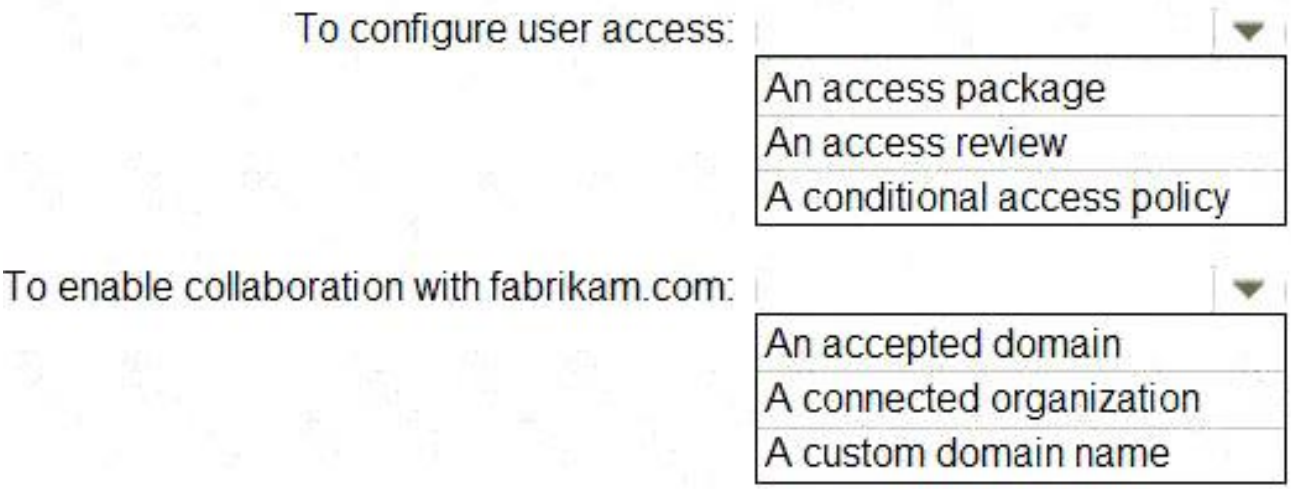
Exam : **SC-300J**

Title : Microsoft Identity and Access Administrator (SC-300日本語版)

