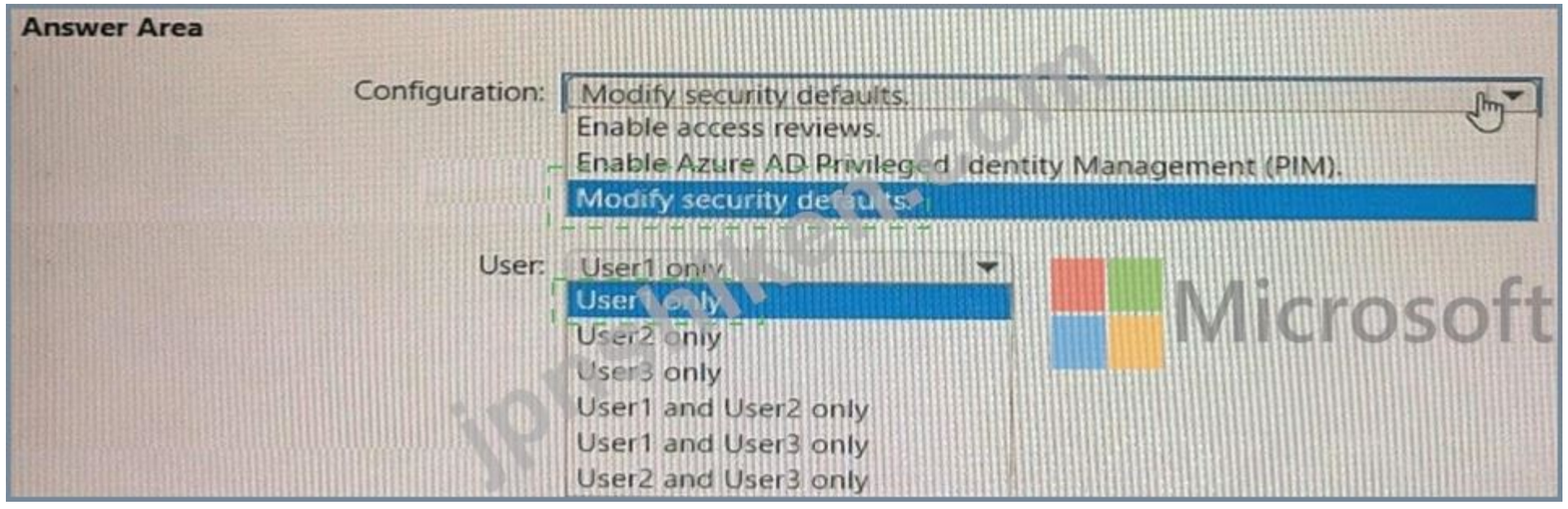
質問: **17**
次の表に示すユーザーを含む Azure AD テナントがあります。

Name	Role
User1	Security administrator
User2	Privileged authentication administrator
User3	Service support administrator

ユーザー2 は、Microsoft Authenticator アプリを使用するには多要素認証 (MFA) のみを構成できると報告しています。
User2 が代替 MFA 方法を構成できることを確認する必要があります。
どのような構成が必要で、どのユーザーが構成を実行する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

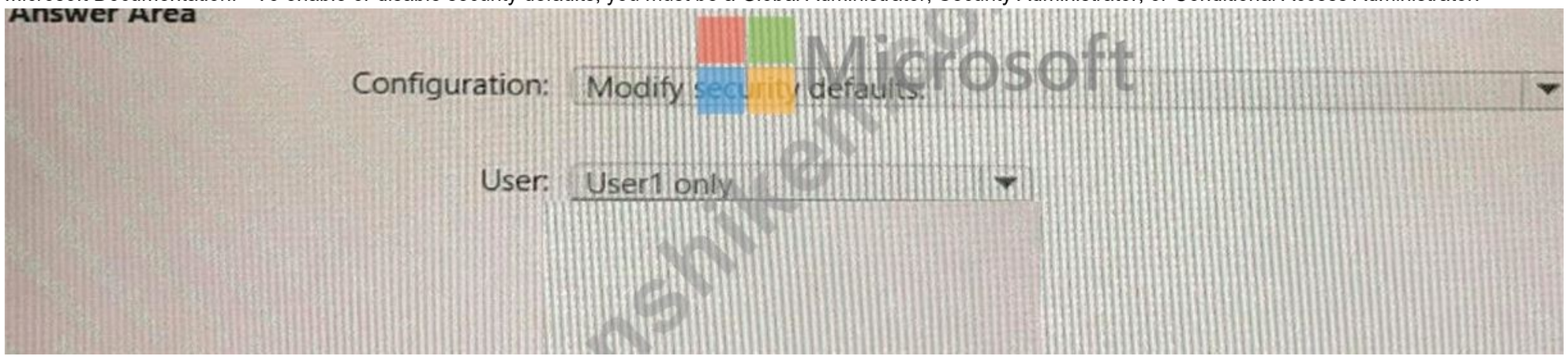


正解:



Explanation:
In Microsoft Entra ID (Azure AD), Security Defaults is a built-in baseline security configuration that enforces basic identity protection, such as requiring all users to register for multi-factor authentication (MFA) using the Microsoft Authenticator app. When security defaults are enabled, users cannot select alternate MFA methods (like SMS or phone call).
According to the Microsoft SC-300 Official St udy Guide and Azure AD Identity Protection documentation , only administrators with elevated security roles-specifically the Security Administrator, Global Administrator, or Conditional Access Administrator-can enable or disable security defaults.
Here's the detailed reasoning:
* User1 (Security Administrator): This role can manage identity security settings, including modifying MFA configurations and security defaults.
* User2 (Privileged Authentication Administrator): This role can reset MFA details for other users but cannot modify tenant-wide MFA or security default settings.

* User3 (Service Support Administrator): This role is limited to viewing service health and support tickets and has no permissions to modify security configurations.
Since User2 is restricted by security defaults (which enforce Microsoft Authenticator only), the only way to allow alternative MFA methods is to disable or customize security defaults. That configuration must be done by User1 (Security Administrator).
Microsoft Documentation: " To enable or disable security defaults, you must be a Global Administrator, Security Administrator, or Conditional Access Administrator."



質問: 18
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)
According to the official Microsoft Identity and Access Administrator (SC-300) Study Guide and the Azure Active Directory documentation under "Enable and configure self-service password reset (SSPR)", when self- service password reset is enabled, the available authentication methods depend on the user's role within Azure AD. Specifically, administrative roles require stronger authentication methods than regular users.
The Microsoft documentation states:
"Security questions are available only to users who are not administrators. Any user assigned an administrative role must use secure authentication methods such as email, mobile app, or phone verification." This restriction ensures that privileged accounts (e.g., User Administrator, Password Administrator, Global Administrator, Security Administrator, etc.) use stronger, phishing-resistant recovery options.
In the provided table:

* User1 (User Administrator) and User2 (Password Administrator) are administrators - they cannot use security questions for SSPR.
* User3 (Security Reader) and User4 (User) are non-administrative roles, therefore, they can use security questions when resetting their passwords.
Hence, only User3 and User4 will be required to answer security questions during password reset.

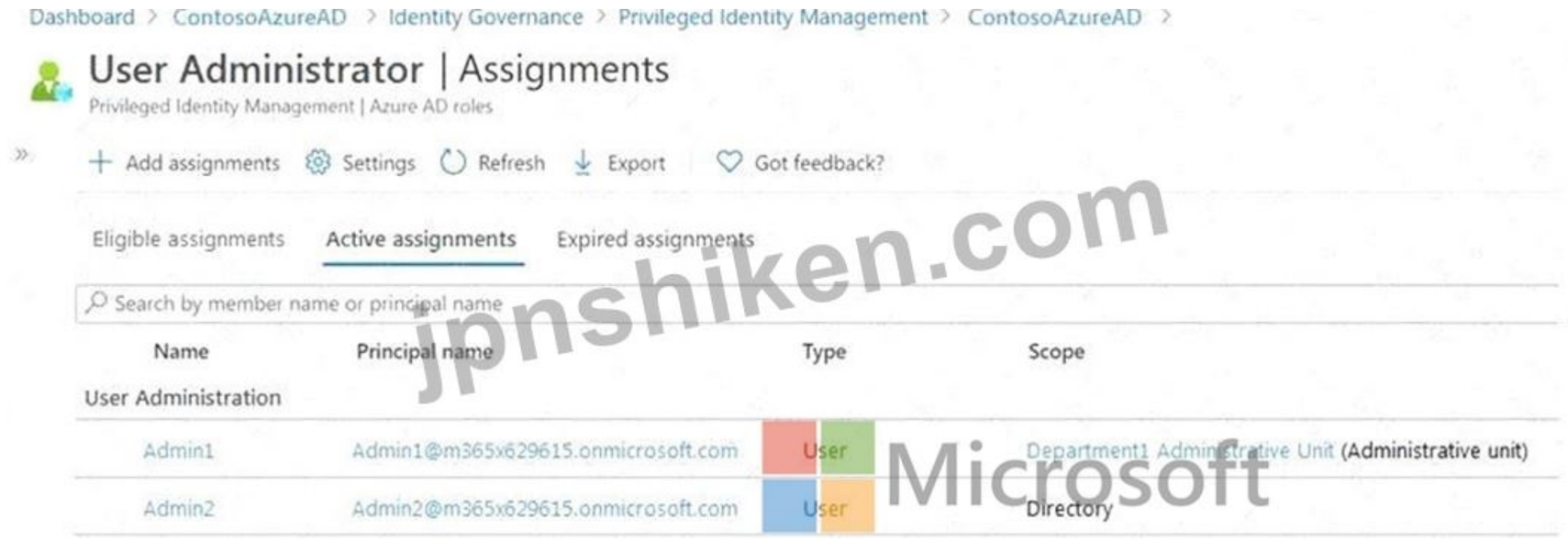
質問: **19**
Department1 という名前の管理単位を含む Azure Active Directory (Azure AD) テナントがあります。
Department1 には、[ユーザー] 展示に示されているユーザーがいます。([ユーザー] タブをクリックします。)



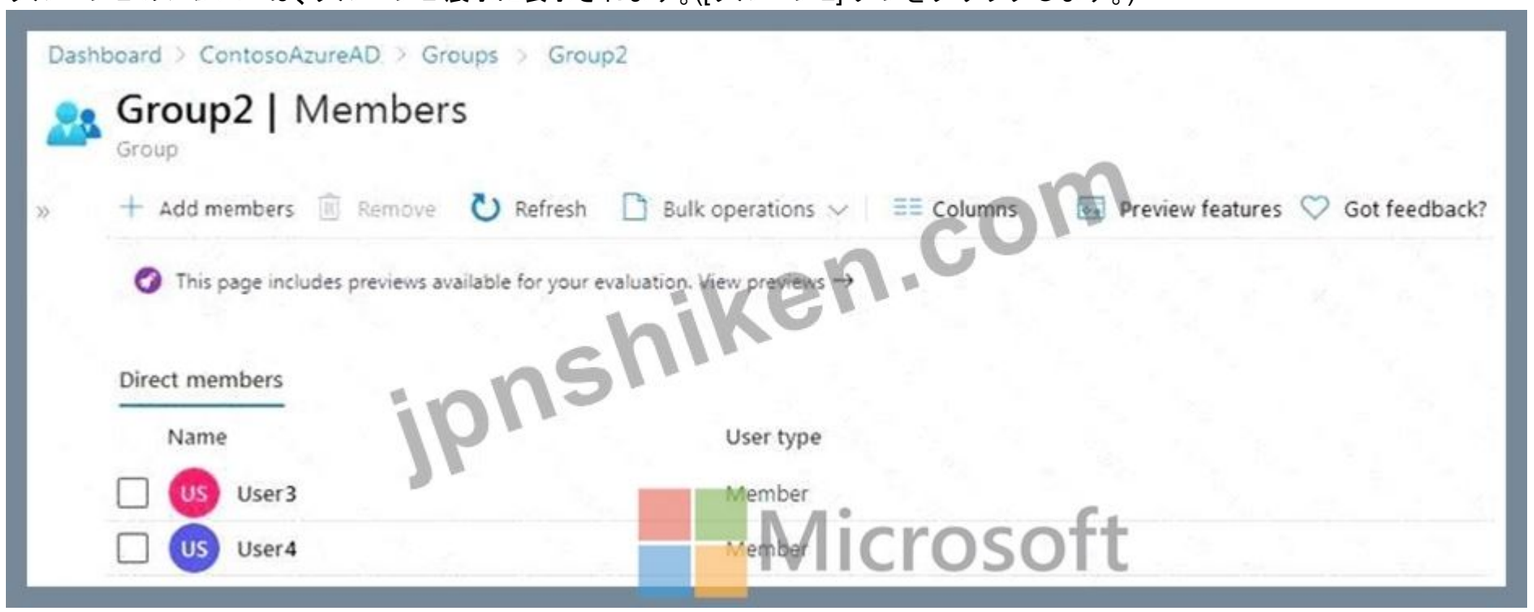
Department1 には、[グループ] 展示に示されているグループがあります。([グループ] タブをクリックします。)



Department1 には、[割り当て] 展示に示されているユーザー管理者の割り当てがあります。([割り当て] タブをクリックします。)



グループ 2 のメンバーは、グループ 2 展示に表示されます。([グループ 2] タブをクリックします。)



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

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

正解:

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Explanation:

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn documentation under "Manage Administrative Units in Azure Active Directory", Administrative Units (AUs) provide a way to delegate administrative permissions over subsets of Azure AD resources - such as specific users or groups - without granting directory-wide privileges.

* Department1 Administrative Unit contains User1, User2, Group1, and Group2.
* Admin1 is assigned the User Administrator role scoped to Department1 AU.
* Admin2 is assigned the User Administrator role scoped to the entire directory.

Context Overview

jpnshiken.com Microsoft

* User3 and User4 are not members of Department1 AU - they belong only to Group2, but group membership does not automatically bring those users under AU scope.
* Admin1's permissions are limited strictly to users and groups within the Department1 AU. # Conclusion: Admin1 cannot reset the passwords of User3 and User4. Answer: No Statement 1: Admin1 can reset the passwords of User3 and User4.
* Both User1 and Group2 are in the Department1 AU, but in Azure AD, the User Administrator role scoped to an AU cannot manage group memberships unless explicitly delegated with Group Administrator privileges or unless the AU is configured to allow it.
* The User Administrator role allows password reset and user management, not group membership management. # Conclusion: Admin1 cannot add User1 to Group2. Answer: No Statement 2: Admin1 can add User1 to Group2.
* Admin2 has the User Administrator role assigned at the directory level, meaning global scope.
* Therefore, Admin2 can manage user credentials, including password resets, for all users in the tenant - including User1. # Conclusion: Admin2 can reset the password of User1. Answer: Yes Statement 3: Admin2 can reset the password of User1.
Supporting Reference (Microsoft Learn):
"Administrative units restrict scope for delegated administrators. A User Administrator scoped to an AU can reset passwords only for users in that AU. A User Administrator assigned at the directory level can reset passwords for any user."

質問**: 20**
contoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
Azure ADの企業間（B2B）コラボレーションユーザーを一括招待する予定です。
一括招待を作成するときに含める必要がある2つのパラメーターはどれですか。それぞれの正解は解決策の一部を示しています注 :それぞれの正しい選択は1ポイントの価値があります。
A. メールアドレス
B. リダイレクトURL
C. ユーザー名
D. 共有キー
E. パスワード
正解**: (**正解を表示します**)**
In Azure AD B2B bulk invitations, the portal and CSV workflow require two core fields: the external user's email address and the Invite Redirect URL that determines where the guest is sent to redeem the invitation.
The study guide notes that the bulk invite template "must include the guest's email address" and that
"InviteRedirectUrl is required to define the post-invite redemption target (such as MyApps or a specific app)." Usernames and passwords are not supplied for B2B guests because "guest accounts authenticate with their home identity provider," and there is no shared key involved in the invitation. Therefore, the only mandatory parameters to successfully process a bulk B2B invite are the email address of each guest and the redirection URL used during invitation redemption.

質問**: 21**
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	User risk level
User1	Low
User2	Medium
User3	High

次の表に示す Azure AD Identity Protection ポリシーがあります。

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

危険なユーザー レポートと危険なサインイン レポートを確認し、次の表に示すように各ユーザーに対してアクションを実行します。

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

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

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.	○	○

正解:

Answer Area

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:

User1 can sign in by using multi-factor authentication (MFA): No

User2 can sign in by using multi-factor authentication (MFA): No

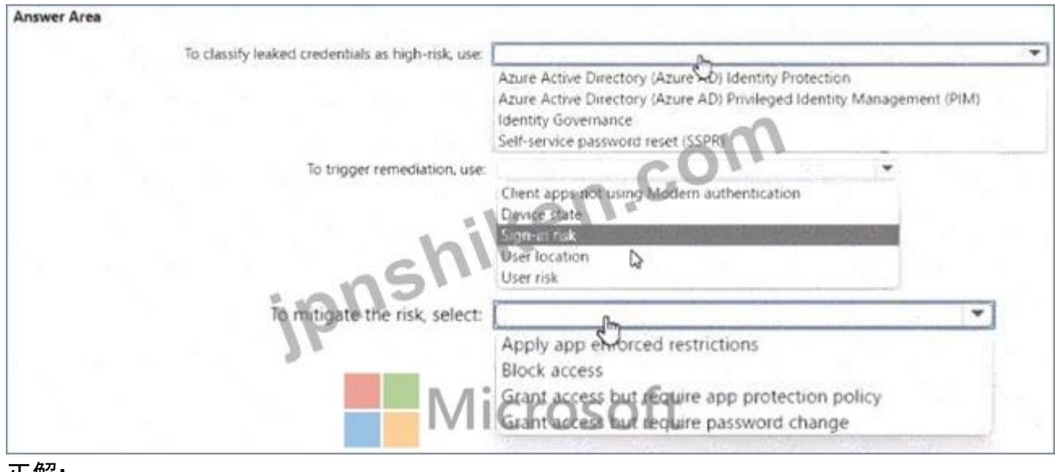
User3 can sign in from an anonymous IP address: No

This scenario is based on Azure AD Identity Protection and its two core conditional access mechanisms:
* User risk policy - evaluates the probability that a user ' s identity might be compromised.
* Sign-in risk policy - evaluates the probability that a sign-in attempt might not be performed by the legitimate user.
Let's analyze step-by-step based on the tables provided:
* Risk level: Low
* User risk policy: Applies to Low and above (so Low, Medium, and High users).
* Control: Block access.
* Action performed: Confirm user compromised. Confirming a user as compromised keeps or increases their risk level until the user is remediated (i.e., password reset). Because the policy blocks access for any user risk "Low and above," User1's sign-in is blocked, and MFA will not be prompted - access is denied.
# User1 # User1 MFA sign-in: No
* Initial risk level: Medium
* Actions performed:
* Confirm sign-in safe # clears that sign-in's risk.
* Confirm user compromised # elevates user risk back to "High."
* Policies applied:
* User risk policy (Low and above): Blocks access.
* Sign-in risk policy: Applies only to High sign-ins (not relevant here).
# User2 Since User2's user risk is set to High after confirming compromised, the User risk policy blocks access for "Low and above." Therefore, MFA is not allowed (the session is denied outright).
# User2 MFA sign-in: No
* User risk: High
* Action performed: Dismiss user risk # resets the user risk to "No risk."
* Sign-in policy: High sign-in risk # block access. If User3 signs in from an anonymous IP, Azure AD Identity Protection detects this as a High sign-in risk (per Microsoft documentation). Since the sign-in risk policy blocks all high sign-ins, access will be blocked.
# User3 # User3 anonymous IP sign-in: No

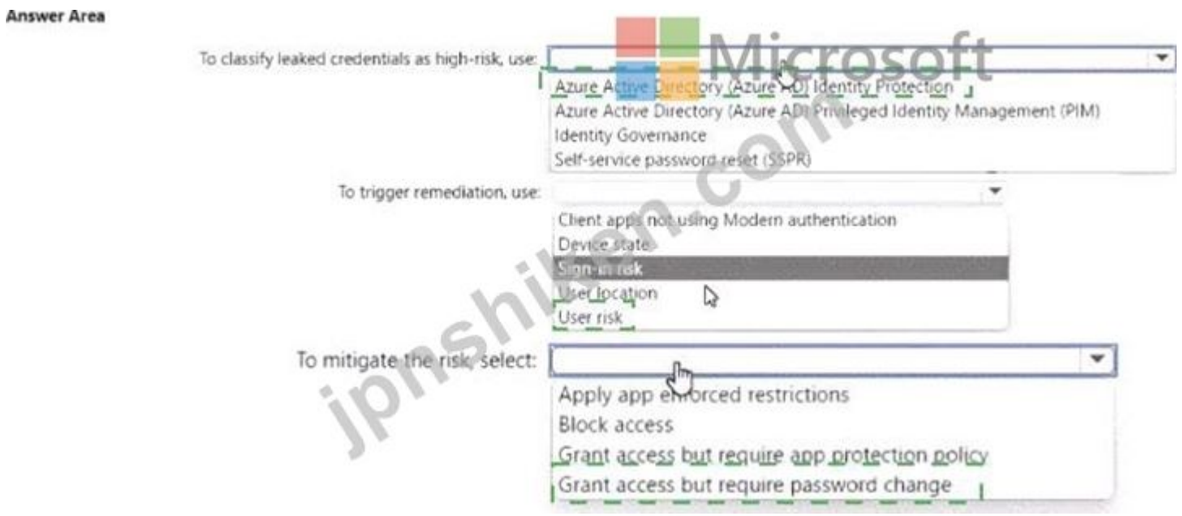
質問: **22**
Azure サブスクリプションがあります。このサブスクリプションには、Linux を実行する VM1 という仮想マシンが含まれています。
VM1 に強化されたセキュリティを構成する必要があります。ソリューションは以下の要件を満たす必要があります。
* ユーザーがMicrosoft Entraの資格情報を使用してVM1にサインインできることを確認します
* ユーザーが多要素認証を使用して認証されていることを確認する
* ユーザーがパスワードを使用して VM1 にサインインできないようにします。
解答に含めることができる認証方法は2つあります。正解はそれぞれ完全な解答となります。注：正解は1つにつき1点です。
A. Microsoft Authenticator アプリ
B. Windows Hello for Business
C. パスキー(FID02)
D. 一時アクセスパス
E. SMS
正解: **(**正解を表示します**)**
The requirement specifies that:
* Users must sign in using Microsoft Entra credentials,

* Multi-factor authentication must be out-of-band,
* Password sign-ins must be prevented.
According to Microsoft Learn: "Configure passwordless authentication in Microsoft Entra ID" and the SC-
300 Exam Ref , the two supported passwordless and MFA-capable authentication methods that satisfy these conditions are:
* Microsoft Authenticator app - Supports passwordless sign-in using push notifications, providing both identity verification and multi-factor authentication in a single step.
* FIDO2 Passkey - Enables secure passwordless authentication through hardware security keys or device-bound passkeys that rely on public key cryptography and satisfy MFA requirements when configured properly.
Both methods eliminate password usage entirely and integrate with Microsoft Entra for strong identity assurance.
Windows Hello for Business is passwordless but limited to Windows devices (VM1 is Linux). Temporary Access Pass (TAP) is a bootstrap mechanism for enrolling in passwordless sign-in, not a long-term solution.
SMS authentication, while MFA-capable, still requires passwords for primary authentication and doesn't meet the passwordless requirement.

質問**: 23**
Microsoft 365 テナントがあります。
認証情報が漏洩したユーザーを特定する必要があります。ソリューションは以下の要件を満たす必要があります。
* 認証情報が漏洩した疑いのあるユーザーによる ID サイン。
* サインインを高リスクイベントとしてフラグ付けします。
* ユーザーがアプリケーションにアクセスできるようにしながら、リスクを軽減するための制御を直ちに実施します。
何を使うべきですか? 回答するには、回答エリアで適切なオプションを選択してください。



正解:



Explanation:



According to Microsoft's SC-300 Study Guide , Exam Ref SC-300: Microsoft Identity and Access Administrator , and the Azure AD Identity Protection documentation , leaked credentials and risky sign-ins are detected and managed through Azure AD Identity Protection. This service identifies, categorizes, and automates the mitigation of risks related to user and sign-in behavior.

* Classify leaked credentials as high-risk:
* Azure AD Identity Protection automatically flags users as high-risk if their credentials appear in public or dark web breach data. Microsoft continuously monitors leaked credentials and matches them against Azure AD user accounts.
* The guide states: "Azure AD Identity Protection detects when user credentials are found on public credential dumps and flags those users as high-risk."
* Trigger remediation:
* The appropriate signal to trigger a policy response for leaked credentials is User risk, not sign-in risk.
* User risk evaluates the likelihood that a user's identity has been compromised, while sign-in risk deals with suspicious conditions during authentication.
* From Microsoft's documentation: "User risk policy is used to automatically remediate leaked credentials by requiring the user to change their password."
* Mitigate the risk:
* To mitigate the risk while still allowing access, the best practice is to grant access but require a password change . This satisfies the requirement to "immediately enforce a control" without fully blocking the user.
* The SC-300 study materials confirm: "When user risk is high, organizations can configure policies to allow sign-in but require a password change to remediate risk."

質問**: 24**

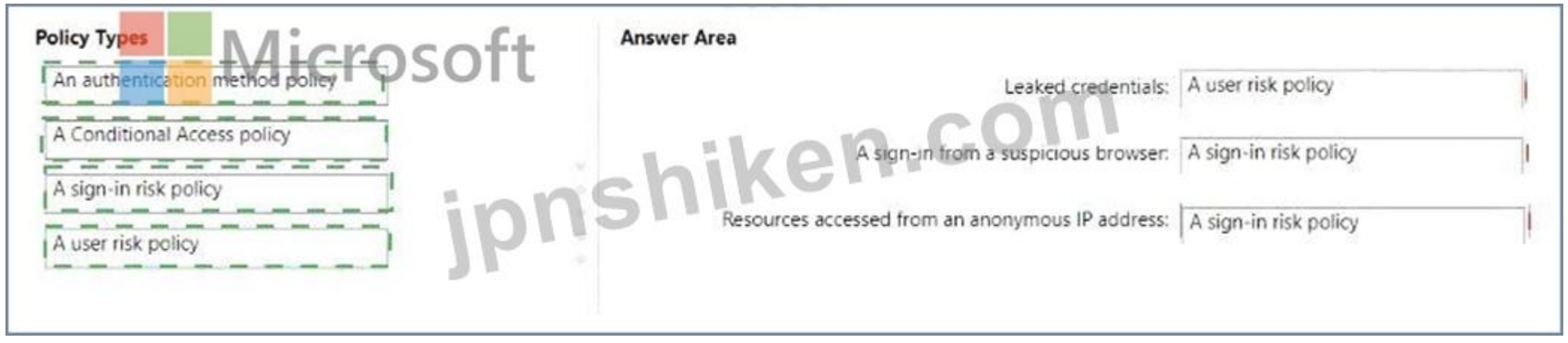
最近のセキュリティ インシデントの問題を解決する必要があります。

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？適切なポリシータイプを適切な問題にドラッグすることで、その答えが見つかります。各ポリシータイプは、1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator official study guide and the Microsoft Learn "Implement and manage Azure AD Identity Protection" module, Azure AD Identity Protection detects two primary categories of risks: user risks and sign-in risks.

* User Risk Policy: A user risk represents the probability that a user ' s identity (credentials) has been compromised. Examples of user risk signals include leaked credentials , unusual sign-ins from different geographies , or sign-ins from infected devices . The Exam Ref SC-300 specifically lists "leaked credentials detected on the dark web or other compromised repositories" as the main trigger for a user risk policy. Such a policy can automatically force password change or enforce MFA to remediate the threat.
* Sign-in Risk Policy: A sign-in risk reflects the likelihood that a specific authentication attempt is not performed by the legitimate user. Sign-in risk is based on context, such as sign-ins from suspicious browsers , anonymous IP addresses (like TOR networks) , or impossible travel sce narios . The SC-300 documentation highlights these examples as conditions best handled with a sign-in risk policy, where conditional access can block or require MFA for the risky sign-in attempt.

Therefore:

* Leaked credentials are addressed through a User Risk Policy, since the account itself is compromised.
* Sign-ins from suspicious browsers and access from anonymous IP addresses are handled through Sign- in Risk Policies, as they relate to risky sessions rather than compromised identities.

質問: **25**

Admin1 という名前のユーザーを含む Azure AD テナントがあります。

Admin1 は、高リスク ユーザーのパスワード変更を要求するポリシー テンプレートを使用して、新しい条件付きアクセス ポリシーを作成します。

ポリシー割り当てにおいて、デフォルトで誰に含まれ、誰に除外されるのでしょうか？ 適切なオプションを正しい対象にドラッグしてください。各オプションは、1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft SC-300: Microsoft Identity and Access Administrator Official Study Guide and Microsoft Learn - Manage Conditional Access policies module, when an administrator creates a Conditional Access policy using the built-in Require password change for high-risk users template, the policy is automatically pre-configured with specific include and exclude assignments.
By default, this template targets "All users" in the tenant because the policy is designed to detect and remediate risky sign-ins or compromised accounts across the entire directory. However, since Azure AD B2B guest accounts and external users often have limited sig n-in scopes and cannot be subjected to organization- specific password policies, Microsoft's security baseline specifically excludes all guest and external users by default.
The intent behind this default configuration is to apply the password change requir ement to internal users while avoiding unnecessary enforcement on guest identities that do not manage credentials within the host tenant.
From the Microsoft Learn - Conditional Access policy templates documentation:
"When you create a policy from the Requi re password change for high-risk users template, the policy is configured to include all users and exclude all guest and external users by default."

質問: **26**
オンプレミスの Linux デバイスがあります。
Microsoft 365 E5 サブスクリプションをお持ちです。
グローバル セキュア アクセス インターネット アクセスを構成する予定です。
デバイスが Global Secure Access に接続できることを確認する必要があります。
何をすべきでしょうか?
A. プライベート ネットワーク コネクタをデプロイします。
B. Adaptive Access 設定を構成します。
C. デバイスに Azure Connected Machine エージェントをインストールします。
D. リモート ネットワークを作成します。
正解: **(**正解を表示します**)**
When configuring Global Secure Access - Internet Access for on-premises or non-Azure servers/devices (including Linux), the devices must first be onboarded into Microsoft Entra through Azure Arc. To onboard Linux servers or machines, the Azure Connected Machine agent must be installed. This agent connects the on- premises device to Azure Arc, enabling visibility, policy application, and integration with Global Secure Access.
Options such as deploying a Private Network Connector (A) or creating a Remote Network (D) apply to routing network traffic for Private Access, not onboarding non-Azure devices. Adaptive Access settings (B) are policy-level controls, not onboarding prerequisites.

質問: **27**
Microsoft 365 E5 サブスクリプションをお持ちです。

アプリ ガバナンス アドオン ライセンスを購入します。
アプリのガバナンス統合を有効にする必要があります。
どのポータルを使用する必要がありますか?
A. Microsoft Defender for Cloud Apps ポータル
B. Microsoft 365 管理センター
C. Microsoft 365 Defender
D. Azure Active Directory 管理センター
E. Microsoft Purview コンプライアンス ポータル
正解: **(**正解を表示します**)**
As documented in Microsoft's App governance for Microsoft 365 guidance, App Governance is a security and compliance add-on that provides visibility and policy-based controls over OAuth-enabled applications integrated with Microsoft 365. Once you purchase and assign the app governance license, the integration and management of this feature are performed through the Microsoft 365 Defender portal.
In the Defender portal, administrators navigate to App governance under the Permissions & Apps section to enable integration, view insights, and configure policies. Microsoft documentation states: "App governance capabilities are surfaced in the Microsoft 365 Defender portal (https://security.microsoft.
com) where you can monitor, alert, and remediate risky app behaviors connected to Microsoft 365 data." Therefore, the integration and monitoring are managed only in Microsoft 365 Defender, not in Azure AD, Purview, or Defender for Cloud Apps.

質問: **28**
次のクラウド プラットフォームのアカウントがあります。
* アズール
* アリババクラウド
* アマゾン ウェブ サービス (AWS)
* Google クラウド プラットフォーム (GCP)
A2ure サブスクリプションを Microsoft Entra Permissions Management を使用して Azure のみの権限管理を行うように設定しています。Permissions Management を使用して管理できる追加のクラウド プラットフォームは何ですか？
A. AWSのみ
B. Alibaba Cloud と AWS のみ
C. Alibaba Cloud と GCP のみ
D. AWS と GCP のみ
E. Alibaba Cloud、AWS、GCP
正解: **(**正解を表示します**)**
To answer this question correctly, we must reference the supported cloud platforms for Microsoft Entra Permissions Management (formerly known as CloudKnox).
1. What is Microsoft Entra Permissions Management? Microsoft Entra Permissions Management is a Cloud Infrastructure Entitlement Management (CIEM) solution. Its primary purpose is to discover, remediate, and monitor permission risks for any identity and any resource across your multi-cloud infrastructure.
2. Supported Cloud Platforms: According to the official Microsoft Entra Permissions Management documentation, the service provides comprehensive visibility and control over permissions for the following specific cloud providers:
* Microsoft Azure
* Amazon Web Services (AWS)
* Google Cloud Platform (GCP)
3. Analysis of the Options:

* Alibaba Cloud: While Microsoft Defender for Cloud (CSPM) and Azure AD (for SSO) have integrations with Alibaba Cloud, Microsoft Entra Permissions Management explicitly supports only the three major public clouds listed above (Azure, AWS, and GCP). It does not currently support Alibaba Cloud for entitlement and permission management.
* The Scenario: You have already configured it for Azure. You need to identify which additional platforms from the list (Alibaba, AWS, GCP) can be managed.
* Conclusion: Since Alibaba Cloud is not supported, the only remaining valid platforms from your list are AWS and GCP.
Reference Extract:
"Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities... across cloud infrastructures Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP)."

質問**: 29**
Microsoft 365 テナントがあります。
Microsoft Entra ID で、利用規約を構成します。
利用規約に同意したユーザーのみがテナント内のリソースにアクセスできるようにする必要があります。他のユーザーのアクセスは拒否する必要があります。
何を設定すればよいでしょうか?
A. Microsoft Defender for Cloud Apps のアクセス ポリシー
B. Microsoft Intune のコンプライアンス ポリシー
C. Microsoft Intune の利用規約
D. Microsoft Entra ID の条件付きアクセス ポリシー
正解**: (**正解を表示します**)**
Per the Microsoft SC-300: Identity and Access Administrator official study guide and Microsoft Learn module: "Implement Conditional Access policies", the enforcement of Terms of Use (ToU) acceptance for accessing organizational resources is done through Conditional Access policies in Microsoft Entra ID.
After uploading a Terms of Use PDF and assigning it to users, administrators must link that ToU to a Conditional Access policy to ensure that only users who have accepted the ToU can access corporate apps or data. The Conditional Access engine enforces this by evaluating whether the user's ToU status equals
"accepted" at sign-in. If not, access is denied until the user accepts the terms.
The Exam Ref SC-300 clarifies:
"Terms of Use documents are enforced through Conditional Access policies. You can require users to accept the terms before accessing specified apps or resources." Alternative options such as Intune compliance policies or Defender for Cloud Apps access policies manage device compliance and session control, but they do not enforce Entra ToU acceptance.

質問**: 30**
Microsoft 365 テナントがあります。
現在、基本認証を使用する電子メール クライアントが Microsoft Exchange Online に接続することを許可しています。
ユーザーが Exchange に接続し、最新の認証プロトコルを使用する電子メール クライアントのみを実行できるようにする必要があります。
何を実装する必要がありますか?
モダン認証を使用する必要がある
A. Microsoft Endpoint Manager のコンプライアンス 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 のアプリケーション制御プロファイル
D. Microsoft Cloud App Security の OAuth ポリシー
正解**: (**正解を表示します**)**
In Microsoft 365, Basic authentication is an outdated protocol that sends credentials in plain text and does not support MFA. To enforce Modern authentication (OAuth 2.0), which is required for stronger identity protection and token-based access, administrators must block legacy authentication using Conditional Access policies in Azure AD.

According to the SC-300 study guide and Microsoft Learn module "Implement Conditional Access policies", this can be achieved by:
* Creating a Conditional Access policy in Azure AD.
* Targeting the Exchange Online cloud app.
* Setting the condition Client apps # Other clients (legacy authentication) to block access.
Modern authentication clients (like Outlook 2016+, Outlook on the web, and Outlook mobile) use secure OAuth tokens that comply with Conditional Access requirements (such as MFA, device compliance, or trusted location).
Compliance policies or application control profiles in Microsoft Endpoint Manager do not manage authentication protocols, and Microsoft Cloud App Security OAuth policies govern third-party app permissions, not Exchange connectivity.
Therefore, the correct approach to ensure only Modern authentication clients can connect is to enforce this through a Conditional Access policy in Azure AD.

質問: **31**
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	Cloud Application Administrator
Admin2	Application Administrator
Admin3	Security Administrator
User1	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 Microsoft Entra ID に追加し、User! を App1 の所有者として設定します。
アプリを使用する前に、App1 では Microsoft Entra ID にアクセスするための管理者の同意が必要です。
次の図に示すように、管理者の同意要求設定を構成します。



Admin1、Admin2、Admin3、User1がレビュー担当者として追加されました。管理者の同意リクエストをレビューして承認できるのはどのユーザーですか？
A. 管理者1のみ
B. 管理者1と管理者2のみ
C. Admin1、Admin2、Admin3のみ
D. Admin1、Admin2、User1のみ
E. 管理者1、管理者2、管理者3、およびユーザー1
正解: **(**正解を表示します**)**

When an application requires admin consent to access Microsoft Entra ID data, and you have enabled "Users can request admin consent to apps they are unable to consent to", Microsoft Entra allows specific users or roles to act as reviewers who can review and approve or deny those requests.
In this scenario:
* The Admin consent requests feature is enabled.
* Admin1, Admin2, Admin3, and User1 were added as reviewers.
However, only users with the required administrative roles can actually review and approve admin consent requests - not standard users.
According to the Microsoft SC-300 study guide and Microsoft Learn documentation ("Configure the admin consent workflow"), the roles that can review and approve admin consent requests include:
* Global Administrator
* Cloud Application Administrator
* Application Administrator
The Security Administrator role can view and audit permissions but cannot approve consent requests, and regular users (with no admin role) cannot perform any action in this workflow.
Applying this to the question:
* Admin1 (Cloud Application Administrator) # # Can approve requests.
* Admin2 (Application Administrator) # # Can approve requests.
* Admin3 (Security Administrator) # # Can review (depending on Entra configuration; Security Administrator has partial consent visibility for security-sensitive apps).
* User1 (None) # # Cannot review or approve because they lack an admin role.
Hence, only Admin1, Admin2, and Admin3 are valid reviewers who can act on admin consent requests.

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: **32**
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. アプリのパスワード
C. Windows Hello for Business
D. SMS
正解: **(**正解を表示します**)**
In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.
After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN.