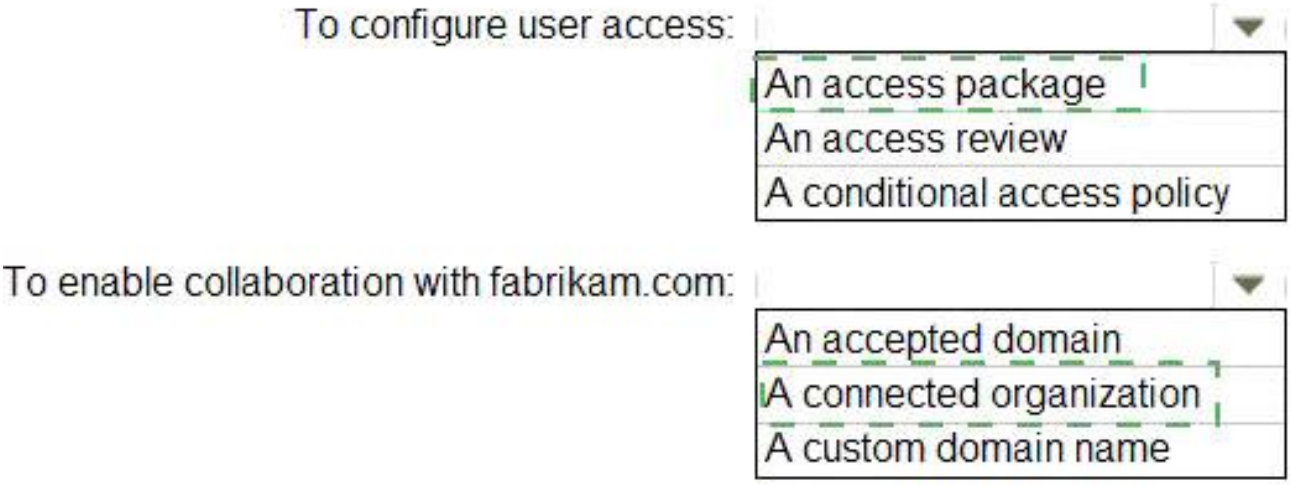
Vendor : Microsoft

Version : DEMO

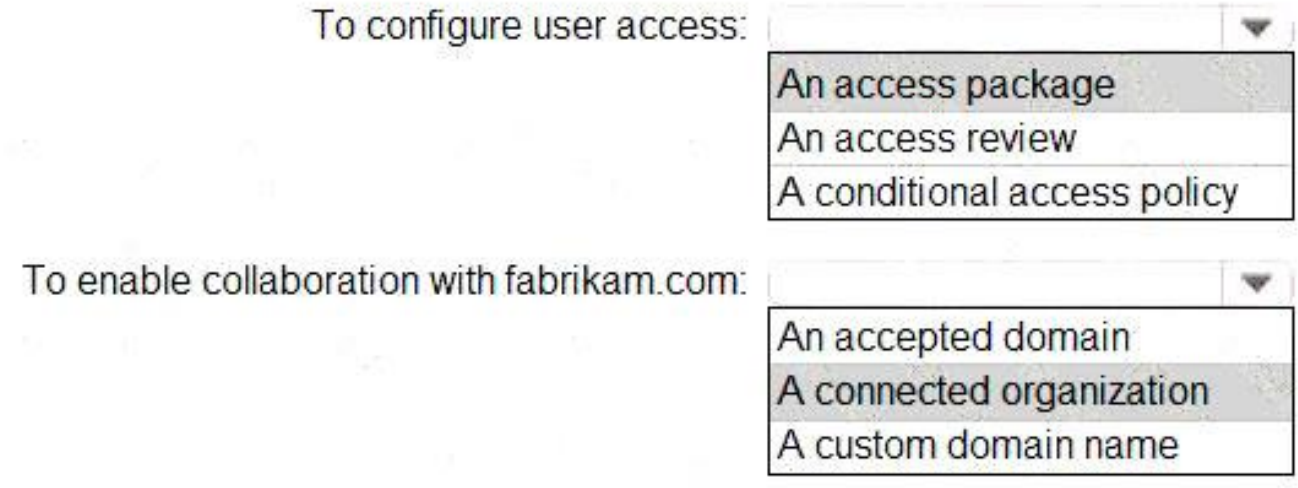
QUESTION NO: 1
マーケティング部門の計画された変更と技術要件を実装する必要があります。
どうすればいいでしょうか?
回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator official study guide and Microsoft Learn modules on Azure AD Identity Governance , the correct way to manage user access-especially for scenarios involving both internal and externa l users-is through Entitlement Management in Azure AD Identity Governance .
Entitlement Management uses access packages to define and automate how users obtain access to resources such as groups, SharePoint sites, and applications. Access packages contain policies that specify who can request access (internal users, external users, or both) and how that access is approved and periodically reviewed. The guide clearly states: "Access packages provide a structured method to configure and automate access for us ers, ensuring that access assignments follow the organization's policy and compliance requirements." To enable external collaboration with another organization (such as fabrikam.com), Microsoft documentation emphasizes that you must create a connected orga nization . A connected organization represents an external directory or domain whose users can be invited to request access packages or participate in identity governance workflows. The connected organization defines trust boundaries for cross- tenant collab oration, without requiring domain federation or acceptance.
In summary:
* Access packages configure and automate user access.
Topic 1, Contoso, LtdOverview
Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc Fabcricam has an Azure Active Diretory (Azure AD) tenant named fabrikam.com.
Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contos.com. The domain cont ains an organizational unit (OU) named Contoso_Resources. The Contoso_Resoureces OU contains all users and computers.
The Contoso.com Active Directory domain contains the users shown in the following table.

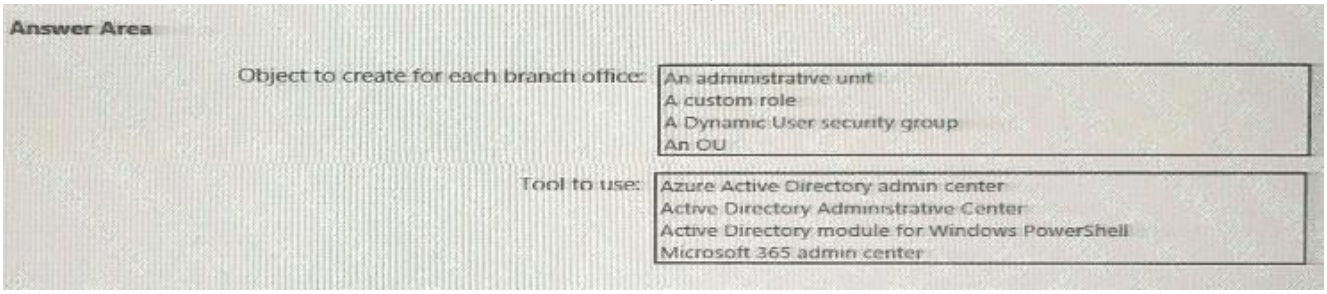
Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named Contoso.com that has the following associated

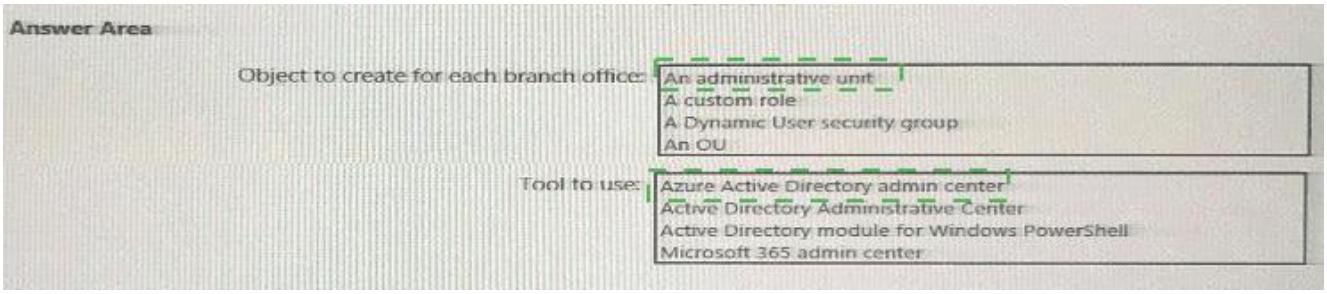
licenses:
Microsoft Office 365 Enterprise E5
Enterprise Mobility + Security
Windows 10 Enterprise E5
Project Plan 3
Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (AD DS). Only the Contoso Resources OU is synced.
Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.
User administrators currently use the Microsoft 365 admin center to manually assign licenses, All user have all licenses assigned besides following exception:
The users in the London office have the Microsoft 365 admin center to manually assign licenses. All user have licenses assigned besides the following exceptions:
The users in the London offic e have the Microsoft 365 Phone System License unassigned.
The users in the Seattle office have the Yammer Enterprise License unassigned.
Security defaults are disabled for Contoso.com.
Contoso uses Azure AD Privileged identity Management (PIM) to project a dministrator roles.
Problem Statements
Contoso identifies the following issues:
* Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
* The user administrators report that it is tedious to manuall y configure the different license requirements for each Contoso office.
* The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
* Currently, the helpdesk administrators can p erform tasks by using the: User administrator role without justification or approval.
* When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.
Planned Changes
Contoso plans to implement t he following changes.
Implement self-service password reset (SSPR). Analyze Azure audit activity logs by using Azure Monitor- Simplify license allocation for new users added to the tenant. Collaborate with the users at Fabrikam on a joint marketing campaign . Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named Corporation. One hundred new A Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Technical Requirements
Contoso identifies the following technical requirements:
* AH users must be synced from AD DS to the contoso.com Azure AD tenant.

* App1 must have a redirect URI pointed tohttps://contoso.com/auth-response.
* License allocation for new users must be assigned automatically based on the location of the user.
* Fabrikam users must have access to the marketing department ' s SharePoint site for a maximumof 90 days.
* Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
* The helpdesk administrators must be able to manage licenses for only the users in their respective office.
* Users must be forced to change their pa ssword if there is a probability that the users ' identity was compromised.

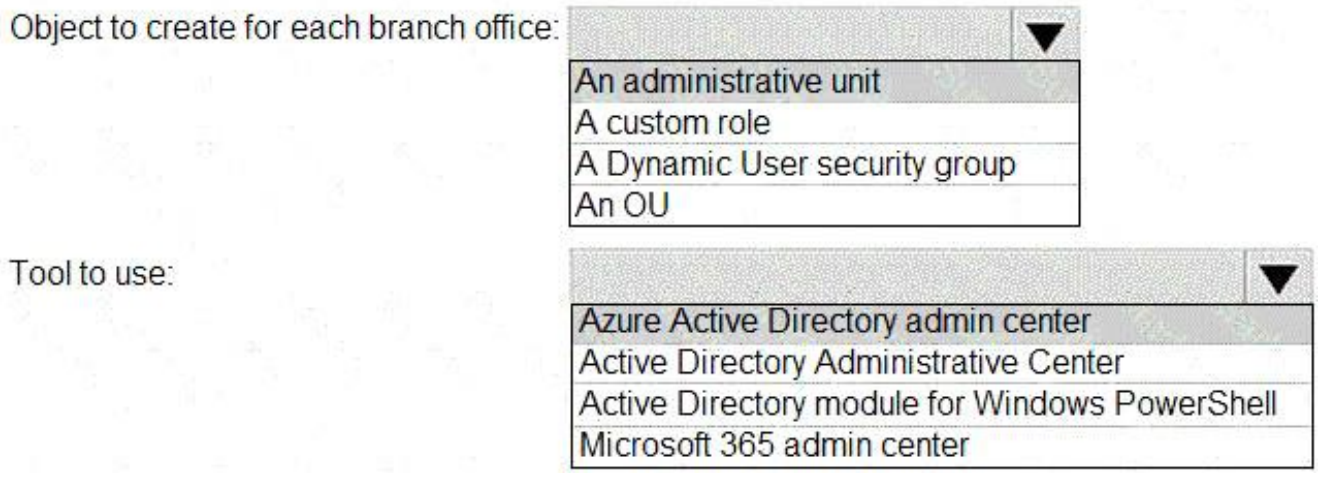
QUESTION NO: 2
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか?
回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