The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

質問: **33**
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	Usage location	Department	Job title
User1	United States	Sales	Associate
User2	Finland	Sales	SalesRep
User3	Australia	Sales	Manager

動的ユーザー グループを作成し、次のルール構文を構成します。

```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

どのユーザーがグループに追加されますか?
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1とユーザー3のみ
F. ユーザー1、ユーザー2、ユーザー3
正解: **(**正解を表示します**)**
Dynamic Azure AD groups use membership rules written against user attributes (for example, user.
department , user.jobTitle , user.country , user.usageLocation). The SC-300 materials show operators such as
-eq, -contains, -startsWith, and logical -and/-or to build precise targeting. In this scenario, the provided rule syntax evaluates users in the Sales department whose jobTitle contains "Sales" (for example, "SalesRep").
From the data: User1 has job title Associate (does not contain "Sales"); User2 has job title SalesRep (contains
"Sales"); User3 has job title Manager (does not contain "Sales"). Because department for all three is Sales, the discriminating condition is the job title match. Therefore, only User2 satisfies the rule and will be added to the dynamic group. The SC-300 guide emphasizes validating rules with the "Preview membership results" tool to confirm which users are included before enforcing at scale.

質問: **34**
営業部門のユーザーの問題を解決する必要があります。Azure ADテナントにどのような設定を行う必要がありますか？
A. ユーザー設定
B. デバイス設定
C. アクセスレビューの設定
D. セキュリティのデフォルト
正解: **B (**コメントを発表する**)**
In Microsoft Entra ID (Azure AD), the per-user device cap is controlled in Devices > Device settings. The SC-
300 materials describe that administrators can configure "Users may join devices to Azure AD" and the
"Maximum number of devices per user" . The guide notes that this limit defaults to five and is used to

"control how many devices a user can join or register in Azure AD"; when users reach the limit, "they cannot add additional devices until the limit is increased or an existing device is removed." For scenarios like field or sales staff who use multiple devices, the study content recommends adjusting this value to meet business needs. Because A. Datum's sales users hit the current cap and a requirement states "Increase the maximum number of devices that can be joined or registered to Azure AD to 10," the fix is to change the tenant's Device settings-not User settings, Access reviews, or Security defaults. This aligns with the exam objective to configure device settings for Azure AD join and registration and addresses the precise symptom reported by users.

質問: **35**
既定のドメイン名 contosso.com を使用するように新しい Microsoft 36S テナントを構成します。
条件付きアクセス ポリシーを使用して、Microsoft 365 リソースへのアクセスを制御できることを確認する必要があります。
まず何をすべきでしょうか?
A. ユーザーの同意設定を無効にします。
B. セキュリティのデフォルトを無効にします。
C. 多要素認証 (MLA) 登録ポリシー1 を構成します。
D. Windows Server Active Directory のパスワード保護を構成します。
正解: **(**正解を表示します**)**
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn module "Plan and implement Conditional Access policies" , enabling or customizing Conditional Access policies requires that Security Defaults in Azure AD be disabled .
Security defaults provide a basic level of protection, such as enforcing MFA for all users and blocking legacy authentication. However, when Security Defaults are enabled, custom Conditional Access policies cannot be created because both features manage sign-in risk and access control.
From the Microsoft documentation:
"To use Conditional Access policies, you must disable security defaults. Conditional Access policies provide more granularity and flexibility than security defaults." Therefore, before you can control access to Microsoft 365 resources through Conditional Access, the first step is to disable Security Defaults in the Azure AD tenant.

質問: **36**
contoso.com の SMTP アドレス スペースを使用する Microsoft Exchange 組織があります。
複数のユーザーが、1 Microsoft Entra へのセルフサービス サインアップに contoso.com の電子メール アドレスを使用しています。
自己署名ユーザーを含む Microsoft Entra テナントに対するグローバル管理者権限を取得します。
ユーザーが Microsoft 365 サービスにセルフサービスでサインアップできるように、contoso.com 2 Microsoft Entra テナントにユーザー アカウントを作成できないようにする必要があります。
どの PowerShell コマンドレットを実行する必要がありますか?
A. Update-MgDomain
B. Update-MgPolicyAuthorizationPolicy
C. Update-MgPolicyPermissionGrantPolicyExclude
D. Update-MgDomainFederationConfiguration
正解: **A (**コメントを発表する**)**
According to the Microsoft SC-300 Study Guide and Microsoft Learn module: "Manage Microsoft Entra domains and custom domain names", when users perform self-service sign-up (email verified users) using a public domain such as contoso.com, Microsoft Entra creates a shadow tenant that you can later claim ownership of by verifying the DNS domain.
Once you become the Global Administrator of the verified tenant, you can control domain behavior, including blocking self-service sign-up using that domain. To disable further self-service creation of accounts for that domain, you must modify the domain configuration using the Update-MgDomain PowerShell cmdlet.
The cmdlet Update-MgDomain allows you to change properties of the domain, such as IsDefault, IsVerified, and crucially, blocking self-service sign-ups.
Example:
Update-MgDomain -DomainId contoso.com -IsAdminManaged $true

This action prevents external or unverified users from using @contoso.com email addresses for new self- service sign-ups.
Other options like Update-MgPolicyAuthorizationPolicy, Update-MgPolicyPermissionGrantPolicyExclude, and Update-MgDomainFederationConfiguration are used for tenant-wide access, permission grants, or federated authentication but not to block self-service domain registration.

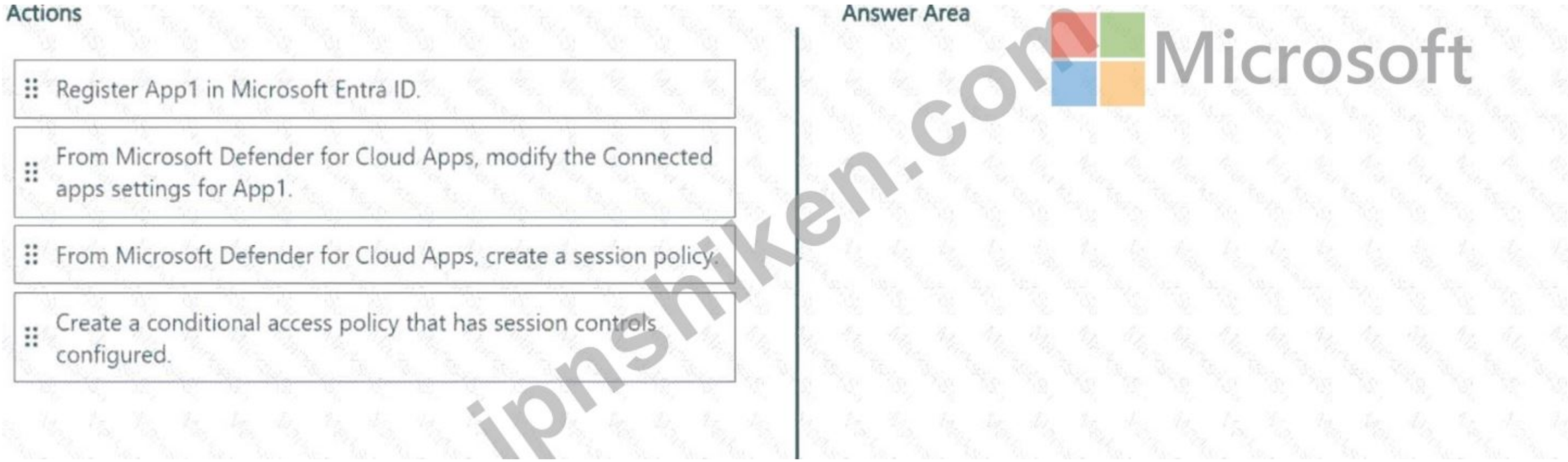
質問: **37**
Microsoft 365 テナントがあります。
すべてのユーザーは携帯電話とラップトップを持っています。
ユーザーは、Wi-Fi アクセスや携帯電話接続がない遠隔地から作業することがよくあります。
ユーザーは、遠隔地から作業する際、インターネットにアクセスできる有線ネットワークにラップトップを接続します。
多要素認証 (MFA) を実装する予定です。
ユーザーはリモート ロケーションからどの MFA 認証方法を使用できますか?
A. Microsoft Authenticator アプリからの通知
B. セキュリティに関する質問
C. 音声
D. アプリパスワード
正解: **(**正解を表示します**)**
The scenario states users may be at locations without Wi-Fi or mobile connectivity for their phones, but their laptops have wired Internet. Azure AD MFA methods that rely on the phone's connectivity-Authenticator push notifications or voice calls/SMS-won't work. While the most resilient MFA option in such situations is a time-based verification code from Microsoft Authenticator (works offline), that option isn't among the choices provided. The SC-300 coverage on MFA and legacy clients notes that app passwords can be used for applications that do not support modern authentication/MFA prompts, allowing users to sign in when MFA interaction is impractical. Given the listed options, the only workable method from the remote location is the app password; notification and voice require phone connectivity, and security questions are not an Azure AD MFA method.

質問: **38**
Sub1 という名前の Azure サブスクリプションがあります。
Microsoft Entra Permissions Management ライセンスを購入します。
You need to onboard Permissions Management.
実行すべき 2 つのアクションはどれですか? それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. Microsoft Entra アプリケーション プロキシを実装します。
B. Microsoft Entra Permissions Management からデータ収集を構成します。
C. Sub1 のロールの割り当てを作成します。
D. Microsoft Entra 管理センターから、診断設定を構成します。
E. Microsoft Entra 管理センターから、アプリ登録を作成します。
F. Azure ポータルから、データ収集ルール (DCR) を作成します。
正解: **(**正解を表示します**)**
According to the official Microsoft SC-300 Study Guide and Microsoft Entra Permissions Management documentation , onboarding Microsoft Entra Permissions Management (formerly CloudKnox) involves two key setup tasks:
* Configuring Data Collection - After purchasing the license, you must connect your Azure subscription (s) to Permissions Management so it can inventory identities, roles, and permissions. This is done from the Microsoft Entra Permissions Management portal, where you enable data collection for each connected cloud environment (Azure, AWS, GCP). This process deploys the required collector identity (service principal) and defines the scope for data gathering.

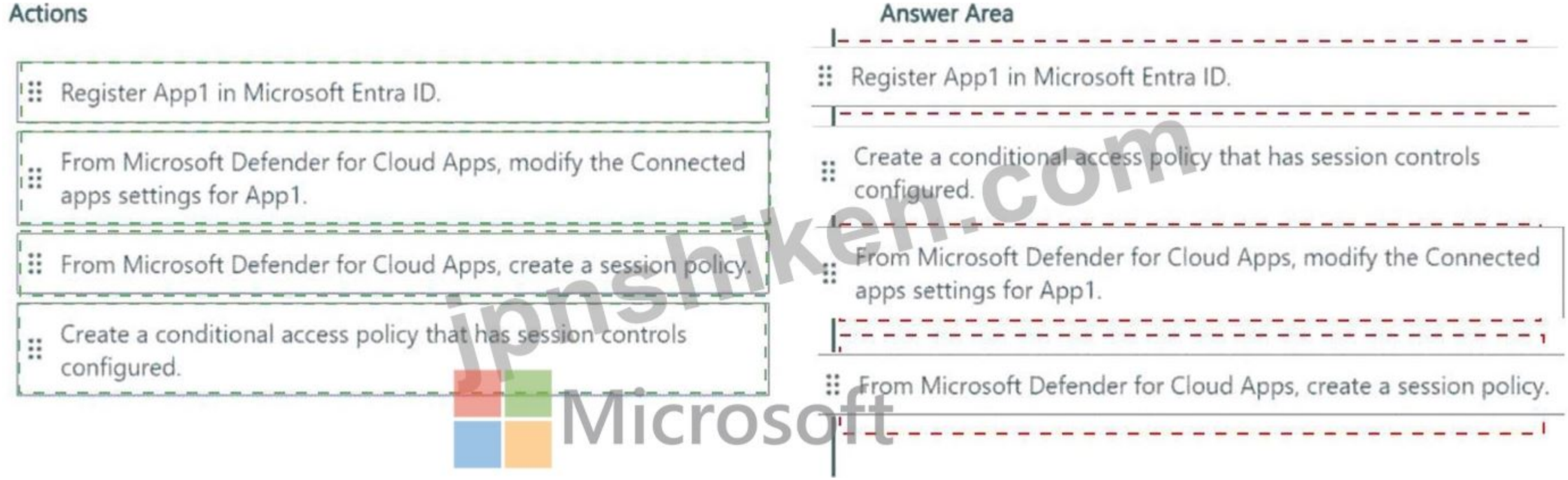
* Creating Role Assignments - Permissions Management requires proper authorization to read role assignments, permissions, and activity data. You must create a role assignment at the subscription level (Sub1) using a least-privilege role (for example, Reader or CloudKnox Service Principal Role) for the Permissions Management application service principal. This ensures it can scan Azure resources for permission analysis.
Microsoft documentation confirms:
"To onboard Azure subscriptions, assign the CloudKnox service principal a Reader role on each subscription, and configure data collection from within Microsoft Entra Permissions Management."

質問**: 39**
Site! という名前の Microsoft SharePoint Online サイトが含まれる Microsoft 365 E5 サブスクリプションがあります。Site!
PDFファイルをホストする
ユーザーが Sitel から直接ファイルを印刷できないようにする必要があります。
Microsoft Defender for Cloud Apps ポータルで作成する必要があるポリシーの種類は何ですか?
A. アクティビティポリシー
B. ファイルポリシー
C. アクセスポリシー
D. セッションポリシー
正解**: (**正解を表示します**)**
In Microsoft Defender for Cloud Apps (MCAS), a Session policy is used to monitor and control user activities in real time when accessing cloud resources through Conditional Access App Control.
The requirement states:
"Prevent users from printing PDF files directly from SharePoint Online." This requires controlling a user's session behavior (e.g., download, print, copy) within a web session - not just detecting or auditing it afterward. According to Microsoft's Identity and Access Administrator training materials:
"Session policies enable real-time monitoring and control of user sessions, allowing you to restrict activities such as printing, downloading, or copying content." By configuring a session policy, administrators can apply real-time controls to prevent printing within SharePoint or Teams sessions while allowing normal view access.
Other options:
* File policy controls data at rest (e.g., classifying or sharing files).
* Activity policy detects historical actions.
* Access policy controls conditions for app access, not user actions.

質問**: 40**
Microsoft 365 E5 テナントがあります。
App1 という名前のクラウド アプリを購入します。
Microsoft Defender for Cloud Apps を使用して、App1 のリアルタイム セッション レベルの監視を有効にする必要があります。
どの順序でアクションを実行すればよいですか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:

Register App1 in Microsoft Entra ID.

Create a conditional access policy that has session controls configured.

From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.

From Microsoft Defender for Cloud Apps, create a session policy.

ipnshiken.com

Let's break this down step by step based on Microsoft Defender for Cloud Apps (MDCA) and Microsoft Entra ID integration for enabling real-time session-level monitoring, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding the Goal: Real-Time Session-Level Monitoring with Microsoft Defender for Cloud Apps:

Microsoft Defender for Cloud Apps (MDCA) is a Cloud Access Security Broker (CASB) solution that provides visibility, control, and threat protection for cloud applications.

Real-time session-level monitoring allows MDCA to inspect and control user activities within a cloud app (App1 in this case) during active sessions. This requires integration with Microsoft Entra ID and the use of Conditional Access policies to route sessions through MDCA for monitoring.

The Microsoft 365 E5 tenant includes licenses for Microsoft Entra ID P2 and Microsoft Defender for Cloud Apps, which are necessary for this functionality.

Step-by-Step Analysis of the Actions:To enable real-time session-level monitoring, the actions must be performed in a logical order that aligns with Microsoft's recommended workflow for integrating a cloud app with MDCA.

Step 1: Register App1 in Microsoft Entra ID.

Before App1 can be monitored by MDCA, it must be registered as an application in Microsoft Entra ID. This step involves adding App1 to the tenant's enterprise applications, which allows Microsoft Entra ID to manage authentication and authorization for the app.

Registering the app in Microsoft Entra ID enables single sign-on (SSO) and allows the app to be governed by Conditional Access policies, which is a prerequisite for session-level monitoring.

This is the first step because none of the other actions can proceed without App1 being recognized by Microsoft Entra ID.

Step 2: Create a conditional access policy that has session controls configured.

Microsoft Defender for Cloud Apps integrates with Microsoft Entra ID Conditional Access to enforce session- level monitoring. A Conditional Access policy must be created to target App1 and include session controls that route user sessions through MDCA.

In the Conditional Access policy, under "Session" controls, you enable the option "Use Conditional Access App Control," which integrates with MDCA. This allows MDCA to monitor and control the session in real time.

This step must come after registering the app in Microsoft Entra ID because the Conditional Access policy needs to target an existing app. It must also precede the MDCA-specific steps because the session control integration sets up the connection between Microsoft Entra ID and MDCA.

Step 3: From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.

After the Conditional Access policy routes sessions to MDCA, you need to configure App1within MDCA by modifying its Connected apps settings. This step involves ensuring that App1 is properly connected to MDCA, which may include configuring API connectors or verifying that MDCA can monitor the app's activities.

This step is necessary to ensure MDCA has the necessary permissions and configurations to monitor App1. It comes after the Conditional Access policy because the policy enables the integration, and now MDCA needs to be set up to handle the app.

Step 4: From Microsoft Defender for Cloud Apps, create a session policy.

Finally, you create a session policy in MDCA to define the real-time monitoring and control rules for App1. A session policy in MDCA allows you to monitor user activities (e.g., file downloads, data sharing) and apply actions (e.g., block, notify) based on predefined conditions.

This step is the last because it relies on the previous steps: the app must be registered, the Conditional Access policy must route sessions to MDCA, and the Connected apps settings must be configured for MDCA to recognize App1. Only then can you define session policies to enforce real-time monitoring.

Why This Order?

The order ensures a logical flow:

Registering the app in Microsoft Entra ID establishes the app's identity in the tenant.

The Conditional Access policy enables the integration with MDCA by routing sessions through it.

Modifying the Connected apps settings in MDCA ensures the app is properly set up for monitoring.

Creating a session policy in MDCA defines the specific monitoring and control rules for real-time session- level monitoring.

Deviating from this order would result in errors. For example, creating a session policy in MDCA before registering the app in Microsoft Entra ID would fail because MDCA wouldn't recognize the app.

Additional Considerations:

The Microsoft 365 E5 license includes Microsoft Entra ID P2 and Microsoft Defender for Cloud Apps, so no additional licensing is required for this scenario.

If App1 is not a supported app for MDCA's app connectors, additional steps (e.g., using a custom app connector) might be needed, but the question implies App1 can be monitored with the standard process.
Session policies in MDCA can include actions like blocking downloads or requiring step-up authentication, which are applied in real time during the user's session.
Conclusion:The correct order to enable real-time session-level monitoring of App1 using Microsoft Defender for Cloud Apps is:
Register App1 in Microsoft Entra ID.
Create a conditional access policy that has session controls configured.
From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.
From Microsoft Defender for Cloud Apps, create a session policy.
References:
Microsoft Defender for Cloud Apps documentation: "Session control with Microsoft Defender for Cloud Apps" (Microsoft Learn:https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy)
Microsoft Entra ID Conditional Access documentation: "Session controls in Conditional Access" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-session) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers integrating Microsoft Defender for Cloud Apps with Microsoft Entra ID for session-level monitoring.

質問**: 41**
Microsoft 365 E5 サブスクリプションをお持ちです。
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 User1 というユーザーが含まれています。
Microsoft Entra Permissions Management を展開する予定です。
User1 が Azure サブスクリプションを Permissions Management にオンボードできることを確認する必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 に割り当てるべき Microsoft Entra ロールはどれですか?
A. セキュリティ管理者
B. アプリケーション管理者
C. 権限管理管理者
D. グローバル管理者
正解**: (**正解を表示します**)**
In Microsoft Entra Permissions Management (formerly CloudKnox), the Permissions Management Administrator role provides the least-privilege rights necessary to onboard cloud environments such as Azure subscriptions, AWS accounts, or GCP projects. This role allows users to configure data collection and onboard environme nts without granting global administrative access.
The Global Administrator role could also perform onboarding but exceeds the least-privilege requirement.
Microsoft's official documentation (SC-300 "Manage Microsoft Entra Permissions Management" module) c learly states:
"The Permissions Management Administrator can onboard and configure environments for Permissions Management and manage discovery and insights across multi-cloud platforms."

質問**: 42**
次の表に示すカスタム ロールを含む Azure サブスクリプションがあります。

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

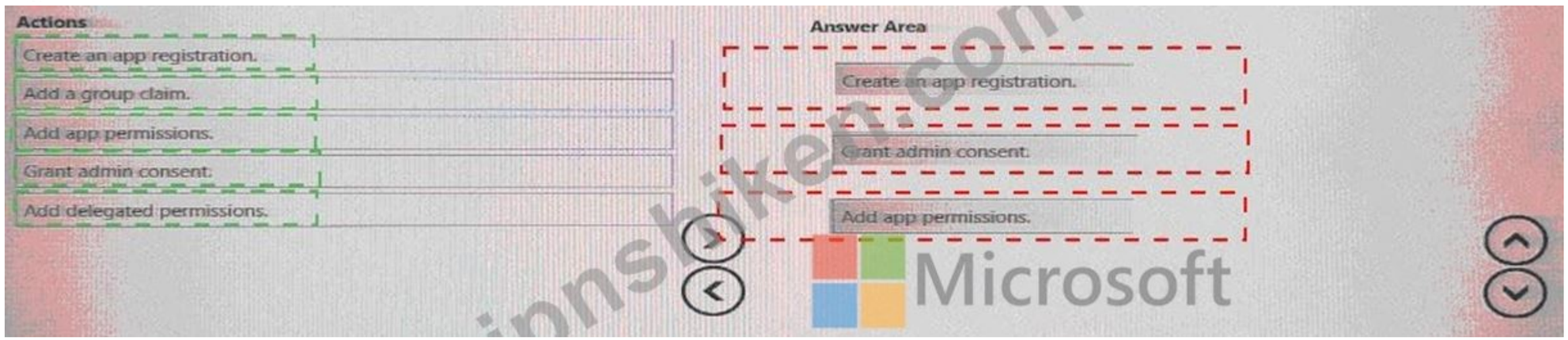
Azure portal を使用して、Role3 という名前のカスタム Azure サブスクリプション ロールを作成する必要があります。Role3 は、既存の役割のベースライン権限を使用します。Role3 を作成するためにどのロールを複製できますか?
A. Role2 のみ
B. 組み込みの Azure サブスクリプション ロールのみ
C. 組み込みの Azure サブスクリプション ロールと Role2 のみ
D. 組み込みの Azure サブスクリプション ロールと組み込みの Azure AD ロールのみ

E. Role1、Role2 組み込み Azure サブスクリプション ロール、および組み込み Azure AD ロール
正解**: C (**コメントを発表する**)**
In Azure RBAC, when creating a custom role through the Azure portal, you can only clone from existing roles of the same scope type. Since Role3 is an Azure subscription-level custom role, it can be cloned only from subscription-level roles-either built-in subscription roles (like Owner, Contributor, Reader) or other custom subscription roles.
Azure AD roles (directory roles) cannot be cloned to create subscription roles because they operate at a completely different control plane (Azure AD vs Azure Resource Manager).
Thus, from the given table:
* Role1 = Azure AD role # cannot be cloned.
* Role2 = Azure subscription role # can be cloned.
Therefore, the correct option is C

質問**: 43**
会社には contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
同社はApp1というWebサービスを開発しています。
App1 が Microsoft Graph を使用して contoso.com 内のディレクトリ データを読み取ることができることを確認する必要があります。
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解**:**



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn module "Implement and manage enterprise applications," when developing an application that needs to access Microsoft Graph or other protected APIs on behalf of an organization, you must perform several configuration steps within Azure Active Directory (Azure AD).

Step 1 - Create an app registration:

Every application that requires access to Microsoft Graph must be registered in Azure AD. The registration process establishes an identity for the app and generates an Application (client) ID and a directory (tenant) ID.

This is done in Azure portal # Azure Active Directory # App registrations # New registration . This enables Azure AD to issue tokens to the app.

Step 2 - Add app permissions:

After registration, you must configure permissions under API permissions in the app's registration settings.

For server-to-server access (no user sign-in), Application permissions are used; for delegated access (on behalf of a user), Delegated permissions are added. In this case, since App1 will read directory data from Microsoft Graph, you assign the Microsoft Graph # Directory.Read.All permission.

Step 3 - Grant admin consent:

Application permissions require admin consent before the app can access directory data. An Azure AD administrator must grant these permissions by selecting "Grant admin consent for contoso.com."

This allows the app to use the permissions organization-wide.

From Microsoft's documentation:

"To enable an application to call Microsoft Graph, register the app, configure required API permissions, and grant admin consent for those permissions."

Correct Answer Order:

* Create an app registration
* Add app permissions
* Grant admin consent

質問**: 44**

RemoteNetworkl 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を含む Microsoft Entra テナントがあります。

Name	Member of
User1	Group1
User2	Group1
User3	Group2

次の表に示すデバイスがあります。



正解:



Explanation:



質問: **45**

Azure サブスクリプションをお持ちです。

Azure AD ログは Log Analytics ワークスペースに送信されます。

ログをクエリし、ユーザーごとのサインイン数をグラフで表示する必要があります。

クエリをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。

```
SigninLogs
| where ResultType == 0
|  login_count = count() by Identity
```

- extend
- print
- project
- render
- summarize

```
|  columnchart
```

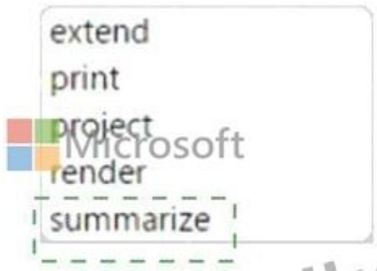
- extend
- print
- project
- render
- summarize

ipnshiken.com

Microsoft

正解:

```
SigninLogs
| where ResultType == 0
|  login_count = count() by Identity
```



Microsoft
jpnshiken.com

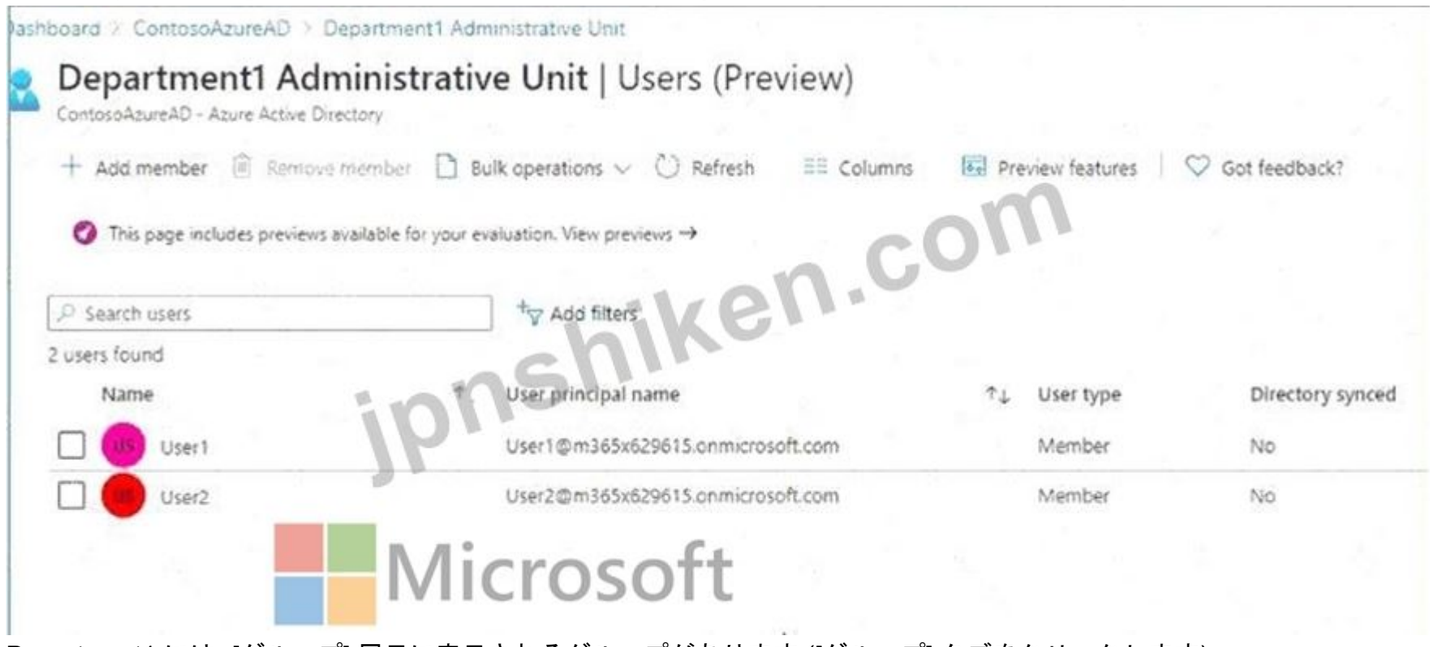
```
|  columnchart
```



Explanation:
Box 1 =
SigninLogs
| where ResultType == 0
| summarize login_count = count() by identity
| render piechart
This query retrieves the sign-in logs, filters the successful sign-ins,summarizesthe count of sign-ins per user, and renders the result as a pie chart.
Box 2 = Render
In Microsoft Entra ID (Azure AD), the SigninLogs table in Azure Monitor Logs (Log Analytics workspace) contains data about user sign-ins. When you want to query and graphically display the number of sign-ins per user, you use Kusto Query Language (KQL) - the same language that powers Log Analytics, Azure Monitor, and Microsoft Sentinel.
The correct syntax must first aggregate the data and then visualize it:
* where ResultType == 0 filters for successful sign-ins (since 0 indicates success).
* summarize login_count = count() by Identity aggregates (counts) all sign-in events per user (Identity field). The summarize operator in KQL is specifically used to group and aggregate data.
* render columnchart graphically displays the summarized results as a column chart. The render operator is used to visualize query output in supported formats such as timechart , piechart , or columnchart .
Therefore, the correct operators to fill in are:
* First blank: summarize
* Second blank: render

According to the Microsoft SC-300 Study Guide and Microsoft Learn module "Query and visualize sign-in logs with Kusto Query Language" , the recommended method to display sign-in frequency per user is:
"Use the summarize operator to aggregate sign-in counts by user, followed by render to visualize results."
Final Query Answer:
SigninLogs
| where ResultType == 0
| summarize login_count = count() by Identity
| render columnchart

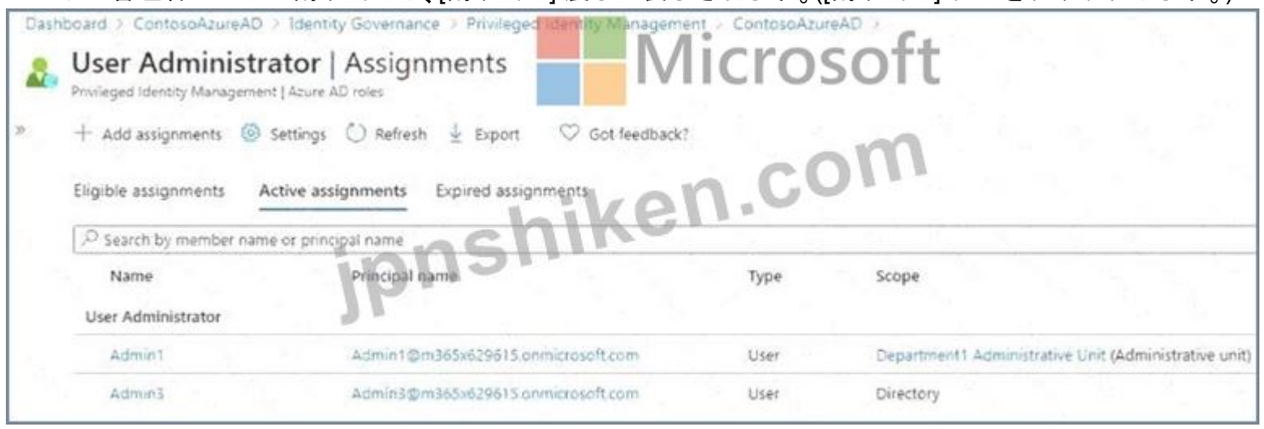
質問**: 46**
Group3 というグループと Department1 という管理単位を含む Microsoft Entra テナントがあります。
部門には、「ユーザー」展示に示されているユーザーがいます。(「ユーザー」タブをクリックします。)



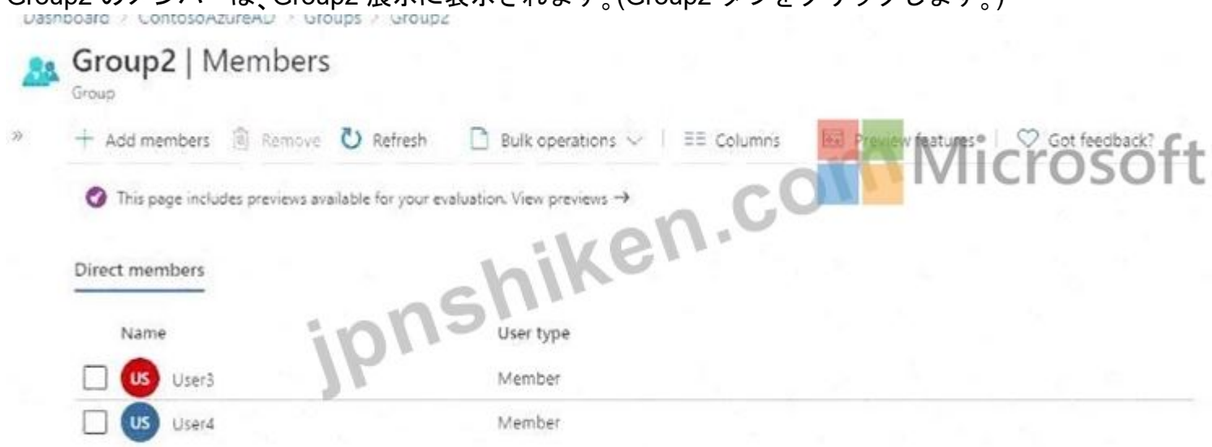
Department1 には、[グループ] 展示に表示されるグループがあります ([グループ] タブをクリックします)。



ユーザー管理者ロールの割り当ては、[割り当て] 展示に表示されます。([割り当て] タブをクリックします。)

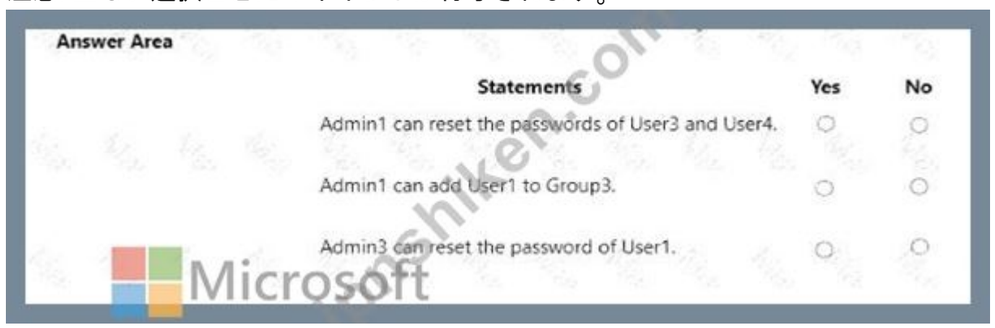


Group2 のメンバーは、Group2 展示に表示されます。(Group2 タブをクリックします。)



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

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft SC-300 Identity and Access Administrator Official Study Guide and Microsoft Learn - Manage administrative units in Azure AD module, Administrative Units (AUs) in Microsoft Entra ID (Azure AD) are logical containers used to delegate administration to specific subsets of users and groups.

The User Administrator role can perform specific actions within the scope to which it is assigned. In this scenario:

* Admin1 is assigned the User Administrator role scoped to the Department1 Administrative Unit, meaning Admin1 can only manage users and groups within that administrative unit.
* User3 and User4 belong to Group2, but Group2 members are not part of Department1's listed users (only User1 and User2 are). Therefore, Admin1 cannot reset the passwords of User3 or User4.
* Additionally, Admin1 cannot add User1 to Group3 because Group3 is not included in Department1's administrative scope. The administrator can only modify group memberships for groups within their AU.
* Admin3 is assigned the User Administrator role at the directory (tenant-wide) scope, granting full privileges over all users and groups in the tenant. Therefore, Admin3 can reset User1's password since the scope includes all users in the directory.

Microsoft documentation explicitly states:

"An administrative unit-scoped role grants the ability to manage only those users and groups within the administrative unit. Directory-scoped roles grant management across the entire tenant."

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**

storage1 という名前のストレージ アカウントと WebApp1 という名前の Web アプリを含む Azure サブスクリプションがあります。WebApp1 はシステム割り当てマネージド ID を使用します。

システム割り当てマネージド ID を使用して、WebApp1 が storage1 に対してファイルの読み取りと書き込みを実行できることを確認する必要があります。

Azure ポータルで storage1 に何を構成する必要がありますか?

A. ファイル共有設定
B. アクセス制御（午前時）設定
C. 共有アクセス署名 (SAS)
D. データ保護
E. アクセスキー

正解: (正解を表示します)
Per Microsoft SC-300 official study guide and Microsoft Learn module "Manage identities using managed identities" , when a web app uses a system-assigned managed identity , Azure automatically creates a service principal representing that identity within Microsoft Entra ID.
To grant the managed identity permission to read and write files in an Azure Storage account, you must configure role-based access control (RBAC) permissions via the Access control (IAM) blade in the Azure portal. Specifically, you would assign roles such as Storage Blob Data Contributor or Storage Blob Data Reader to the managed identity at the appropriate resource scope (e.g., storage account or container).
Other options like SAS tokens , access keys , or File share settings rely on key-based or manual authentication methods, which contradict the principle of least privilege and managed identity automation.
Access control (IAM) ensures secure, identity-based access through Azure AD.
Correct Answer: B. the Access control (IAM) settings

質問: **48**
次の表に示すユーザーを含むAzureActive Directory（Azure AD）テナントがあります。

Name	Type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1はGroup1の所有者です。
次の設定を持つアクセスレビューを作成します。
レビューするユーザー :グループのメンバー
範囲：全員
グループ :グループ1
レビュアー :メンバー（自己）
User3のアクセスレビューを実行できるユーザーはどれですか？
A. User1、User2、およびUser3
B. User3のみ
C. User1のみ
D. User1とUser2のみ
正解: (正解を表示します)
Based on the Microsoft SC-300: Identity and Access Administrator Official Study Guide and Microsoft Learn module "Manage access reviews in Azure AD" , when creating an access review with the setting Reviewers: Members (self) , each user who is a member of the target group is only allowed to review their own access , not the access of others.
Here's how the logic applies in this scenario:
* The scope of the access review is set to Everyone , meaning both internal members and external (guest) users within Group1 will be included in the review.
* The reviewers option is configured as Members (self) - this setting instructs Azure AD to send review tasks to each user so they can attest to their own need for continued group membership.
* Therefore, User3 (a Guest user) will receive the review task to confirm or deny their own access to Group1.
* User1 and User2 , though they are members and User1 is the group owner, will not review User3's access because "Members (self)" does not delegate review authority to other members or owners - it only applies to individual self-assessment.
Microsoft documentation explicitly clarifies:
"When you select Members (self) as the reviewer type, each user reviews only their own access. Owners or administrators do not approve or deny access on their behalf." Hence, in this scenario, only User3 can perform the access review for their own membership in Group1.

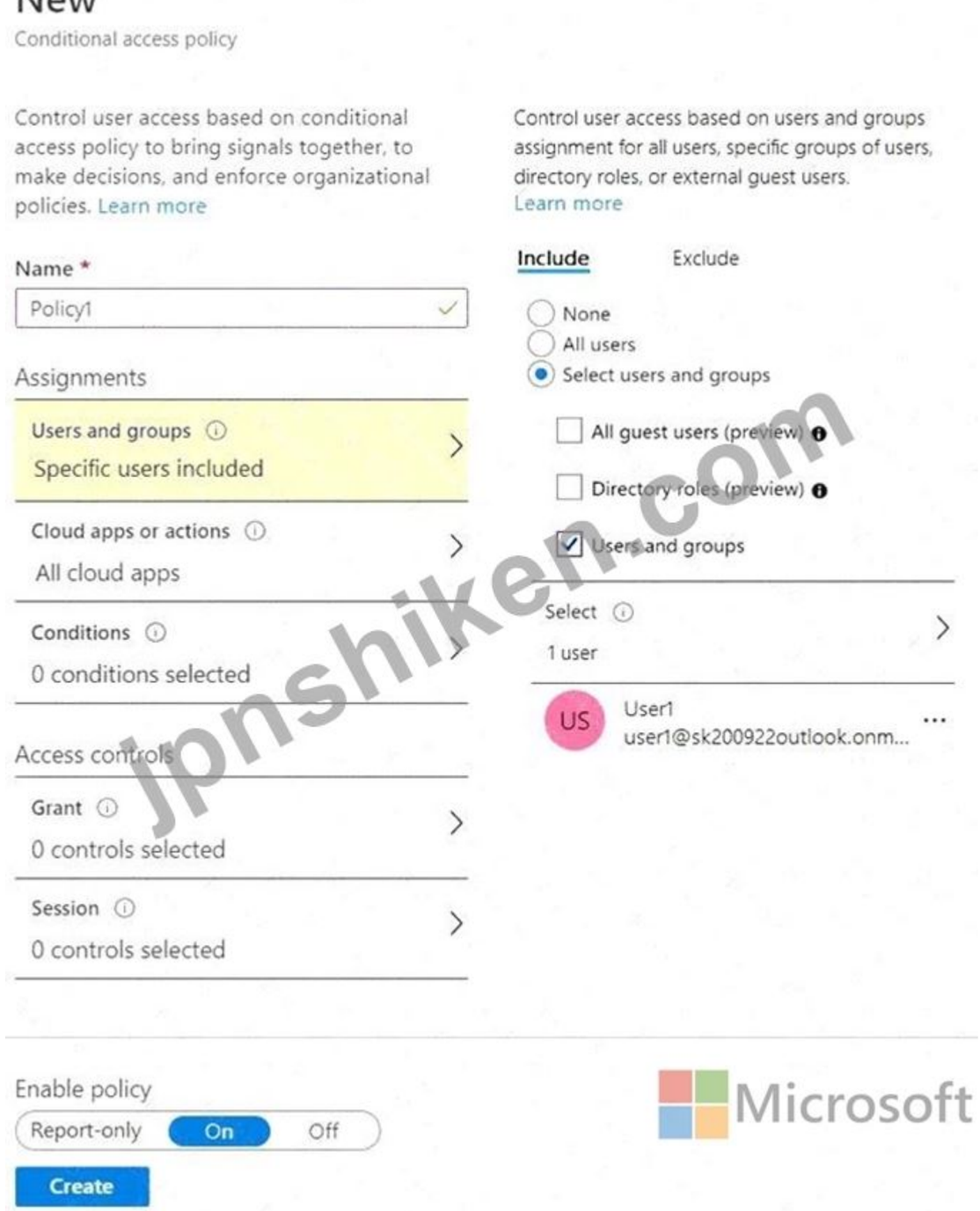
質問: **49**

Log Analytics ワークスペースを作成します。
監査の技術要件を実装する必要があります。
Azure AD では何を構成する必要がありますか?
A. 企業ブランディング
B. 診断設定
C. 外部ID
D. アプリ登録
正解: **(**正解を表示します**)**
To meet auditing and monitoring requirements, Azure AD must send sign-in logs and audit logs to an external location such as a Log Analytics workspace, Azure Storage account, or Event Hub. This is configured using Diagnostics settings in Azure AD.
According to Microsoft documentation in "Monitor Azure Active Directory activity logs in Azure Monitor" and the SC-300 learning objective "Implement and monitor identity governance" , you must enable diagnostic settings to stream directory logs to a Log Analytics workspace.
The scenario specifies:
"You create a Log Analytics workspace. You need to implement the technical requirements for auditing." By configuring Azure AD's Diagnostics settings, you can:
* Send Sign-in logs, Audit logs, and Provisioning logs to Log Analytics.
* Correlate identity events with security insights in Azure Sentinel or Microsoft Defender for Cloud Apps.
Microsoft documentation confirms:
"To collect and analyze Azure AD sign-in and audit data, configure diagnostic settings to send logs to Log Analytics." Other options do not meet the requirement:
* A. Company branding: Only affects login pages, not logging or auditing.
* C. External Identities: Controls guest access, not logging.
* D. App registrations: Used for app integration, not auditing.

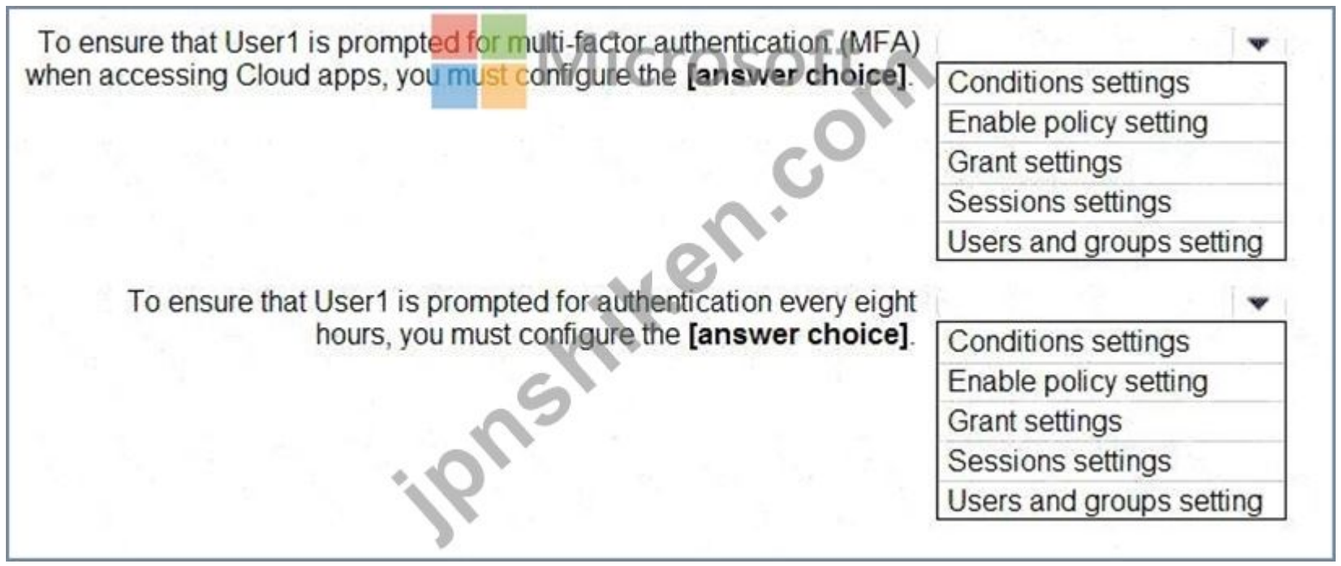
質問: **50**
Azure Active Directory (Azure AD) テナントがあります。
テナントの場合、ユーザーはアプリケーションを登録できますが、[いいえ] に設定されています。
Admin1 という名前のユーザーは、App1 という名前の新しいクラウド アプリをデプロイする必要があります。
Admin1 が App1 を Azure AD に登録できることを確認する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
Admin1 に割り当てるべきロールはどれですか?
A. Azure AD のアプリケーション開発者
B. サブスクリプション1のアプリ構成データ所有者
C. サブスクリプション1の管理対象アプリケーション共同作成者
D. Azure AD のクラウド アプリケーション管理者
正解: **A (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Manage application registrations in Azure AD," the ability to register applications in Azure Active Directory is controlled by the tenant-level setting "Users can register applications" found under User settings
App registrations .
When this setting is set to No, only specific roles with app registration permissions can create or manage app registrations. To follow the principle of least privilege, the appropriate role should grant only the ability to register applications - not broader administrative capabilities.

The roles with permissions related to application registration include:
Application Developer - allows users to register and manage applications they own. This role is specifically designed for users who need to create app registrations when the tenant setting is disabled.
Cloud Application Administrator and Application Administrator - provide broader privileges, including managing all applications, credentials, and permissions, which exceed the minimum needed for this scenario.
Managed Application Contributor and App Configuration Data Owner - are Azure resource-level roles and have no relevance to Azure AD application registration.
From Microsoft documentation:
"If 'Users can register applications' is set to No, assign the Application Developer role to users who need to register apps." Therefore, to allow Admin1 to register App1 while adhering to the principle of least privilege, assign the Application Developer role.

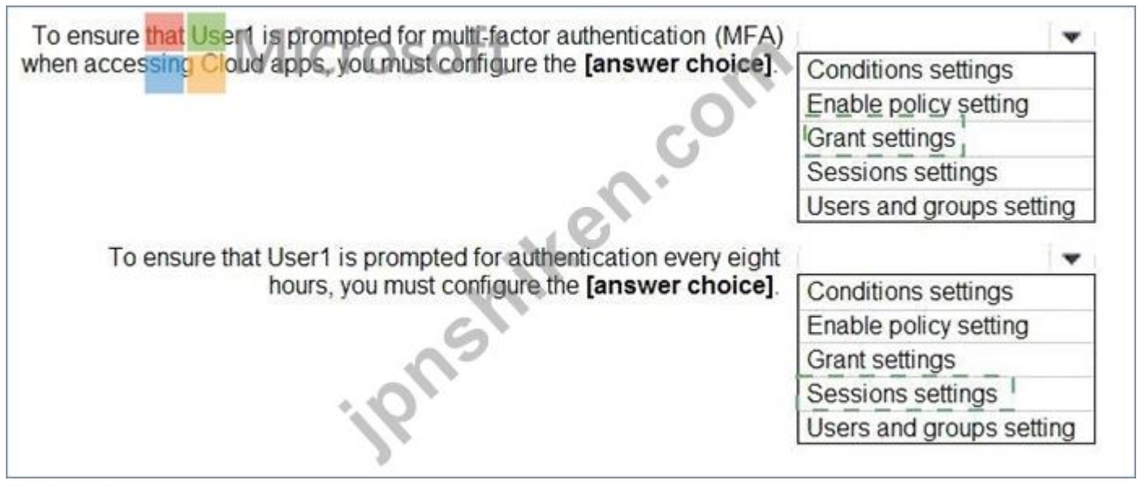
質問**: 51**
セキュリティの既定値が無効になっている Azure Active Directory (Azure AD) テナントがあります。
次の図に示すように、条件付きアクセス ポリシーを作成します。



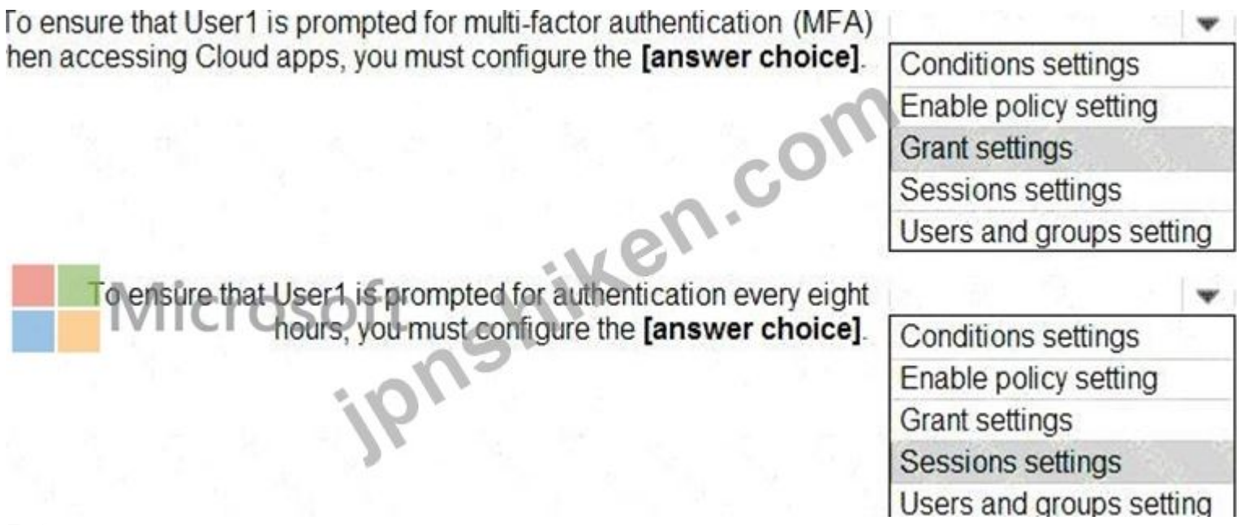
ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:



Reference:
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn module "Implement Conditional Access policies", a Conditional Access policy in Azure AD determines how access decisions are enforced based on user, application, and session signals.
When the goal is to prompt for MFA, this control is found in the Grant settings section of the policy configuration. The Grant control allows administrators to require specific conditions such as multi-factor authentication, device compliance, hybrid Azure AD join, or app protection. The official Microsoft documentation specifies:
"To require users to perform multi-factor authentication, navigate to the 'Grant' section of your Conditional Access policy and select 'Grant access' # 'Require multi-factor authentication'." Therefore, the first answer (for requiring MFA) corresponds to Grant settings.
On the other hand, if you want to ensure that a user is reauthenticated periodically - for example, every eight hours - this is configured under the Session settings section. Session controls define user experience within the session after access is granted. Microsoft documentation states:
"Session controls enable limiting user sessions, such as enforcing reauthentication frequency, requiring sign- in every X hours, or restricting persistent browser sessions." Hence, to prompt User1 to authenticate every eight hours, the appropriate configuration is within Session settings.

質問: **52**
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の場合、以下の要件を満たす必要があります。
* ユーザーが Microsoft 365 資格情報を使用して Azure 仮想マシンにサインインできることを確認します。
* 新しい仮想マシンを作成する権限を委任します。
各要件にはどのような機能を利用すべきでしょうか？ 適切な機能を正しい要件にドラッグして答えてください。各機能は1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。



正解:



Explanation:



Microsoft
ipnshiken.com

Comprehensive and Detailed Explanation with all Microsoft SC-300: Identity and Access Administrator documents: = Based on the Microsoft SC-300: Microsoft Identity and Access Administrator official study guide, Exam Ref SC-300 , and Microsoft Learn Identity & Access Management modules, Azure provides several mechanisms to manage identity integration and role delegation between Microsoft 365 and Azure resources.

* Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials: This requirement refers to enabling Azure AD-based authentication for virtual machines. This capability is provided by Azure AD Managed Identities and Azure AD join support for Azure VMs. Managed identities allow Azure resources, such as virtual machines, to authenticate to Azure AD-secured services using Microsoft Entra (Azure AD) credentials, eliminating the need to manage credentials manually. As stated in the Microsoft Identity study guide:

"Azure AD-managed identities provide an automatically managed identity in Azure AD for applications or services to use when connecting to resources secured by Azure AD. This includes support for user sign-in to Azure VMs using Microsoft 365 or Azure AD credentials."

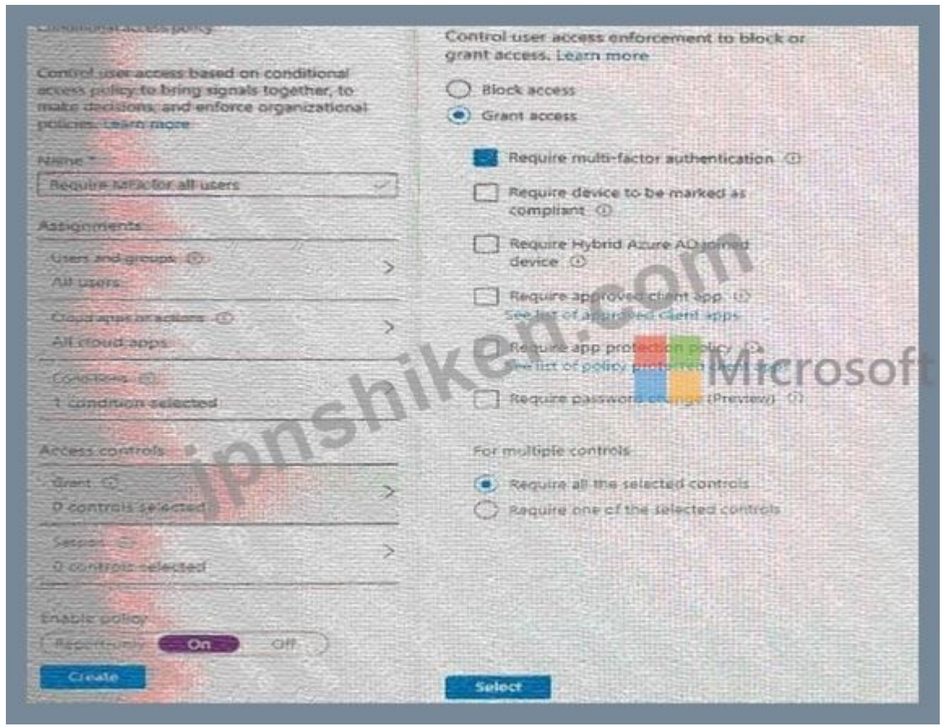
* Delegate the ability to create new virtual machines: To delegate resource creation and management in Azure, Azure role-based access control (Azure RBAC) is used. Azure RBAC enables granular access management for Azure resources by assigning roles such as Virtual Machine Contributor , Owner , or Contributor at different scopes (subscription, resource group, or resource). Microsoft documentation clarifies:

"Azure RBAC allows you to assign roles to users, groups, or service principals, granting permissions to create, modify, or delete Azure resources, including virtual machines."

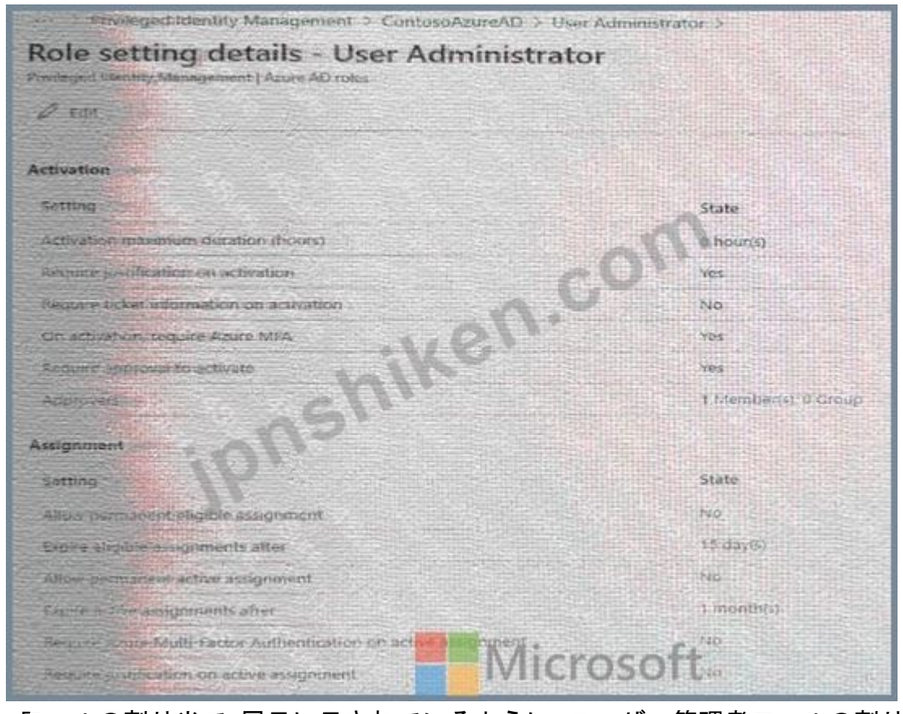
質問**: 53**

Microsoft 365 テナントがあります。

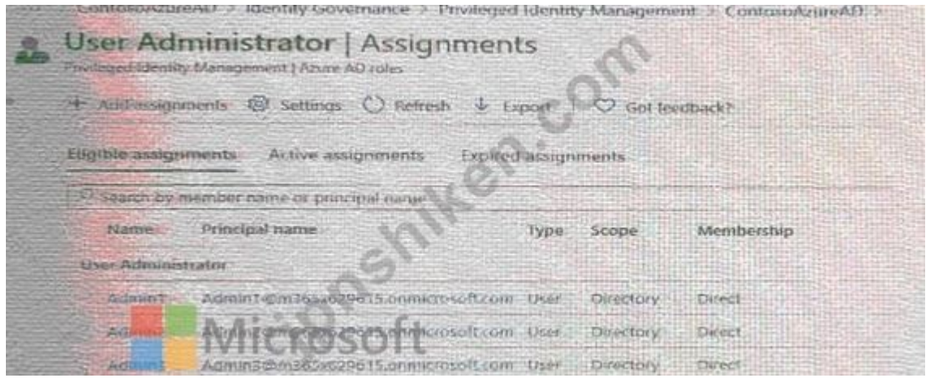
条件付きアクセス ポリシーの図に示されているように、条件付きアクセス ポリシーを構成します ([条件付きアクセス ポリシー] タブをクリックします)。



ユーザー管理者ロールの設定は、"ロール設定の詳細"の図のように表示されます。("ロール設定の詳細"タブをクリックします。)

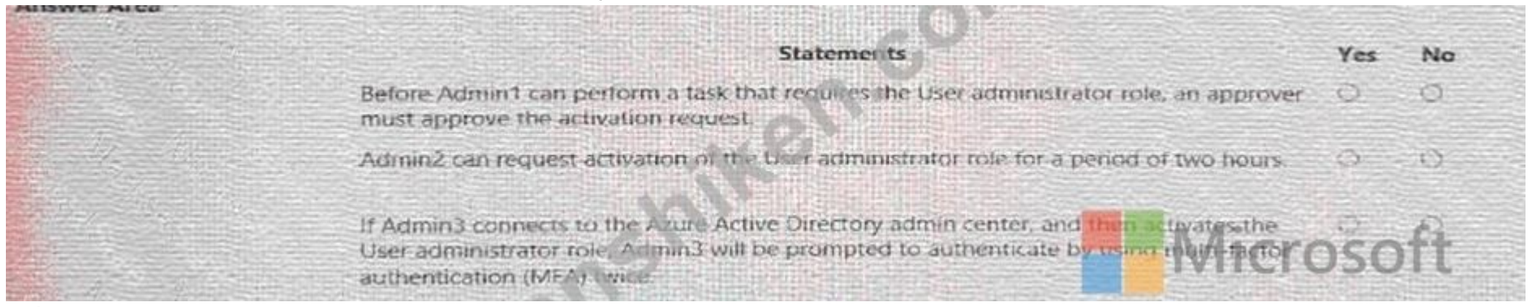


"ロールの割り当て"展示に示されているように、ユーザー管理者ロールの割り当てを表示します。("ロールの割り当て"ラボをクリックします。)

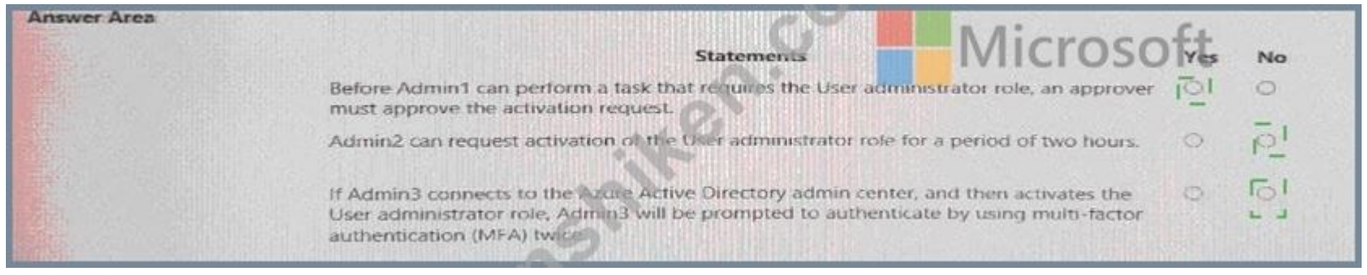


以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:

Statement

Answer

1. Before Admin1 can perform a task that requires the User Administrator role, an approver must approve the activation request.

Yes

2. Admin2 can request activation of the User Administrator role for a period of two hours.

No

3. If Admin3 connects to the Azure Active Directory admin center, and then activates the User Administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.

Based on Microsoft's SC-300 Identity and Access Administrator Study Guide , Microsoft Learn module

"Manage Azure AD roles by using Privileged Identity Management (PIM)" , and Exam Ref SC-300 , the following logic applies:

* Approval requirement (Admin1) - In the Role setting details image, Require approval to activate is set to Yes, and one approver is listed. This means before any user (e.g., Admin1) can activate the User Administrator role, approval must be granted. Therefore, Admin1 must have the activation request approved before performing any User Administrator tasks. # (Yes)

* Activation duration (Admin2) - The configuration shows Activation maximum duration (hours): 8 hours . This defines the maximum allowed time a user can remain active after role activation. Admin2 can activate for up to 8 hours, not 2 hours unless specifically limited during activation. Hence, the statement claiming Admin2 can activate for "two hours" is incorrect. # (No)

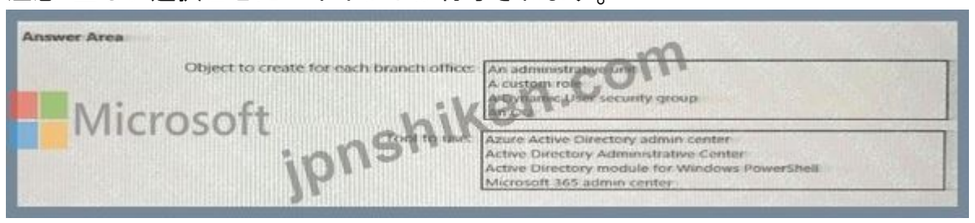
* MFA enforcement (Admin3) - Two relevant controls exist:
* Conditional Access policy requiring MFA for all users.
* PIM role setting On activation, require Azure MFA = Yes.
According to Microsoft documentation, when both Conditional Access and PIM MFA enforcement apply, Azure AD intelligently avoids redundant prompts by honoring a single valid MFA session token.
This means Admin3 would only be prompted once for MFA, even though both mechanisms require it. # (No) Therefore, as verified by official Microsoft materials and SC-300 documentation:

質問: **54**
Microsoft Office 365 EnterpriseE3ライセンスが割り当てられている2,500人のユーザーがいます。ライセンスは個々のユーザーに割り当てられます。
Azure Active Directory管理センターの[グループ]ブレードから、Microsoft 365 EnterpriseE5ライセンスをユーザーに割り当てます。
最小限の管理作業で、Office 365 EnterpriseE3ライセンスをユーザーから削除する必要があります。
何を使うべきですか？
A. Azure ActiveDirectory管理センターのIdentityGovernanceブレード
B. Set-AzureAdUserコマンドレット
C. Azure ActiveDirectory管理センターのライセンスブレード
D. Set-WindowsProductKeyコマンドレット
正解: **(**正解を表示します**)**
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn module "Manage licenses in Azure Active Directory", the most efficient way to manage or remove product licenses from a large group of users is by using group-based licensing through the Licenses blade in the Azure Active Directory admin center.
In this scenario:
* 2,500 users were individually assigned Office 365 E3 licenses.
* The same users are now assigned Microsoft 365 E5 licenses via group assignment (using group-based licensing).
When a user is assigned a license directly and later receives another license through a group, Azure AD continues to track both - the direct and inherited assignments. To remove the E3 licenses efficiently, you can use the Licenses blade to remove all direct assignments in bulk rather than editing each user individually.
* In the Azure AD admin center, navigate to: Azure Active Directory # Licenses # All products # Office 365 E3.
* Select Licensed users.
* Select all users (or filter based on the direct assignment type).
* Click Remove license assignment to remove the E3 licenses.
Step-by-Step (as per Microsoft documentation): This method removes the E3 licenses for all directly assigned users in a single operation-achieving the goal with the least administrative effort.
* A. Identity Governance blade: Used for access reviews, entitlement management, and lifecycle workflows-not license management.
* B. Set-AzureADUser cmdlet: Manages user properties but does not directly manage license assignments (you would need Set-AzureADUserLicense or Set-MgUserLicense , which is more manual).
* D. Set-WindowsProductKey cmdlet: Used for activating Windows OS, not Microsoft 365 licensing.
Why the other options are incorrect:

質問: **55**
contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
Azure AD 外部 ID の価格が月間アクティブ ユーザー数 (MAU) に基づいていることを確認する必要があります。
何を設定すればよいでしょうか?
A. アクセスレビュー
B. 使用条件

C. リンクされたサブスクリプション
D. ユーザーフロー
正解: **(**正解を表示します**)**
Azure AD External Identities (B2B) uses Monthly Active Users (MAU) billing. The SC-300 content explains that to enable MAU-based pricing, the Azure AD tenant must be linked to an Azure subscription so that usage can be metered and billed. The configuration is performed in Azure AD # External Identities # All settings # Linked subscription, where administrators associate the tenant with a subscription and resource group. Only after this association do External Identities sign-ins count against MAU rather than per- user licenses. Access reviews (A) and terms of use (B) are governance features that do not affect billing. User flows (D) are specific to Azure AD B2C and are unrelated to enabling MAU billing for B2B External Identities. The study guide highlights: "To use MAU billing for External Identities, link your Azure AD tenant to an Azure subscription so guest usage is charged per monthly active user." Therefore, the correct prerequisite to ensure MAU billing is configuring a linked subscription.

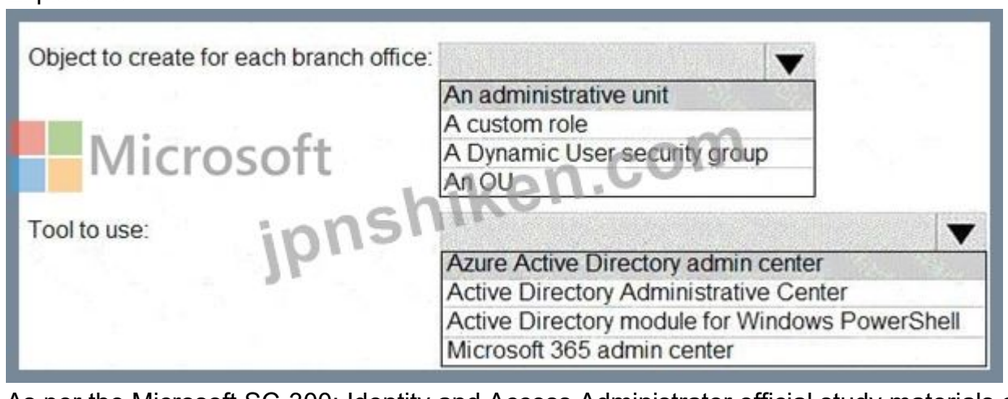
質問: **56**
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



As per the Microsoft SC-300: Identity and Access Administrator official study materials and Microsoft Learn documentation on "Manage administrative units in Azure Active Directory" , Administrative Units (AUs) are designed to delegate administrative permissions within large organizations based on divisions such as geography or department. They provide scoped administrative control -allowing helpdesk or user administrators to manage users only within a specific subset of the directory, such as a branch office or department.
In this scenario, Contoso's technical requirement states:

"The helpdesk administrators must be able to manage licenses for only the users in their respective office." To fulfill this, you must create an administrative unit for each branch office (e.g., Montreal, London, Seattle) and assign helpdesk administrators scoped to those AUs. This ensures that each helpdesk admin can only manage licenses for the users within their respective office, enforcing the principle of least privilege.
The Azure Active Directory admin center is the correct tool for creating and managing administrative units.
SC-300 guidance clarifies that administrative units are Azure AD objects , not on-premises Active Directory objects like Organizational Units (OUs). Therefore, they are created and managed exclusively through the Azure portal , Microsoft Graph , or PowerShell for Azure AD , but the most straightforward interface for exam purposes is the Azure AD admin center .

質問: **57**
あなたの会社にはMicrosoft365テナントがあります。
同社には300人のユーザーがいるコールセンターがあります。コールセンターでは、ユーザーはデスクトップコンピューターを共有し、毎日別のコンピューターを使用する場合があります。コールセンターのコンピューターは、生体認証用に構成されていません。
コールセンターに携帯電話を持ち込むことは禁止されています。
コールセンターユーザーがMicrosoft365サービスにアクセスするときは、多要素認証（MFA）を要求する必要があります。
ソリューションに何を含める必要がありますか？
A. 名前付きネットワークの場所
B. MicrosoftAuthenticatorアプリ
C. Windows Hello forBusiness認証
D. FIDO2トークン
正解: **(**正解を表示します**)**
SC-300 materials describe FIDO2 security keys as a passwordless method that works well for shared workstations and environments where phones are not permitted. The documentation explains that "FIDO2 security keys are phishing-resistant, standards-based credentials that allow users to sign in with a portable hardware device" and that "the user performs a gesture on the key (PIN or biometrics) to complete authentication." It further clarifies that "Azure AD passwordless methods (FIDO2 security keys, Windows Hello for Business, Authenticator) satisfy strong authentication requirements and can meet MFA prompts." Because the call-center computers don't have biometrics and phones are prohibited, Authenticator and Windows Hello for Business are unsuitable. A named network location does not provide MFA by itself. By issuing FIDO2 keys (tokens) to agents, you meet the MFA requirement with a factor the user has (the key) plus a secure local gesture (PIN), which SC-300 documents as accepted for Azure AD strong/MFA.

質問: **58**
Automation1 という名前の Azure Automation アカウントと、Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。Vault1 には Secret 1 という名前のシークレットが含まれています。
Automation1 に対してシステム割り当てマネージド ID を有効にします。
Automation! が Secret1 の内容を読み取れるようにする必要があります。ソリューションは以下の要件を満たす必要があります。
* Automation1 が Vault1 に保存されている他のシークレットにアクセスできないようにします。
* 最小権限の原則に従ってください。
何をすべきでしょうか?
A. Vault1 から、アクセス制御 (1AM) 設定を構成します。
B. Automation1 から、ID 設定を構成します。
C. Secret1からアクセス制御（1AM）設定を構成します
D. Automation1 から、実行アカウント設定を構成します。
正解: **(**正解を表示します**)**

As per the Microsoft SC-300 Study Guide and Azure Key Vault documentation, when you enable a system- assigned managed identity for a resource (in this case, Automation1), that identity can be granted permissions to specific Key Vault resources using Azure role-based access control (RBAC).
Since the requirement states that Automation1 must be able to read only one secret (Secret1) and not other secrets in the vault, you must assign permissions at the Secret level - not at the vault level.
Assigning permissions at the Vault1 level (option A) would potentially allow access to all secrets, violating the principle of least privilege.
Therefore, you must go to Secret1 # Access control (IAM) and assign the Key Vault Secrets User role (or similar least-privileged role) to the system-assigned identity of Automation1.
This aligns with Microsoft's documentation:
"To restrict access to individual secrets or keys, use Azure role assignments at the specific secret, key, or certificate level rather than the vault level."

質問**: 59**
Microsoft 365 テナントがあります。
すべてのユーザーは、Microsoft 365 サービスにアクセスするときに、多要素認証 (MFA) に Microsoft Authenticator アプリを使用する必要があります。
一部のユーザーから、サインイン要求を開始せずに Microsoft Authenticator アプリで MFA プロンプトを受け取ったという報告があります。
ユーザーが開始していない MFA リクエストを報告した場合は、そのユーザーを自動的にブロックする必要があります。
解決策: Azure ポータルから、多要素認証 (MFA) のアカウント ロックアウト設定を構成します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解**: (**正解を表示します**)**
In SC-300, the mitigation for unsolicited MFA prompts (push fatigue) is Fraud alert on Azure AD MFA. The materials state that administrators can "allow users to report suspicious MFA prompts and automatically block the user when they select Report fraud in Mi crosoft Authenticator." By contrast, Account lockout settings are designed to "temporarily lock an account after a configurable number of consecutive MFA denials to thwart brute-force attempts," and they do not initiate an automatic block tied to a user's fraud report. The study guide further clarifies that fraud alerts "can automatically block the user for a specified period (default 90 days) when a fraudulent attempt is reported," which is precisely the behavior required in the scenario. Therefore, merely configuring Account lockout settings will not meet the goal of automatically blocking users when they report an unsolicited prompt.

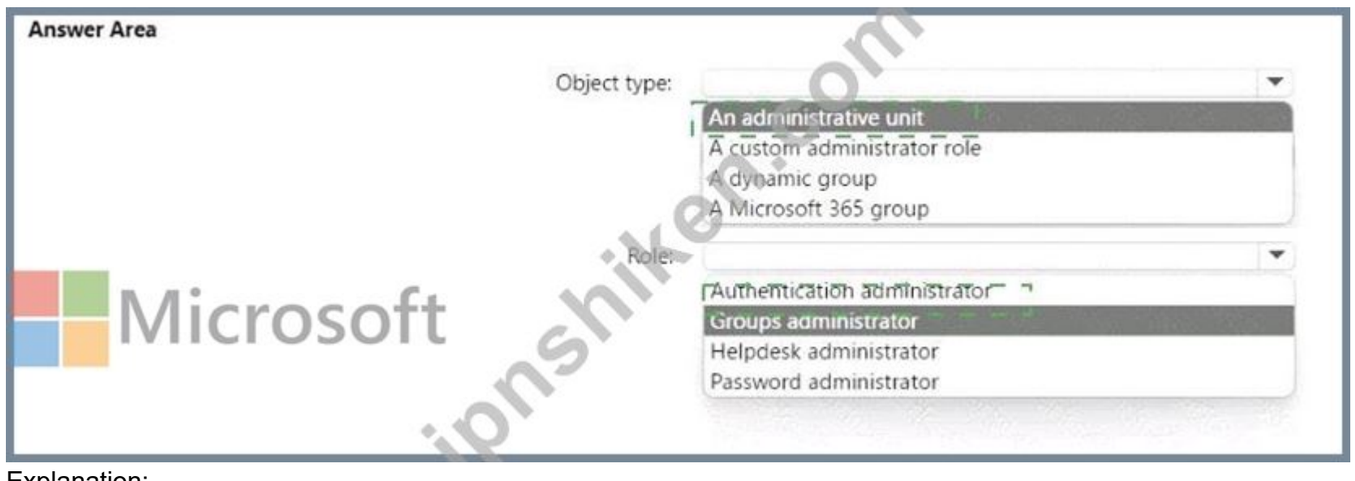
質問**: 60**
Contoso, Ltd.という会社に勤務しており、contoso.comというMicrosoft Entraテナントを保有しています。Contoso社は、以下の2つのパートナー企業と共同でプロジェクトに取り組んでいます。
* adatum.com という Microsoft Entra テナントを持つ A. Datum Corporation という会社
* Fabrikam, Inc. という会社で、fabtikam.com という Microsoft Entra テナントがある場合、adatum.com から contoso.com に新しいゲスト ユーザーを招待しようとすると、エラー メッセージが表示されます。
fabiikam.com から contoso.com に新しいゲストユーザーを招待できました。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。どのような設定が必要ですか？
A. 検証可能な資格情報
B. 名前付き場所
C. ゲスト招待設定
D. コラボレーションの制限
正解**: (**正解を表示します**)**
As per the Microsoft Entra External Collaboration documentation and SC-300 exam guide , when guest invitations fail for a specific organization, it is typically caused by collaboration restrictions settings under External identities # Cross-tenant access settings .

"If you can invite users from one external tenant but not from another, verify the collaboration restrictions under External Identities settings. The setting 'Collaboration restrictions' allows or blocks invitations from specific domains." In this case, invitations from fabrikam.com work, but adatum.com fails - meaning adatum.com is likely blocked by collaboration restrictions . Adjusting these restrictions will allow guest invitations from adatum.
com.

質問: **61**
5,000人のユーザーがいるMicrosoft 365テナントがあります。そのうち100人は経営幹部で、経営幹部には専任のサポートチームがいます。
サポートチームがパスワードをリセットし、多要素認証（MFA）設定を経営幹部のみに管理できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
どのオブジェクト タイプと Azure Active Directory (Azure AD) ロールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:
Object type: An administrative unit
Role: Authentication administrator

In Azure AD Identity and Access Administration, Administrative units (AUs) let you scope delegated admin privileges to a subset of users. The study materials describe AUs as a way to "delegate administration to a subset of users by using administrative units," ensuring the support team's privileges apply only to the executives and not tenant-wide. You would place the 100 executives in a dedicated AU and then assign the support team a suitable role scoped to that AU , satisfying least-privilege principles.
For the required tasks- reset passwords and manage MFA settings -the correct least-privileged role is Authentication administrator . The role capabilities are documented as allowing you to "view, set, and reset authentication method information for non-administrators" and to "require users to re-register for MFA," which covers managing MFA settings for the executives. By contrast, Password administrator is limited to
"reset passwords for non-administrators" and does not include managing authentication methods/MFA, and Helpdesk administrator focuses on basic user help tasks and password resets without full MFA method management. Therefore, assigning Authentication administrator scoped to an Administrative unit containing only the executives meets the scenario and adheres to least privilege.

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: **62**
Microsoft365テナントがあります。
Azure Active Directory（Azure AD）では、利用規約を構成します。
利用規約に同意したユーザーのみがテナント内のリソースにアクセスできるようにする必要があります。他のユーザーはアクセスを拒否する必要があります。
何を設定する必要がありますか？
A. Microsoft Cloud AppSecurityのアクセスポリシー。
B. Microsoft EndpointManagerの利用規約。
C. AzureADの条件付きアクセスポリシー
D. Microsoft EndpointManagerのコンプライアンスポリシー
正解: **(正解を表示します)**
The SC-300 exam section "Implement Conditional Access" and the Azure AD Terms of Use documentation explain that Terms of Use must be enforced using Azure AD Conditional Access. The policy ensures users cannot access Microsoft 365 resources until they accept the presented terms. Conditional Access provides the
"Require terms of use" control under Access Controls # Grant.
The study guide states:
"Administrators can require users to accept organization terms of use by including a Terms of Use control in a Conditional Access policy. Access is denied until acceptance." Microsoft Cloud App Security and Endpoint Manager policies (Options A, B, D) are unrelated - they cannot enforce user acceptance before access. The only supported method is through Azure AD Conditional Access.
Correct Answer: C. a conditional access policy in Azure AD

質問: **63**
Sub1 という名前の Azure サブスクリプションがあり、そこには 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、Azure ロールベースのアクセス制御 (Azure RBAC) を使用する KV1 と KV2 という名前の 2 つの Azure キー コンテナーが含まれています。
サブスクリプションには、次の表に示すユーザーが含まれます。

Name	Role	Role scope
User1	Key Vault Administrator	Sub1
User2	Key Vault Reader	RG1
User3	Key Vault Secrets User	KV1

KV1 には Secret 1 という名前のシークレットが含まれています。KV2 には Secret2 という名前のシークレットが含まれています。
各シークレットの値を読み取ることができるのはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



質問**: 64**

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**)**
In Azure AD Identity Protection, a sign-in risk policy can trigger Conditional Access controls (like MFA) when risky sign-ins are detected.
According to the SC-300 training module "Implement and manage user risk policies", a sign-in risk is associated with a specific authentication attempt, for instance, when a user connects from an anonymous IP address, TOR network, or unfamiliar location. To enforce MFA only when such sign-in conditions are detected, administrators must use a sign-in risk policy.
Microsoft states: "Sign-in risk policies can enforce MFA or block access when sign-in risk meets the configured threshold, such as sign-ins from anonymous IPs."

質問: **65**
contoso.com という名前の Azure AD テナントがあり、このテナントには All Company という名前のグループが含まれており、次の Identity Governance 設定があります。
* 外部ユーザーがこのディレクトリにサインインすることをブロックする: はい
* 外部ユーザーを削除する 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 1 日に、次の設定を持つ Package1 という名前のアクセス パッケージを作成します。
* リソースの役割
o 名称：全社
o タイプ: グループとチーム
o 役割: メンバー
* ライフサイクル
o アクセスパッケージの割り当ての有効期限: 日付
o 割り当ての有効期限 :2022年4月1日
2022 年 3 月 1 日に、次の表に示すゲスト 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 日に、レポート リーダー ロールを Guest1 に割り当てます。
2022 年 4 月 1 日に、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 All Company グループに追加します。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

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:

Answer Area

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:

Answer Area

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.	●	○

In Azure AD Entitlement Management , the tenant-level lifecycle settings govern what happens to external users when their last access package assignment ends. The SC-300 materials explain that when "Block external users from signing in to this directory = Yes," a guest whose final assignment expires or is removed is immediately blocked from sign-in to the resource directory. With "Remove external user = Yes" and a configured period (here 30 days), the guest account is deleted from the directory after that interval provided the user has no other active access package assignments . These lifecycle actions are tied to access package assignments , not to unrelated memberships or role grants that were not delivered via entitlement management.

Applying the timelines: Guest1 and Guest2 received Package1 on Mar 1 with an assignment expiration of Apr 1 . On Apr 1 , their last assignment ended, so they were blocked the same day, and then removed after
30 days -on or about May 1 . Therefore, on May 5 , neither Guest1 nor Guest2 remains in the directory .
The fact that Guest1 was granted a Reports reader role on Mar 2 does not prevent lifecycle removal because it is not an access package assignment . Guest3 , however, was invited on Apr 1 and added to the All Company group on Apr 4 outside of entitlement management; since there was no access package assignment to expire , the lifecycle removal policy does not apply , so Guest3 is still present on May 5 .

質問**: 66**
AU1 という管理単位を含む Microsoft Entra テナントがあります。AU1 は割り当てられたメンバーシップ用に構成されています。
テナントには次の表に示すユーザーが含まれます。

Name	Department	Administrative unit
User1	HR	*None*
User2	IT	AU1

The tenant contains the groups shown in the following table.

Name	Members	Administrative unit
HR	User1	AU1
IT	User2	AU1

AU1 の場合、次の構成を更新します。
会員種別: ダイナミックユーザー
動的メンバーシップルール: (user.department -eq "hr")
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

Statements	Yes	No
HR is a member of AU1.	○	○
User1 is a member of AU1.	○	○
User2 is a member of AU1.	○	○

正解:



ipnshiken.com
Microsoft

Explanation:

HR is a member of AU1: No

User1 is a member of AU1: Yes

User2 is a member of AU1: No

Let's break this down step by step based on Microsoft Entra ID dynamic membership rules, administrative units, and group membership, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding Administrative Units and Dynamic Me mbership in Microsoft Entra ID:

Administrative Units (AUs):Administrative Units in Microsoft Entra ID are used to delegate administrative tasks to a subset of users, groups, or devices. They allow you to scope administrative roles (e.g., User Administrator) to specific users or groups within the AU.

Membership Types for AUs:

Assigned Membership:Members (users, groups, or devices) are manually added to the AU by an administrator.

Dynamic Membership:Members are automatically added or removed based on a dynami c membership rule, similar to dynamic groups. Dynamic membership for AUs can be applied to users or devices (but not groups directly).

The question states that AU1 is initially configured for assigned membership but is then updated to useDynamic Usermember ship with the rule (user.department -eq " HR ").

Dynamic Membership Rule:The rule (user.department -eq " HR ") means that AU1 will automatically include all users whose department attribute in Microsoft Entra ID is set to " HR " . This rule applies to users, not groups or devices, because the membership type is " Dynamic User. " Impact of Changing AU1 to Dynamic Membership:

When AU1's membership type is changed from assigned to dynamic, the existing assigned memberships (e.

g., User2, HR group, IT group) are no longe r relevant. Thedynamic rule takes over, and AU1's membership is determined solely by the rule (user.department -eq " HR ").

Dynamic User Membership:Only users whose attributes match the rule will be members of AU1. Groups (like HR and IT) are not evaluated b y this rule because the membership type is " Dynamic User, " not " Dynamic Group. " Let's evaluate the users based on the rule:

User1:Department = " HR " . The rule (user.department -eq " HR ") matches, so User1 will be dynamically added to AU1.

User2:Department = " IT " . The rule does not match, so User2 will not be a member of AU1, even though they were previously assigned to AU1 and are a member of the IT group.

Groups (HR and IT):The dynamic membership rule for AU1 applies to users, not groups. Therefore, groups l ike HR and IT are not directly evaluated by the rule. However, we need toconsider whether group membership in AU1 affects the statements.

Statement 1: HR is a member of AU1:

Analysis:

The HR group is listed in the second table with AU1 as its administrative unit, indicating that it was initially assigned to AU1 when AU1 used assigned membership.

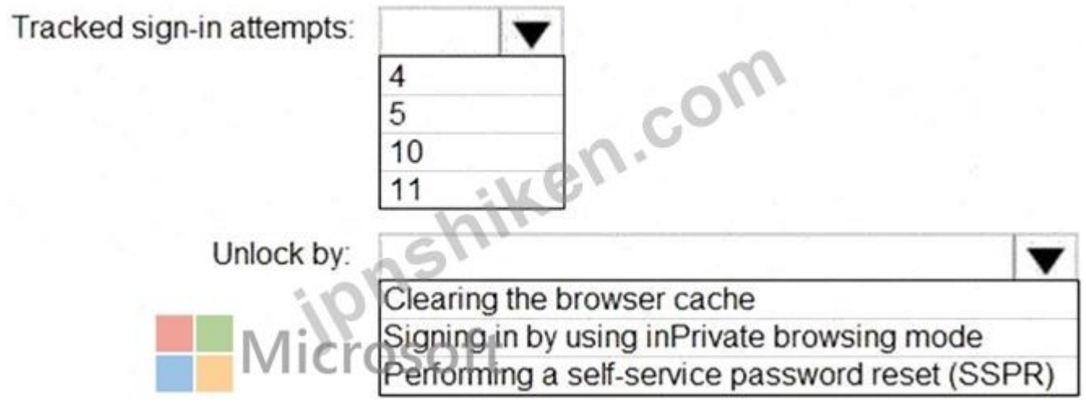
However, AU1's membership type has been updated to " Dynamic User " with the rule (user.department -eq " HR "). Dynamic User membership applies to users, n ot groups.

In Microsoft Entra ID, administrative units with dynamic user membership do not include groups as members unless the AU's membership type is explicitly set to " Dynamic Group " (which is not the case here).
When AU1 was changed to dynamic membersh ip, the HR group would no longer be considered a member of AU1 because the dynamic rule only evaluates users. Groups are not dynamically added to AUs based on user attributes.
Conclusion:The HR group is not a member of AU1 after the change to dynamic membe rship. Therefore, this statement isNo.
Statement 2: User1 is a member of AU1:
Analysis:
User1 has the department attribute set to " HR " (from the first table).
The dynamic membership rule for AU1 is (user.department -eq " HR "), which matches User1's departme nt.
Therefore, User1 will be automatically added to AU1 as a member based on the dynamic rule.
Additionally, User1 is a member of the HR group, which was initially assigned to AU1. However, since AU1 now uses dynamic membership, the HR group's assignment to AU1 is irrelevant. User1's membership in AU1 is determined solely by the dynamic rule, not their group membership.
Conclusion:User1 is a member of AU1 because their department matches the dynamic rule. Therefore, this statement isYes.
Statement 3: User2 is a member of AU1:
Analysis:
User2 has the department attribute set to " IT " (from the first table).
The dynamic membership rule for AU1 is (user.department -eq " HR "), which does not match User2's department.
User2 was initially assigned to AU1 (as shown in the first table) and is a member of the IT group, which was also assigned to AU1. However, when AU1's membership type was changed to " Dynamic User, " the assigned memberships (including User2 and the IT group) are no longer relevant.
The dynamic rule onl y includes users with the department " HR, " so User2 is not added to AU1.
Conclusion:User2 is not a member of AU1 because their department does not match the dynamic rule.
Therefore, this statement isNo.
Additional Considerations:
If AU1's membership type w ere " Dynamic Group " instead of " Dynamic User, " we would evaluate whether the HR and IT groups match a group-based rule. However, the question specifies " Dynamic User, " so the rule applies to user attributes only.
The initial assigned memberships (e.g., Use r2, HR group, IT group) are overridden by the dynamic membership rule. Microsoft Entra ID does not retain assigned memberships when an AU or group is converted to dynamic membership.
The HR and IT groups being assigned to AU1 initially does not affect the dynamic membership of users, but it might be relevant for administrative scoping (e.g., if an admin role is scoped to AU1). However, the statements are about membership, not administrative roles.
Conclusion:Based on the dynamic membership rule (user.depart ment -eq " HR ") for AU1:
HR group:Not a member of AU1 because dynamic user membership does not apply to groups.
User1:A member of AU1 because their department is " HR, " matching the rule.
User2:Not a member of AU1 because their department is " IT, " which does not match the rule.Therefore, the answers are:
HR is a member of AU1:No
User1 is a member of AU1:Yes
User2 is a member of AU1:No
References:
Microsoft Entra ID documentation: " Dynamic membership rules for groups and administrative units " (Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership)
Microsoft Entra ID documentation: " Manage administrative units " (Microsoft Learn:https://learn.microsoft.
com/en-us/entra/identity/role-based-access-control/administrative-uni ts) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers dynamic membership rules and administrative units in Microsoft Entra ID.

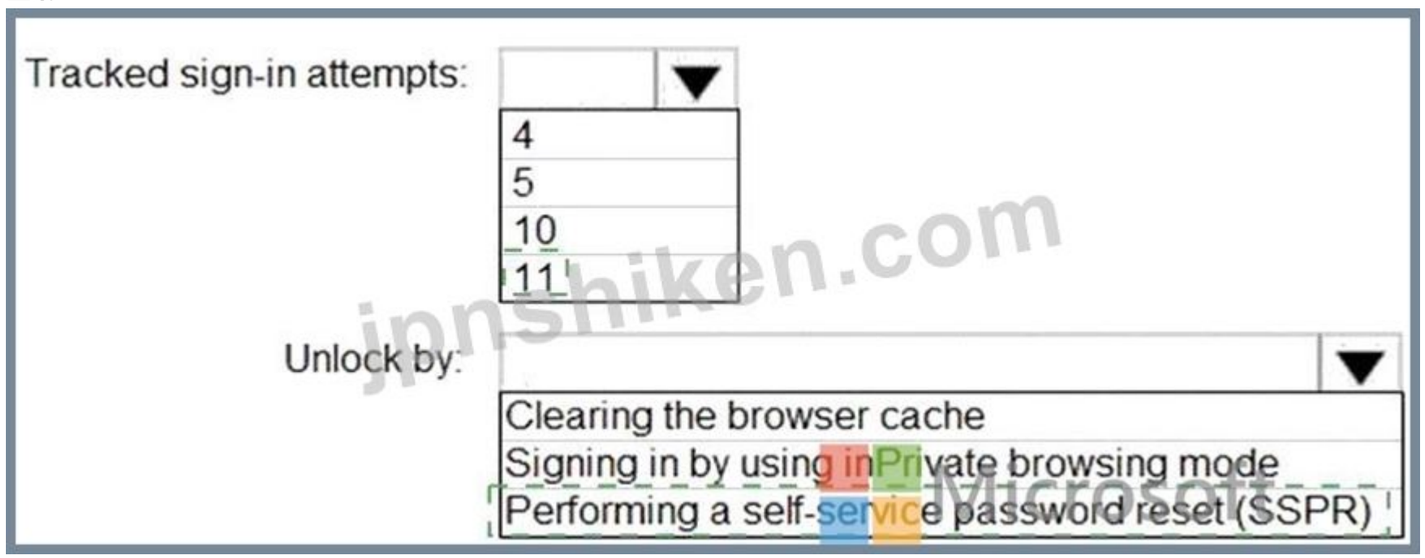
質問: **67**
Azure サブスクリプションをお持ちです。
エンタイトルメント管理から、カスタム拡張機能を含む Catalog1 という名前のカタログを作成する予定です。
最初に何を作成し、Catalog1 を配布するには何を使用すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。
正解:
First create: # An Azure Automation account
* Distribute Catalog1 by using: # An access package
According to the Microsoft SC-300 study guide and Microsoft Entra Identity Governance documentation, when creating custom extensions for Entitlement Management catalogs, the extensions must be hosted in an Azure Automation account. This automation account provides the execution environment for scripts or runbooks that perform external actions when certain events occur, such as user assignments or access removals.
Entitlement Management in Microsoft Entra (formerly Azure AD) allows administrators to automate user access lifecycle processes through access packages. These packages are distributed to internal or external users and define which resources (applications, groups, teams, or SharePoint sites) they can request access to
- all under a governance framework.
* First create an Azure Automation account
* To use a custom extension in a catalog, Microsoft Entra requires an Azure Automation account.
* The automation account hosts runbooks (PowerShell scripts or actions) that execute when access package events trigger (e.g., user request approval, role assignment, or removal).
* The automation account acts as the backend engine for entitlement management extensions.
Step-by-Step Breakdown: As per Microsoft documentation:
"To add a custom extension to an access package, create an Azure Automation account that contains the runbook to handle the automation triggered by access lifecycle events."
* Distribute Catalog1 by using an access package
* Once the catalog (Catalog1) and custom extension are configured, access to the resources in that catalog is granted through access packages.
* Each access package defines eligibility, approval workflows, and access duration for users.
* Access packages serve as the distribution mechanism of catalogs - users request access through them, and the catalog defines what access is granted.
From Microsoft SC-300 content:
"In Entitlement Management, catalogs define available resources, while access packages define who can request them and under what conditions. Access packages are the method of distributing access in a catalog."

質問: **68**
User1 というユーザーが、次の誤ったパスワードを入力してテナントにサインインしようとします。
パ55w0rd12
パ55w0rd12
パ55w0rd12
Pa55w.rd12
Pa55w.rd123
Pa55w.rd123
Pa55w.rd123
Pa55word12
Pa55word12

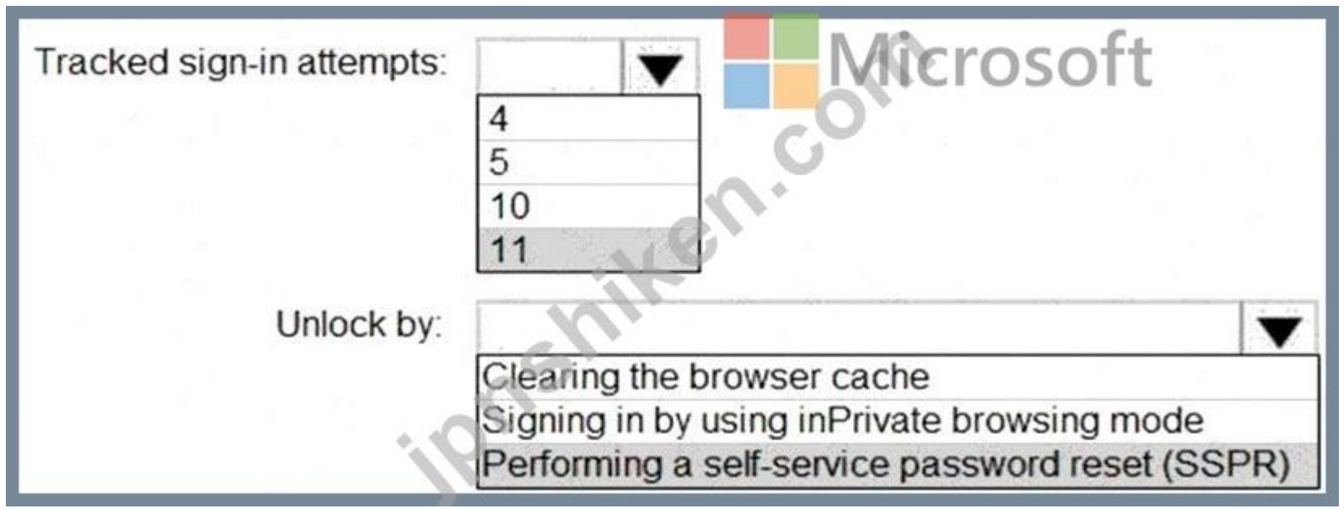
Pa55word12
Pa55w.rd12
User1 に対して追跡されたサインイン試行の回数と、300 秒のロックアウト期間が終了する前に User1 がアカウントのロックを解除する方法を特定する必要があります。
何を特定すべきでしょうか？ 適切なものを選択してください
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



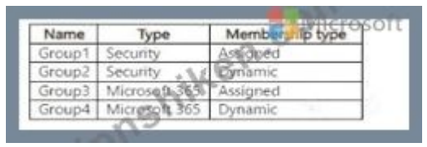
Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

質問: **69**
App1 の計画された変更と技術要件を満たす必要があります。
何を実装する必要がありますか?
A. Microsoft Endpoint Manager で設定されたポリシー
B. Microsoft Endpoint Manager のアプリ構成ポリシー
C. Azure AD でのアプリ登録
D. Azure AD アプリケーション プロキシ
正解: **(正解を表示します)**
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Publish on-premises apps for remote access using Azure AD Application Proxy", Azure AD Application Proxy enables secure remote access to internal, on-premises web applications without requiring VPN access.
In the scenario, App1 is an on-premises application hosted within the Litware network, and the technical requirements specify that it must be securely accessible to both internal and external users - including Fabrikam guest accounts - through Azure AD authentication.
Microsoft's official documentation states:
"Azure AD Application Proxy provides secure remote access to on-premises web applications, integrating with Azure AD for single sign-on (SSO) and conditional access policies." Given that the environment already includes a server (SERVER1) running the Azure AD Application Proxy connector, and that Litware wants to enforce Azure AD Conditional Access and MFA for App1, Azure AD Application Proxy is the correct implementation.
The other options are not suitable:
* A. Policy set in Microsoft Endpoint Manager: Used for device compliance and app management, not for publishing on-premises apps.
* B. App configuration policy in Endpoint Manager: Used for mobile app configuration (e.g., MAM policies), not for access publishing.
* C. App registration in Azure AD: Used for modern cloud or SaaS apps integration, but App1 is on- premises and needs proxy access.
Azure AD Application Proxy

質問: **70**
You have a Microsoft Entra tenant that contains the groups shown in the following table.



Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic
Group3	Microsoft 365	Assigned
Group4	Microsoft 365	Dynamic

グループに対して特権 ID 管理 (PIM) を実装する必要があります。
PIM を使用して管理できるグループはどれですか?
A. グループ1のみ
B. グループ1とグループ2のみ
C. グループ1とグループ3のみ
D. グループ3とグループ4のみ
E. グループ1、グループ2、グループ3、およびグループ4
正解: **(**正解を表示します**)**
Privileged Identity Management (PIM) for groups in Microsoft Entra ID can only be applied to eligible assignment groups, specifically security groups and Microsoft 365 groups that have a membership type of Assigned. According to Microsoft documentation ("Manage Privileged Access Groups in PIM"), only assigned groups can be enabled for PIM. Dynamic groups are not supported for PIM because their memberships are automatically managed based on rules, and PIM requires manual activation and approval for eligible roles or memberships.
From the official study guide and Microsoft Learn module "Implement Privileged Identity Management (PIM) for Groups" :
"Only groups with an Assigned membership type can be managed in Privileged Identity Management.
Dynamic membership groups cannot be enabled for privileged access."
Therefore, among the listed groups:
* Group1 (Security, Assigned) # Supported
* Group2 (Security, Dynamic) # Not supported
* Group3 (Microsoft 365, Assigned) # Supported
* Group4 (Microsoft 365, Dynamic) # Not supported
# Correct Answer: C. Group1 and Group3 only

質問: **71**
RG1 と RG2 という 2 つのリソース グループと、storage1 というストレージ アカウントを含む Azure サブスクリプションがあります。
次の表に示すように、サブスクリプションのロールを割り当てます。



User	Role
User1	Reader
User2	Reader
User3	Reader
User4	Owner

次の表に示すように、RG1 にロールを割り当てます。

User	Role
User1	Reader and Data Access
User2	Contributor

次の図に示すように、storage1 にロールを割り当てます。