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 .

QUESTION NO: 3
Log Analyticsワークスペースを作成します。
監査に必要な技術要件を実装する必要があります。
Azure ADでは何を構成すべきですか？
A. 診断設定
B. 外部ID
C. アプリ登録
Answer: B
Explanation:
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.

QUESTION NO: 4
ADatumユーザーの同期が必要です。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。
あなたはどうすべきでしょうか？
A. PowerShell から Set-ADSyncScheduler を実行します。
B. PowerShell から Start-ADSyncSyncCycle を実行します。
C. 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。
Answer: A
Explanation:
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.

QUESTION NO: 5
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。

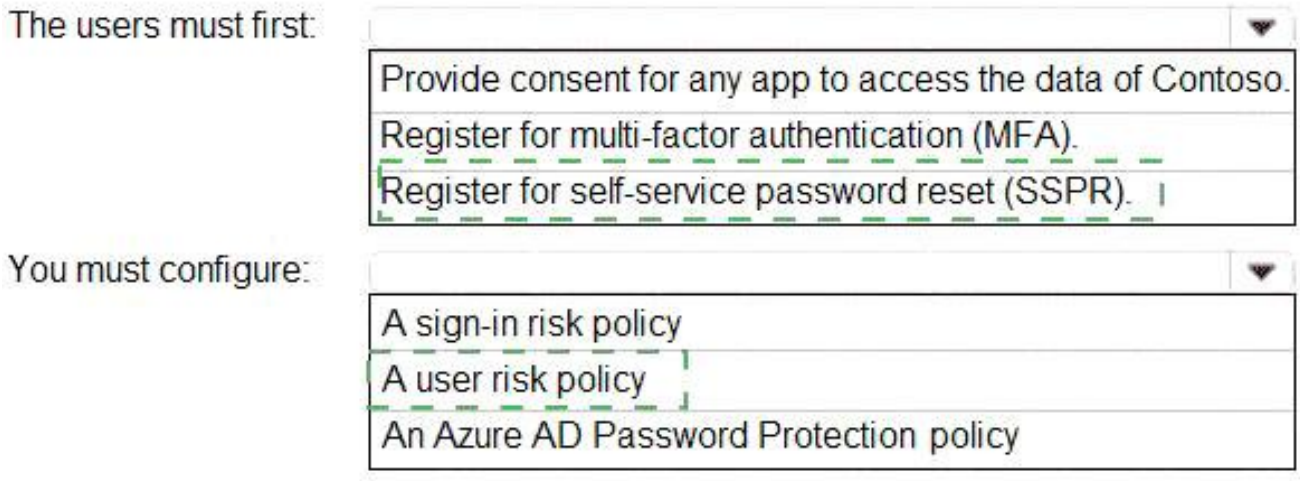
The users must first:

Provide consent for any app to access the data of Contoso.
Register for multi-factor authentication (MFA).
Register for self-service password reset (SSPR).

You must configure:

A sign-in risk policy
A user risk policy
An Azure AD Password Protection policy

Answer:



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.

QUESTION NO: 6
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

Answer: A

Explanation:

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 grou p, 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