```
[
    {
        "RoleAssignmentId": "9dea588b-7569-4cfb-b92b-92748cdc550b",
        "Scope": "/subscriptions/7fefd66e-8694-4b54-beae-
17fd819d4873/resourceGroups/RG2/providers/Microsoft.Storage/storageAccounts/storage1",
        "DisplayName": "User3",
        "SignInName": "User3@contoso.com",
        "RoleDefinitionName": "User Access Administrator",
        "RoleDefinitionId": "/subscriptions/7fefd66e-8694-4b54-beae-
17fd819d4873/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
        "ObjectId": "919948b2-bc94-41a0-9562-9399576cc8f0",
        "ObjectType": "User",
        "RoleAssignmentDescription": "",
        "ConditionVersion": "",
        "Condition": ""
    }
]
```


他の Azure リソースにはロールは割り当てられません。

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



正解:



Explanation:



This scenario tests your knowledge of Azure Role-Based Access Control (RBAC) and the scope hierarchy in Azure (Management Group # Subscription # Resource Group # Resource).

* At the subscription level, User1 has the Reader role. This allows the user to view all resources within the subscription, but not access data stored inside those resources.

* At the RG1 level, User1 also has Reader and Data Access. This role is special - it grants both read access to resource configuration and data access to the underlying data plane (for example, the blobs in a storage account).

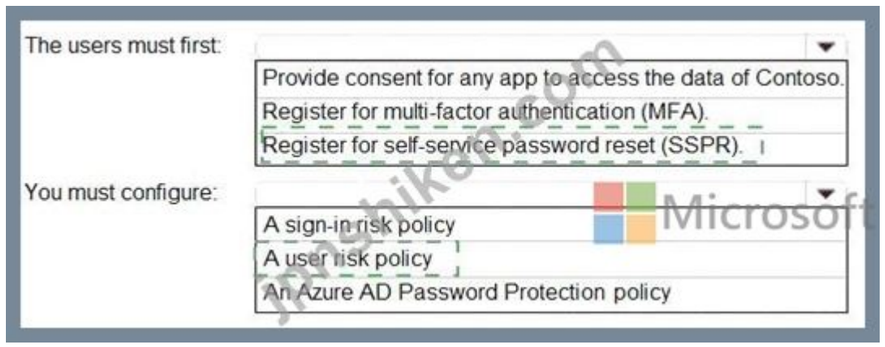
1# # User1 can read the data stored in storage1 # YES Since storage1 is inside RG1, and Reader and Data Access covers both resource and data access, User1 can read data stored in storage1 (e.g., list blobs, view content).
Answer: YES
* At the subscription level, User2 has the Reader role (read-only, no create permissions).
* At the RG1 level, User2 has the Contributor role - this allows full management permissions on resources within RG1.
* The question asks about RG2, not RG1.
2# # User2 can create a virtual network in RG2 # YES However, RG2 does not have any explicit assignment for User2.
But since Contributor at the subscription level gives create/delete permission across all resources, and here User2's Contributor role is scoped to RG1 only, it does not extend to RG2.
So User2 cannot create resources in RG2 because Contributor permission doesn't propagate across resource groups unless assigned at a higher scope.
Correct Answer: NO (User2 cannot create in RG2)
* The JSON data shows that User3 has the User Access Administrator role assigned directly on the storage1 resource. The User Access Administrator role allows managing role assignments (RBAC) at that specific scope - granting or removing access to others.
3# # User3 can assign roles for storage1 # YES Therefore, User3 can assign (and remove) RBAC roles for storage1.
Answer: YES
* Microsoft Learn: Implement Role-Based Access Control (RBAC)
* Microsoft Learn: Understand scope inheritance in Azure RBAC
* Microsoft Learn: Manag e access using the User Access Administrator role
* Exam Ref SC-300: Manage access to Azure resources using roles and assignments Key References from Microsoft SC-300 Official Materials:

質問: 72

ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

According to the Microsoft Identity and Access Administrator (SC-300) official study guide and Microsoft Learn module "Implement and manage user risk policies", the scenario where "users must be forced to change their password if there is a probability that their identity was compromised" directly maps to the Azure AD Identity Protection "User risk policy." In Azure AD Identity Protection, user risk represents the likelihood that an account's credentials have been compromised. When Azure AD detects a high user risk (for example, leaked credentials, atypical sign-in behavior, or sign-ins from unfamiliar locations), the User Risk Policy can be configured to automatically block access or require the user to reset their password upon the next sign-in.

Before a user can reset their password or complete remediation, they must have a registered authentication method (for password reset and MFA). Therefore, users must first register for multi-factor authentication (MFA) - this registration enables the authentication methods (like phone number or authenticator app) that are also used during password reset verification.

The SC-300 documentation specifically highlights:

"To enforce a password change when a user's identity risk is high, the user must be registered for MFA, and a user risk policy must be configured to require password change." Thus, the correct configuration is:

* Users must first register for MFA - to ensure they have verified methods available.
* Configure a user risk policy - to automatically trigger password reset upon detection of compromised credentials.

Correct Answers:

* Users must first: Register for multi-factor authentication (MFA).
* You must configure: A user risk policy.

Topic 3, A Datum CorpOverview

A Datum Corporation is a consulting company in Montreal.

A Datum recently acquired a Vancouver-based company named Litware, Inc.

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

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

The tenant contains the users shown in the following table.

Problem Statements

A Datum identifies the following issues:

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

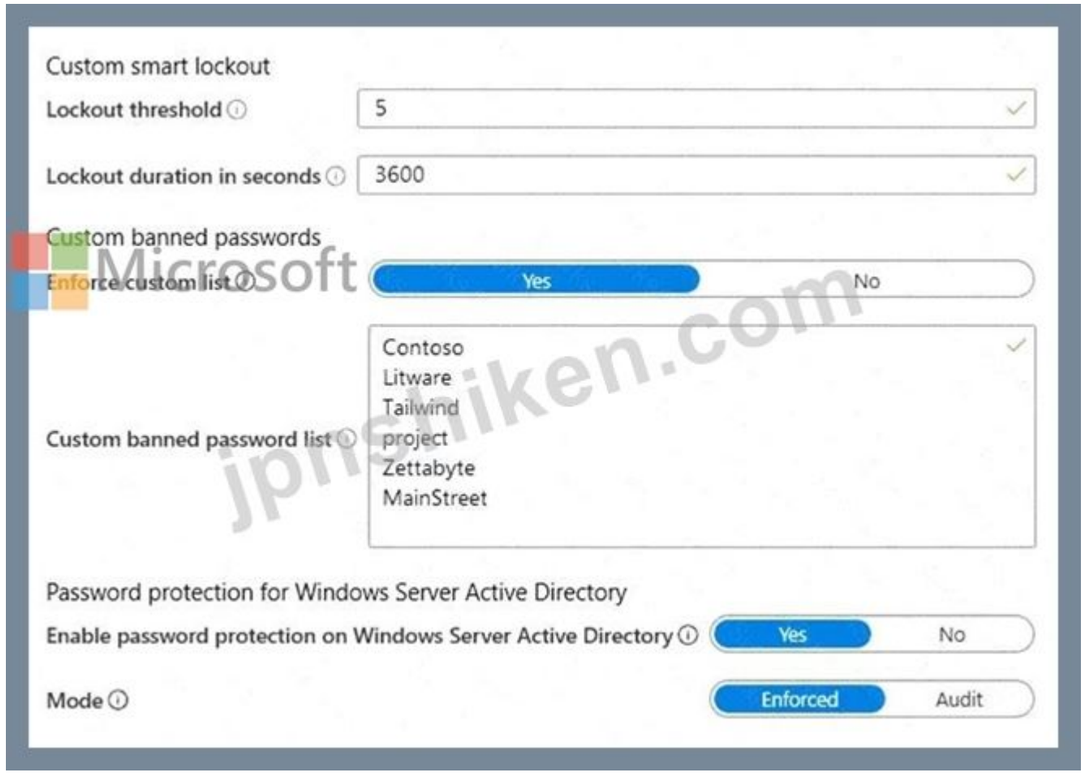
Requirements
A Datum plans to implement the following changes;
* Configure self-service password reset {SSPR}.
* Configure multi-factor authentication (MFA) for all users.
* Configure an access review for an access package named Package1.
* Require admin approval for application access to organizational data.
* Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
* Ensure that only users that are assigned specific admin roles can invite guest users.
* Increase the maximum number of devices that can be joined or registered to Azure AD to 10.
Technical Requirements
A Datum identifies the following technical requirements:
* Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
* Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
* Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
* Email
* Phone
* Security questions
* The Microsoft Authenticator app
* Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
* The principle of least privilege must be used.

質問: 73
Microsoft 365 サブスクリプションをお持ちです。
ユーザーが企業アプリケーションに自分のプロファイルへのアクセスを許可できるようにする必要があります。ソリューションでは、ユーザーが委任されたユーザー権限（読み取り権限とプロファイル権限）にのみ同意できるようにする必要があります。
最初に何を設定する必要がありますか?
A. セキュリティのデフォルト
B. 管理者の同意設定
C. 権限の分類
D. 個人情報保護設定
正解: (正解を表示します)
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Learn documentation ("Configure how end-users consent to applications"), application consent management in Microsoft Entra ID is governed by the Admin consent settings under Enterprise applications # Consent and permissions # User consent settings.
By default, users can grant delegated permissions to apps, but organizations often need to restrict which permissions users may consent to - for example, allowing consent only to low-impact permissions like User.
Read (basic profile information).
Microsoft Documentation Reference:
"In the Admin consent settings, you can control how end users grant consent to applications. You can limit user consent to low-risk permissions, such as permissions that only allow apps to access the user's basic profile data." The configuration steps outlined in Microsoft's official SC-300 training materials are:
* In the Entra admin center, go to Enterprise applications # Consent and permissions # User consent settings.
* Under User consent for applications, choose Allow user consent for apps from verified publishers for selected permissions (recommended).

* Under Select permissions to allow, specify User.Read and User.ReadBasic.All, which correspond to User.Read and User.Read profile delegated permissions.
This ensures that users can only consent to applications accessing their basic profile data and no additional permissions beyond what's explicitly approved.
Why not the other options:
* A. Security defaults: Controls basic security policies (e.g., MFA, legacy authentication) - unrelated to app consent.
* C. Permission classifications: Used for labeling permission risk levels but doesn't enforce consent behavior.
* D. Identity Protection settings: Related to risky user or sign-in detections, not app consent control.

質問: **74**
あなたの会社は最近、Azure Active Directory（Azure AD）特権ID管理（PIM）を実装しました。
PIMでの役割を確認すると、会社のIT部門の15人のユーザー全員が永続的なセキュリティ管理者権限を持っていることがわかります。
IT部門のユーザーが、必要な場合にのみセキュリティ管理者の役割にアクセスできるようにする必要があります。
セキュリティ管理者の役割の割り当てには何を構成する必要がありますか？
A. 役割設定の詳細から対象の割り当てを期限切れにします
B. 役割設定の詳細からアクティブな割り当てを期限切れにします
C. アクティブへの割り当てタイプ
D. 適格への割り当てタイプ
正解: **D (**コメントを発表する**)**
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and the Microsoft Learn module "Configure Azure AD P rivileged Identity Management (PIM)" , Azure AD PIM provides two types of role assignments: Active and Eligible.
An Active assignment means the user permanently holds the role with immediate access. An Eligible assignment means the user can activate the role only when needed, after providing justification or approval.
This follows the least privilege principle by reducing exposure to high-privilege roles.
The official documentation states:
"Users assigned as eligible must activate their role when they need to perform privileged tasks. This ensures that administrative privileges are granted only for a limited time and when necessary."
Because all IT users currently have permanent Security Administrator roles, the correct remediation is to change their assignment type from Active to Eligible so they can activate it only when required.
Options A and B relate to expiration settings but do not convert the assignment type.

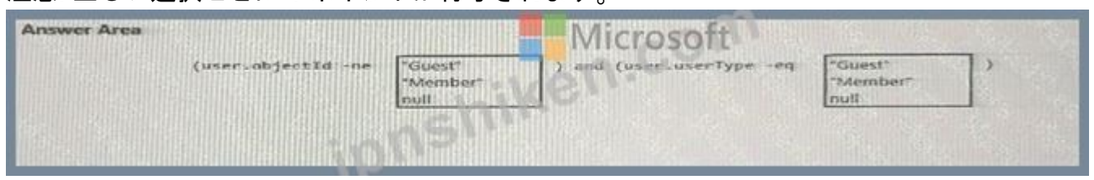
質問: **75**
展示に示されているように、Azure Active Directory（Azure AD）パスワード保護を構成します。 [展示]タブをクリックします。）



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**)**
Azure AD Password Protection combines a global banned password dictionary with any custom banned password list and applies fuzzy matching (norm alizing case, detecting common char acter substitutions, and splitting words) to block weak variants. In the exhibit, custom enforcement is enabled and the list contains:
Contoso , Litware , Tailwind , and project (plus others). The SC-300 content describes th at if a user attempts a password containing or derived from these terms, even with substitutions like 0 for o or @ for a , it will be rejected.
* C0nt0s0 # matches Contoso via character substitution # blocked .
* Pr0jectlitw@re # includes project and litware wit h substitutions # blocked .
* T@ilw1nd # matches Tailwind with common substitutions # blocked . With custom list enforcement turned on, all three candidate passwords are rejected.

質問: **76**
管理要件を満たすには、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完成させるべきでしょうか？答えは、適切な値を正しいターゲットにドラッグすることです。各値は1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



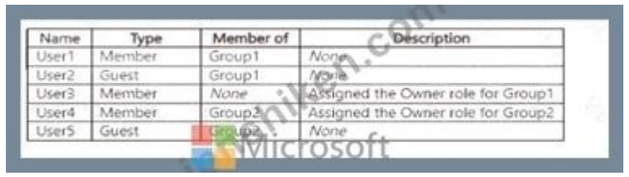
Explanation:
According to the Microsoft Identity and Access Administrator (SC-300) Exam Ref and the Azure AD Dynamic Membership Rules documentation , when you create a dynamic group in Azure Active Directory (now Entra ID), you define rules that automatically add or remove users based on their attributes.
The scenario requires a group named LWGroup1 that contains all Azure AD user accounts for Litware but excludes all guest accounts . In Azure AD, internal users created within the tenant are designated with the attribute user.userType = " Member " , while external or guest accounts from partner organizations have user.userType = " Guest " .
To ensure only internal (Litware) users are included, the membership rule must:
* Ensure the user object exists - by checking (user.objectId -ne null) which confirms that the rule only applies to valid user objects.
* Include only members, excluding guests - by filtering with (user.userType -eq " Member ") .
Hence, the dynamic rule that satisfies these conditions is:
(user.objectId -ne null) and (user.userType -eq " Member ")
This rule guarantees that LWGroup1 dynamically includes all internal users from litware.com and excludes all external users or guest accounts (such as Fabrikam users).
This logic aligns precisely with the Microsoft Learn module "Manage groups in Azure Active Directory" and SC-300 study guide section "Implement and manage dynamic membership rules" , which states: "Use user.userType to distinguish between internal members and external guests when configuring membership rules for dynamic groups."
Correct Answer:
(user.objectId -ne null) and (user.userType -eq " Member ")

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: **77**
Microsoft 365 E5 サブスクリプションと Azure サブスクリプションを所有しています。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. Azure ストレージ アカウント
D. Log Analytics ワークスペース
正解: **(**正解を表示します**)**

質問: **78**
Group! と Group2 という 2 つのグループと、次の表に示すユーザーを含む Microsoft Entra テナントがあります。



Name	Type	Member of	Description
User1	Member	Group1	None
User2	Guest	Group1	None
User3	Member	None	Assigned the Owner role for Group1
User4	Member	Group3	Assigned the Owner role for Group2
User5	Guest	Group2	None

グループ2はグループ1のメンバーです。
次の設定を持つアクセス レビューを構成します。
* 名前: レビュー 1
* レビュー対象を選択: チーム + グループ
* レビュー範囲: チーム + グループを選択
* グループ: グループ1
* 対象: ゲストユーザーのみ
* レビュー担当者を選択: グループ所有者
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



質問: **79**
Sub1 ilia1 というAzureサブスクリプションがあり、そこには storage1 というストレージアカウントが含まれています。App1 と App2 という2つのアプリをデプロイする必要があります。これらのアプリはそれぞれ以下の構成になっています。
* 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でホストされます。
ソリューションでは管理上の労力を最小限に抑える必要があります。
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、回答領域で適切なオプションを選択してください。



正解:



Explanation:



In SC-300 materials covering Microsoft Entra application identities and managed identities for Azure resources, an app you register in the tenant is represented for access control by a service principal : "An application registration creates an application object in its home tenant and a corresponding service principal in any tenant where the app is used. The service principal is the identity used for sign-in, consent, and authorization to resources." This aligns with App1 being a registered app that must authenticate to Storage by Microsoft Entra; the principal you grant roles to on the storage account is the service principal of that app.
For App2, the requirement is to access Storage "by using a single Microsoft Entra identity" while the workload runs on two VMs (VM1 and VM2). SC-300 explains: "A user-assigned managed identity is an independent Azure resource. You can assign the same user-assigned identity to one or more Azure resources." In contrast, "A system-assigned managed identity is enabled on a single Azure resource and is deleted with that resource." Because App2 must share one identity across multiple hosts, the correct choice is a user- assigned managed identity , which provides a single, reusable identity whose lifecycle is separate from VM1 and VM2 and can be granted Storage roles once and used by both machines.

質問**: 80**
App1という名前のAzureADエンタープライズアプリケーションを含むcontoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
請負業者はuser1@outlook.comのクレデンシャルを使用します。
請負業者にApp1へのアクセスを提供できることを確認する必要があります。請負業者は、user1 @ outlook.comとして認証できる必要があります。
あなたは何をするべきか？
A. New-AzADUserコマンドレットを実行します。
B. 外部コラボレーション設定を構成します。
C. WS-FedIDプロバイダーを追加します。
D. contoso.comでゲストユーザーアカウントを作成します。
正解**: D (**コメントを発表する**)**
SC-300 coverage of Azure AD B2B collaboration states that to grant an external person access to your enterprise application, you invite them as a guest using their existing identity (such as a Microsoft account like user1@outlook.com). The documentation emphasizes that B2B "lets you collaborate with external users by adding them to your directory as guest users using their existing credentials." Once invited, the guest can authenticate in their home identity provider and be assigned to the target enterprise application (App1) through app role assignment or group membership. You do not need to create a new managed user or add a WS-Federation identity provider for Outlook.com; Azure AD natively supports Microsoft Accounts for B2B invitations, controlled by External collaboration settings (which generally allow invitations to any domain by default). Consequently, to ensure the contractor can authenticate as user1@outlook.com and access App1, you should create a guest user (invite) in the contoso.com tenant and assign that guest to App1.

質問**: 81**
ネットワークには、Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory ドメインが含まれています。
テナントには、次の表に示すグループが含まれます。

Name	Source	Member of
Group1	Cloud	Group3
Group2	Active Directory domain	None
Group3	Cloud	None

テナントには次の表に示すユーザーが含まれます。

Name	Directory-synced	Member of
User1	No	Group1
User2	No	Group3
User3	Yes	Group2

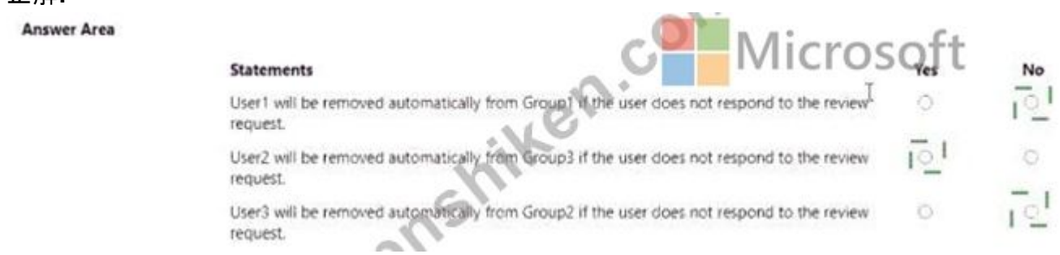
次の表に示すようにアクセス レビューを作成します。

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

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



正解:



Explanation:



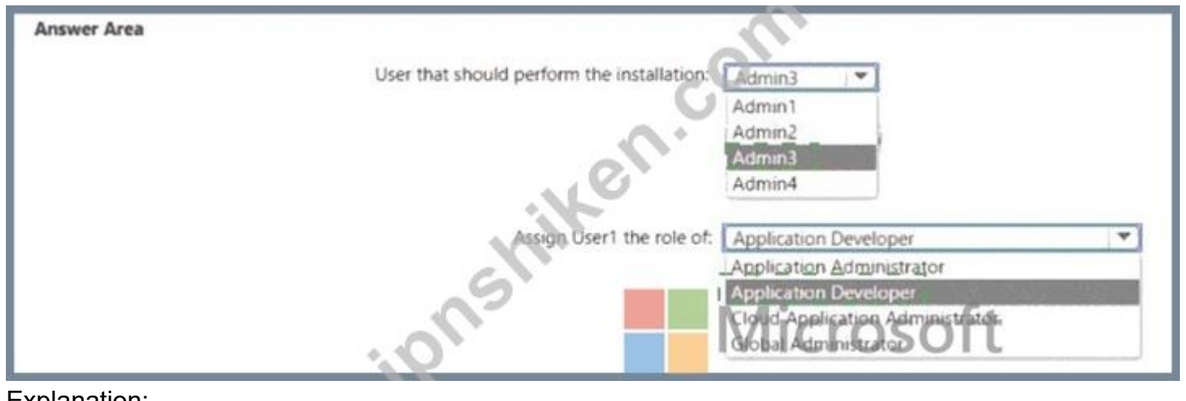
質問: **82**
次の表に示すユーザーを含むハイブリッド Microsoft 365 サブスクリプションがあります。

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

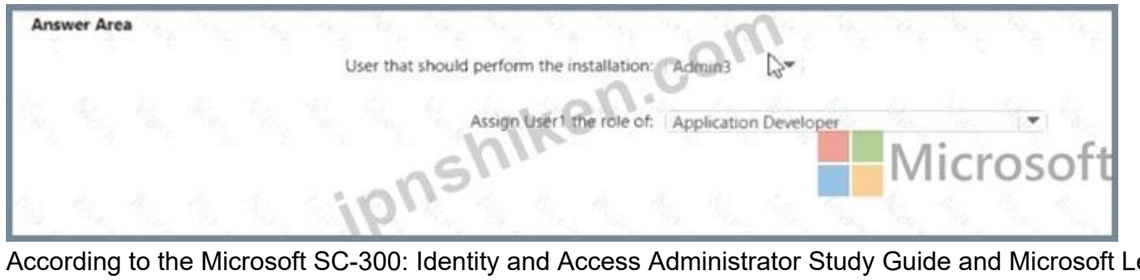
オンプレミスの app1 を展開する予定です。app1 は Azure AD に登録され、Azure AD アプリケーション プロキシを使用します。
アプリケーションプロキシコネクタのインストールを委任し、User1 が Azure AD に App1 を登録できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
どのユーザーがインストールを実行し、Users1 にどのロールを割り当てる必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn module "Implement and manage Application Proxy for on-premises apps" , Azure AD Application Proxy requires that the connector installation be performed by a user with either the Global Administrator or Application Administrator or Cloud Application Administrator role.

Part 1 - User that should perform the installation The Application Proxy connector must be installed by a user who can register and manage applications in Azure AD. The documentation specifies that both Application Administrator and Cloud Application Administrator roles can perform Application Proxy connector installation. Since the question requires adherence to the principle of least privilege, Admin3 (Cloud Application Administrator) is the most appropriate user - because this role grants the required permissions without the broader rights of the Global Administrator.
"Cloud Application Administrator can create, manage, and delegate enterprise applications and Application Proxy connectors, without tenant-wide permissions."
Therefore, Admin3 should perform the installation.
Part 2 - Role for User1 After the connector is installed, User1 needs to register App1 in Azure AD. The role required to register and configure application registrations is the Application Developer role. According to Microsoft documentation:
"Users assigned the Application Developer role can register applications in Azure AD and manage app registrat ions they own." This role is the least privileged role that allows creating new application registrations, unlike Application Administrator or Cloud Application Administrator, which can manage all apps tenant-wide.
Therefore, assign User1 the role of Application Developer.

質問: **83**
次の表に示すリソースを含む Azure サブスクリプションがあります。

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 レビューを作成できますか?
A. グループ1、アプリ1、貢献者、およびロール1
B. ホテルと貢献者のみ
C. グループ1、ロール1、および貢献者のみ
D. グループ1のみ
正解: **A** (コメントを発表する)
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 conf igured 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/governan ce/toc.json
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview According to the Microsoft Identity and Access Administrator (SC-300) official study guide and Microsoft Learn training module "Manage Access Reviews" , Azure AD Access Reviews allow administrators to periodically evaluate user access to critical resources across Azure AD and Azure.
The exam objectives explicitly list access review capabilities that apply to the following resource types:
Groups (Microsoft 365 or security groups) - Access reviews can be used to ensure that group memberships are up to date. In this case, Group1 is eligible since it has an Assigned membership type , which means access reviews can target its members.
Enterprise applications (Ap p1) - Access reviews can assess users who have access to enterprise applications registered in Azure AD, ensuring that only the right users retain application access.
Azure AD roles (Role1) - Access reviews can be created for privileged directory roles (li ke Global Administrator or custom roles such as Role1) to validate continued need for elevated permissions.
Azure subscription roles (Contributor) - Access reviews can also be applied to Azure resources and management groups when integrated with Azure AD P rivileged Identity Management (PIM). This ensures least-privilege access by reviewing roles like "Contributor." Therefore, based on Microsoft documentation:
"Access reviews can be configured for Azure AD groups, enterprise applications, Azure AD roles, and Azure resource roles to ensure that access rights remain appropriate." This means all four - Group1, App1, Contributor, and Role1 - are supported targets for access reviews.

質問: **84**

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が承認なしでユーザー管理者ロールを使用できることを確認します。
* User3がUser2の役割要求を承認したら、User2がユーザー管理者の役割を使用できるようにします。
最初に何を作るべきでしょうか？
A. 役割割り当て
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**)**

質問: **85**
A Datum から新規ユーザーにライセンスを割り当てる必要があります。ソリューションは技術要件を満たしている必要があります。
どのようなタイプのオブジェクトを作成する必要がありますか?
A. 配布グループ
B. 動的ユーザーセキュリティグループ
C. 行政単位
D. あなたの中に
正解: **B (**コメントを発表する**)**
In Azure AD, license automation is implemented through group-based licensing. The SC-300 materials explain that "you can assign licenses to a group in Azure Active Directory; when you assign a license to a group, all users who are members of the group are assigned that license". They also clarify that "dynamic group membership uses rules to automatically add or remove users based on user attributes", which is the recommended way to on-board new populations without manual effort. For licensing, the guide is explicit that
"group-based licensing works with security groups and Microsoft 365 Groups" and that "distribution lists are not supported for license assignment". Administrative Units are described as "a scoping mechanism for delegating administrative permissions to subsets of users and devices", not a licensing entity. Likewise, Organizational Units (OUs) are on-premises AD containers and "do not control license assignment in Azure AD".
Given the requirement to allocate licenses automatically to new A. Datum users as they appear, the least- effort, policy-driven approach is to create an Azure AD Dynamic User security group with a membership rule that targets those users (for example, by domain, company attribute, or a synced attribute), then assign the required Microsoft 365/Azure AD licenses to that group. As the documentation notes, "when users join or leave the group based on the rule, licenses are added or removed automatically."

質問: **86**
Microsoft 365 テナントがあります。
Azure Monitor を使用して、Azure Active Directory (Azure AD) 監査ログ情報を表示できるようにする必要があります。
まず何をすべきでしょうか?
A. Get-AzureADAuditDirectoryLogs コマンドレットを実行します。
B. Azure AD ブックを作成します。
C. Set-AzureADTenantDetail コマンドレットを実行します。
D. Azure AD の診断設定を変更します。
正解: **(**正解を表示します**)**
According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Learn module: "Monitor and troubleshoot Azure Active Directory", to integrate Azure Active Directory audit logs with Azure Monitor, Log Analytics, or Event Hubs, you must first configure Diagnostic settings in Azure AD.

Azure AD logs - including Audit Logs and Sign-in Logs - are stored natively within Azure AD for a limited retention period (14-30 days, depending on license). However, to analyze these logs over time, perform custom queries, or integrate them with monitoring or SIEM solutions, administrators must send them to Azure Monitor logs, Azure Storage, or Event Hubs.
The official documentation explicitly states:
"To send Azure AD logs to Azure Monitor, create a diagnostic setting in Azure Active Directory. From there, select which log categories (AuditLogs, SignInLogs, or NonInteractiveUserSignInLogs) you want to send to a Log Analytics workspace, Event Hub, or storage account." Steps outlined in the study guide and Microsoft Learn:
* Sign in to the Azure portal as a Global Administrator.
* Navigate to Azure Active Directory # Diagnostic settings.
* Select Add diagnostic setting.
* Choose the log categories (e.g., AuditLogs, SignInLogs).
* Select a destination - for instance, a Log Analytics workspace (for Azure Monitor integration).
This configuration is required before Azure Monitor can query or visualize Azure AD audit data.

質問**: 87**
A Datumユーザー向けのライセンスを特定する必要があります。ソリューションには技術要件が必要です。
どのようなタイプのオブジェクトを作成する必要がありますか?
A. Dynamoユーザーセキュリティグループ
B. あなたの中に
C. 配布グループ
D. 行政単位
正解**: (**正解を表示します**)**
According to the Microsoft SC-300: Identity and Access Administrator official study guide and the Microsoft Learn module "Manage user and group licenses in Microsoft Entra ID (Azure AD)", when you need to automatically assign licenses to users based on specific attributes (such as department, location, or a custom attribute like LWLicenses), you should use a Dynamic User Security Group in Azure Active Directory (Entra ID).
In the scenario, 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 the Microsoft 365 group that has the appropriate license assigned." This requirement directly maps to a Dynamic User security group, which supports dynamic membership rules that automatically include users when their attributes meet defined conditions (for example, user.
extensionAttribute15 -eq "E5"). When a license is assigned to this dynamic group, Azure AD automatically provisions or removes licenses for members based on their attribute values - eliminating manual license management.
Per Microsoft documentation:
"You can assign licenses to a group that has dynamic membership. When a user's attributes change, Azure AD automatically adds or removes them from the group, which updates their license assignments accordingly." Now, analyzing the other options:
* B. An OU (Organizational Unit): Used in on-premises Active Directory, not Azure AD. It cannot manage cloud-based license assignments.
* C. A Distribution Group: Used for email distribution in Exchange Online; cannot be used for license assignment.
* D. An Administrative Unit: Used for scoping administrative permissions, not for license assignment.
Therefore, the only object type that satisfies both the technical and automation requirements is a Dynamic User Security Group.
Correct Answer: A. A Dynamic User security group

質問**: 88**
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 0

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

jpnshiken.com

Microsoft



すべてのアクセスレビューリクエストがMeganBowenによって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取るようにする必要があります。
解決策：各マネージャーをフォールバックレビューアとして追加します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**
From the exhibit and the SC-300 Study Guide (Access Reviews section), the access review is configured with the reviewer type set to (Preview) Manager, and Megan Bowen as the fallback reviewer.
In Azure AD Access Reviews, when "Manager" is selected as the reviewer type, the system automatically assigns each user's Azure AD-defined manager to review their access. However, if a user does not have a manager assigned in Azure AD, the review task defaults to the fallback reviewer (in this case, Megan Bowen).
Therefore, if all access review requests are going to Megan Bowen, that means users in the tenant do not have managers properly assigned in Azure AD user attributes.
Adding the department managers as fallback reviewers does not solve the issue because the fallback reviewer receives only the reviews for users without a manager, not based on department.
Microsoft documentation states:
"When 'Manager' is selected as the reviewer, the manager property from Azure AD is used. If a user does not have a manager, the fallback reviewer is used. Adding managers as fallback reviewers will not assign reviews based on departments."

質問: **89**
User1 という名前のユーザーと App1 という名前の登録済みアプリを含む Azure AD テナントがあります。
User1 は、Appl のアプリ登録を削除します。
アプリの登録を復元する必要があります。
アプリの登録を削除してから復元できる最大日数は何ですか?
A. 14
B. 30
C. 60
D. 180
正解: **B (**コメントを発表する**)**
As per Microsoft documentation and the SC-300 course objective "Manage application registrations", when an app registration or enterprise app is deleted in Azure AD, it enters a soft-deleted state. You can restore the app registration within 30 days from the date of deletion using the Azure portal, PowerShell, or Microsoft Graph API.
After 30 days, the app registration and its associated service principal are permanently deleted and cannot be recovered.

質問: **90**
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)
In a new Azure AD (now Microsoft Entra ID) tenant, the default multifactor authentication (MFA) method that is automatically enabled is Microsoft Authenticator .
As per the Microsoft Learn module: Implement and manage Microsoft Entra multifactor authentication and Exam Ref SC-300 , the Microsoft Authenticator app is the default and recommended method because it provides the strongest and most phishing-resistant form of MFA compared to SMS or voice calls.
The guide states:
"New Azure AD tenants have Microsoft Authenticator app enabled by default as the primary method for MFA registration and verification. Users are prompted to register the app when MFA is enforced through security defaults or Conditional Access." Other methods such as SMS , voice call , and email OTP are optional and must be explicitly enabled by an administrator.

質問: **91**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryフォレストに同期するAzureActive Directory（Azure AD）テナントがあります。
Active Directoryでユーザーアカウントが無効になっている場合でも、無効になっているユーザーは最大30分間AzureADに対して認証できることがわかります。
Active Directoryでユーザーアカウントが無効になっている場合、そのユーザーアカウントがAzureADへの認証をすぐに阻止されるようにする必要があります。
解決策：条件付きアクセスポリシーを構成します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: (正解を表示します)
Conditional Access policies control access based on conditions such as user risk, device state, or application context. They do not directly affect account authentication or respond to disabled account states in Active Directory.
If a user's on-premises account is disabled, Azure AD still allows cached credentials to authenticate until the next sync (if using PHS). Conditional Access cannot force immediate disablement - it only acts after successful authentication attempts.
From Microsoft Learn:
"Conditional Access evaluates access after authentication and cannot prevent sign-in for disabled or deleted accounts during synchronization delay." Therefore, Conditional Access does not meet the goal of instantly preventing authentication when an AD account is disabled.
Correct Answer: B. No

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: **92**
Azure AD Identity Protection を使用し、次の表に示すリソースを含む Azure AD テナントがあります。

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 Multi-Factor Authentication (MFA) はすべてのユーザーに対して有効になっています。
User1 は、追加調査を必要とする中程度の重大度のアラートをトリガーします。
次回サインインするときに、User1 にパスワードをリセットさせる必要があります。ソリューションでは、管理の労力を最小限に抑える必要があります。
何をすべきでしょうか?

A. サインイン リスク ポリシーを構成します。

B. User1 を侵害ありとしてマークします。

C. 中程度または低程度の重大度でトリガーされるようにユーザー リスク ポリシーを再構成します。

D. User1 の Azure MFA 登録をリセットします。

正解**: (**正解を表示します**)**

According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Learn: "Azure AD Identity Protection - User Risk Policies and Remediation", Azure AD Identity Protection provides mechanisms to automatically or manually remediate risky user accounts based on detected user risk levels (low, medium, high).
The scenario states:
* A User risk policy (Risk1) exists that requires users with a high severity risk to reset their password upon next sign-in.
* User1 has triggered a medium severity alert, not high.
* The goal is to force User1 to reset his password on the next sign-in, with minimal administrative effort.
* A. Configure a sign-in risk policy: This policy targets sign-in risks (suspicious sign-ins), not user risks, and would not directly force a password reset - it only enforces MFA or blocks access.
* B. Mark User1 as compromised: # When an administrator marks a user as compromised in Azure AD Identity Protection, it immediately elevates the user's risk level to "high." Since the existing User risk policy (Risk1) automatically forces password reset for high-risk users, User1 will be required to change his password the next time he signs in - satisfying the requirement automatically. This approach uses the existing configuration, meeting the "minimize administrative effort" criterion.
* C. Reconfigure the user risk policy to trigger on medium or low severity: This would affect all users globally, not just User1, which is not minimal effort and could increase false positives.
* D. Reset the Azure MFA registration for User1: This affects MFA credentials, not password resets, and doesn't remediate risk.
Analysis of Options: From Microsoft's documentation:
"Marking a user as compromised increases their risk level to High, triggering any configured user risk policy to require password reset upon next sign-in." Therefore, the most efficient and compliant action according to Microsoft's SC-300 study materials is to mark User1 as compromised.

質問**: 93**

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。
すべてのユーザーは、Microsoft 365サービスにアクセスするときに、多要素認証（MFA）にMicrosoftAuthenticatorアプリを使用する必要があります。
一部のユーザーは、サインイン要求を開始せずにMicrosoftAuthenticatorアプリでMFAプロンプトを受信したと報告しています。
ユーザーが開始しなかったMFA要求を報告した場合、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）の通知設定を構成します。
これは目標を達成していますか？

A. はい

B. いいえ

正解: **(**正解を表示します**)**

In the SC-300 materials covering Azure AD MFA configuration, Microsoft distinguishes between Notifications (which control whether the Microsoft Authenticator sends push prompts) and Fraud alert settings (which determine what happens when a user reports an unexpected prompt). The study guide notes that notifications "enable push approvals to the app," but this does not take action when a user reports a suspicious prompt. To satisfy the requirement "block the users automatically when they report an MFA request they didn't initiate," you must use Fraud alert options. The documentation states that administrators can "allow users to submit fraud alerts" and "block users who report fraud" so that "reported accounts are immediately blocked until an administrator unblocks them." These options are part of the tenant's MFA service settings, not the Notifications section. In other words, simply configuring Notifications won't automatically block users who tap Report in Microsoft Authenticator; you must explicitly enable the setting to block users upon fraud reports. Therefore, the proposed solution-changing Notifications settings-does not meet the goal. The correct approach is to enable Fraud alert and select Block users who report fraud, ensuring automatic protection when users report unexpected MFA prompts.

質問: **94**

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザー プロファイルに部門が定義されていないすべてのユーザーを含む動的ユーザー グループを作成する必要があります。

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

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



The SC-300 materials on Dynamic membership rules for groups specify that user attributes can be evaluated with comparison operators such as -eq, -ne, -match, -notIn, etc. For attributes that may be unset, the documentation explains that you can compare the attribute to the literal null to target users with no value. The guide's rule syntax section states that for string attributes like user.department, "to include users where an attribute has no value, compare the attribute to null (for example, (user.department -eq null))." It further clarifies that quoted strings (for example, "null") are treated as the literal

word null, not as the absence of a value, and that $null is not used in Azure AD dynamic rule syntax. Because the requirement is to include all users that do not have a department defined, the correct expression is to select users where the department attribute is empty/unset, which is achieved with the equals operator against null. Therefore, the completed rule is (user.department -eq null), which adds only those users whose profile has no Department value.

質問: **95**
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と、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。
何を使えばいいのでしょうか？
A. ログ分析
B. サインインログ
C. 監査ログ
D. プロビジョニングログ
正解: **(**正解を表示します**)**
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Entra ID (Azure AD) documentation, sign-in logs are the primary source for diagnosing and troubleshooting authentication and access issues for Azure AD-integrated services, including Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security).
The sign-in logs record all user authentication attempts - successful and failed - along with critical details such as:
* User identity (User Principal Name)
* Application name (in this case, "Microsoft Cloud App Security" or "Microsoft Defender for Cloud Apps")
* IP address and device details
* Conditional Access policy outcomes
* Failure reasons (e.g., MFA requirement, denied by Conditional Access, invalid token, etc.) These logs can be accessed directly from the Microsoft Entra admin center # Monitoring # Sign-in logs.
They allow administrators to quickly identify why a user was unable to access a specific cloud service, without needing to configure or collect extra data sources.
Other log types do not fit this scenario:
* Audit logs record changes (e.g., policy updates, role assignments) but not authentication attempts.
* Provisioning logs track synchronization and provisioning events from connected applications.
* Log Analytics is a log aggregation workspace; it's not the first-line diagnostic tool and requires extra configuration.
Hence, to identify the cause of User1's access error with minimal administrative effort, the correct choice is sign-in logs.

質問: **96**
Active Directoryフォレストと同期するAzure Active Directory (Azure AD)テナントがあります。テナントは認証を介して使用します。
企業のセキュリティポリシーには次のように記載されています。
ドメイン コントローラーはインターネットと直接通信してはなりません。
サーバーには必要なソフトウェアのみをインストールする必要があります。
Active Directory ドメインには、次の表に示すオンプレミス サーバーが含まれています。

Name	Description
Server1	Domain controller (PDC emulator)
Server2	Domain controller (infrastructure master)
Server3	Azure AD Connect server
Server4	Unassigned member server

サーバーに障害が発生した場合でも、ユーザーが Azure AD に対して認証できることを確認する必要があります。
追加のパススルー認証エージェントをどのサーバーにインストールする必要がありますか?
A. サーバー2

B. サーバー4
C. サーバー1
D. サーバー3
正解: **(**正解を表示します**)**
The environment uses Azure AD Pass-through Authentication (PTA), which enables users to sign in using their on-premises passwords without storing them in the cloud. For high availability, Microsoft recommends installing multiple PTA agents on separate servers that can securely communicate with Azure AD.
From the SC-300 study material:
"Pass-through authentication agents should not be installed on domain controllers. Install agents on dedicated or member servers that have internet access and are domain-joined." Let's analyze the servers:
* Server1 (PDC emulator) and Server2 (Infrastructure master) - Domain controllers; should not directly connect to the internet or run additional software.
* Server3 (Azure AD Connect server) - Already hosts Azure AD Connect, which is sufficient for synchronization; installing PTA here would violate the "only required software" policy.
* Server4 (Unassigned member server) - Domain-joined, not a DC, and can securely communicate with Azure AD; the best candidate for installing an additional PTA agent.

質問: **97**
次の表に示すオブジェクトを含むAzureActive Directory（Azure AD）テナントがあります。

Name	Type	Directly assigned license
User1	User	*None*
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	*None*
Group3	Mail-enabled security group	*None*

Group3にメンバーとして追加できるオブジェクトはどれですか？
A. User2とGroup2のみ
B. User2、Group1、およびGroup2のみ
C. User1、User2、Group1、Group2
D. User1とUser2のみ
E. User2のみ
正解: **(**正解を表示します**)**
Azure AD supports several group types with different membership rules. For Microsoft 365 groups, "group nesting isn't supported; only user identities can be members." For mail-enabled security groups used in Azure AD/Exchange Online, the SC-300 materials emphasize that only user objects are supported as members when managed in Azure AD, while "Microsoft 365 groups can't be added to other groups." Security groups are commonly nestable for access scenarios, but the mail-enabled security group membership experience in Azure AD limits member selection to users; thus you cannot add Group1 (security group) or Group2 (Microsoft 365 group) as members of Group3 (mail-enabled security group). Licensing assignments shown in the table are irrelevant to membership eligibility. Consequently, the only valid members you can add to Group3 are the user objects - User1 and User2.

質問: **98**
Microsoft Entra ID P1 ライセンスを持つ Microsoft Entra テナントがあります。
過去に発生したサインインを調査するには、Microsoft Entra ID サインイン ログを確認する必要があります。
Microsoft Entra ID はサインイン ログにイベントをどのくらいの期間保存しますか?
A. 14日間
B. 30日間
C. 90日間
D. 365日

正解: **C** (正解を表示します)

The retention period for Microsoft Entra (Azure AD) sign-in logs depends on the license (Free, P1, P2).

Microsoft's data retention documentation states that with a Microsoft Entra ID P1 license, sign-in data is retained for 30 days.

The relevant table in the "Microsoft Entra data retention" documentation shows:
* With Entra ID P1 or P2: sign-in activity is retained for 30 days

* (With Free tier, sign-in logs are retained for 7 days)

Therefore, under your scenario (tenant has ID P1 license), the logs are available for 30 days.

質問: **99**

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。

何を使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: **C** (コメントを発表する)

To compare and analyze role permissions of multiple users within an Azure AD tenant, the correct and most efficient tool is the Microsoft Entra admin center.

According to the Microsoft Identity and Access Administrator Study Guide and Microsoft Entra documentation , the Entra admin center provides the Roles and Administrators blade where administrators can:
* View all directory roles.
* Compare role permissions and assignments.
* See which users have which roles and what each role allows.

The guide clarifies:

"Administrators can use the Entra admin center to view and compare role definitions and assigned members without using additional portals or manual PowerShell scripts." The other options serve different purposes:
* Microsoft 365 Defender portal focuses on security incidents and threat management.
* Microsoft 365 admin center handles licensing and user management but not detailed role comparison.
* Microsoft Purview compliance portal deals with compliance, data governance, and auditing.

質問: **100**

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**)**
According to Microsoft Defender for Cloud Apps documentation and the SC-300 study guide, an OAuth app policy monitors third-party applications that request access to Microsoft 365 data through Microsoft Graph API permissions. These apps can request delegated or application permissions. When an app is authorized by many users and requests high permissions such as Calendars.ReadWrite, it can introduce security risks.
Defender for Cloud Apps allows administrators to create OAuth app policies to generate alerts when an app:
* Requires high permissions (e.g., read/write to mailboxes, calendars, or files).
* Is authorized by more than a specified number of users (for example, more than 20).
This matches the requirement in the question exactly. Other policy types (anomaly detection, access, or activity) monitor user or session behavior, not app consent behavior.
As per Microsoft's documentation:
"Use OAuth app policies to detect risky OAuth apps, monitor application permissions, and alert when apps are authorized by an unusual number of users or request excessive permissions."

質問: **101**
組織データへのアプリケーションアクセスに関して計画されている変更を実施する必要があります。何を設定すればよいでしょうか？
A. 認証方法
B. ユーザーの同意設定
C. パッケージにアクセスする
D. アプリケーションプロキシ
正解: **(**正解を表示します**)**
The requirement is:
"Require admin approval for application access to organizational data." According to the Microsoft SC-300 exam guide and Microsoft documentation on "Configure consent settings for applications", Azure AD provides User consent settings under Enterprise applications # Consent and permissions to control how applications can request permissions to access organizational data.
By default, users can consent to allow apps to access organizational data on their behalf, which can create security risks. To ensure tighter control, administrators can:
* Disable user consent entirely, or
* Require admin consent workflow so that when users try to grant an app access, it must first be approved by an administrator.
The SC-300 study materials explicitly describe:
"To require administrator approval before an app can access organizational data, configure the User consent settings to use the admin consent workflow." This aligns perfectly with the stated requirement - to ensure admin approval is required before apps gain access to organizational data.
Other options are incorrect:
* Authentication methods manage MFA and SSPR, not app consent.
* Access packages are part of Identity Governance for resource access, not app consent.
* Application Proxy publishes on-premises apps, not related to app consent permissions.

質問: **102**
Azure AD テナントがあります。
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を提供しようとすると、失敗します。
ユーザーがApp1の管理者の同意をリクエスト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。
まず何をすべきでしょうか?
A. テナントの管理者の同意リクエストを有効にします。

B. テナントの管理者の同意要求のレビュー担当者を指定します。
C. App1の権限設定から、テナントに対するApp1の管理者の同意を付与します。
D. Appl の条件付きアクセス ポリシーを作成します。
正解**: A (**コメントを発表する**)**
Azure AD (Entra ID) allows administrators to control how users request permission for applications that require admin consent. By default, only administrators can grant such consent.
According to the SC-300 Study Guide (Identity Management & Governance) and Microsoft Entra Documentation , the least privileged and compliant method to enable user-driven admin consent requests is to:
* Enable admin consent requests in the tenant.
* Designate one or more reviewers (optional) to handle these requests.
Once enabled, users who encounter an app that needs admin consent can submit a request for approval instead of being blocked. This ensures controlled delegation without globally granting broad permissions to all apps.
"Enable admin consent requests in Azure AD to allow users to request approval for apps that need tenant- wide permissions, ensuring least privilege and administrator oversight."

質問**: 103**
Sub1 という名前の Azure サブスクリプションがあります。
Microsoft Entra Permissions Management を展開する予定です。
権限管理がSub1にアクセスできることを確認する必要があります。ソリューションは最小権限の原則に従う必要があります。
PowerShell コマンドをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解**:**


Explanation:


In Microsoft Entra Permissions Management (formerly CloudKnox), onboarding an Azure subscription requires granting the Permissions Management service principal the minimum rights needed to discover identities, roles, and permissions across that subscription. The SC-300 materials emphasize the principle of least privilege for onboarding: assign Reader at the subscription scope so the service can inventory resources and permissions without the ability to change them. After onboarding, if you want automated remediation/right-sizing, you can additionally grant User Access Administrator (or

perform changes manually), but that elevation is not required merely to onboard and collect data.
Accordingly, you complete the PowerShell by creating an RBAC assignment for the application (service principal) at the subscription scope using New-AzRoleAssignment and specifying -RoleDefinitionName Reader . Creating a new custom role (New-AzRoleDefinition) is unnecessary, and New-AzTag is unrelated to RBAC. Choosing Owner or Contributor would ex ceed the access required for onboarding and violate least-privilege guidance. The correct, minimal configuration is therefore: assign Reader to the Permissions Management application at the /subscriptions/ < SubscriptionId > scope using New-AzRoleAssignment .

質問**: 104**
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	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

ユーザー管理者ロールに次の割り当てを追加します。
* スコープの種類: ディレクトリ
* 選抜メンバー :グループ1
* 割り当てタイプ: アクティブ
* 課題開始は2022年8月15日
* 任務終了日: 2022年12月15日
Exchange 管理者の役割に次の割り当てを追加します。
* スコープの種類: ディレクトリ
* 選抜メンバー :グループ2
* 割り当てタイプ: 適格
* 課題開始日: 2022年10月15日
* 任務終了日: 2023年1月15日
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



jpnshiken.com
Microsoft

正解:



Microsoft
ipnshiken.com

Explanation:

< On November 15, 2022, Admin1 can reset the password of Admin2. = Yes

On October 15, 2022, Admin2 signs in and can administer Exchange Online. = No On September 1, 2022, Admin3 can reset the password of Admin1. = Yes

\

In SC-300 materials, Microsoft Entr a Privileged Identity Management (PIM) distinguishes Active and Eligible assignments. An Active assignment "grants the role immediately until it expires," whereas an Eligible assignment "does not grant permissions until the user activates the role for a limited time." Group-based role assignment applies the role to all members of the group within the configured start/end dates. The User Administrator role is documented as being able to "manage users and groups, including reset passwords for most admin rol es except highly privileged roles." Applying these rules to the scenario:

* User Administrator # Group1 (Active 8/15-12/15) : Admin1 and Admin3 are members of Group1, so both hold User Administrator actively on 9/1 and 11/15. Therefore, Admin1 can reset Adm in2's password on 11/15 , and Admin3 can reset Admin1's password on 9/1 .

* Exchange Administrator # Group2 (Eligible 10/15-1/15) : Admin2 (member of Group2) is only eligible starting 10/15 ; eligibility alone does not grant Exchange admin permissions until he activates the role (which typically requires justification/MFA and sets a time-bound active window). Thus, simply signing in on 10/15 does not let Admin2 administer Exchange Online.

These behaviors are emphasized in SC-300 guidance on PIM: active assignme nt = immediate permissions ; eligible assignment = must activate before permissions apply ; group assignment = role applies to all group members for the assignment window .

質問**: 105**

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**: A (**コメントを発表する**)**

In Azure AD Monitoring and Reporting documentation and the SC-300 Study Guide (Module: Monitor and report on identity and access) , sign-in logs in Azure Active Directory are retained for a default duration of 14 days.

The sign-in logs contain information about user sign-in activity, including application usage, conditional access policies, and multi-factor authentication details. These logs are accessible through the Azure portal # Azure Active Directory # Sign-ins, or programmatically via Microsoft Graph.

Microsoft specifies:

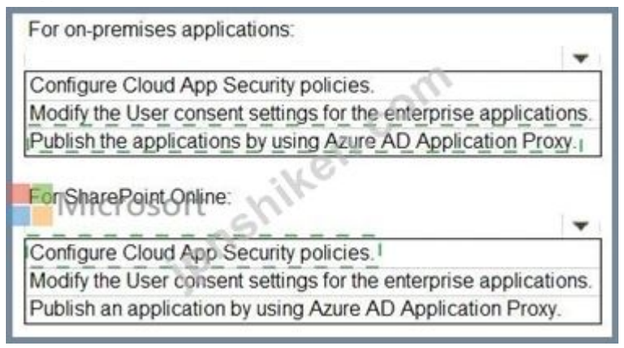
"Azure AD stores sign-in activity for 14 days by default. For longer retention, you must integrate with Azure Monitor (Log Analytics), Azure Storage, or Event Hub." This 14-day retention limit applies to

tenants without additional premium log retention solutions.

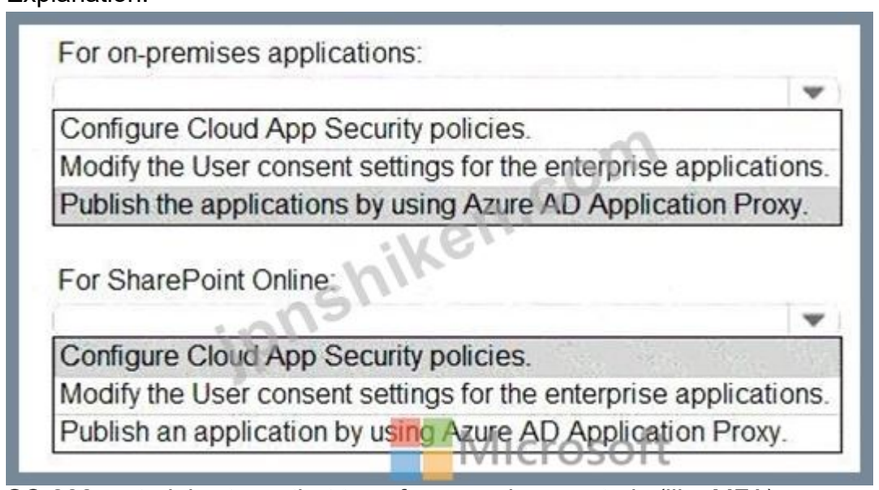
質問: 106
認証要件とアクセス要件を満たすには、オンプレミス アプリケーションと SharePoint Online の制限を実装する必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

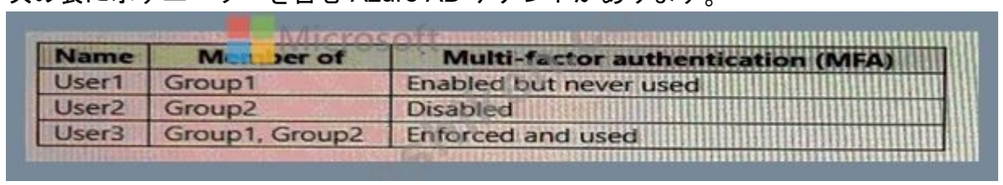


SC-300 materials stress that to enforce modern controls (like MFA) on on-premises apps, you must front them with Azure AD so Conditional Access can evaluate sign-ins. The documentation states that Azure AD Application Proxy " provides secure remote access to on-premises applications " and that apps published through it can have " Conditional Access policies, including multifactor authentication "

applied at sign- in. In other words, once the legacy app is published by Application Proxy, Azure AD sits in the path, enabling you to meet the requirement to enforce MFA when accessing on-premises applications and to combine it with your location-based exemptions.
For SharePoint Online restrictions, SC-300 points to Microsoft Cloud App Security (Defender for Cloud Apps) for real-time governance: you can create session policies that " control and limit activities in real time " and, for SharePoint Online and other Microsoft 365 apps, " monitor user sessions and block download, cut, copy, and print " when conditions (device state, risk, or location) warrant it. Since the scenario already has anomaly detections enabled, configuring Cloud App Security policies aligns directly with the requirement to place access restrictions on SharePoint Online without altering tenant-wide consent settings. Thus, publish on-prem apps with Application Proxy to bring them under Conditional Access (for MFA), and use Cloud App Security policies to enforce SharePoint Online session and download controls.

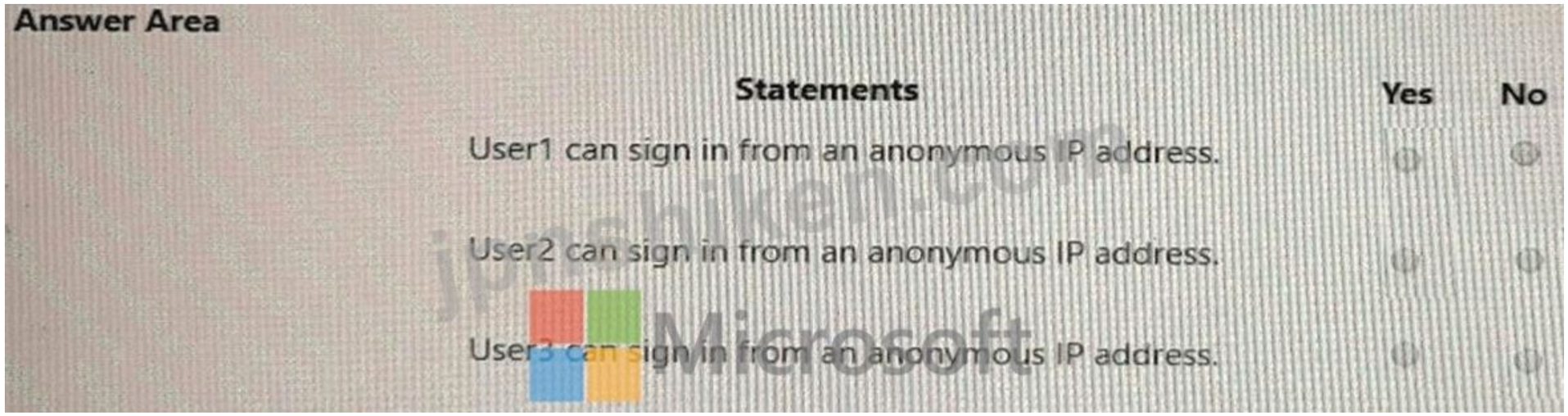
有効的な**SC-300J**問題集はJPNTest.com提供され、**SC-300J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-300J**試験問題集を提供します。JPNTest.com SC-300J試験問題集はもう更新されました。ここで**SC-300J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-300J-mondaishu　**385**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」

質問: **107**
次の表に示すユーザーを含む Azure AD テナントがあります。

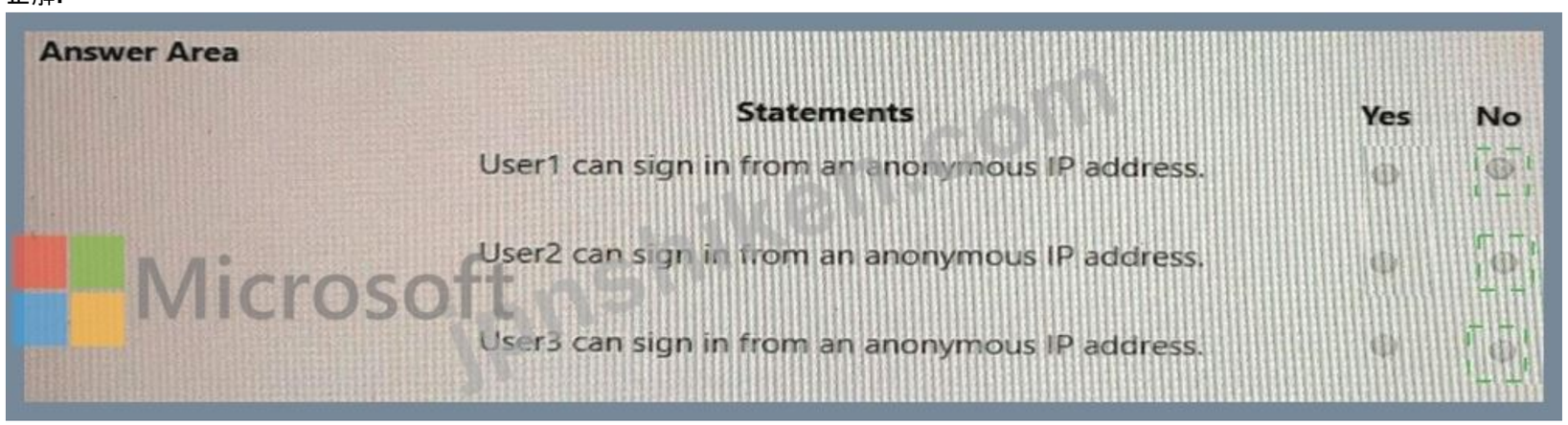


Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

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



正解:



Explanation:

User1 can sign in from an anonymous IP address: No

User2 can sign in from an anonymous IP address: No

User3 can sign in from an anonymous IP address: No

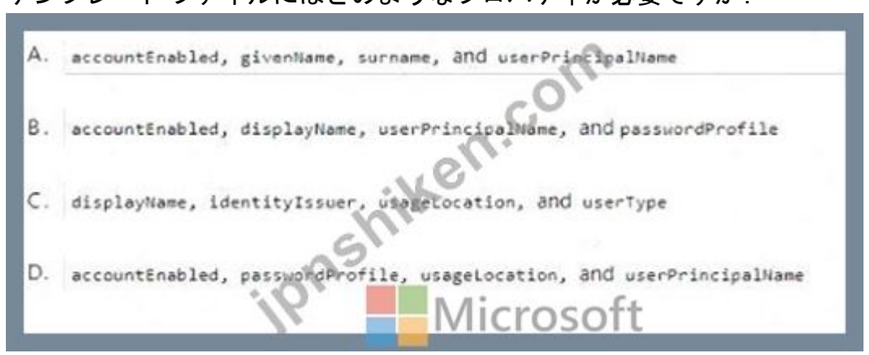
According to the Microsoft SC-300 Study Guide, Exam Ref SC-300, and Microsoft Entra Conditional Access and Identity Protection documentation, when multiple conditional access (CA) and risk policies are active, Azure AD evaluates them collectively, and if any applicable policy denies access, the user is blocked.

Let's break down the setup:

* User risk policy
* Applies to Group1
* User risk: Low and above
* Access: Block access
* Enforced: On
* Sign-in risk policy
* Applies to Group2
* Sign-in risk: Low and above
* Access: Require MFA

* Enforced: On
* CAPolicy1: Users connect from a trusted IP address (Status: On)
* CAPolicy2: Users' devices are marked as compliant (Status: On)
* CAPolicy3: Sign-in risk is low (Report-only # not enforced)
Identity Protection policies configured: Conditional Access Policies configured:
User Analysis: User
Member of
MFA Status
Applicable Policies
Result
User1
Group1
Enabled but never used
User risk policy # Block access if risk # Low
Cannot sign in (blocked by user risk policy).
User2
Group2
Disabled
Sign-in risk policy # Require MFA
Cannot complete sign-in (MFA required but disabled).
User3
Group1, Group2
Enforced and used
Both policies apply # Block access (user risk policy takes precedence)
Blocked (since one policy enforces deny).
Additionally, CAPolicy1 (trusted IP) denies anonymous IP addresses because anonymous IPs are not trusted or registered - Azure marks such attempts as "risky sign-ins." Thus, regardless of MFA capability, no user can sign in from an anonymous IP address.

質問**: 108**
Azure AD テナントがあります。
テンプレート ファイルをアップロードして、25 個の新しいユーザー アカウントを一括作成する必要があります。
テンプレート ファイルにはどのようなプロパティが必要ですか?

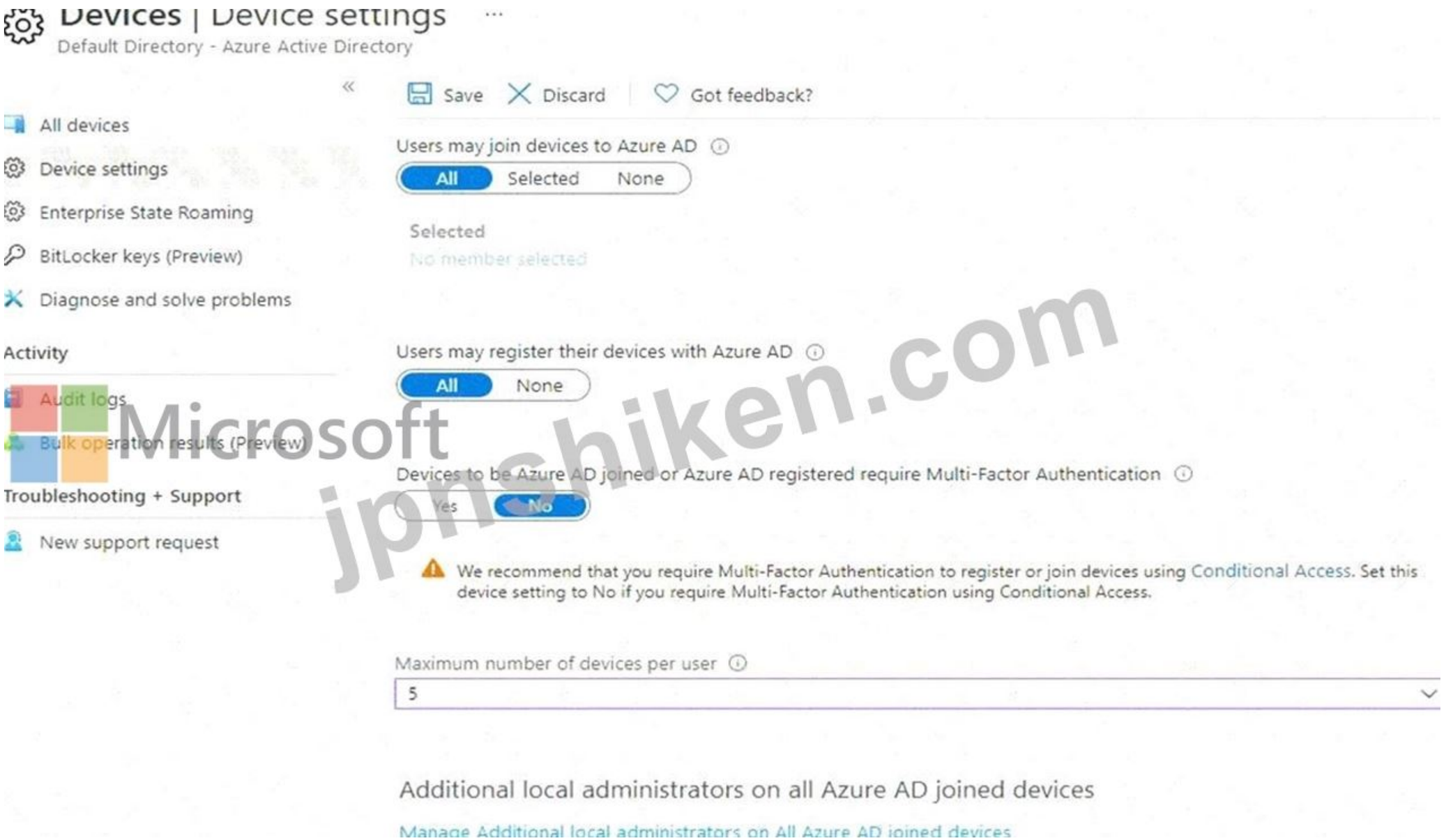


A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解**: (**正解を表示します**)**
When performing a bulk user creation in Azure Active Directory (via a CSV template upload), certain attributes are required to successfully create user objects.
According to Microsoft's Azure AD user bulk import documentation, the required properties are:
* accountEnabled - Boolean (True/False) value to enable or disable the account.
* passwordProfile - Includes the user's initial password details.
* usageLocation - Specifies the country or region for license assignment.
* userPrincipalName - Unique sign-in name for the user.
Other properties such as givenName, surname, or displayName are optional.
From Microsoft Docs:
"The minimum required attributes for user creation are accountEnabled, displayName, mailNickname, userPrincipalName, and passwordProfile. However, when bulk importing, usageLocation is also required for license assignment compliance." Therefore, among the given options, Option D matches these required fields exactly.
Correct Answer: D. accountEnabled, passwordProfile, usageLocation, and userPrincipalName

質問**: 109**
Azure Active Directory Premium Plan 2 ライセンスを持つ 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	Cloud device administrator
Admin2	Device administrator
User1	**None**

jp-shikaku.com
Microsoft
次の図に示すデバイス設定があります。



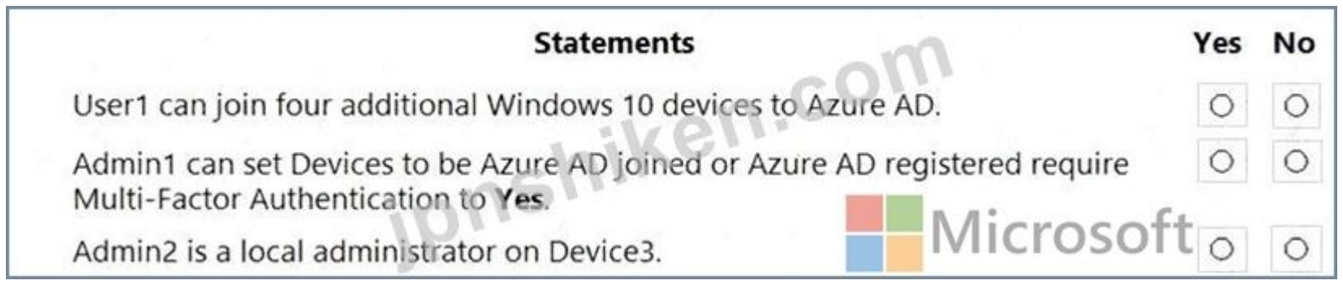
User1 には次の表に示すデバイスがあります。

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

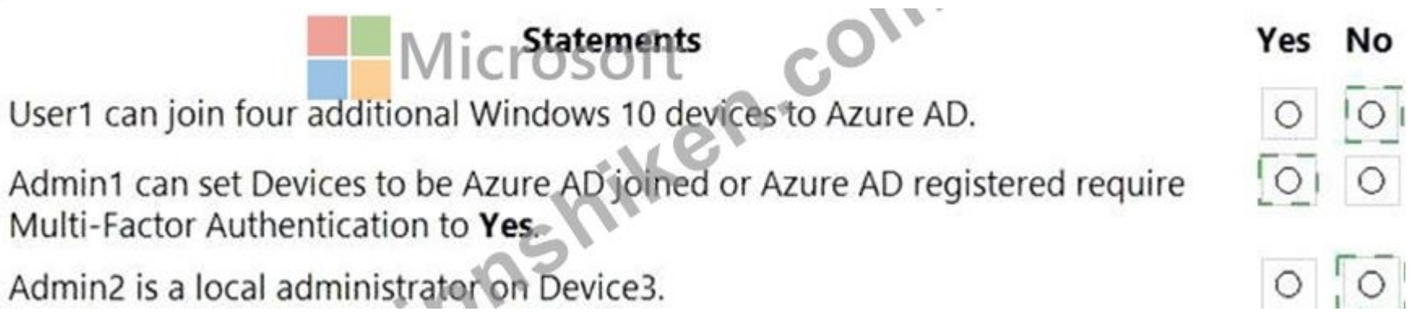
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Microsoft
ipnshiken.com



正解:



Explanation:

< User1 can join four additional Windows 10 devices to Azure AD. # No

2# # Admin1 can set "Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication" to Yes. # Yes

3# # Admin2 is a local administrator on Device3. # No

This scenario draws from Module: Manage device identities in Azure Active Directory in the Microsoft SC-300 Official Study Guide and Microsoft Learn content.

Statement 1: User1 can join four additional Windows 10 devices to Azure AD - NO In the Device Settings, the "Maximum number of devices per user" is configured as 5. User1 already has one Azure AD joined device (Device1) and three Azure AD registered devices (Device2, Device3, Device4). Since both Azure AD joined and Azure AD registered devices count toward the same limit, User1 has already registered 4 devices.

This means they can add only one more, not four additional Windows 10 devices. Therefore, the statement is No.

Microsoft documentation states: "The maximum number of devices per user setting applies collectively to all Azure AD-joined and Azure AD-registered devices." Statement 2: Admin1 can set Devices to be Azure AD joined or Azure AD registered require MFA to Yes - YES The Cloud Device Administrator role (Admin1's role) has the delegated permissions to manage device settings in Azure AD, including enforcing MFA requirements for device registration and join operations. The role allows management of the Azure AD device configuration blade, including toggling settings like MFA for join/register, join limits, and device ownership policies. Therefore, Admin1 can enable the MFA requirement for device join/registration.

As per Microsoft Learn: "Cloud Device Administrator can manage all aspects of device settings, including device join and registration MFA requirements." Statement 3: Admin2 is a local administrator on Device3 - NO Admin2 holds the Device Administrator role.

However, per Microsoft's documentation, only Azure AD-joined Windows 10 devices grant local administrator rights to users in the Device Administrator role. Azure AD-registered devices (such as Device3) are personal devices that do not have local administrator assignment through Azure AD roles. Since Device3 is Azure AD registered, not joined, Admin2 is not a local admin on it.

Microsoft guidance clarifies: "Users assigned to the Device Administrator role are added as local administrators only on Azure AD-joined devices, not on Azure AD-registered or hybrid devices."

質問**: 110**

Contoso という Azure AD テナントがあり、Terms1 という利用規約 (ToU) とアクセス パッケージが含まれています。Contoso ユーザーは、Fabrikam という外部組織と共同作業を行っています。Fabrikam ユーザーは、アクセス パッケージを使用する前に、Terms1 に同意する必要があります。

どのユーザーが利用規約1に同意したか、または拒否したかを特定する必要があります。

何を使うべきでしょうか?

A. プロビジョニングログ
B. 使用状況と分析レポート
C. サインインログ
D. 監査ログ
正解: **(**正解を表示します**)**
When users accept or decline a Terms of Use (ToU) in Azure AD, these actions are recorded in the audit logs.
The Microsoft Identity and Access Administrator documentation specifies that audit logs capture "Terms of use acceptance records" including who accepted , who declined, timestamp, and version of the ToU accepted.
The other options are incorrect because:
* Provisioning logs capture provisioning events (not ToU).
* Usage and Insights reports provide activity metrics, not compliance actions.
* Sign-in logs capture authentication activity but not ToU acceptance.
Therefore, to identify which users accepted or declined Terms1, you should use the Audit logs in Azure AD.

質問: **111**
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	User type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 は Group1 の所有者です。
次の設定を持つアクセス レビューを作成します。
レビュー対象: チーム + グループ
対象: すべてのユーザー
グループ: グループ1
レビュー担当者: ユーザーは自分のアクセスをレビューします
User3 のアクセスレビューを実行できるのはどのユーザーですか?
A. ユーザー1のみ
B. ユーザー3のみ
C. ユーザー1とユーザー2のみ
D. ユーザー1、ユーザー2、ユーザー3
正解: **(**正解を表示します**)**
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on the Microsoft Entra access review settings and the principles outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Access Review Settings:

What to review: Teams + GroupsThis indicates that the access review is evaluating memberships in Teams and Groups within the Microsoft Entra tenant. Since the group specified is Group1, the review focuses on Group1 membership.
Scope: All usersThe scope defines who is being reviewed. " All users " in this

質問: **112**
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. バンドル ID
C. パッケージ名
D. リダイレクト URI
正解: **(**正解を表示します**)**
When registering an application in Azure Active Directory (Azure AD) for authentication, one of the key configuration items is the redirect URI. According to Microsoft Identity Platform Documentation and the SC-
300 official study guide, the redirect URI (or reply URL) specifies where Azure AD should send the authorization code or access token after a successful sign-in.
The guide explains:
"During app registration, Azure AD requires a redirect URI to identify where authentication responses are sent. For web apps, this must be a valid HTTPS endpoint where your app listens for responses from the Azure AD authorization endpoint." In contrast:
* The executable name, bundle ID, and package name are identifiers relevant to desktop or mobile app packaging and are not part of Azure AD web app registration configuration.
* Only the redirect URI ensures proper return of authentication tokens in OAuth 2.0 and OpenID Connect flows.
Thus, when registering a .NET web app (App1) for Azure AD authentication, you must configure the redirect URI to handle token responses securely.

質問: **113**
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**)**
According to the Microsoft Identity and Access Administrator (SC-300) Exam Study Guide and Microsoft Learn module "Implement and manage hybrid identity with Azure AD Connect", when a VPN solution authenticates users through an on-premises Active Directory and does not natively support Azure MFA, the correct method is to integrate Azure MFA using the Network Policy Server (NPS) extension for Azure MFA.
The NPS extension acts as an intermediary between the VPN server and Azure AD. The VPN server sends authentication requests to the NPS server. The NPS server validates the credentials against the on-premises Active Directory, and then the NPS extension triggers the Azure MFA challenge for secondary authentication.
Microsoft documentation states:
"To enable Azure Multi-Factor Authentication for on-premises resources such as VPNs, RD Gateway, and other services using RADIUS authentication, you must install the Azure MFA extension for the

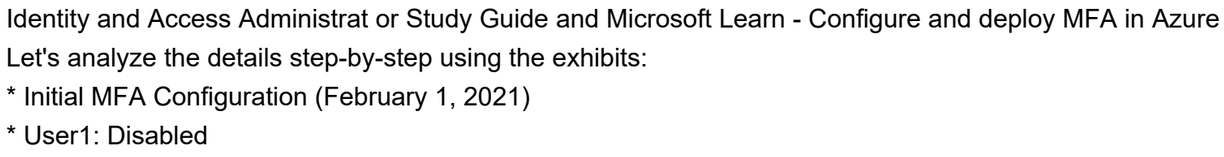
Network Policy Server (NPS)." Therefore, the correct recommendation is to deploy and configure NPS on-premises, install the Azure MFA NPS Extension, and configure the VPN server to forward RADIUS requests to NPS.

質問: **114**

次の表に示す Azure Active Directory (Azure AD) ユーザーを作成します。

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

2021 年 2 月 1 日に、次の図に示すように多要素認証 (MFA) 設定を構成します。



次の表に示すように、デバイス上の Azure AD に対するユーザー認証。

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

2021 年 2 月 26 日、各ユーザーの多要素認証ステータスはどうなりますか?

A.

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B.

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C.

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D.

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

正解: **(**正解を表示します**)**

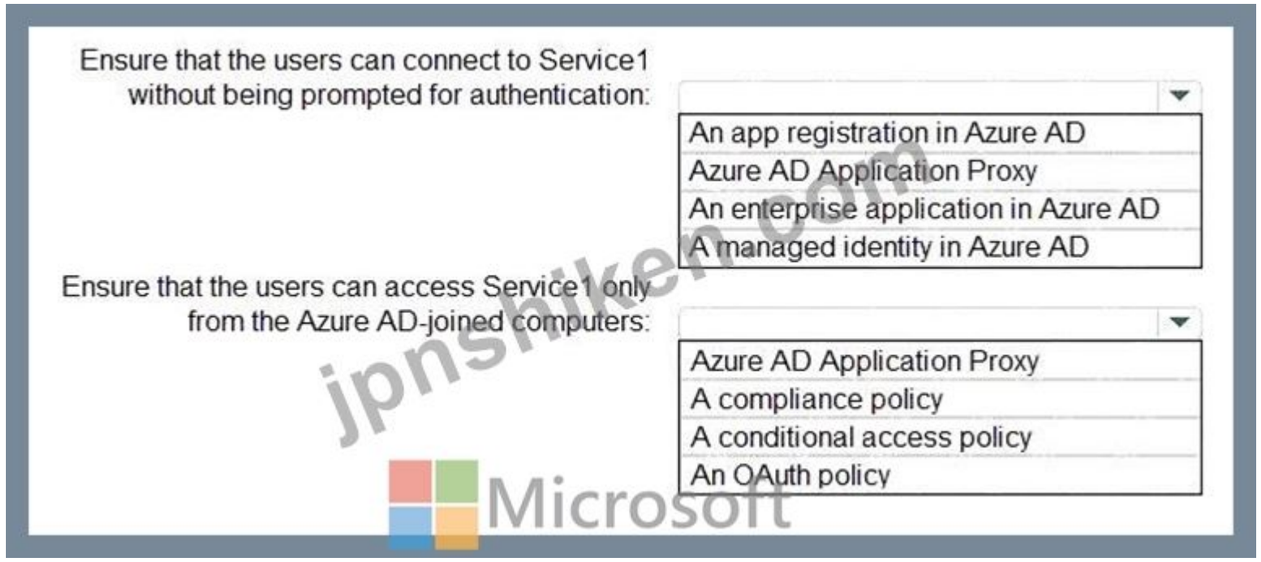
This scenario is based on how Azure AD Multi-Factor Authentication (MFA) statuses transition between Disabled , Enabled , and Enforced states, as documented in the Microsoft SC-300: Microsoft Identity and Access Administrat or Study Guide and Microsoft Learn - Configure and deploy MFA in Azure Active Directory .

Let's analyze the details step-by-step using the exhibits:

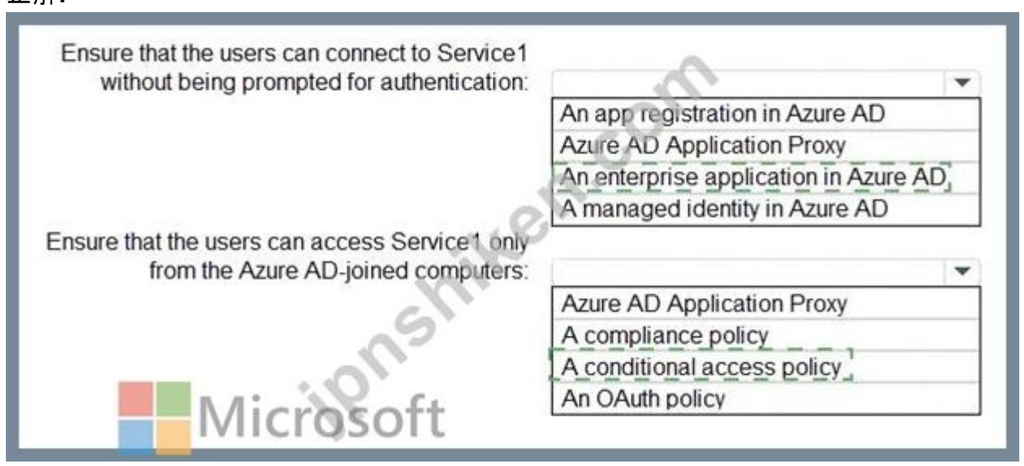
* Initial MFA Configuration (February 1, 2021)
* User1: Disabled
* User2: Enabled
* User3: Enforced
* MFA Policy Setting
* "Allow users to remember multi-factor authentication on devices they trust" is enabled .
* "Number of days users can trust devices for" is 20 days . This means that once a user completes MFA on a trusted device, they won't be prompted again for 20 days on that same device.

* User Sign-in Activity:
* User1: Signs in on Feb 2 and again on Feb 21
* User2: Signs in on Feb 5
* User3: Already in Enforced state (so continuous MFA enforcement applies) State Transitions per Microsoft Documentation:
* Disabled: User cannot register or use MFA.
* Enabled: User is registered for MFA but not yet required at every sign-in. Once they complete registration, they remain Enabled until admin enforces it.
* Enforced: User must use MFA at every sign-in.
Timeline Evaluation:
* User1 wa s initially Disabled , so even though they sign in multiple times (Feb 2 and Feb 21), MFA remains disabled unless the admin manually changes the setting - therefore, User1 = Disabled .
* User2 was Enabled on Feb 1, and signed in on Feb 5 - this allows them to register for MFA (move from Enabled # Enforced) once registration completes. By Feb 26, they would be in Enforced state.
* User3 was already Enforced from the start, and their state remains unchanged.
Thus, by February 26, 2021 , the MFA status should be:
* Use r1: Disabled
* User2: Enforced
* User3: Enforced
This matches Option B exactly.
Microsoft references (Azure AD MFA Overview):
"Enabled users move to Enforced when they complete MFA registration. Enforced users must use MFA every time they sign in."

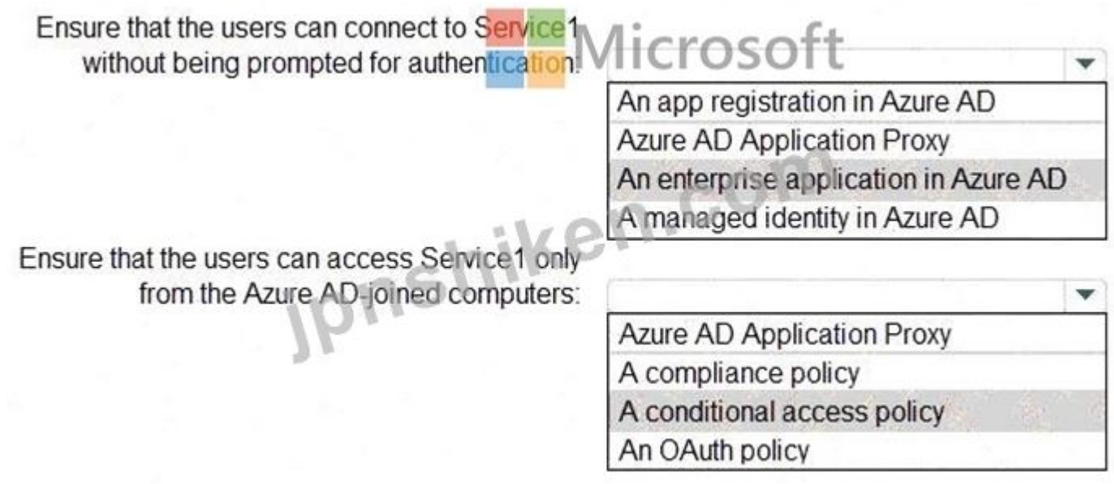
質問**: 115**
会社には Microsoft 365 テナントがあります。
すべてのユーザーは、Windows 10 を実行し、Azure Active Directory (Azure AD) テナントに参加しているコンピューターを所有しています。
会社はService1というサードパーティのクラウドサービスに加入しています。Service1は、OAuthに基づくAzure ADの認証と承認をサポートしています。Service1はAzure ADギャラリーに公開されています。
ユーザーが認証を求められることなくService1に接続できるようにするソリューションを推奨する必要があります。このソリューションでは、Azure ADに参加しているコンピューターからのみユーザーが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。
各要件に対して何を推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn modules on "Implement access management for apps" and "Implement Conditional Access

policies" , Azure AD provides centralized identity and access management for integrated SaaS applications (such as Service1) that support Azure AD authentication and OAuth .
* Ensure that users connect to Service1 without being prompted for authentication: When a third- party application is published in the Azure AD gallery , it supports federated single sign-on (SSO) using SAML, OAuth, or OpenID Connect. Registering the application as an enterprise application (rather than creating a new app registration) enables Azure AD to manage SSO automatically. The Microsoft documentation states:
"Enterprise applications from the Azure AD gallery can be configured for single sign-on so that users can access the app using their Azure AD credentials without being prompted to reauthenticate."
Therefore, to achieve seamless sign-on with minimal administrative overhead, the correct option is An enterprise application in Azure AD .
* Ensure that users can access Service1 only from Azure AD-joined computers: To restrict access based on device compliance or join status, Azure AD uses Conditional Access policies . Conditional Access allows enforcement of conditions such as "Require device to be marked as compliant" or
"Require hybrid Azure AD-joined or Azure AD-joined device." The official Microsoft guidance under
"Plan and implement Conditional Access policies" confirms:
"You can enforce that users only access cloud resources from devices that are Azure AD-joined or compliant by applying Conditional Access device filters." Thus, to ensure that only Azure AD-joined devices can access Service1, you implement a Conditional Access policy .

質問**: 116**
次の表に示すリソースを含む Azure サブスクリプションがあります。

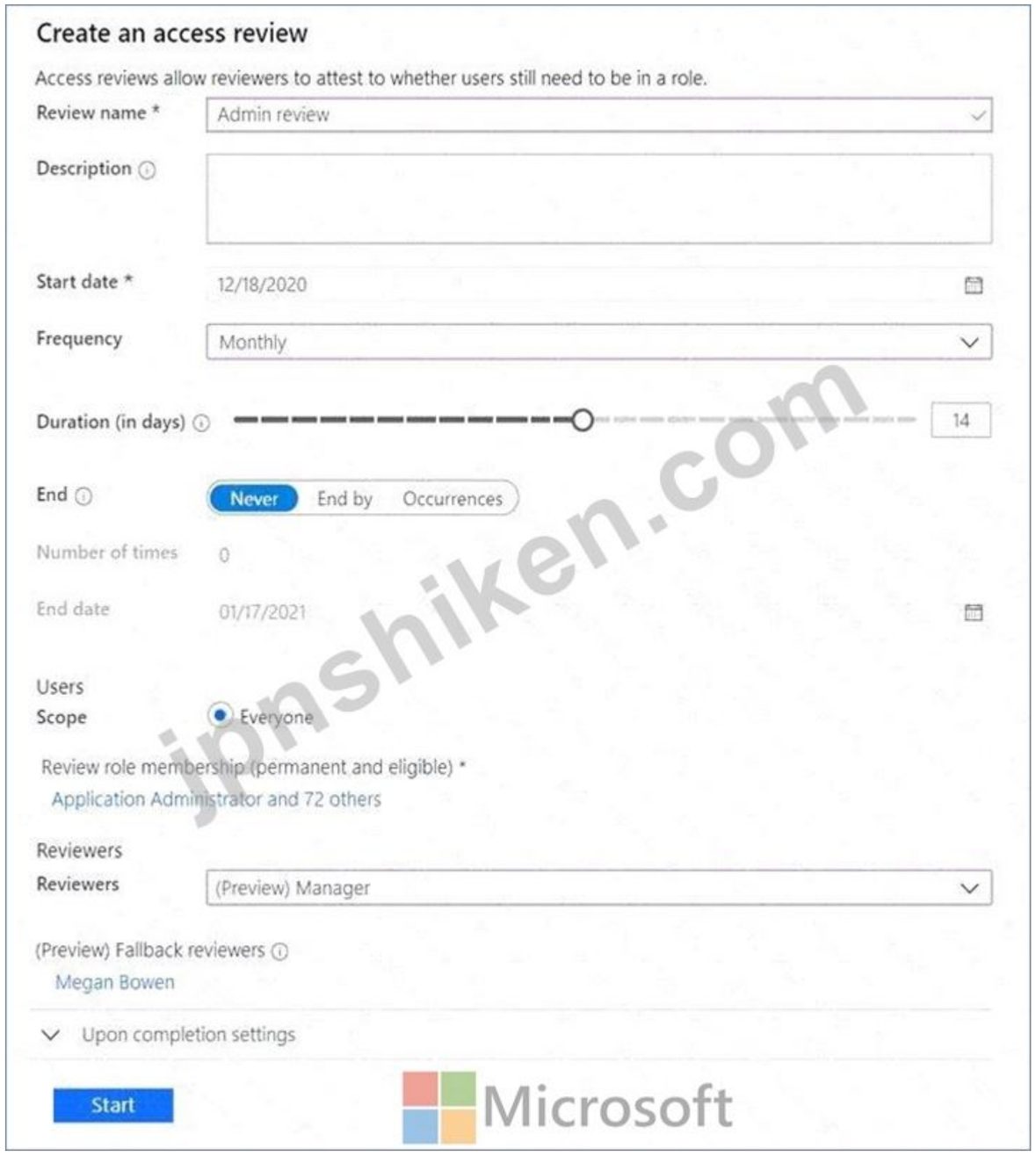
Name	Type
VM1	Virtual machine
App1	Azure App Service
Vault1	Azure Key Vault
storage1	Storage account

属性ベースのアクセス制御 (ABAC) を使用して、リソースへのアクセス許可を付与する必要があります。
どのリソースに権限を付与できますか?
A. Vault1
B. VM1
C. App1
D. storage 1
正解**: (**正解を表示します**)**
According to Microsoft Learn: "Configure Attribute-Based Access Control (ABAC) for Azure resources" , ABAC allows you to assign access permissions based on resource attributes and user attributes (claims).
Currently, ABAC is available for Azure Storage (Blob and Queue) and Azure Key Vault (limited preview for specific scenarios). However, the generally available and supported ABAC implementation as per SC-300 and Azure documentation is for Azure Storage accounts .
This means that you can use ABAC in storage1 to grant fine-grained access (for example, based on object tags or user department claims) while resources like VM1 , App1 , and Vault1 still rely on traditional RBAC (role-based access control).

質問**: 117**
タスク7
サインイン試行が 10 回失敗したら、アカウントを 5 分間ロックアウトする必要があります。
正解**:**
See the Explanation for the complete step by step solution.
Explanation:
To configure the account lockout settings so that accounts are locked out for five minutes after 10 failed sign- in attempts, you can follow these steps:

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

質問**: 118**
注: この問題は、同じシナリオを提示する一連の問題の一部です。一連の問題にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 テナントがあります。10 の部門に分かれて
100 人の IT 管理者がいます。
図に示すアクセス レビューを作成します。(図タブをクリックします。)



すべてのアクセス レビュー リクエストは Megan Bowen によって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取れるようにする必要があります。
解決策: ロールごとに個別のアクセス レビューを作成します。
これは目標を満たしていますか?

A. はい
B. 番号 D18912E1457D5D1DDCBD40AB3BF70D5D

正解: **B** (コメントを発表する)

In this scenario, all access review notifications are going to Megan Bowen, the fallback reviewer, instead of department managers. Creating a separate access review for each role does not meet the requirement because the issue lies in the reviewer selection, not the number of reviews.
Microsoft documentation clarifies:
"To have reviews sent to each user's manager, the reviewer type must be set to 'Manager'. The system uses the 'manager' attribute from Azure AD user properties." Thus, you don't need separate reviews for each role; you need to configure the reviewer type to Manager or update user account manager attributes. Therefore, the proposed solution (creating separate reviews) does not meet the goal.

質問: **119**
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	Microsoft Entra role
User1	Global Administrator
User2	Attribute Definition Administrator
User3	Security Administrator

テナントには、次の表に示す ID が含まれます。

Name	Type
Group1	Security group
Service1	Service principal
MI1	Managed identity

カスタム セキュリティ属性を作成できるのはどのユーザーですか。また、その属性をどの ID に割り当てることができますか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



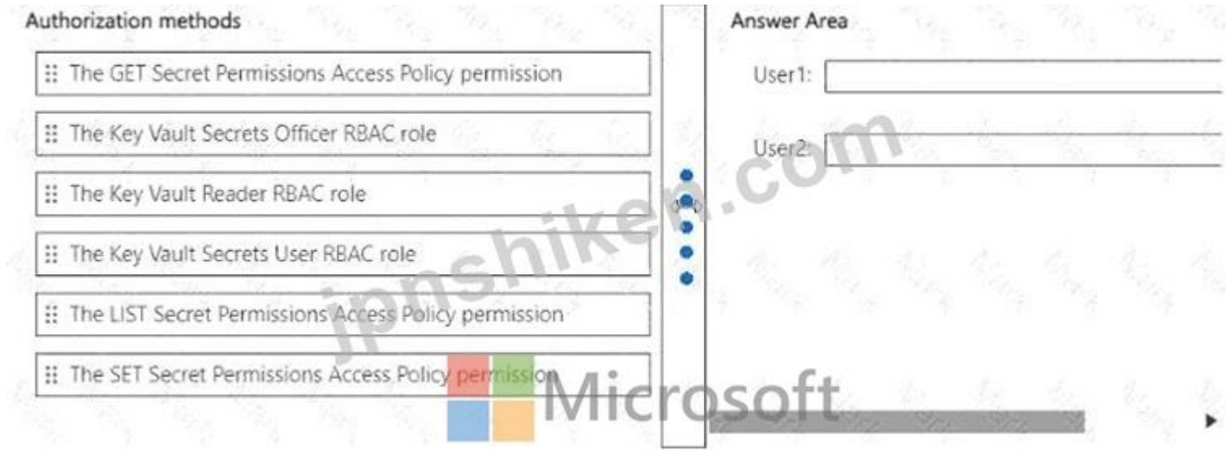
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Learn documentation ("Manage and use custom security attributes in Microsoft Entra ID"), custom security attributes allow administrators to define key-value pairs that can be applied to various Microsoft Entra objects. These attributes can be used for fine-grained access control, app governance, and conditional policies.
Who can create custom security attributes:
Custom security attributes can only be created and managed by users assigned either of these roles:
* Global Administrator
* Attribute Definition Administrator
The Security Administrator role does not have the permissions required to create or modify attribute schema definitions.
Hence, from the table:
* User1 (Global Administrator) #
* User2 (Attribute Definition Administrator) #
* User3 (Security Administrator) #
Therefore, User1 and User2 only can create custom security attributes.
To which identities can custom security attributes be assigned:
As per Microsoft documentation:
"Custom security attributes can be assigned to supported Microsoft Entra objects, including users, groups, service principals, and managed identities." This means attributes can be attached to:
* Group objects (Group1) #
* Managed identities (MI1) #
* Service principals (Service1) #
Thus, the correct assignable identities are Group1, MI1, and Service1 only.

質問: **120**
次の表に示すリソースを含む Azure サブスクリプションがあります。

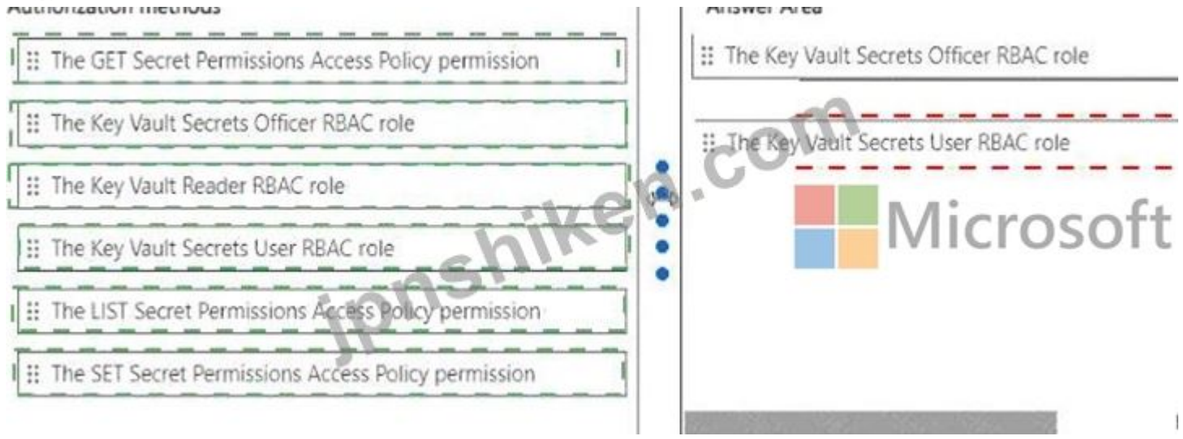
Name	Type	Description
User1	User	*None*
User2	User	*None*
Vault1	Azure Key Vault	Contains a secret named Secret1
Vault2	Azure Key Vault	Contains a secret named Secret2
Secret1	Secret	Stored in Vault1
Secret2	Secret	Stored in Vault2

サブスクリプションでは Privileged Identity Management (PIM) が使用されます。
PIM を使用して次のアクセス制御を構成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ます。
* User2 が Vault2 に保存されているシークレットの内容を読み取ることができることを確認します。
ソリューションは最小権限の原則に従う必要があります。
各ユーザーにはどの認証方法を使用すべきでしょうか？適切な認証方法を適切な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

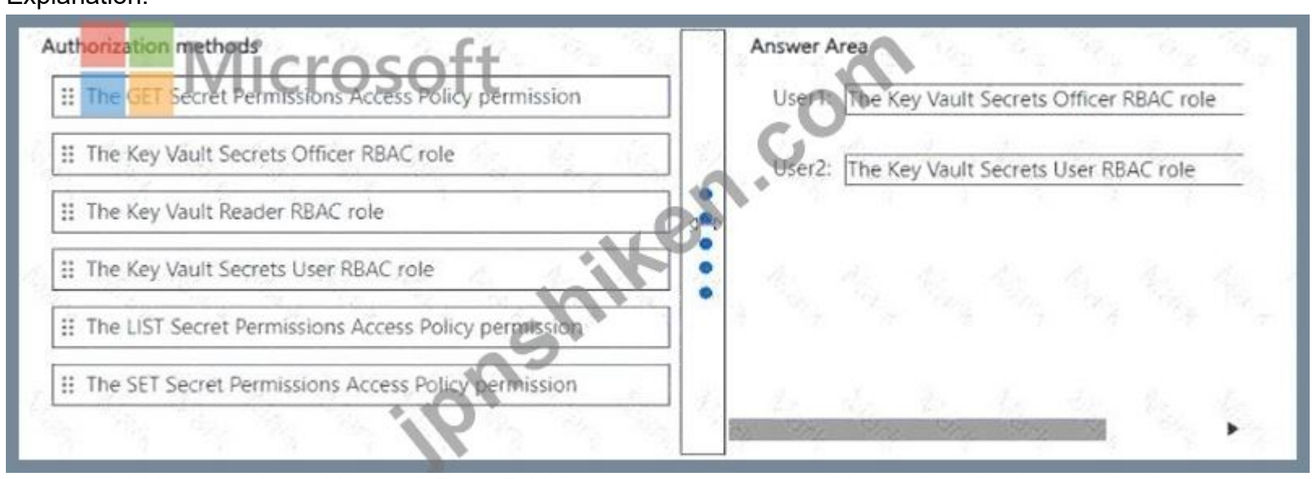
するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



In the SC-300 materials on Microsoft Entra PIM for Azure resources and Azure Key Vault authorization, you' re guided to use Azure RBAC (data-plane roles)-not legacy access policies-when you need time-bound, approvable, least-privilege access managed through PIM. The guide explains that PIM can make users Eligible or Active for Azure resource roles and that Key Vault provides specific data actions via built-in RBAC roles. For secrets, the roles are scoped to a vault (and can be further restricted by resource scope) and are purpose-built:

* Key Vault Secrets Officer - described as allowing a user to "create, read, update, and delete secrets" without granting key or certificate permissions. This precisely satisfies User1's requirement to read and update Secret1 while keeping scope limited to secrets (least privilege compared to broader Owner
/Contributor).
* Key Vault Secrets User - documented to "read secret contents" only. This matches User2's requirement to read the contents of the secrets stored in Vault2 while preventing modification or management actions.
The SC-300 coverage stresses that RBAC roles for Key Vault separate permissions for keys, secrets, and certificates, enabling least privilege and PIM governance (eligible/activation, approvals, MFA, and just-in- time) for access to sensitive data.

質問**: 121**
お客様は、Group1とGroup2という2つのグループを含むMicrosoft 365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	Registered for multifactor authentication (MFA)
User1	Group1	Yes
User2	Group2	Yes
User3	Group2	No

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。
* ユーザー: グループ!
* 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
サインインリスクポリシーには、以下の設定が含まれています。
* ユーザー: グループ2
* サインインリスク: 低以上
* アクセス制御
o アクセスを許可する: 多要素認証を要求する
追加の条件付きアクセス ポリシーは設定されていません。
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。



Microsoft
jpnshiken.com

正解:



Explanation:



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: **122**
ネットワークには、Azure AD テナントと同期するオンプレミスの Active Directory ドメインが含まれています。
ユーザーは、Windows 10 を実行し、ドメインに参加しているコンピューターにサインインします。
Azure AD シームレス シングル サインオン (Azure AD シームレス SSO) を実装する予定です。
Azure AD シームレス SSO をサポートするように Windows 10 コンピューターを構成する必要があります。
何をすべきでしょうか?
A. ローカルイントラネットゾーンの設定を変更する
B. 設定アプリからサインイン オプションを構成します。
C. エンタープライズ状態ローミングを有効にします。
D. Azure AD Connect 認証エージェントをインストールします。
正解: **(**正解を表示します**)**
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Exam Ref SC-300 , Azure AD Seamless Single Sign-On (SSO) allows users on corporate Windows 10 devices connected to the corporate network to automatically sign in to Azure AD-connected services such as Microsoft 365 or Azure without needing to re-enter their credentials.
Seamless SSO works by automatically signing users in using their on-premises Active Directory credentials when they are on the corporate network. This feature is enabled through Azure AD Connect and uses a service account (AZUREADSSOACC) to securely communicate authentication tokens.
However, for Azure AD Seamless SSO to function correctly on domain-joined Windows 10 computers, specific browser configurations are required. In particular, users must be able to automatically

authenticate to the Azure AD SSO endpoint (https://autologon.microsoftazuread-sso.com).
The Microsoft documentation specifies:
"To enable Seamless SSO on Windows devices, ensure that the Azure AD SSO URL (https://autologon.
microsoftazuread-sso.com) is added to the Local intranet zone in Internet Explorer or Microsoft Edge (IE mode). This allows the browser to use the user's current Windows credentials for integrated authentication without prompting." Therefore:
* Option A (Modify the Local intranet zone settings) is correct - adding the Azure AD SSO URL to the Local intranet zone allows integrated Windows authentication to pass through automatically, enabling seamless sign-on.
* Option B (Configure Sign-in options from the Settings app) applies to user-specific credential management but not domain-wide SSO configuration.
* Option C (Enable Enterprise State Roaming) synchronizes settings and credentials across devices but does not enable seamless SSO.
* Option D (Install the Azure AD Connect Authentication Agent) is used for Pass-through Authentication, not Seamless SSO.
From Microsoft Learn's "Plan, deploy, and manage Azure AD Seamless SSO" module:
"To enable users to sign in automatically, configure the browsers and add the Azure AD SSO service URL to the Local intranet security zone. This ensures credentials are passed transparently for single sign-on."
\

質問**: 123**
次のオブジェクトを含むAzureActive Directory（Azure AD）テナントがあります。
Device1という名前のデバイス
User1、User2、User3、User4、およびUser5という名前のユーザー
Group1、Group2、Group3、Group4、およびGroup5という名前のグループ
グループは、次の表に示すように構成されます。

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

Microsoft Office 365 Enterprise E5ライセンスを直接割り当てることができるグループはどれですか？
A. Group1およびGroup4のみ
B. Group1、Group2、Group3、Group4、およびGroup5
C. Group1およびGroup2のみ
D. グループ1のみ
E. Group1、Group2、Group4、およびGroup5のみ
正解**: (**正解を表示します**)**
SC-300 teaches that group-based licensing supports security groups and Microsoft 365 groups, with assigned or dynamic user membership. The guide states: "Licenses can be assigned to groups whose members are users
; nested groups aren't processed and devices cannot be licensed ." Applying this to the table: Group1 (Security-Assigned) and Group2 (Security-Dynamic User) are valid; Group4 (Microsoft 365-Assigned) and Group5 (Microsoft 365-Dynamic User) are also valid. Group3 is a Security-Dynamic Device group and therefore ineligible because "device objects do not receive user licenses." Consequently, the Office 365 E5 license can be assigned directly to Group1, Group2, Group4, and Group5 only.

質問**: 124**
Microsoft Entra テナントがあります。

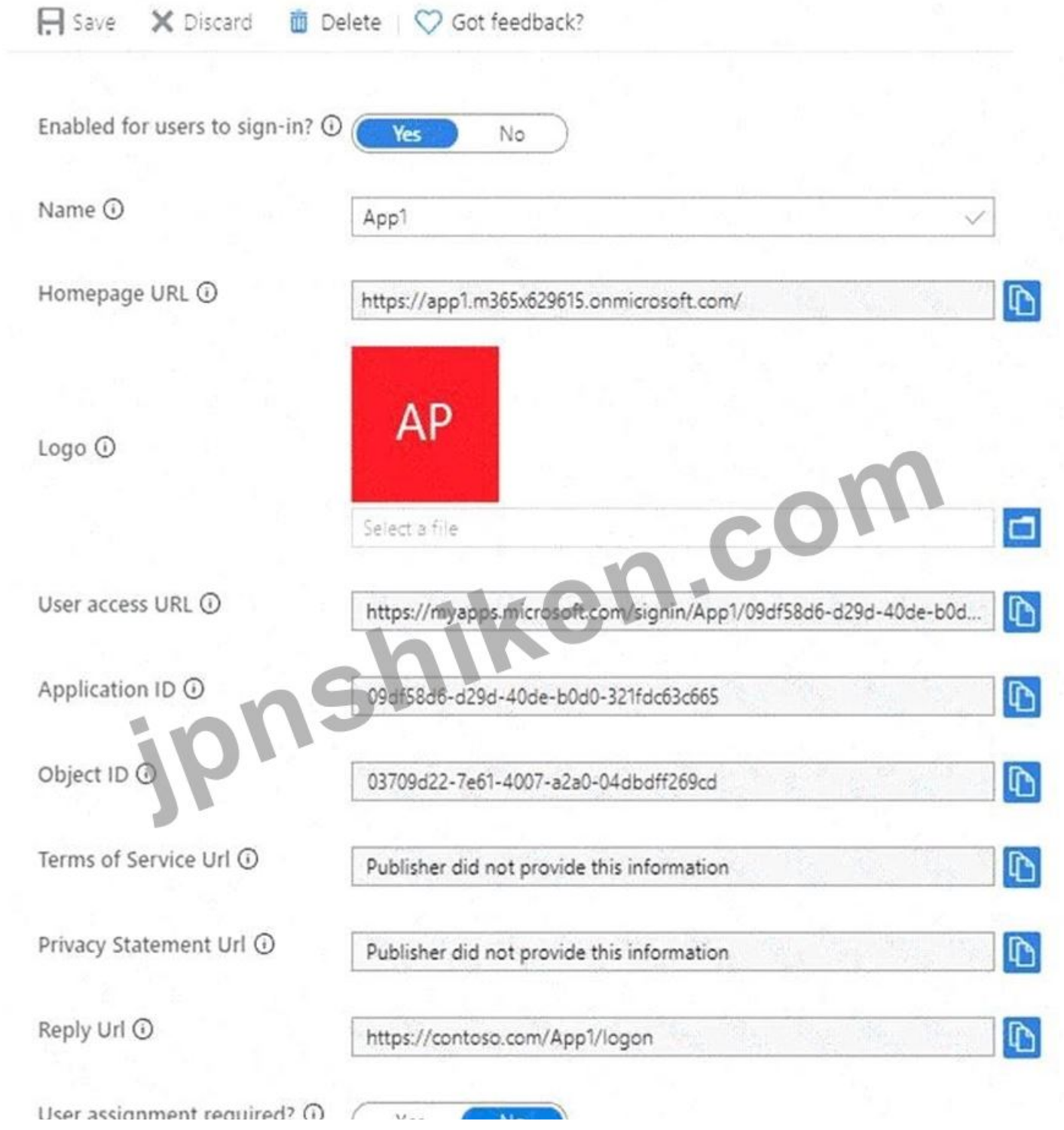
テナントへの管理アクセスを管理するには、条件付きアクセスポリシーを作成する必要があります。このソリューションでは、フィッシング対策が施された多要素認証（MFA）方式を使用して管理者が認証されることを保証する必要があります。
ソリューションに含めるべき 3 つの認証方法はどれですか? それぞれの正解は完全なソリューションを示します。
A. Windows Hello for Business
B. FID02 セキュリティキー
C. 証明書ベースの認証（多要素）
D. 音声通話
E. SMS
F. メールOTP
G. 証明書ベースの認証（単一要素）
H. Microsoft 認証システム
正解: **(**正解を表示します**)**
According to Microsoft's identity and access documentation for Conditional Access and phishing-resistant MFA, phishing-resistant MFA methods are those that cannot be socially engineered or replayed. These are Windows Hello for Business, FIDO2 security keys, and certificate-based authentication (CBA) when configured for multi-factor (e.g., smart card with PIN + certificate).
The SC-300 materials highlight that these are the only methods that fully meet NIST AAL3 phishing resistance requirements. Voice calls, SMS, email OTP, and Microsoft Authenticator are not phishing-resistant because they can be intercepted or phished.
Therefore, when building a Conditional Access policy to secure administrative access, you must allow only phishing-resistant methods to meet Microsoft's best practice.

質問: **125**
Azure サブスクリプションをお持ちです。このサブスクリプションには、Windows Server を実行する仮想マシンが 50 台含まれています。
仮想マシンに対して Microsoft Entra ログインを有効にします。
ユーザーから、Microsoft Entra 資格情報を使用して仮想マシンにサインインできないという報告がありました。
ユーザーが仮想マシンにサインインできることを確認する必要があります。
まず何をすべきでしょうか?
A. 仮想マシンが https://enterpriseregistration.windows.net にアクセスできることを確認します。
B. プライマリ更新トークンを取り消します。
C. Microsoft Entra 管理センターから、仮想マシンのデバイス登録を削除します。
D. OpenSSH の SSH クライアント サポートを有効にします。
正解: **A (**コメントを発表する**)**
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn documentation on "Enable Microsoft Entra login for Windows Server and Windows virtual machines in Azure", successful sign-in to Azure VMs using Microsoft Entra (formerly Azure AD) credentials requires network connectivity to specific Microsoft identity endpoints. One of the most critical endpoints is
https://enterpriseregistration.windows.net , which is used during the device registration and Microsoft Entra Join process.
When you enable Microsoft Entra login for Azure VMs, each VM must register itself as a device in the directory to allow authentication using Entra credentials. If the VM cannot reach the enterprise registration service, the registration fails, meaning the VM will not appear as a valid device in Entra ID. Consequently, users attempting to log in with their Entra credentials will encounter sign-in errors because the system cannot validate their device trust and user token against the identity service.
Microsoft documentation explicitly states:
"To enable Microsoft Entra sign-in to Windows VMs in Azure, the VM must be able to communicate with Microsoft Entra endpoints, including https://enterpriseregistration.windows.net , to complete device registration." Options B, C, and D are unrelated to initial configuration issues. Revoking refresh tokens or deleting device registrations would not resolve connectivity or registration failures. SSH support (option D) is applicable to Linux VMs, not Windows.

質問: **126**

Azure Active Directory (Azure AD) に登録されている、App1 という名前のカスタム クラウド アプリがあります。

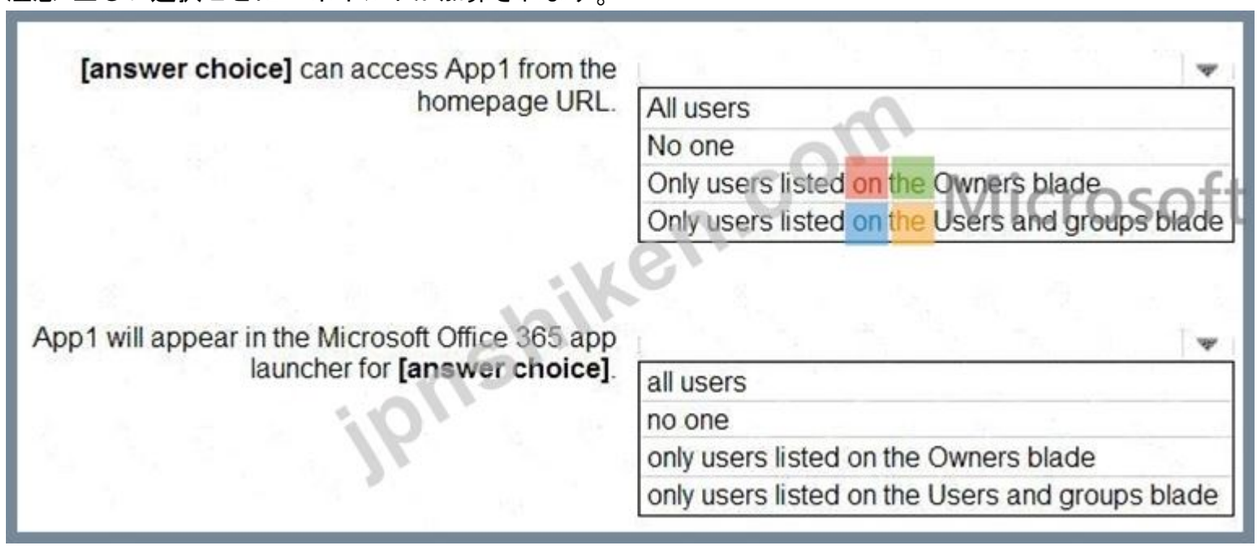
App1 は次の図に示すように構成されています。



jpnshikon.com



ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

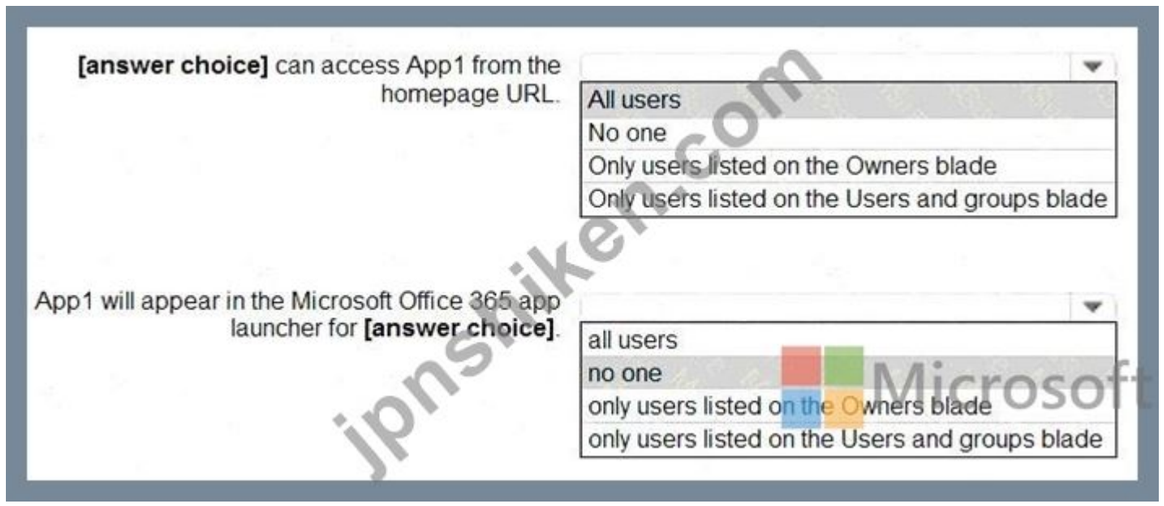


正解:



Explanation:

< [answer choice] can access App1 from the homepage URL: # Only users listed on the Users and groups blade App1 will appear in the Microsoft Office 365 app launcher for [answer choice]: # Only users listed on the Users and groups blade



According to Microsoft's official documentation and the SC-300: Microsoft Identity and Access Administrator study guide, when you register and configure an enterprise application in Azure Active Directory, two specific settings directly influence user visibility and access:

* User assignment required?
* If this option is set to Yes, Azure AD requires users to be explicitly assigned to the app before they can sign in.
* Only users or groups listed on the Users and groups blade (app assignments) will have access.
* This means that even if the application is visible in Azure AD, users not assigned to it cannot authenticate or launch it.
* Visible to users?
* If set to Yes, the app appears in the Microsoft 365 app launcher (also known as the My Apps portal).
* However, when "User assignment required" is Yes, the visibility is limited only to those who are assigned to the app.

From the exhibit:

* "User assignment required?" = Yes
* "Visible to users?" = Yes

This configuration implies:

* Only assigned users (those listed on the Users and groups blade) can sign in to App1 via the homepage URL.
* App1 will appear in the Microsoft 365 app launcher (My Apps portal) only for those same assigned users.

As per Microsoft Learn documentation ("Manage enterprise apps in Azure AD"):

"When User assignment required is set to Yes, only users assigned to the application can access it. If Visible to users is also Yes, the application will appear in My Apps for those assigned users."

質問**: 127**

db1 という名前の Azure SQL データベースを含む Azure サブスクリプションがあります。

App1 に匿名で接続するユーザーに製品情報を提供する、App1 という名前の Azure App Service Web アプリをデプロイします。

App1にdb1へのアクセス権限を与える必要があります。ソリューションは以下の要件を満たす必要があります。

* 資格情報は App1 でのみ使用可能である必要があります。
* 管理上の労力は最小限に抑える必要があります。

どのタイプの資格情報を使用する必要がありますか?

A. ユーザーが割り当てたマネージド ID

B. Azure AD ユーザー アカウント

C. SQL Server アカウント

D. システムによって割り当てられたマネージドID

正解**: (**正解を表示します**)**

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn documentation on Managed Identities for Azure Resources , the recommended and most secure method for an Azure resource (like an App Service) to access another Azure resource (such as an Azure SQL Database) is through Managed Identities.

Managed identities allow Azure services to authenticate securely to other Azure services that support Azure AD authentication, without requiring the use of credentials stored in code, configuration files, or key vaults.

There are two types of managed identities:

* System-assigned managed identity
* Created and tied directly to the lifecycle of a specific Azure resource (e.g., App Service).
* When the resource (App1) is deleted, the identity is automatically deleted as well.
* Best suited when a single resource requires authentication to access another Azure service.
* User-assigned managed identity
* Created as an independent Azure resource.
* Can be assigned to multiple services and managed separately.
* Useful for scenarios requiring shared identity or cross-service authentication management.
* App1 (Azure App Service) must access db1 (Azure SQL Database).
* Credentials should be available only to App1, meaning other resources should not share or reuse the identity.
* Administrative effort should be minimized, implying automatic management of credentials and lifecycle.

Scenario Analysis: Hence, a system-assigned managed identity is the best solution because it meets all three conditions:

* No manual credential management (Azure handles authentication token issuance automatically).
* The identity exists only for App1 (it's unique to that resource).
* Simplified lifecycle - identity is created and deleted automatically with App1.

Official Microsoft Documentation (aligned with SC-300 exam objectives):

"System-assigned managed identities are ideal for scenarios where a single Azure resource requires access to another Azure service and you want Azure to automatically manage the identity's lifecycle."

"Managed identities eliminate the need for developers to manage credentials in code or configuration files."

質問**: 128**

Microsoft 365 サブスクリプションがあり、その中に Site1 という Microsoft SharePoint Online サイトと Group1 という Microsoft 365 グループが含まれています。Group1 のメンバーが Site1 に 90 日間アクセスできるようにする必要があります。管理の手間を最小限に抑えるソリューションが必要です。どのようなソリューションを使用すればよいでしょうか？

A. アクセスレビュー

B. ライフサイクルワークフロー

C. アクセスパッケージ

D. 条件付きアクセスポリシー

正解**: (**正解を表示します**)**

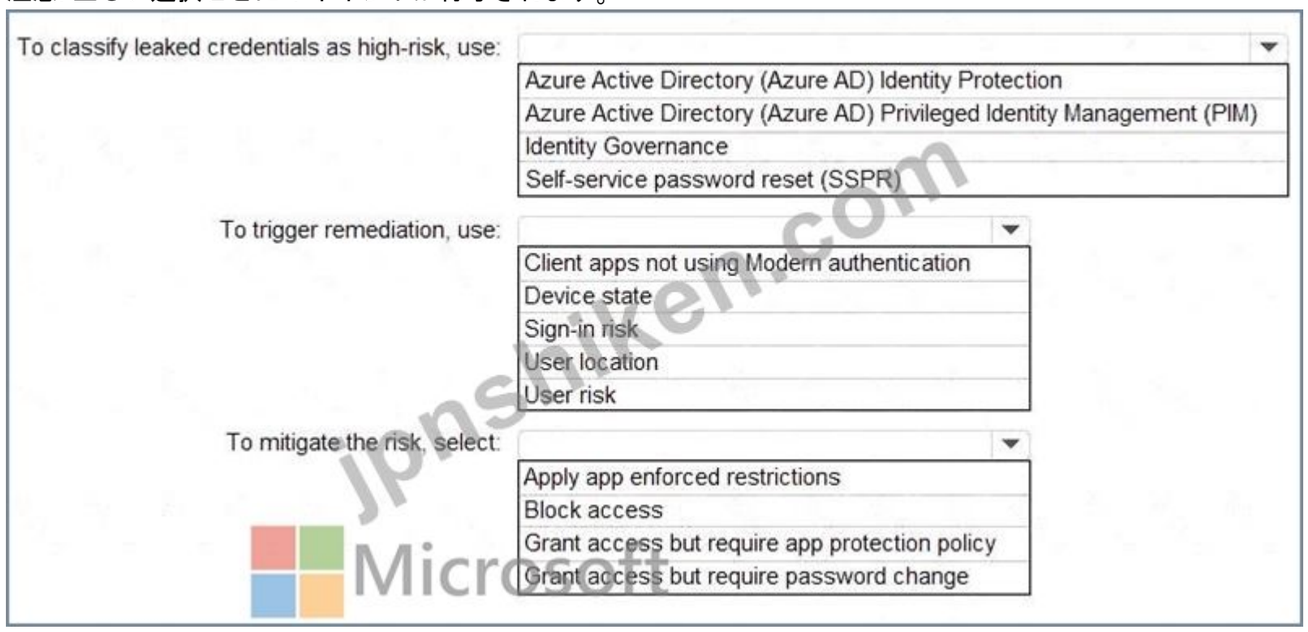
Comprehensive and Detailed Explanation with all Microsoft SC-300: Identity and Access Administrator documents: = According to the SC-300 exam guide and the official Microsoft Entra ID (Azure AD) Entitlement Management documentation, access packages provide a streamlined way to manage resource access lifecycle for users - including SharePoint Online sites, Microsoft 365 Groups, Teams, and applications - with the ability to define time-limited access.

When you configure an access package, you can:

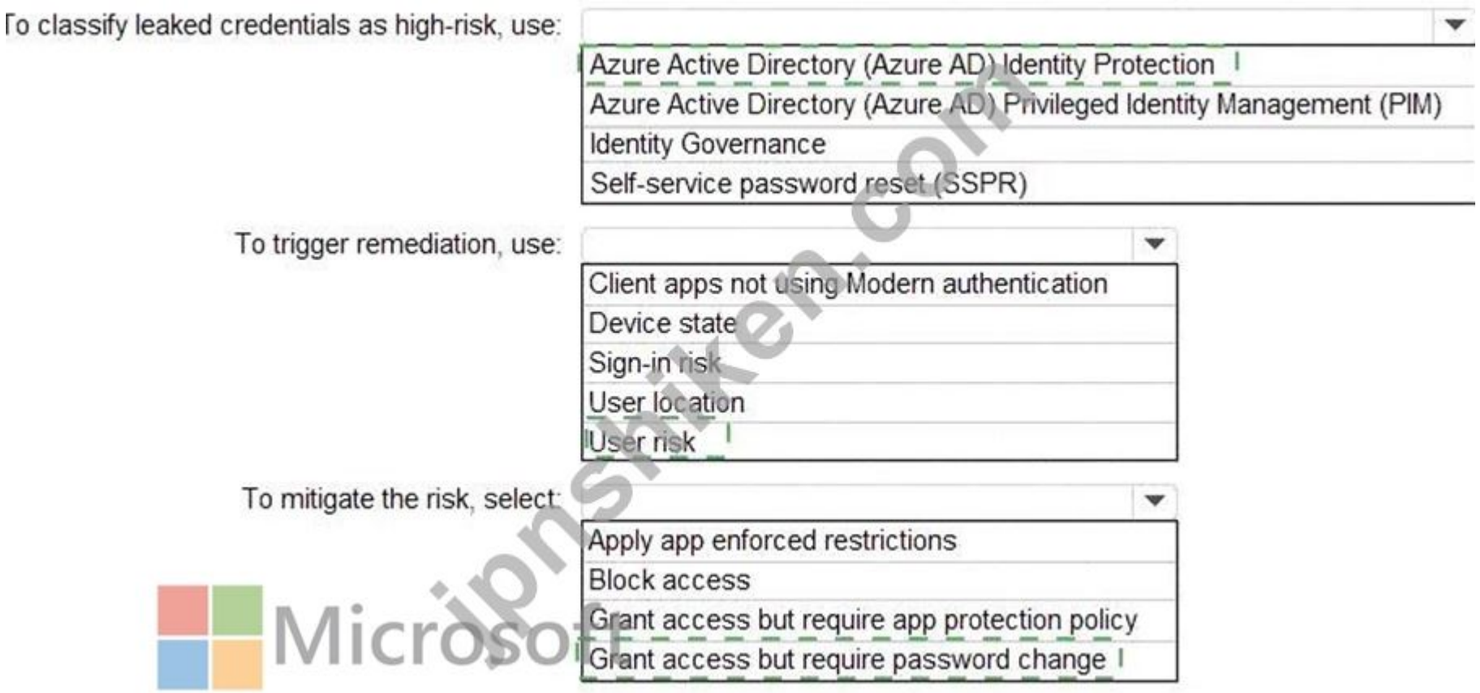
* Include resources like SharePoint Online sites and Microsoft 365 groups.
* Assign users or groups (like Group1) as eligible requesters.
* Set an access duration (for example, 90 days) after which access automatically expires.

The feature requires minimal administrative effort because the process is automated: the access duration ensures that permissions are revoked without manual intervention.
Microsoft documentation confirms:
"Entitlement management access packages enable you to define access policies for users and automatically remove access after a specified time period, minimizing administrative overhead." Therefore, to grant Group1 members access to Site1 for 90 days, the correct and most efficient solution is to use an access package rather than an access review, workflow, or Conditional Access policy.

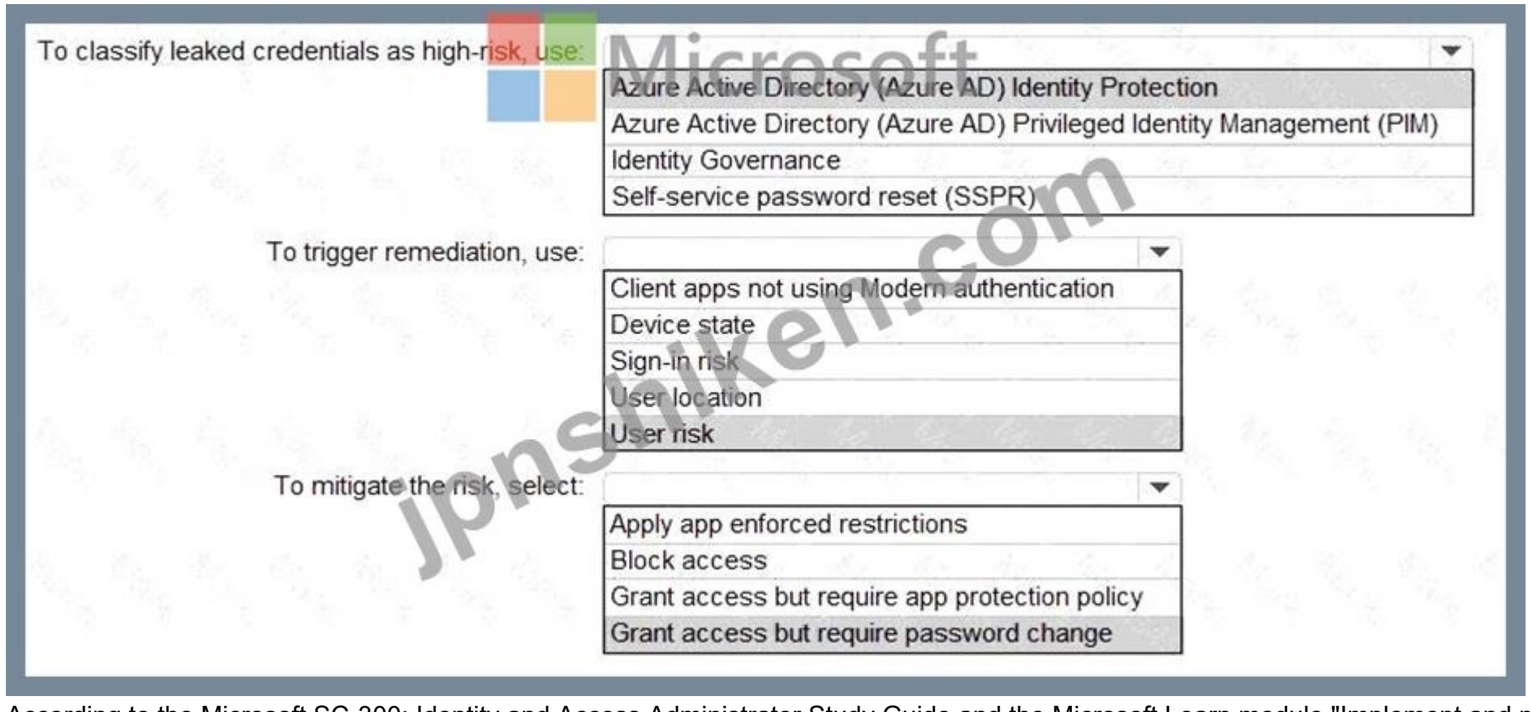
質問**: 129**
Microsoft 365 テナントがあります。
資格情報が漏洩したユーザーを特定する必要があります。ソリューションは以下の要件を満たす必要があります。
* 資格情報が漏洩した疑いのあるユーザーによる ID サインイン。
* サインインを高リスクイベントとして禁止します。
* ユーザーがアプリケーションにアクセスできるようにしながら、リスクを軽減するための制御を直ちに実施します。
何を使うべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解**:**



Explanation:

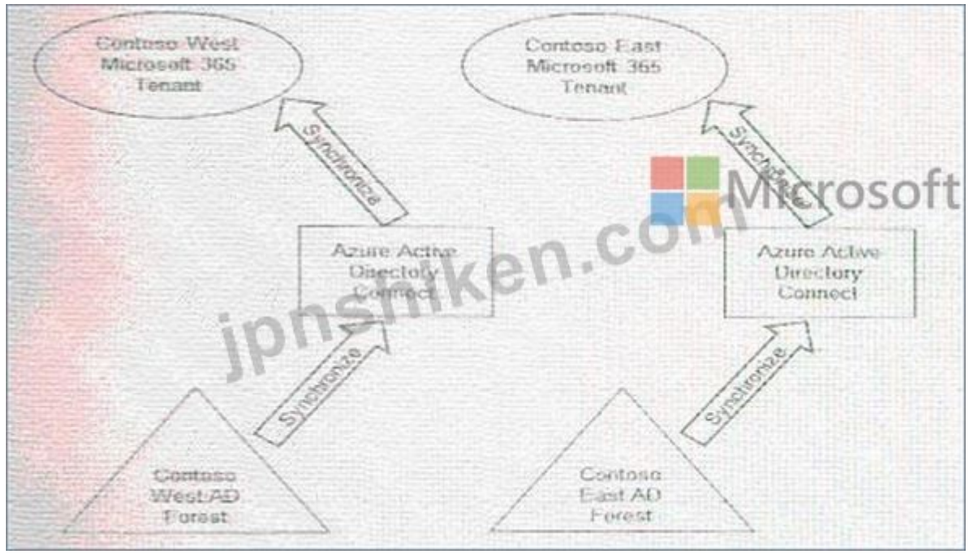


According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Implement and manage Azure AD Identity Protection," Azure AD Identity Protection is the service responsible for detecting risky behaviors such as leaked credentials, suspicious sign-ins, and compromised accounts in a Microsoft 365 or Azure AD environment.

1# # Classify leaked credentials as high-risk Identity Protection automatically flags leaked or compromised credentials detected through Microsoft's threat intelligence signals and dark web monitoring. It classifies these users with a high user risk level.

"Identity Protection detects leaked credentials and marks the user risk as high when evidence of compromise is found." Thus, the feature used for this classification is Azure AD Identity Protection.
2# # Trigger remediation Remediation for leaked credentials is driven by User Risk policies. The User risk policy in Identity Protection can automatically respond to users identified as high-risk. This triggers actions such as forcing a password reset.
"User risk policy can be configured to respond to risky users by requiring password change or blocking access." Hence, User risk is the correct trigger.
3# # Mitigate the risk To allow users to continue accessing applications after remediation, the proper action is Grant access but require password change. This enforces an immediate credential reset to mitigate the compromise but still allows access once the user remediates their risk.
"To automatically remediate high user risk while maintaining access, configure the policy to grant access but require a password change."

質問: **130**
あなたの会社には、Contoso East と Contoso West という名前の 2 つの部門があります。両方の部門の Microsoft 365 ID アーキテクチャを次の図に示します。



Contoso East 部門のユーザーに、Contoso West テナントの Microsoft SharePoint Online サイトへのアクセスを割り当てる必要があります。このソリューションには追加の Microsoft 3G5 ライセンスが必要であってはなりません。
あなたは何をするべきか？
A. Contoso East Active Directory フォレストを Contoso West テナントに同期するように、Contoso Cast の既存の Azure AD Connect サーバーを構成します。
B. Contoso West テナントで Azure AD アプリケーション プロキシを構成します。
C. 2 番目の Azure AD Connect サーバーを Contoso East にデプロイし、Contoso East Active Directory フォレストを Contoso West テナントに同期するようにサーバーを構成します。
D. Contoso East ユーザーを Contoso West テナントのゲストとして招待します。
正解: **(**正解を表示します**)**
In SC-300, Microsoft emphasizes Azure AD B2B collaboration for cross-tenant access without extra Microsoft 365 licensing. The guidance explains that organizations can invite external users as guests to their tenant to access Microsoft 365 resources such as SharePoint Online and Teams , and guest access does not require an additional Microsoft 365 license for the guest . The host tenant remains licensed for the workloads being accessed, and Azure AD billing for B2B collaboration is handled through External Identities (MAU) if configured. The study content also notes that synchronizing a single on-premises AD forest to multiple Azure AD tenants is not a supported topology with a single Azure AD Connect server, and deploying another AAD Connect to sync the same identities to a second tenant introduces complexity and is unnecessary when the requirement is simply to let users in one tenant access resources in another. Application Proxy (publishing on-prem apps) is unrelated to granting SharePoint Online cross-tenant access. Therefore, the minimum-effort, license-compliant approach is to invite Contoso East users as B2B guests in the Contoso West tenant and assign them the required SharePoint permissions.
質問: **131**
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	Member of
User1	Group1
User2	Group2
User3	Group3

テナントには次の表に示す認証方法があります。

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

アプリに表示される番号と携帯電話に表示される番号を照合してクラウド アプリにサインインするユーザーは誰でしょうか?

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**)**

According to Microsoft's SC-300: Microsoft Identity and Access Administrator Study Guide and Exam Ref SC-300 , the behavior of the sign-in process depends on which authentication methods are enabled for the user or their group. Azure AD supports multiple strong authentication methods, such as Microsoft Authenticator app, FIDO2, and SMS, which can be targeted to specific user groups.

The question specifies that the tenant's configuration enables the following methods:

* FIDO2 # Group2 (Yes)
* Microsoft Authenticator app # Group1 (Yes)
* SMS # Group3 (Yes)

And user membership is:

* User1 # Group1
* User2 # Group2
* User3 # Group3

The key phrase in the question is:

"Sign in to cloud apps by matching a number shown in the app with a number shown on their phone." This specific sign-in experience refers to the number matching feature in the Microsoft Authenticator app.

* Number matching is a security enhancement in Azure AD MFA that requires the user to confirm a sign- in by matching a number displayed on the sign-in screen with the number shown in their Microsoft Authenticator app notification.
* According to Microsoft Learn:

"When using the Microsoft Authenticator app for MFA, users will be prompted to enter or match a number displayed on the screen. This feature strengthens authentication by preventing accidental approvals." Therefore:

* Only User1, who is a member of Group1 (the group enabled for Microsoft Authenticator app), will experience number matching when signing in.
* User2 uses FIDO2, which employs a hardware key or biometric verification - not number matching.
* User3 uses SMS, which involves a one-time passcode (OTP) - again, not number matching.

Hence, only User1 will sign in to cloud apps using number matching.

質問**: 132**

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



正解:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn module "Implement and Manage Microsoft Entra Connect" , when organizations need authentication to always validate user passwords directly against the on-premises Ac tive Directory Domain Services (AD DS) environment, the correct configuration is Pass-through Authentication (PTA).

Here's why:

* Pass-through Authentication (PTA) ensures that when a user attempts to sign in to Microsoft Entra ID (formerly Azure AD), their credentials are not validated in the cloud. Instead, the authentication request is securely passed to an on-premises authentication agent, which validates the credentials against the on- premises AD DS domain controller in real time.
* This configuration provides an immediate reflection of on-premises account states - if an account is disabled, locked, or the password is changed, those changes take effect instantly for cloud authentication as well.

To configure PTA, you must use Microsoft Entra Connect, which is the hybrid identity synchronization tool that links on-premises directories to Microsoft Entra ID. During Entra Connect setup, administrators can choose between Password Hash Synchronization, Pass-through Authentication, or Federation as the sign-in method.

Microsoft documentation explicitly states:

"Pass-through Authentication allows users to sign in to both on-premises and cloud-based applications using the same passwords. Authentication occurs against your on-premises Active Directory."

Therefore, to meet the requirement that authentication always validates passwords against the on-premises AD DS domain:

質問: **133**
Microsoft Entra テナントがあります。
次の表に示すエンドユーザー デスクトップ環境があります。

Name	Description
Office staff	Contains Windows 11 devices that are Microsoft Entra joined
Contractors	Contains Windows 11 devices that are Microsoft Entra registered
Frontline workers	Contains Windows 11 Enterprise multi-session remote desktops that are Microsoft Entra joined
Senior managers	Contains Windows 11 single-session hosts that are Microsoft Entra joined
Developers	Contains Windows 365 devices that are Microsoft Entra joined

Global Secure Access を展開する必要があります。
Global Secure Access クライアントはどのような環境にインストールできますか?
A. 請負業者、開発者、最前線で働く人々、オフィススタッフ、そして上級管理職
B. 開発者、オフィススタッフ、上級管理職のみ
C. 最前線の従業員と上級管理職のみ
D. 請負業者とオフィススタッフのみ
正解: **(**正解を表示します**)**

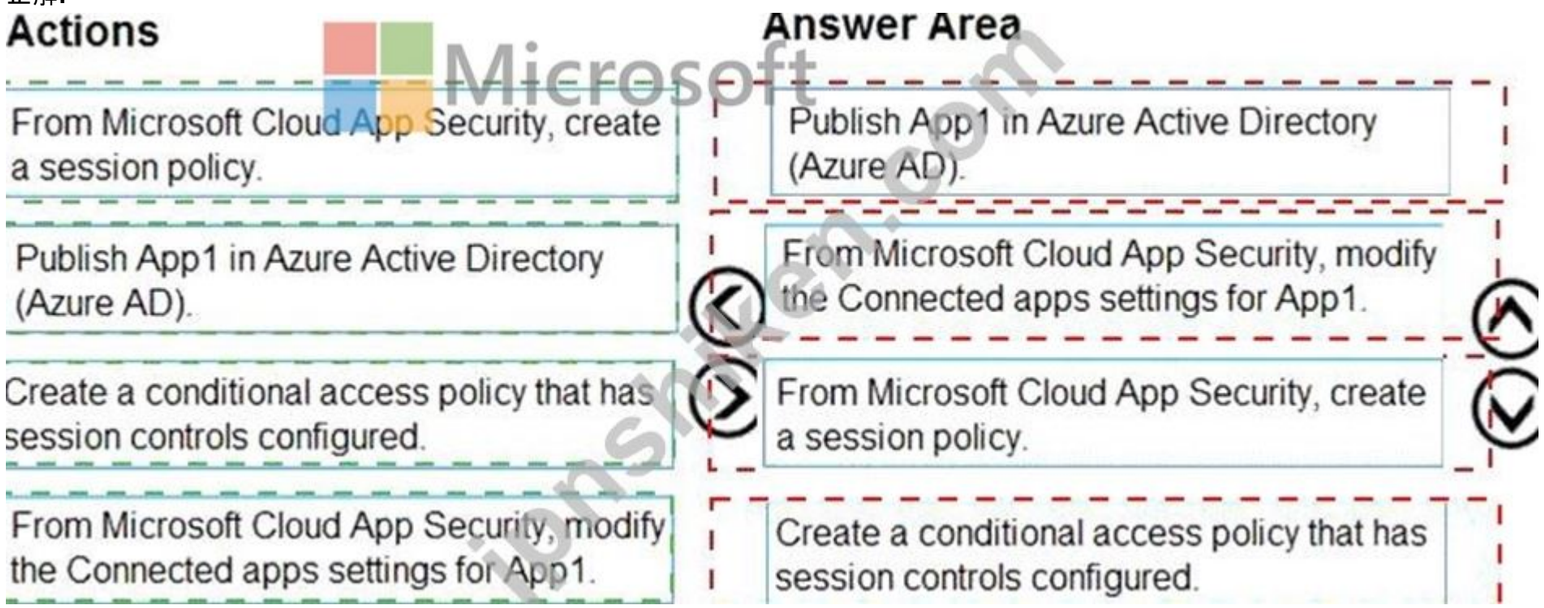
質問: **134**
条件付きアクセス ポリシーを使用する Azure Active Directory (Azure AD) テナントがあります。
条件付きアクセスの使用状況を分析するために、サードパーティのセキュリティ情報およびイベント管理 (SIEM) を使用する予定です。
条件付きアクセス ポリシー データを含む Azure AD ログをダウンロードする必要があります。
Azure AD から何をエクスポートする必要がありますか?
A. JSON形式のサインイン
B. CSV形式のサインイン
C. JSON形式の監査ログ
D. CSV形式の監査ログ
正解: **(**正解を表示します**)**
As per the Microsoft SC-300: Identity and Access Administrator Study Guide and official Microsoft Learn content under "Monitor and troubleshoot Azure AD using reports and logs", Conditional Access policy data is captured in the Sign-ins log within Azure Active Directory. Each sign-in record contains detailed information about the authentication process, including which conditional access policies were evaluated, the policies applied, and their enforcement results (e.g., "Grant access," "Block," or "Require MFA").
The Audit logs in Azure AD, on the other hand, track directory-level changes such as policy creation, modification, or administrative actions - they do not include user authentication or conditional access evaluation data. Therefore, to analyze Conditional Access activity in an external SIEM system, you must export Sign-in logs, which contain the conditional access evaluation details.
Microsoft documentation specifies that exporting in JSON format is preferred for integration with third-party SIEM systems because JSON preserves nested policy evaluation data structures that CSV format cannot fully represent. CSV exports omit detailed conditional access results (e.g., policy IDs and results per policy), making them unsuitable for automated parsing and deep analysis.
Thus, based on official Microsoft documentation:
"Conditional Access policy evaluation results are only available in Sign-in logs and should be exported in JSON format for SIEM integration."
Correct Answer: A. sign-ins in JSON format

質問: **135**
Microsoft 365 E5 テナントがあります。

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 レベルの監視を有効にする必要があります。
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:

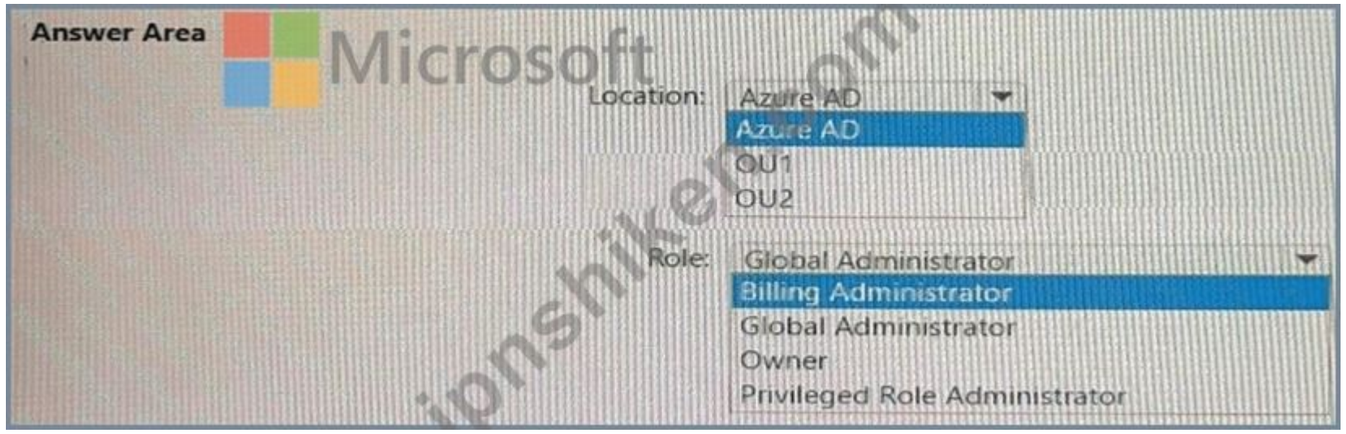


According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Defender for Cloud Apps documentation (formerly Microsoft Cloud App Security, or MCAS), enabling real-time session-level monitoring-known as session control-requires a structured integration between Azure AD Conditional Access and Microsoft Cloud App Security (MCAS).
Here's the correct sequence and rationale:
* Publish App1 in Azure ADThe app must first be registered or published in Azure Active Directory so that it can participate in Conditional Access and App Control integration. Without Azure AD integration, Cloud App Security cannot monitor or enforce policies on the app's traffic.
* Create a Conditional Access Policy with Session ControlsIn Azure AD Conditional Access, you define the conditions (users, apps, risk levels) and set Session controls # Use Conditional Access App Control (Monitor only / Block download). This links Azure AD sign-in events to MCAS for real-time monitoring.
* Modify the Connected Apps Settings in Cloud App SecurityIn Microsoft Cloud App Security, navigate to Connected apps > Conditional Access App Control apps and ensure that App1 is connected. This ensures traffic from Azure AD sign-ins can be intercepted for session-level monitoring.
* Create a Session Policy in Cloud App SecurityFinally, you configure a Session Policy (e.g., monitor file downloads, block uploads, restrict copy/paste, etc.) within Cloud App Security. The session policy enforces the desired controls and visibility in real time when users interact with App1.
This order aligns with Microsoft Learn guidance:
"To monitor user sessions in real time, integrate the app with Azure AD Conditional Access, configure session control, connect the app in Microsoft Cloud App Security, and create session policies."
Final Order:
* Publish App1 in Azure AD
* Create a Conditional Access policy with session controls
* Modify Connected apps settings for App1 in Cloud App Security
* Create a Session policy in Cloud App Security

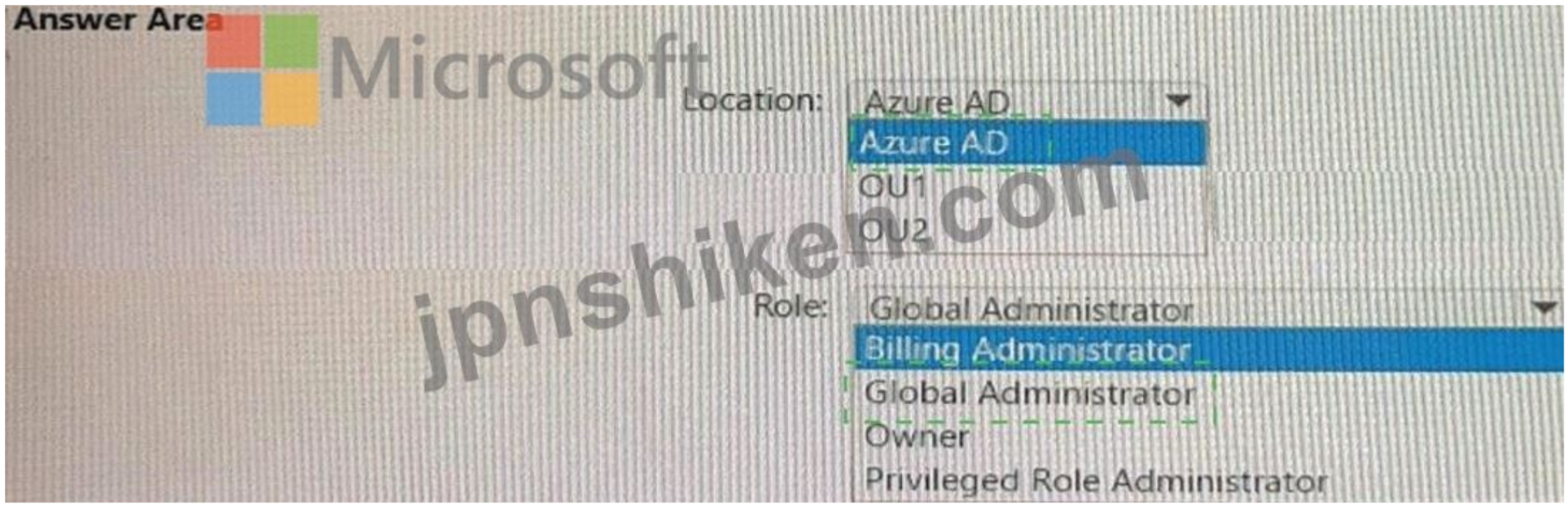
質問**: 136**
ネットワークには、Azure AD テナントと同期するオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。AD DS ドメインには、次の表に示す組織単位 (OU) が含まれています。

Name	Description
OU1	Syncs with Azure AD
OU2	Does **NOT** sync with Azure AD

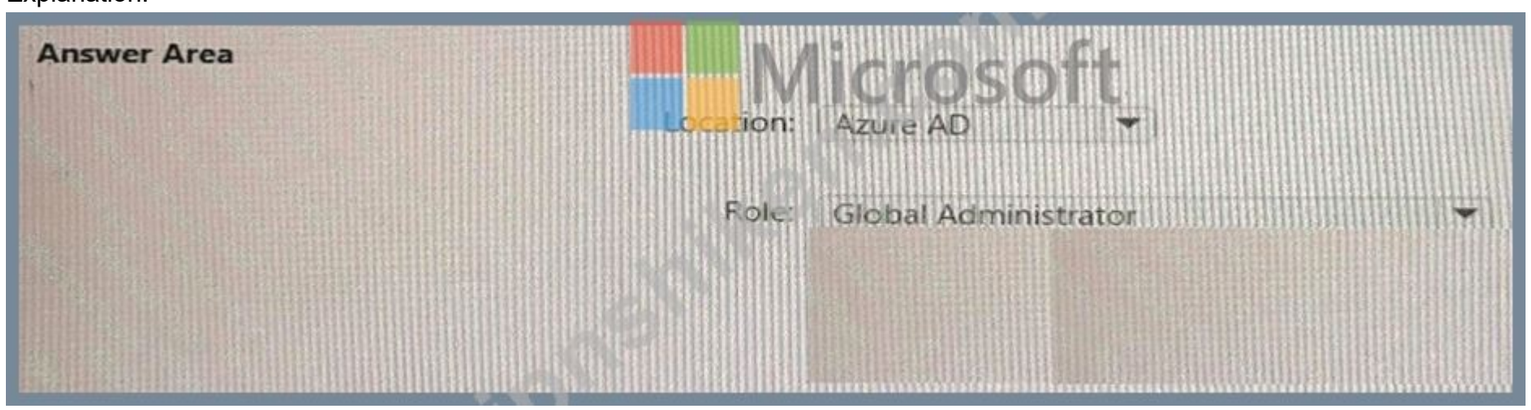
BreakGlass という名前の Break-Glass アカウントを作成する必要があります。
BreakGlass はどこで作成し、BreakGlass にはどのようなロールを割り当てる必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Entra ID documentation , a break-glass account (also known as an emergency access account) is a cloud-only account that must not depend on any on-premises identity infrastructure, such as Active Directory synchronization or conditional access.

* Location: The break-glass account must be created directly in Azure AD (cloud-only) - not in an on- premises Organizational Unit (OU1 or OU2).

* OU1 syncs with Azure AD, meaning if on-premises synchronization fails or the domain controller is unavailable, accounts in OU1 might not authenticate.
* OU2 doesn't sync at all, so creating the account there wouldn't provide Azure AD access.
Therefore, the only resilient option is Azure AD (cloud-only) to ensure access even if directory sync or on-premises systems are unavailable.
* Role: Microsoft recommends assigning the Global Administrator role to break-glass accounts. This ensures full tenant recovery capability in emergencies such as Conditional Access lockouts or MFA misconfiguration.
* The Billing Administrator or Privileged Role Administrator roles don't provide sufficient rights to recover access or modify Conditional Access settings.
* The Global Administrator role has full control over all Azure AD resources and configuration settings.
Reasoning: Microsoft documentation states:
"Create at least two cloud-only emergency access accounts with the Global Administrator role. These accounts must be excl uded from Conditional Access policies and protected with strong authentication methods."

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: **137**
あなたの会社には、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	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

次の表に示すアプリの登録があります。

App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

会社のポリシーにより、ユーザー権限の変更が禁止されています。
会社の各ユーザーのカレンダーで予定を作成できるのはどのユーザーですか?
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: **C** (コメントを発表する)
Microsoft Graph permissions can be of two types: Delegated and Application.
* Delegated permissions require a signed-in user and can access only that user's data.
* Application permissions are used by background services or daemons to access data across the organization without user consent if the app is granted admin consent.

In the scenario:
* App1 (User1) uses Delegated # can access only the user's data.
* App2 (User2) uses Delegated and Application (Calendars.ReadWrite) # can create appointments across all users. However, User2 has no role to grant consent for application-level permissions.
* App3 (User3, User4) uses Application (Calendars.Read) # only read, not write permissions.
Since User3 is an Exchange administrator, they have the authority to grant admin consent to an application.
Although App3 only has "Read," the Exchange administrator can manage calendar data organization-wide and can create appointments using Exchange management tools.
Hence, as per Microsoft's permissions model and SC-300 guidance, User3 is the only user who has both role and access capabilities to create appointments in every user's calendar.

質問: **138**
米国東部 Azure リージョンに Managed1 というユーザー割り当てマネージド ID を含む Azure サブスクリプションがあります。サブスクリプションには、次の表に示すリソースが含まれています。

Name	Type	Location
VM1	Virtual machine	West US
storage1	Storage account	East US
WebApp1	Azure App Service app	East US

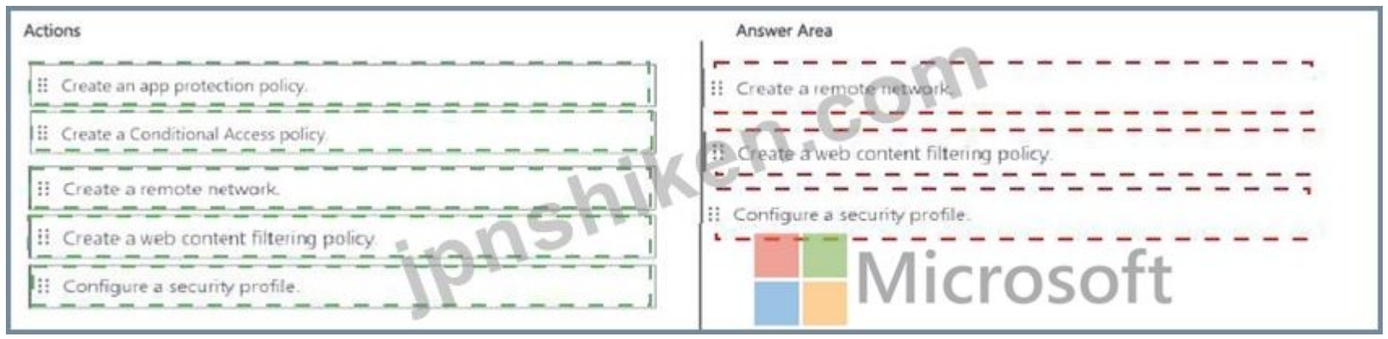
どのリソースが Managed 1 を ID として使用できますか?
A. VM1、ストレージ1、WebApp1
B. storage1 と WebApp1 のみ
C. WebApp1 のみ
D. VM1 と WebApp1 のみ
正解: **A** (コメントを発表する)

質問: **139**
Microsoft 365 E5 サブスクリプションをご利用です。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 台含まれており、これらのデバイスに Global Secure Access クライアントを展開します。
ユーザーがデバイスから httpsy/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 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクションリストから回答領域に移動し、正しい順序で並べます。

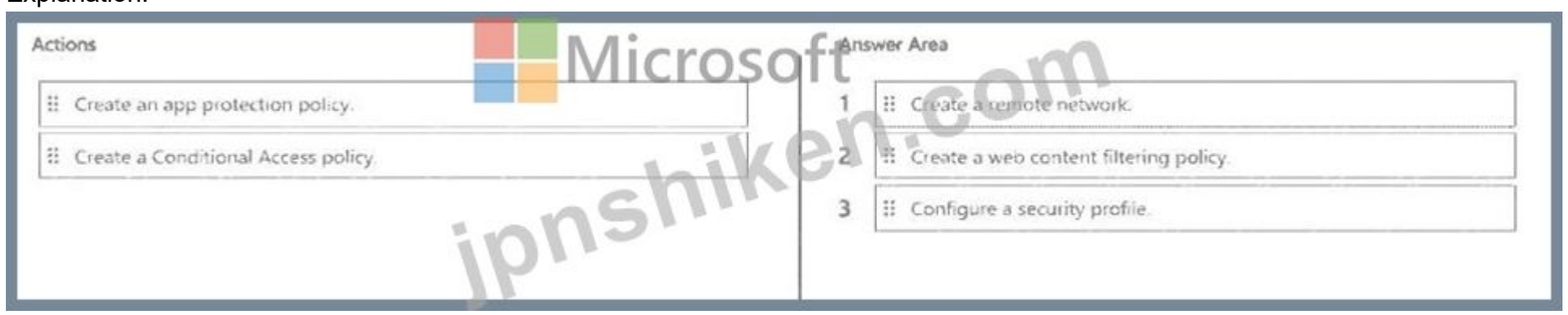


Microsoft
jpnshiken.com

正解:



Explanation:



In a Microsoft 365 E5 environment with Global Secure Access (Microsoft Entra Internet Access) deployed, to block users from accessing a specific website (for example, https://contoso.com), the configuration process involves creating network, filtering, and security control components in sequence.

According to the Microsoft SC-300 Study Guide and official Microsoft Learn module "Configure Microsoft Entra Internet Access and Private Access", the required workflow is as follows:

* Create a remote network - This step establishes the connectivity fabric that links user devices (running the Global Secure Access client) with the Microsoft Entra Global Secure Access services. It defines network parameters and routes traffic through the Microsoft Entra inspection layer.
* Create a web content filtering policy - Within Microsoft Entra Internet Access, administrators can define filtering rules that control outbound web traffic. Here, you would add https://contoso.com as a blocked domain or URL category. This policy ensures that traffic destined for that domain is denied.
* Configure a security profile - Security profiles combine web content filtering policies, Conditional Access policies, and inspection settings. You then assign the security profile to the remote network or user group so the filtering rule applies to traffic from the enrolled devices.

These steps align with Microsoft's recommended process to "create a remote network, define filtering policy, and link via a security profile" for enforcing secure outbound access control through Global Secure Access.

質問**: 140**

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

このセクションの質問に回答すると、その質問に戻ることはできなくなり、これらの質問はレビュー画面に表示されなくなります。

Microsoft 365 E5 サブスクリプションをお持ちです。

User1 という名前のユーザーを作成します。

User1 が ID セキュア スコア改善アクションのステータスを更新できることを確認する必要があります。

解決策: ユーザー管理者の役割を User1 に割り当てます。

これは目標を達成していますか?

A. はい

B. いいえ

正解**: B (**コメントを発表する**)**

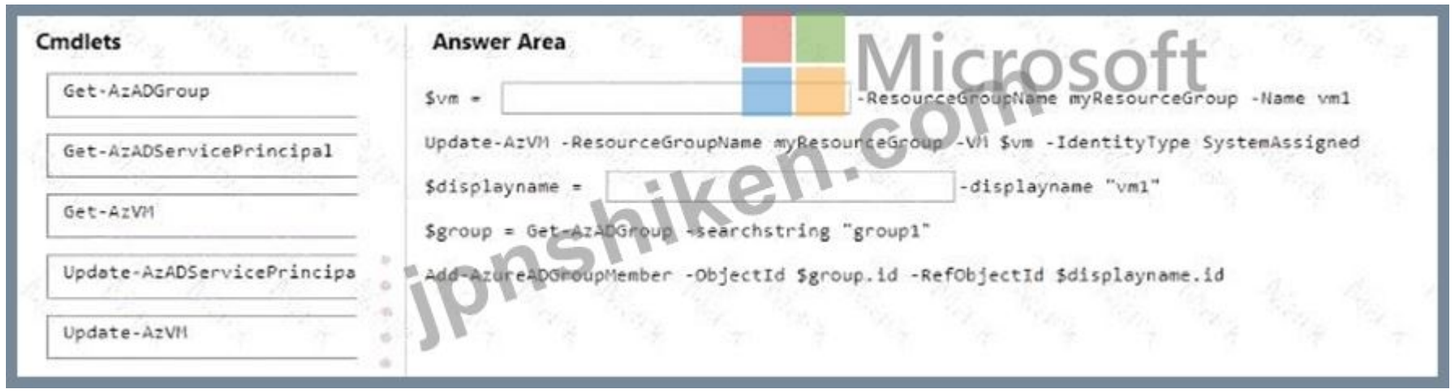
The User Administrator role allows management of user accounts, licenses, and group memberships within Azure AD but does not grant access to security configurations, Secure Score dashboards, or improvement actions.
According to Microsoft's Secure Score documentation:
"Only users with Global Administrator, Security Administrator, or Security Reader roles can access Microsoft Secure Score. To modify improvement action statuses, the user must be a Security Administrator or Global Administrator." Therefore, a User Administrator cannot update Secure Score improvement actions.

質問: **141**
注: この問題は、同じシナリオを提示する一連の問題の一部です。一連の問題にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
Microsoft Entra テナントに同期する Active Directory フォレストがあります。
Active Directory でユーザー アカウントが無効になっている場合でも、無効になっているユーザーは最大 30 分間 Microsoft Entra に対して認証できることがわかります。
Active Directory でユーザー アカウントが無効になっている場合は、そのユーザー アカウントが直ちに Microsoft Entra に対して認証されないようにする必要があります。
解決策: Microsoft Entra パスワード保護を構成します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解: **B (**コメントを発表する**)**
The SC-300 curriculum emphasizes synchronization behavior between on-premises Active Directory (AD) and Microsoft Entra ID using Microsoft Entra Connect. By default, directory synchronization occurs every 30 minutes, which means a user disabled in AD can still authenticate to Microsoft Entra for up to 30 minutes until the next synchronization cycle.
The proposed solution- Microsoft Entra Password Protection -is not related to authentication delay or sign-in blocking. Password Protection enforces strong password policies and prevents the use of weak or compromised passwords during account creation or reset. It does not control sign-in states or enforce real- time disablement.
To meet the goal of immediately blocking authentication when an account is disabled in AD, you must implement Microsoft Entra Connect with Pass-through Authentication (PTA) or federation (AD FS) . These options validate sign-ins against the on-premises AD in real time, ensuring instant blocking of disabled accounts.
Microsoft documentation confirms:
"Password Protection does not affect authentication latency or synchronization frequency. To ensure disabled accounts cannot sign in, use Pass-through Authentication or federation for real-time validation."

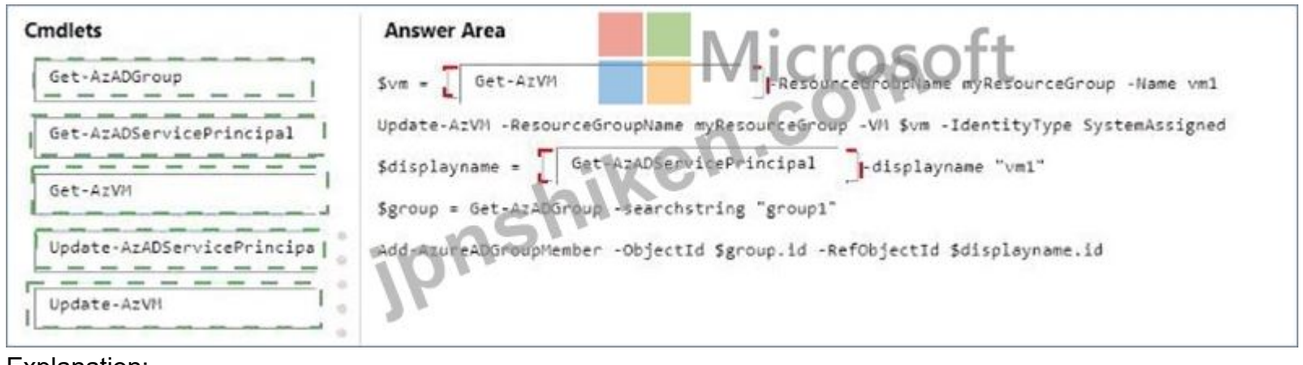
質問: **142**
Microsoft Defender for Cloud Apps および Yammer を使用する Microsoft 365 ES サブスクリプションがあります。
ユーザーがリスクの高い場所から Yammer にサインインできないようにする必要があります。
Microsoft Defender for Cloud Apps ポータルでは何をすればよいですか?
A. アクセス ポリシーを作成します。
B. アクティビティ ポリシーを作成します。
C. ヤマーを不当に扱う。
D. 異常検出ポリシーを作成します。
正解: **A (**コメントを発表する**)**
Defender for Cloud Apps (MCAS) provides Access policies to control sign-in and session access to sanctioned apps based on conditions such as user, device, and location. SC-300 notes that access policies can allow, block, or require additional controls and are evaluated at sign-in, making them appropriate to prevent logons from risky or specific locations. In contrast, Activity policies alert on or govern in-app actions (downloads, sharing) after sign-in, and Anomaly detection policies use heuristics to surface suspicious behavior, not enforce blocking. "Unsanctioning" an app merely flags it and can

integrate with firewall/proxy tagging; it does not directly enforce a conditional sign-in block. Therefore, to block Yammer sign-ins from high-risk locations, you create an Access policy in Defender for Cloud Apps targeting Yammer with a condition for the designated high-risk locations and set the action to Block (or require step-up).

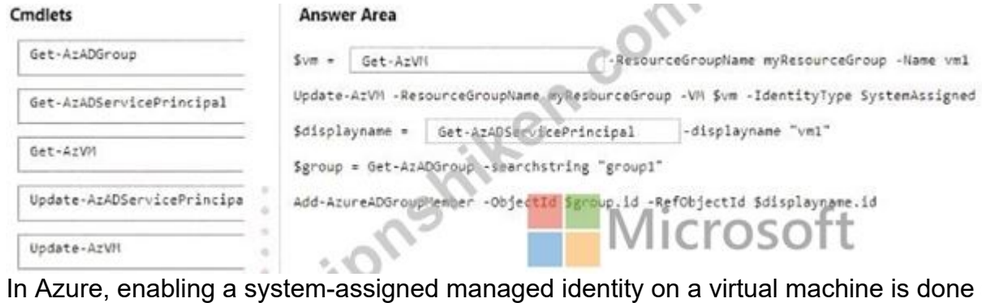
質問: **143**
contoso.com という Microsoft Entra テナントにリンクされた Azure サブスクリプションがあります。このサブスクリプションには、Group1 というグループと VM1 という仮想マシンが含まれています。
次の要件を満たす必要があります。
* VM1 に対してシステム割り当てマネージド ID を有効にします。
* VM1をGroup1に追加します。
PowerShell スクリプトはどのように完成させるべきでしょうか？適切なコマンドレットを適切なターゲットにドラッグしてください。各コマンドレットは、1 回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



In Azure, enabling a system-assigned managed identity on a virtual machine is done on the VM resource itself. With the Az PowerShell module, you first retrieve the VM object and then update it to enable the identity. The correct sequence is to call Get-AzVM to load VM1 into a vari able and then Update-AzVM - IdentityType SystemAssigned to turn on the built-in identity for that VM. After the

identity is enabled, Azure AD automatically creates a service principal that represents the VM's managed identity. To add this identity to an Azure AD security group (Group1), you must reference that service principal. The Az.Resources cmdlet Get-AzADServicePrincipal -DisplayName " vm1 " returns the service principal object for the VM's system- assigned identity. You then look up the target group with Get-AzADGroup and add the service principal as a member using Add-AzureADGroupMember , passing the group's ObjectId and the service principal's Id.
This aligns with Microsoft guidance that VM system-assigned identities are represented in Entra ID as service principals , and that group membership operations use the service principal's object id when adding an application/managed identity to a group.
Filled script:

```
$vm = Get-AzVM -ResourceGroupName myResourceGroup -Name vm1
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned
$displayname = Get-AzADServicePrincipal -DisplayName " vm1 "
$group = Get-AzADGroup -SearchString " group1 "
Add-AzureADGroupMember -ObjectId $group.Id -RefObjectId $displayname.Id
```

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

Security questions:Users answer predefined security questions they set up during registration.
Important Note:Methods like smartcards, FIDO2 security tokens, and Windows Hello are not supported for SSPR. These methods are typically used for authentication during sign-in (e.g., MFA or passwordless sign- in), not for the SS PR process.
Analysis of the Options:
A). A smartcard:
Smartcards are a form of certificate-based authentication often used for sign-in to Windows devices or VPNs.
They require a physical card and a reader, and they are typically used for primary authenticat ion, not for SSPR.
Microsoft Entra ID SSPR does not support smartcards as an authentication method for password reset.
Smartcards are not listed as an available method in the SSPR configuration settings.
Conclusion:This is incorrect.
B). A mobile app code:
A mobile app code refers to a time-based one-time password (TOTP) generated by an authenticator app, such as the Microsoft Authenticator app.
This is a supported method for SSPR in Microsoft Entra ID. Users can register the Microsoft Authenticator app (or another compatible app) and use the generated code to verify their identity during a password reset.
Since the setting " Number of methods required to reset: 1 " means only one method is needed, a mobile app code is a valid option if the user has registered it.
Conclusion:This is correct.
C). An FIDO2 security token:
FIDO2 security tokens (e.g., YubiKey) are hardware-based security keys that support passwordless authentication in Microsoft Entra ID. They are part of Microsoft's passwordless authentication stra tegy and can be used for sign-in.
However, FIDO2 security tokens are not supported for SSPR. The SSPR process does not allow users to verify their identity using a FIDO2 security key because the reset process is designed to work with simpler, more accessib le methods like email, SMS, or app-based codes.
Conclusion:This is incorrect.
D). A Windows Hello PIN:
Windows Hello PIN is a device-specific authentication method used to sign in to Windows devices. It is part of Windows Hello, which also includes biometric authentication (e.g., facial recognition, fingerprint).
Windows Hello PIN is not supported for SSPR in Microsoft Entra ID. The SSPR process occurs in a web- based portal (e.g., aka.ms/sspr) and does not integrate with device-specific authenticatio n methods like Windows Hello. Additionally, Windows Hello PIN is tied to a specific device, whereas SSPR is designed to be device-agnostic.
Conclusion:This is incorrect.
Additional Considerations:
The setting " Require users to register when signing in: Yes " ensures that users have at least one authentication method registered. However, the question does not specify which methods are enabled by the administrator. In Microsoft Entra ID, the default enabled methods for SSPR typically include email, mobile phon e (SMS), mobile app code, and mobile app notification. Security questions may also be enabled but are less common due to security concerns.
If the administrator has disabled certain methods (e.g., mobile app code), the answer could change. However, the que stion does not indicate any such restrictions, so we assume the default methods are available.
The " Number of methods required to reset: 1 " setting means users only need to use one method to reset their password, but they may have multiple methods registered. The question asks for a " valid authentication method available to users, " so we need to identify a method that SSPR supports.
Conclusion:Based on the SSPR settings and the supported authentication methods in Microsoft Entra ID:
A mobile app cod e (option B) is a valid authentication method for SSPR, as it is supported by default and aligns with the configuration.
Smartcards, FIDO2 security tokens, and Windows Hello PIN are not supported for SSPR.Therefore, the correct answer isB.
References:
Micr osoft Entra ID documentation: " Self-service password reset authentication methods " (Microsoft Learn:

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#authentication- methods) Microsoft Entra ID documentation: " Configure self-service password reset " (Microsoft Learn:https://learn.
microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers SSPR configuration and supported authe ntication methods.

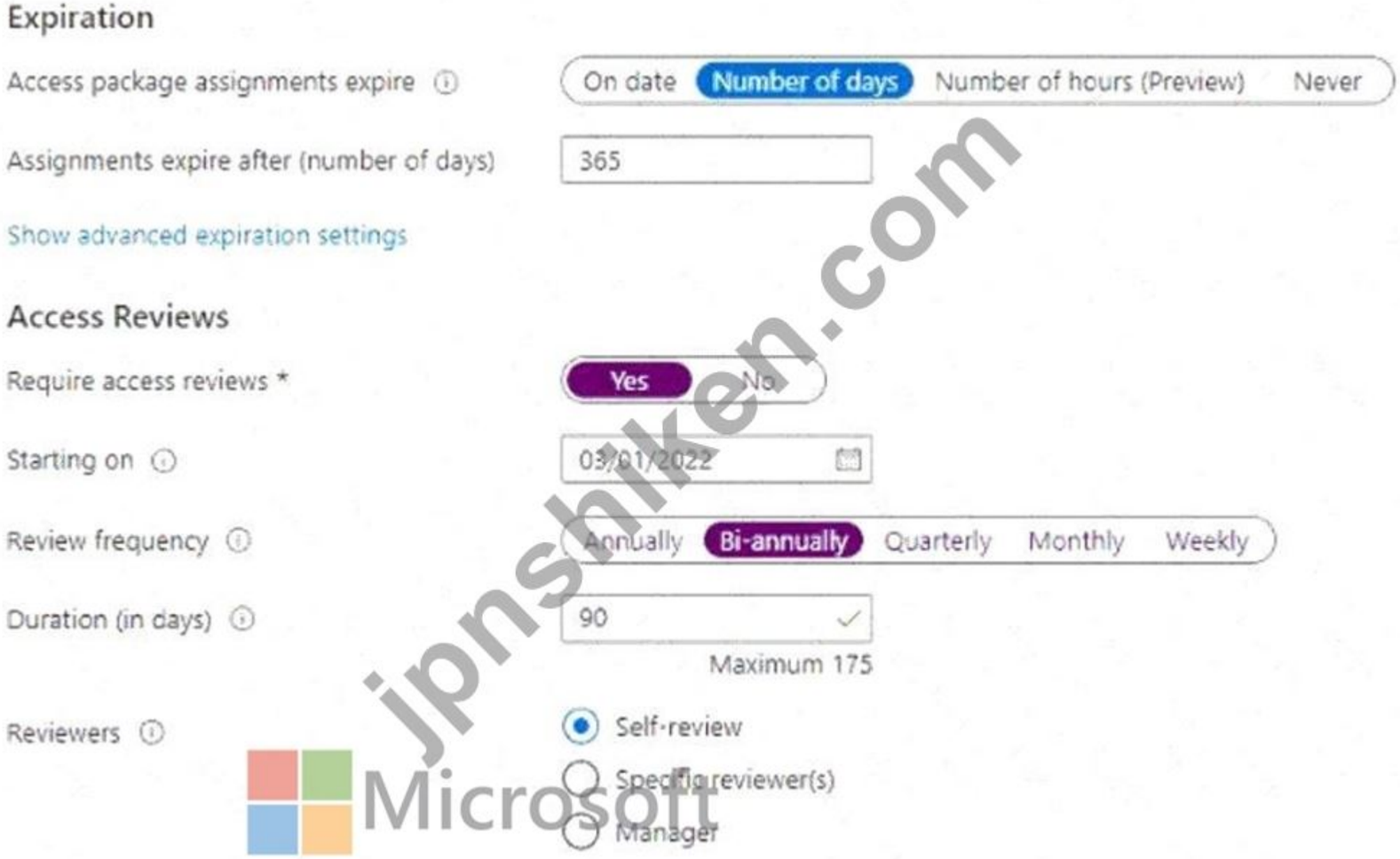
質問**: 145**
User1 という名前のユーザーと Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。
User1 が Vault1 に保存されている証明書、鍵、シークレットのメタデータを読み取れるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 に割り当てるべきロールはどれですか?
A. Key Vault 暗号化ユーザー
B. Key Vault 暗号化担当者
C. Key Vault リーダー
D. Key Vault シークレット ユーザー
正解**: (**正解を表示します**)**
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Azure Key Vault roles, permissions, and the principle of least privilege, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Azure Key Vault and the Requirement:
Azure Key Vault is a service that securely stores and manages cryptographic keys, secrets, and certificates. It uses role-based access control (RBAC) to manage permissions for users, groups, and applications.
The question requires that User1 canread the metadataof certificates, keys, and secrets in Vault1. In Azure Key Vault, "metadata" refers to the properties of these objects (e.g., name, creation date, expiration date), not the actual content (e.g., the secret value, key value, or certificate private key).
The solution must follow theprinciple of least privilege, meaning User1 should be granted the minimum permissions necessary to perform the task, without access to unnecessary actions (e.g., modifying or deleting objects).
Azure Key Vault RBAC Roles and Permissions:
Azure Key Vault supports built-in RBAC roles that define specific permissions for managing keys, secrets, and certificates. Let's examine each role in the options:
Key Vault Crypto User:
This role allows a user to perform cryptographic operations using keys (e.g., encrypt, decrypt, sign, verify) and to read key metadata.
Permissions include: Microsoft.KeyVault/vaults/keys/read (read key metadata) and cryptographic operations like encrypt, decrypt, etc.
However, this role does not grant permissions to read metadata for secrets or certificates, and it includes cryptographic operation permissions, which are not needed for the task.
Key Vault Crypto Officer:
This role is designed for managing keys and performing cryptographic operations. It includes permissions to create, delete, update, and read keys, as well as perform cryptographic operations.
Permissions include: Microsoft.KeyVault/vaults/keys/* (full control over keys).
This role does not grant access to secrets or certificates and provides more permissions than needed (e.g., create, delete), violating the principle of least privilege.
Key Vault Reader:
This role provides read-only access to the metadata of all objects in the Key Vault (keys, secrets, and certificates).
Permissions include: Microsoft.KeyVault/vaults/read (read vault properties) and Microsoft.KeyVault/vaults/*
/read (read metadata for keys, secrets, and certificates).
Importantly, this role does not allow access to the actual content of the objects (e.g., the secret value, key value, or certificate private key), only the metadata. It also does not allow write operations (e.g., create, update, delete).
This aligns perfectly with the requirement to "read the metadata" and follows the principle of least privilege.
Key Vault Secrets User:

This role allows a user to read the content of secrets (not just metadata) and perform operations like getting the secret value.
Permissions include: Microsoft.KeyVault/vaults/secrets/get (read secret values) and Microsoft.KeyVault
/vaults/secrets/read (read secret metadata).
This role does not grant access to keys or certificates, and it provides more access than needed (reading the secret value, not just metadata), violating the principle of least privilege.
Applying the Principle of Least Privilege:
The task requires User1 to read the metadata of certificates, keys, and secrets, but not to access their content or perform any write operations.
Key Vault Readeris the most appropriate role because:
It grants read-only access to the metadata of all objects (keys, secrets, certificates).
It does not allow access to the content of the objects (e.g., secret values), which is not required.
It does not allow write operations (e.g., create, delete), adhering to the principle of least privilege.
The other roles either provide too much access (e.g., Key Vault Crypto Officer, Key Vault Secrets User) or do not cover all required objects (e.g., Key Vault Crypto User, Key Vault Secrets User).
Analysis of the Options:
A: Key Vault Crypto User:
Incorrect. This role only allows reading key metadata and performing cryptographic operations, but it does not provide access to secrets or certificates metadata. It also grants unnecessary cryptographic permissions.
B: Key Vault Crypto Officer:
Incorrect. This role provides full control over keys, which is far more than needed, and does not grant access to secrets or certificates metadata.
C: Key Vault Reader:
Correct. This role provides read-only access to the metadata of keys, secrets, and certificates, exactly matching the requirement while following the principle of least privilege.
D: Key Vault Secrets User:
Incorrect. This role allows reading secret values (not just metadata) and does not provide access to keys or certificates metadata. It grants more access than needed.
Additional Considerations:
If the question had asked for User1 to read the content of secrets (not just metadata), the Key Vault Secrets User role might be considered, but it still wouldn't cover keys and certificates.
Custom RBAC roles could be created to fine-tune permissions, but the question asks for a built-in role, and Key Vault Reader is the best fit.
The question does not specify whether User1 needs to perform other actions (e.g., cryptographic operations, managing the vault). If additional permissions were needed, a combination of roles or a custom role might be required, but the principle of least privilege guides us to the minimal role.
Conclusion:To ensure User1 can read the metadata of certificates, keys, and secrets in Vault1 while following the principle of least privilege, theKey Vault Readerrole should be assigned. This role provides the exact permissions needed without granting unnecessary access. Therefore, the correct answer isC.
References:
Azure Key Vault documentation: "Azure Key Vault RBAC roles" (Microsoft Learn:https://learn.microsoft.
com/en-us/azure/key-vault/general/rbac-guide)
Azure Key Vault documentation: "Secure access to a key vault" (Microsoft Learn:https://learn.microsoft.com
/en-us/azure/key-vault/general/secure-your-key-vault)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Azure Key Vault access control and the principle of least privilege.

質問**: 146**
Azure サブスクリプション、Google Cloud Platform (GCP) アカウント、Amazon Web Services (AWS) アカウントがあります。
すべてのプラットフォームにわたる権限割り当てに関連するリスクを評価するためのソリューションを推奨する必要があります。ソリューションは管理作業を最小限に抑える必要があります。推奨事項には何を含めるべきですか？
A. マイクロソフト センチネル
B. クラウド アプリ向け Microsoft Defender

C. Microsoft Entra ID 保護
D. Microsoft のアクセス許可管理
正解**: (**正解を表示します**)**
According to the Microsoft Identity and Access Administrator (SC-300) study materials and Microsoft Learn module: "Manage permissions across multicloud environments" , Microsoft Entra Permissions Management is the dedicated solution for unified Cloud Infrastructure Entitlement Management (CIEM)
. It enables organizations to discover, remediate, and continuously monitor permission risks across Azure , AWS , and Google Cloud Platform (GCP) environments.
Entra Permissions Management automatically integrates with multicloud environments through read-only connectors, allowing you to assess permissions, identify excessive privilege assignments, and recommend least-privilege configurations. It provides a Permissions Creep Index (PCI) score that quantifies risk, helping administrators maintain a principle of least privilege across all platforms - while minimizing manual effort through automated analysis and unified dashboards.
In contrast, Microsoft Defender for Cloud Apps focuses on app discovery and data protection, not infrastructure entitlement management. Microsoft Entra ID Protection monitors risky sign-ins and identities only within Entra ID, while Microsoft Sentinel provides security information and event management (SIEM) but does not evaluate privilege assignments directly.
Therefore, the verified recommendation from the official Microsoft documentation is to use Microsoft Entra Permissions Management for unified, automated privilege risk assessment across Azure, AWS, and GCP.
Correct Answer: D. Microsoft Entra Permissions Management

質問**: 147**
Package1 という名前のアクセス パッケージと User1 という名前のユーザーを含む Azure AD テナントがあります。
Package1 は次の図に示すように構成されています。



User1 が Package1 のレビュー頻度を変更できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
User1 に割り当てるべきロールはどれですか?

A. 特権ロール管理者
B. ユーザー管理者
C. 外部IDプロバイダー管理者
D. セキュリティ管理者

正解: **B** (コメントを発表する)

This question refers to Azure AD Entitlement Management under Identity Governance . The goal is to let User1 modify the review frequency (i.e., Access Reviews) for an existing access package named Package1
, following the principle of least privilege .
In Azure AD, the ability to create and manage access packages, catalogs, and access reviews is granted through certain administrative roles:
* Global Administrator and Identity Governance Administrator - Full control over all Identity Governance settings.
* Catalog Owner or Access Package Manager - Manage access packages and settings within a catalog.
* User Administrator - Can configure access reviews and manage users, groups, and limited governance settings.
* Privileged Role Administrator , Security Administrator , and External Identity Provider Administrator - Have no direct control over access review settings in Entitlement Management.

jpnshiken.com

From Microsoft documentation ("Azure AD Entitlement Management Delegation and Roles"):
"A user administrator can manage access reviews and entitlement management settings for the directory and assigned catalogs, including adjusting the review frequency or review settings." Thus, to modify the Access Review configuration (frequency, reviewers, etc.) in Package1 , the User Administrator role provides the minimum necessary privilege without granting excessive permissions like Identity Governance Administrator or Global Administrator.

質問: **148**
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: **(**正解を表示します**)**
According to the Microsoft SC-300: Identity and Acces s Administrator study materials and Microsoft Defender for Cloud Apps documentation, connecting third-party cloud applications such as GitHub , AWS , and Google Workspace to Defender for Cloud Apps allows the administrator to monitor user activities and OAut h app authentications in those external services.
The App connectors feature within Microsoft 365 Defender / Microsoft Defender for Cloud Apps provides deep visibility into sanctioned cloud applications by integrating their APIs. When an app connector is added
- such as the GitHub app connector - Defender for Cloud Apps begins ingesting audit logs, including OAuth authorization events , sign-in attempts, and token consent grants.
The relevant Microsoft documentation states:
"App connectors use APIs from con nected apps to extend visibility and control to cloud services, enabling monitoring of OAuth application authorizations and security activities." Since the question specifically asks to monitor OAuth authentication requests , adding the GitHub app connector fulfills this requirement because it brings OAuth consent and token data from GitHub into Microsoft 365 Defender (via Defender for Cloud Apps).

質問: **149**
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。
* アカウントが削除される際には、Automation1に付与されたすべての権限が削除され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。
何を使うべきでしょうか？
A. クライアントシークレット
B. システムによって割り当てられた管理ID
C. 証明書
D. ユーザーに割り当てられた管理ID
正解: **(**正解を表示します**)**

質問: **150**
SSPR の計画された変更を実装します。
User3 が SSPR を使用しようとすると何が起こりますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



This question asks you to apply the stated Technical Requirements for Self-Service Password Reset (SSPR) to complete the form. The specific scenario about " User3 " is a distraction, as the configuration applies to all users.

The relevant technical requirements are:

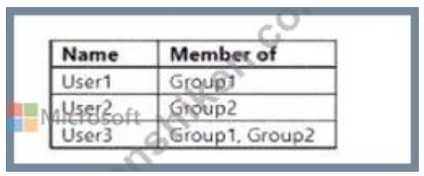
* " Users must provide one authentication method to reset their password by using SSPR. "
* This directly dictates the value for the Number of authentication methods required , which is 1

.

* " Available methods must include: Email, Phone, Security questions, The Microsoft Authenticator app "
* This lists all the options that are configured to be available for SSPR, which determines the value for Authentication methods that can be used : Email , Phone , Security questions , The Microsoft Authenticator app .

質問**: 151**

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	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

次の設定を持つユーザー リスク ポリシーがあります。

* 課題:
o 含める: グループ 1
o 除外: グループ2
* サインインリスク 中以上
* アクセス制御:
o アクセスを許可する: パスワードの変更を要求する

ユーザーがサインインしようとすると、次の表に示すようにユーザーのリスク レベルが検出されます。

User	Risk level
User1	High
User2	Medium
User3	High

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



正解:



Explanation:



This scenario is based on the Microsoft Entra (Azure AD) Identity Protection feature, which is a major topic in the SC-300: Microsoft Identity and Access Administrator exam. According to the official study guide and Microsoft documentation:

"A user risk policy in Microsoft Entra ID is used to detect when a user account is at risk and to enforce remediation actions, such as requiring the user to change their password on the next sign-in."

* Assignments:
* Include: Group1
* Exclude: Group2
* Sign-in risk: Medium and above
* Access control: Require password change

Given Policy Settings: User Details: User
Group Membership
Risk Level
User1
Group1

High
User2
Group2
Medium
User3
Group1, Group2
High
* User1:
* Included in Group1 (policy applies).
* Not a member of Group2 (not excluded).
* Risk level = High, which is # Medium, meeting policy threshold. # User1 must change their password.
* User2:
* Member of Group2 (excluded).
* Even though their risk level is Medium, exclusion overrides inclusion. # User2 will not be prompted to change their password.
* User3:
* Member of both Group1 (included) and Group2 (excluded).
* Exclusion always takes precedence in Microsoft Entra conditional access and risk policies. # User3 will not be required to change their password.
Analysis:
Official Microsoft SC-300 Source Excerpt: From the Microsoft Identity and Access Administrator Study Guide (Exam Ref SC-300) and Microsoft Learn ("Configure and manage user risk policies"):
"When a user is included in both the include and exclude assignments of a policy, the exclude setting takes precedence. Risk policies can enforce password change for users with detected risk levels that meet or exceed the configured threshold."

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: **152**
User! という名前のユーザーと、RG1 および RG2 という名前の 2 つのリソース グループを含む Azure サブスクリプションがあります。
User1 が次のタスクを実行できることを確認する必要があります。
* すべてのリソースを表示します。
* 仮想マシンを再起動します。
* RG1 でのみ仮想マシンを作成します。
* RG1 でのみストレージ アカウントを作成します。
必要なロールベース アクセス制御 (RBAC) ロール割り当て* の最小数はいくつですか?
A. 1
B. 2
C. 3
D. 4
正解: **(**正解を表示します**)**

In Azure RBAC, access is granted by assigning roles to principals at a scope (subscription, resource group, or resource). The SC-300 materials emphasize using the least-privilege principle and scoping assignments appropriately so users can " view at the widest scope and create only where required ." To meet the requirements: assign Reader at the subscription so User1 can " view all resources ." Creation rights must be limited to RG1, so assign Virtual Machine Contributor at RG1 (this role can " start, stop, and restart virtual machines and create them ," but cannot grant access) and Storage Account Contributor at RG1 (can " create and manage storage accounts "). No additional assignments are needed at RG2 because the subscription-level Reader grants view rights without create permissions there. This yields three assignments total: 1) Reader @ subscription, 2) Virtual Machine Contributor @ RG1, 3) Storage Account Contributor @ RG1. This aligns with SC-300 guidance that role assignments should be " as narrowly scoped as possible " while satisfying operational tasks.

質問: **153**
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。

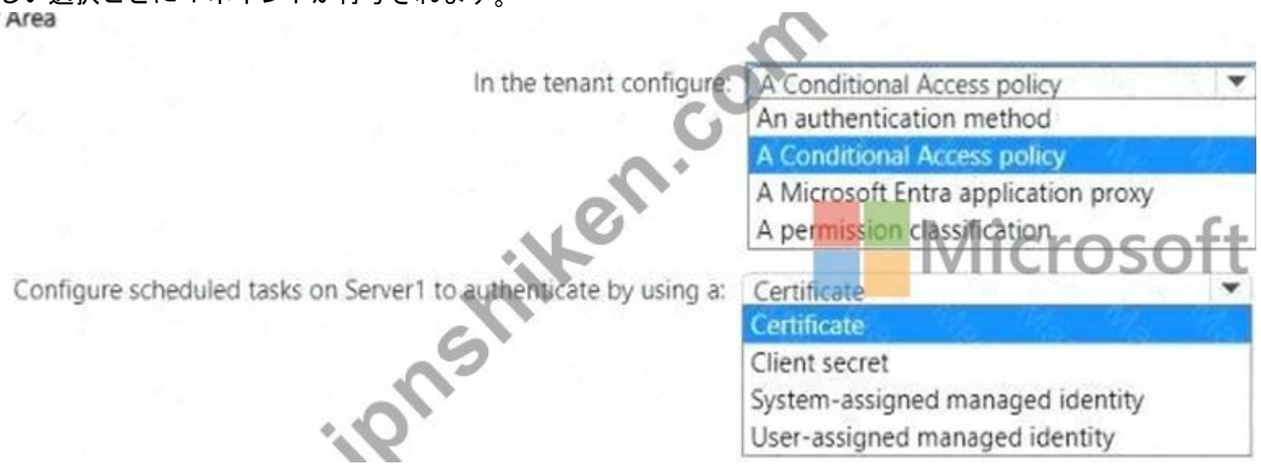
Name	Member of
User1	Group1
User2	None
User3	None

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. User1、User2、およびUser3
C. ユーザー1とユーザー3のみ
D. User3のみ
正解: **(**正解を表示します**)**

質問: **154**
ADatumユーザーを同期する必要があります。ソリューションは技術要件を満たしている必要があります。
何をすべきでしょうか?
A. Microsoft Azure Active Directory Connect ウィザードから、同期オプションのカスタマイズを選択します。
B. PowerShell から、Set-ADSyncScheduler を実行します。
C. PowerShell から Start-ADSyncSyncCycle を実行します。
D. Microsoft Azure Active Directory Connect ウィザードから、ユーザー サインインの変更を選択します。
正解: **(**正解を表示します**)**
The SC-300 coverage of Azure AD Connect explains that when you need to bring in a new set of on-premises users or change what is synchronized (for example, adding an additional domain/OU such as ADatum or adjusting filtering), you reopen the Azure AD Connect wizard and choose "Customize synchronization options." The guide notes that this path lets you "modify directory/OU filtering, add or remove forests, and enable optional sync features" so that only the intended users are synchronized. It contrasts with operational commands: Start-ADSyncSyncCycle merely triggers an immediate delta/full sync of the current configuration; Set-ADSyncScheduler changes the sync cadence or pause/resume behavior; and "Change user sign-in" alters the authentication method (e.g., PHS vs. PTA) but does not control scoping of which users are synced. To meet a requirement to sync the ADatum users according to technical constraints (such as OU /domain selection or feature toggles), you must first configure the scope by running the wizard and selecting Customize synchronization options, then perform/allow a sync cycle to bring those users into Azure AD as defined.

質問: **155**
ユーザーが 70 歳以上のサインイン アラートをトリガーしたときにアクセスをブロックする条件付きアクセス ポリシーを作成します。
次の条件下でポリシーをテストする必要があります。
* ユーザーが別の国からサインインします。
* ユーザーがサインイン リスクを引き起こします。
テストを完了するには何を使用すればよいですか?
A. 条件付きアクセス What If ツール
B. Azure AD のサインイン ログ
C. Azure AD のアクセスレビュー
D. Microsoft Defender for Cloud Apps のアクティビティ ログ
正解: **A (**コメントを発表する**)**
The Conditional Access What If tool is designed to simulate sign-ins under various conditions to test Conditional Access policies without performing real sign-ins. Microsoft's SC-300 guide specifies that this tool is essential for validating the effect of a policy based on user, location, device, or risk level.
In this case, the administrator wants to test a policy that blocks access when a high-severity sign-in alert (sign-in risk) occurs and when a user signs in from another country. These scenarios are based on risk and location conditions-both supported in the What If tool simulation.
Microsoft Learn: "Use the What If tool to simulate sign-ins and verify whether a specific Conditional Access policy will be applied."

質問: **156**
Windows Server を実行する Server! という名前のオンプレミス サーバーがあります。
App1 という名前のアプリ登録を含む Microsoft Entra テナントがあります。App1 には、Microsoft Graph アプリケーションのアクセス許可があります。
App1をサポートするには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 は企業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 の資格情報はプレーンテキストとして保存しないでください。
* サーバー 1 上の非対話型のスケジュールされたタスクは、App1 に対して認証できる必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
Answer Area



ipnshiken.com
Microsoft

正解:



Explanation:



According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn documentation ("Implement app registration and authentication with Microsoft Entra ID") , when configuring app registrations and securing non-interactive service applications (like scheduled tasks), two key elements must be addressed - secure authentication and conditional access enforcement.

Step 1: Secure App Access from the Corporate Network To ensure App1 is accessible only from the corporate network, you must configure a Conditional Access policy in Microsoft Entra ID. Conditional Access policies allow you to restrict access to applications based on conditions such as:

* User or workload identity
* Location (e.g., trusted IP ranges or corporate networks)
* Device compliance and sign-in risk

As Microsoft documentation states:

"Conditional Access policies can restrict access to specific applications based on location, risk, or device status. Use named locations to allow access only from your trusted network." Therefore, a Conditional Access policy is required to meet the first requirement.

Step 2: Secure Authentication for Non-Interactive Tasks For non-interactive scheduled tasks running on an on- premises server (Server1) that need to authenticate to App1 using application permissions, credentials must be securely stored. Storing plain-text secrets (like passwords or client secrets) violates security best practices.

Microsoft recommends using certificates for application authentication because certificates are securely stored and provide higher security than secrets.

From the SC-300 material and Microsoft Learn:

"When registering applications that use non-interactive authentication, use a certificate-based credential instead of a client secret. Certificates are more secure and meet compliance requirements for secure app authentication." This approach also ensures that Server1's scheduled tasks can authenticate silently using the private key of the certificate.

質問**: 157**

お客様は、Groups1、Group2、Group3という名前の3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	Role	Member of
User1	Global Administrator	Group1
User2	*None*	Group2
User3	Global Reader	Group2, Group3

次の設定を持つ ｢CAT｣という名前の条件付きアクセス ポリシーを作成します。

* ユーザー

* 含む
#ユーザーとグループ:グループ1
除外する
#ユーザーとグループ:グループ2
#ディレクトリの役割: グローバル管理者
o 対象リソース
#含める: すべてのクラウドアプリ
o アクセス制御
#許可: 多要素認証を要求する
CA2という名前の条件付きアクセス ポリシーを作成し、以下の設定を行います。
* ユーザー
* 含む
#ユーザーとグループ:グループ2
除外する
#ユーザーとグループ:グループ3
o 対象リソース
#含める: すべてのクラウドアプリ
o アクセス制御
#許可: アクセスをブロック
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。



正解:



Explanation:



Microsoft
jpnshiken.com

SC-300 materials explain that Conditional Access (CA) evaluates assignments (who/what) and conditions /exclusions before applying grant controls. Policy CA1 targets Group1 and requires MFA, but explicitly excludes Global Administrator and Group2. User1 is in Group1 and holds the Global Administrator role, so the directory-role exclusion means CA1 does not apply and no other policy targets User1 # no MFA prompt.

Policy CA2 targets Group2 and blocks access to all cloud apps, with an exclusion for Group3. User2 is in Group2 and not in Group3, so CA2 applies and blocks SharePoint Online sign-in. User3 is in Group2 and Group3; because Group3 is excluded from CA2, the block does not apply. User3 is not in Group1, so CA1 doesn't apply either; therefore, User3 can sign in normally. The SC-300 guidance also notes that exclusions take precedence over inclusions, and block access is an enforcing control when a matching policy applies, while policies are evaluated independently with the most restrictive applicable outcome applied per user and sign-in.

質問**: 158**

fabrikam.comという名前のドメインを使用するMicrosoft365テナントがあります。Azure Active Directory（Azure AD）のゲスト招待設定は、展示に示されているように構成されています。 [展示]タブをクリックします。）



bsmith@fabrikam.comという名前のユーザーは、Microsoft SharePointOnline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ます。

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrkam.com	A user in fabrikam.com

どのユーザーにパスコードが電子メールで送信されますか？

A. User2のみ

B. User1のみ

C. User1とUser2のみ

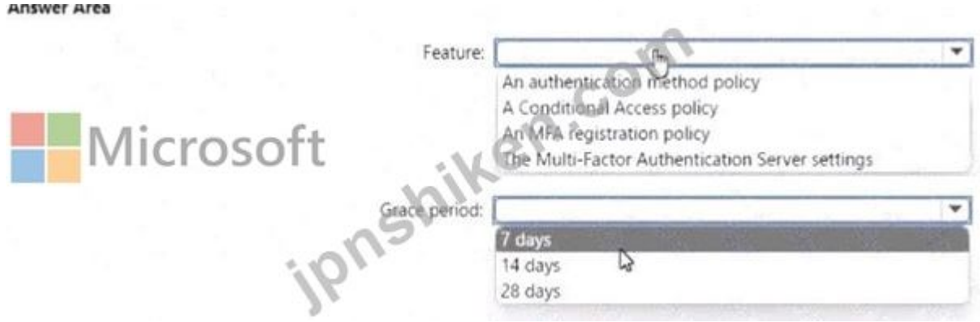
D. User1、User2、およびUser3

正解: **(**正解を表示します**)**

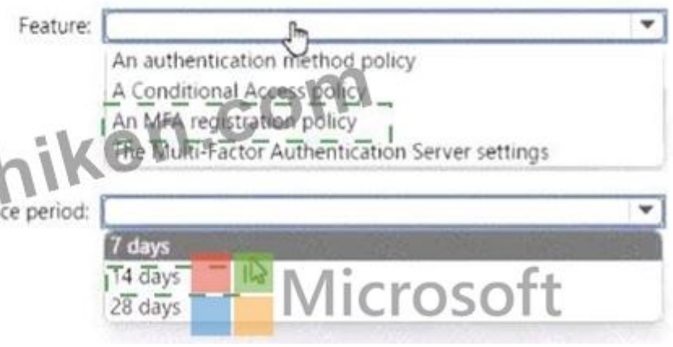
With Email one-time passcode (OTP) for guests enabled, the SC-300 materials describe OTP as an authentication method "used for B2B guest users who do not have, or cannot use, an Azure AD or Microsoft account to complete sign-in." In the scenario: User1@contoso.com is already a guest in the tenant and will authenticate using their home directory; no OTP is sent. User3@fabrikam.com is an

internal member of the same tenant and therefore does not receive a guest OTP. User2@outlook.com has never accessed resources in the tenant; when the library is shared, the tenant sends a guest invitation. With OTP enabled, the service provides a passcode by email to complete authentication when a straightforward federated or previously established sign-in path is not available for the invitee. Hence, under the guest invite/OTP configuration shown, User2 is the user who will be emailed a one-time passcode.

質問: **159**
計画された変更をサポートし、MFA の技術要件を満たす必要があります。
どの機能を使用する必要がありますか? また、ユーザーはどのくらいの時間前に登録を完了する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
Answer Area



正解:
Answer Area



Explanation:
Feature: An MFA registration policy
Grace period: 14 days
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn documentation under "Plan, implement, and manage multifactor authentication (MFA)", when an organization wants to require users to register for multi-factor authentication methods (such as Microsoft Authenticator, phone number, or email), this is managed through the MFA registration policy within Azure AD Identity Protection.
This feature is called "Combined security information registration" or MFA registration policy, and it allows administrators to enforce users to register for MFA and Self-Service Password Reset (SSPR).
The policy defines which users are required to register and sets a grace period - the amount of time a user can postpone registration after first being prompted.
From the Microsoft official exam reference:
"The MFA registration policy allows users to postpone registration for a defined grace period. The default and maximum supported value is 14 days." During the grace period, users can skip the registration prompt but will be reminded every time they sign in until they complete registration or the grace period expires. Once the 14-day period ends, users must register their authentication methods before accessing resources.
Therefore, based on Microsoft's SC-300 study materials and Azure AD documentation:
* The correct feature used to enforce this is An MFA registration policy.

* The standard and maximum grace period before users must complete registration is 14 days.

質問: **160**
contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
Fabrikam, Inc. という会社のユーザーにリソース アクセスを提供するために、権限管理を実装します。Fabrikam は fabrikam.com というドメインを使用します。
アクセスが不要になった場合、Fabrikam ユーザーはテナントから自動的に削除される必要があります。
次の設定を構成する必要があります。
外部ユーザーがこのディレクトリにサインインすることをブロックする: いいえ
外部ユーザーの削除: はい
このディレクトリから外部ユーザーを削除するまでの日数: 90
Identity Governance ブレードでは何を構成する必要がありますか?
A. アクセスパッケージ
B. 権限管理設定
C. 利用規約
D. アクセスレビュー設定
正解: **(正解を表示します)**
According to Microsoft's SC-300 Exam Guide and Microsoft Learn module: Manage Identity Governance in Azure AD, the removal and lifecycle management of external users (B2B guests) within Azure Active Directory's Entitlement Management are configured through Entitlement management settings under the Identity Governance blade.
In scenarios where external partners (such as Fabrikam) are granted access via access packages, administrators can define lifecycle settings to ensure that when access is no longer required, the users are automatically removed from the directory. The Entitlement Management directory settings control two specific parameters:
* Block external user from signing in to this directory - determines whether external users can still sign in after access expiration.
* Remove external user - enables automatic deletion of the guest account after a specified number of days.
* Number of days before removing external user - defines the delay period (in this case, 90 days).
Microsoft documentation states:
"To automatically remove external users from your directory after access expires, configure the Entitlement management settings. You can set whether to block sign-in and specify how many days after access expiration the user should be removed."

質問: **161**
お客様は、User1、User2、User3 という名前の 3 人のユーザーと、Appl という名前のエンタープライズ アプリを含む Microsoft 365 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、次の表に示すデバイスが含まれています。

Name	Compliance state
Device1	Compliant
Device2	Compliant
Device3	Compliant

このサブスクリプションには、以下の表に示すグループが含まれています。

Name	Members
Group1	User1, User3
Group2	User2, User3
Group3	User1

次の設定を持つ2つの条件付きアクセス ポリシーを作成します。
* 名前: ポリシー1
* ユーザー:
含まれるもの :グループ1
除外対象: グループ3
* 対象リソース:
o 含める: すべてのリソース
* アクセス制御: アクセスをブロックする
* 名前: ポリシー2
* ユーザー:
o 含める: グループ2
* 対象リソース:
含まれるもの: アプリ1
* アクセス制御:
* アクセスを許可する: デバイスが準拠しているとマークされていることを要求します
以下の各記述について、記述が正しい場合は「はい」を選択し、そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



In Conditional Access (CA), assignments determine who the policy applies to using Include and Exclude lists. A user targeted by Include but present in Exclude is not affected. CA evaluates all applicable

policies for a sign-in. If any applicable policy has Block access , the sign-in is denied , even when other policies would grant access. When policies Grant access with conditions, the user must meet the configured controls (for example, Require device to be marked as compliant) to succeed.
Applying these rules: Policy1 includes Group1 and excludes Group3 , targets All resources , and Blocks access . Group1 contains User1 and User3 ; Group3 contains User1 . Therefore, User1 is excluded from Policy1 and not blocked, but User3 remains included and is blocked from all resources. Policy2 includes Group2 , targets App1 , and Grants access requir ing a compliant device . Group2 contains User2 and User3
; all devices (Device1-Device3) are Compliant . Thus, User2 can access App1 from Device2 because Policy2 is satisfied and no block applies. User1 is not in Group2 and not blocked by Policy1, so access to App1 from Device1 is allowed. User3 , however, is affected by Policy1 (Block) ; block overrides any grant in Policy2, so User3 cannot sign in to App1 from Device3 .

質問**: 162**
次の表に示すグループを含む 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、Group1 のアクセス レビューを作成します。

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

次の表に示すように、Group2 のアクセス レビューを作成します。

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

各グループに必要なAzure AD Premium P2ライセンスの最小数はいくつですか？ 回答するには、回答エリアで適切なオプションを選択してください。注：正解は1つにつき1ポイントです。
Answer Area

Group1: 525
- 1
- 500
- 525

Group2: 1
- 1
- 100
- 295
- 395

正解:



Microsoft
ipnshiken.com

Explanation:

Based on the official Microsoft SC-300 study guide and Microsoft Entra ID (Azure AD) licensing documentation, the licensing requirement for Access Reviews depends on who is being reviewed and how the review is configured .

Access reviews are an Azure AD Premium P2 feature (included in Microsoft 365 E5), and the licensing model specifies that:

"Each user who is part of an access review (either being reviewed or reviewing) must have an Azure AD Premium P2 license, except in cases where guest users are reviewed by internal reviewers - in that case, only the reviewers require a license." Let's analyze each configuration:

* Members: 500 internal + 25 guest users = 525 total members.

* Review Type: Teams + Groups

* Review Scope: All users

* Reviewers: Users review own access

Group1 Since all users (internal and guest) review their own access, every member is considered an active participant in the review. Therefore, each of the 525 members (500 internal + 25 guests) must have an Azure AD Premium P2 license.

Group1 = 525 licenses required

* Members: 295 internal + 100 guest users = 395 total members.

* Review Type: Teams + Groups

* Review Scope: Guest users only

* Reviewers: Group owner

Group2 Here, only guest users are being reviewed, and the reviewer is the group owner (User2). Since the guest users don't require licenses when being reviewed by an internal reviewer, only the group owner (User2) needs a P2 license.

Group2 = 1 license required

According to Microsoft Licensing Guidance (SC-300 Official Content):

"If guest users review their own access, each guest requires a P2 license. If the review is conducted by an internal user (owner or admin), only that reviewer requires the license."



質問: **163**

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	*None*
User2	*None*
Admin1	Application administrator
Admin2	Authentication administrator

エンタープライズ アプリケーションのユーザー設定には次の構成があります。

* ユーザーは、アプリが自分に代わって会社のデータにアクセスすることに同意できます。
* ユーザーは、自分が所属するグループの企業データへのアクセスをアプリに許可することができます。
* ユーザーは、同意できないアプリに対して管理者の同意をリクエストできます: はい
* 管理者の同意リクエストを確認できるユーザー: Admin2、User2

ユーザー1 は、会社のデータにアクセスするために同意が必要なアプリを追加しようとします。

どのユーザーが同意できますか?

A. ユーザー1

B. ユーザー2

C. 管理者1

D. 管理者2

正解: **(**正解を表示します**)**

In Azure AD, user consent and admin consent workflows control which users or administrators can approve access to organizational data requested by applications.

The question states:

* "Users can request admin consent to apps they are unable to consent to: Yes"
* "Who can review admin consent requests: Admin2, User2"

When User1 attempts to add an app that requires consent to access company data, and if that app requires admin consent, the request is routed to those designated as admin consent reviewers. In this case, Admin2 and User2 are listed, but only one has the administrative capability to approve the request.

Based on Microsoft documentation:

"Only users who hold an administrative role such as Global Administrator, Cloud Application Administrator, or Authentication Administrator and are designated as reviewers can grant consent on behalf of the organization." Here, Admin2 holds the Authentication Administrator role - an Azure AD admin-level role - while User2 has no administrative privileges. Thus, Admin2 is the only eligible user to approve the admin consent request.

質問: **164**

Microsoft 365 E5 サブスクリプションがあります。

Microsoft Defender for Cloud Apps セッション ポリシーを作成する必要があります。

最初に何をすべきですか？

A. Microsoft Defender for Cloud Apps ポータルから、[ユーザーの監視] を選択します。
B. Microsoft Defender for Cloud Apps ポータルから、[アプリのオンボーディング/メンテナンス] を選択します。
C. Azure Active Directory 管理センターから、条件付きアクセス ポリシーを作成します。
D. Microsoft Defender for Cloud Apps ポータルから、継続的なレポートを作成します。
正解**: (**正解を表示します**)**
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide , Exam Ref SC-300
, and Microsoft Defender for Cloud Apps (MDCA) documentation , a session policy in Defender for Cloud Apps (formerly Microsoft Cloud App Security) is used to monitor and control user sessions in real time. These policies provide granular session-level access controls such as limiting downloads, blocking uploads, or monitoring user activity in SaaS applications integrated with Defender for Cloud Apps. However, before a session policy can function, the Conditional Access App Control feature must be enabled. This integration connects Azure Active Directory (Azure AD) with Microsoft Defender for Cloud Apps , allowing session control to be enforced through Conditional Access policies .
The SC-300 official training content under "Implement and configure Microsoft Defender for Cloud Apps" states:
"To apply session controls using Microsoft Defender for Cloud Apps, you must first configure a Conditional Access policy in Azure AD that routes user sessions to Defender for Cloud Apps for inspection. Only after this step can you define a session policy within the Defender for Cloud Apps portal." Thus, the correct first step is to create a Conditional Access policy in Azure AD that uses the Use Conditional Access App Control option. This action establishes the required connection path so that session control policies in Defender for Cloud Apps can take effect.

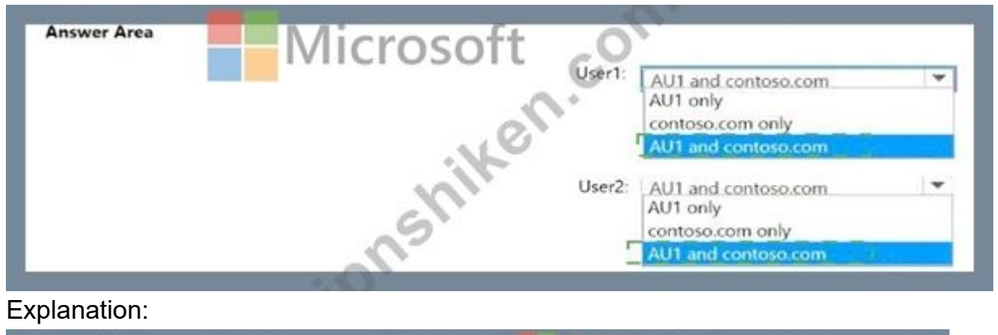
質問**: 165**
App1という名前のAzureADエンタープライズアプリケーションを含むcontoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
請負業者はuser1@outlook.comのクレデンシャルを使用します。
請負業者にApp1へのアクセスを提供できることを確認する必要があります。請負業者は、user1 @ outlook.comとして認証できる必要があります。
あなたは何をするべきか？
A. New-AzureADMSInvitationコマンドレットを実行します。
B. 外部コラボレーション設定を構成します。
C. WS-FedIDプロバイダーを追加します。
D. Azure ADConnectを実装します。
正解**: (**正解を表示します**)**
According to the Microsoft Identity and Access Administrator (SC-300) official study guide and Microsoft Learn module "Manage External Identities" , when granting external users (such as contractors) access to Azure AD resources, the recommended method is to invite them as guest users (B2B collaboration users) into your Azure AD tenant.
The New-AzureADMSInvitation cmdlet is the PowerShell command used to create an Azure AD B2B guest invitation. It sends an invitation to an external user (such as user1@outlook.com) and, upon acceptance, creates a corresponding guest user account in the tenant (for example, user1_outlook.com#EXT#@contoso.
com). This account can then be assigned to enterprise applications like App1.
From Microsoft documentation:
"To provide external users access to resources in your organization, invite them as guests using Azure AD B2B collaboration. You can do this by running the New-AzureADMSInvitation cmdlet or via the Azure portal."
* B. Configure the External collaboration settings: These settings define collaboration policies (who can invite guests, restrictions, etc.) but do not invite users themselves.
* C. Add a WS-Fed identity provider: This is used to federate another identity provider (e.g., ADFS or another Azure AD tenant), not to onboard an individual external user.
* D. Implement Azure AD Connect: This tool synchronizes on-premises directories with Azure AD; it's not relevant for external users from Outlook.com.
Why not the other options: # Correct Answer: A. Run the New-AzureADMSInvitation cmdlet.

質問**: 166**
contoso.com という Microsoft Entra テナントがあり、このテナントには AU1 という管理単位と、User1 および User2 という 2 人のユーザーが含まれています。User1 は AU1 のメンバーです。

次のロールの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スコープに対してロールを割り当てることができますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Entra documentation , role assignments in Entra ID (formerly Azure AD) can be scoped at directory (tenant- wide) or administrative unit (AU) levels.
An Administrative Unit (AU) is a logical grouping of Azure AD resources (users, groups, devices) that allows administrators to delegate management responsibilities. When you assign roles scoped to an AU, the permissions of the role apply only to objects within that AU.
From Microsoft's "Manage role-based access control (RBAC) with administrative units" module:
"You can assign directory roles to users either at the tenant level or scoped to an administrative unit. Only users who are members of the AU can be assigned roles scoped to that AU." Applying this to the scenario:
* User1 is a member of AU1. Therefore, User1 is eligible for a role assignment scoped to AU1 and/or tenant-wide (contoso.com). User1 can have the Security Administrator role assigned at both AU1 and contoso.com.
* User2 is not a member of AU1. Users who are not members of an administrative unit cannot be assigned roles scoped to that AU. Thus, User2's User Administrator role can be assigned only at the tenant-wide (contoso.com) level.
This aligns with the Microsoft Learn reference:
"Only members of an administrative unit can be assigned directory roles scoped to that administrative unit.
Roles can always be assigned at the organization level regardless of AU membership."

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: **167**
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. Vault1 の権限モデルを構成します
C. ユーザー割り当てのマネージド ID を VM1 に追加します。
D. Azure ロールを VM1 に割り当てます。
正解: **(**正解を表示します**)**
To ensure VM1 can retrieve the values of secrets stored in Vault1 while minimizing administrative effort, you should assign an Azure role to VM1 .
1. Managed Identities and Key Vault Access: VM1 has a system-assigned managed identity . This identity acts as a Service Principal in Microsoft Entra ID (formerly Azure AD). To access Key Vault secrets, this identity must be granted permissions on the Key Vault.
2. Permission Models (RBAC vs. Access Policies): Azure Key Vault supports two permission models:
* Azure role-based access control (Azure RBAC): The recommended, modern authorization system. It allows you to manage access to Key Vault keys, secrets, and certificates centrally using Azure IAM (Identity and Access Management), just like other Azure resources. It provides fine-grained access control and integrates with PIM (Privileged Identity Management).
* Vault access policy: The legacy model where permissions are defined within the Key Vault ' s own " Access policies " blade.
3. Why " Assign an Azure role " (Option D) is the Correct First Step:
* Minimizing Administrative Effort: Using Azure RBAC is the recommended best practice for minimizing effort because it unifies access management across Azure resources.
* The Action: To grant the required access (reading secrets) under the RBAC model, you must assign a specific role to the managed identity. The appropriate role is Key Vault Secrets User , which grants permission to read secret contents (Get and List operations) without granting administrative privileges (adhering to Least Privilege).
* Scenario Analysis: While older Key Vaults defaulted to Access Policies, new vaults and the " minimize effort " requirement point towards the RBAC model. Option A (" Configure the Resource access settings ") is vague and likely refers to the " Access configuration " or " Access policies " blade, but " Assign an Azure role " is the definitive action to grant access in the modern RBAC workflow. If the vault were in Access Policy mode, one would typically " Add an access policy, " but that specific option is not listed, reinforcing that RBAC (Option D) is the intended path.
Documentation Extract:
" Azure RBAC is an authorization system built on Azure Resource Manager that provides centralized access management of Azure resources... The Azure RBAC model allows users to set permissions on different scope levels... To grant access to a specific user, group, or application... assign a role. For example, the Key Vault Secrets User role allows a user to read secret contents. " (Source: Microsoft Learn - Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control)

質問: **168**
contoso.comのデフォルトドメイン名を使用するように新しいMicrosoft365テナントを構成します。
条件付きアクセスポリシーを使用して、Microsoft365リソースへのアクセスを制御できることを確認する必要があります。
あなたは最初に何をすべきですか？
A. ユーザー同意設定を無効にします。
B. セキュリティのデフォルトを無効にします。
C. 多要素認証（MFA）登録ポリシーを構成します。

D. Windows Server ActiveDirectoryのパスワード保護を構成します。
正解: (正解を表示します)
Reference:
New Microsoft 365/Azure AD tenants enable Security defaults by default. The SC-300 materials emphasize that Security defaults and Conditional Access cannot be used together; to create and enforce custom Conditional Access policies (for example, requiring MFA under specific conditions), you must turn off Security defaults first. After disabling Security defaults, you can define Conditional Access policies that target specific users, apps, locations, or device states, and require controls such as MFA or session restrictions.
Disabling user consent, configuring on-premises password protection, or merely creating an MFA registration policy do not enable Conditional Access; they address different capabilities. Therefore, the first step to control access with Conditional Access is to disable Security defaults.

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**」