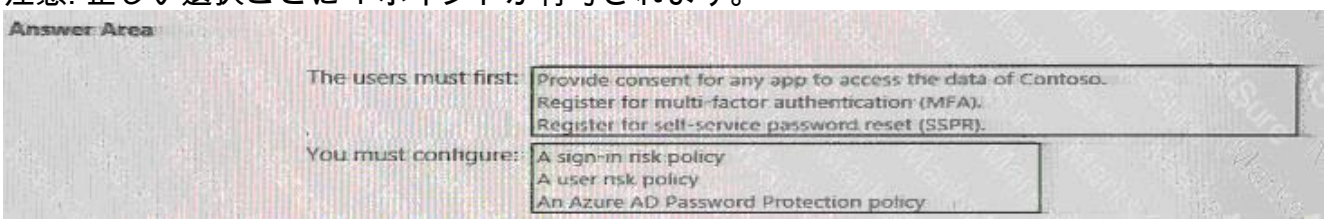
QUESTION NO: 7

ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。

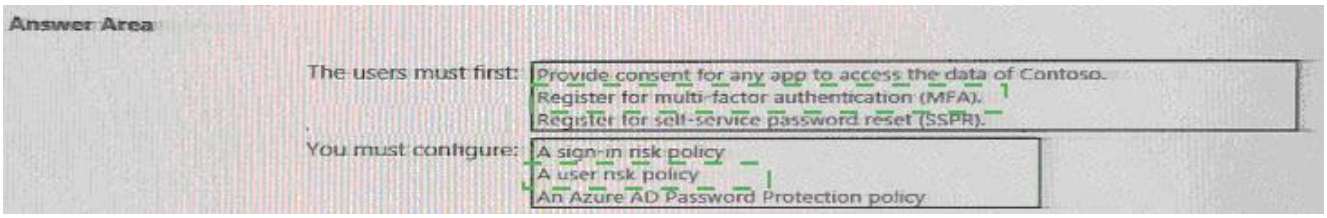
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか?

回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



Explanation:
The users must first: Register for multi-factor authentication (MFA)
You must configure: A user risk policy
According to Microsoft SC-300 official learning materials and Exam Ref SC-300: Mic rosoft Identity and Access Administrator , when the requirement is to address the probability that user identities were compromised, the appropriate feature is Azure AD Identity Protection.
Identity Protection detects risky sign- ins and risky users through continuous analysis of login behavior, location, device, and credential exposure signals.
Two types of policies can be created:
* Sign-in risk policy - Triggers actions based on suspicious sign-in behavior (for example, unfamiliar location).
* User risk policy - Triggers actions when the user's overall identity is deemed at risk (for example, compromised credentials).
The documentation specifies:
"When user risk is detected, the policy can require the user to change their password to remediate the risk.
Users must first be registered for MFA to perform secure password change operations."
Therefore, before the user risk policy can be enforced, users must be enrolled in multi-factor authentication (MFA). MFA is used during the remediation step (password change) to verify the user's identity securely.
Thus, to meet the requirement for "the probability that user identities were compromised," you configure a user risk policy in Azure AD Identity Protection, and ensure that users first register for MFA so that they can complete password change or verification flows when risks are detected.

QUESTION NO: 8
ユーザー管理者ロールの計画された変更を満たす必要があります。
何をすべきでしょうか?
A. アクセスレビューを作成します。
B. ロール設定を変更する
C. 管理者ユニットを作成します。
D. アクティブな割り当てを変更します。
Answer: B
Explanation:
In Azure AD Privileged Identity Management (PIM) for Azure AD roles, the exam materials describe that you tailor how a role (for example, User administrator) is used by editing its Role settings. These settings control activation behavior, including require multi-factor authentication, justification, approval, assignment
/activation durations, and notifications . The guide states that administrators can "configure activation requirements and time-bound eligibility on a per-role basis" and "enforce approval

workflows and MFA at activation." Access reviews are used to periodically verify who still needs a role , but they do not implement the operational changes to how the role is activated. Active assignments simply shows and changes who currently holds active/eligible assignments; it does not set policy for the role's activation behavior.
Administrative units scope certain directory tasks, but they are not how you change PIM activation/approval
/MFA requirements. Therefore, to meet planned changes for the User administrator role (such as least privilege activation with approval, justification, and MFA), you update PIM # Azure AD roles # User administrator # Role settings. This aligns with the SC-300 objective to "configure PIM settings and policies for Azure AD roles," ensuring governance by policy rather than ad-hoc assignment.

QUESTION NO: 9
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
Answer: B
Explanation:
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 rem ove 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 "distributio n 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 sec urity 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 th e group based on the rule, licenses are added or removed automatically."

QUESTION NO: 10
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
Answer: D
Explanation:
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 se cure 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.
answer: D. Azure AD Application Proxy
Topic 2, Litware, IncOverview
Litware, Inc. is a pharmaceutical company that has a subsidiary named fabrikam, inc Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a V PN connection.
Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash s ynchronization disabled.
Litware.com contains a user named User1 who oversees all application development. Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litw are.com by using gu est accounts in the litware.com tenant.
Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices in Microsoft Cloud App Security are enabled.
Litware has an Azure s ubscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector.

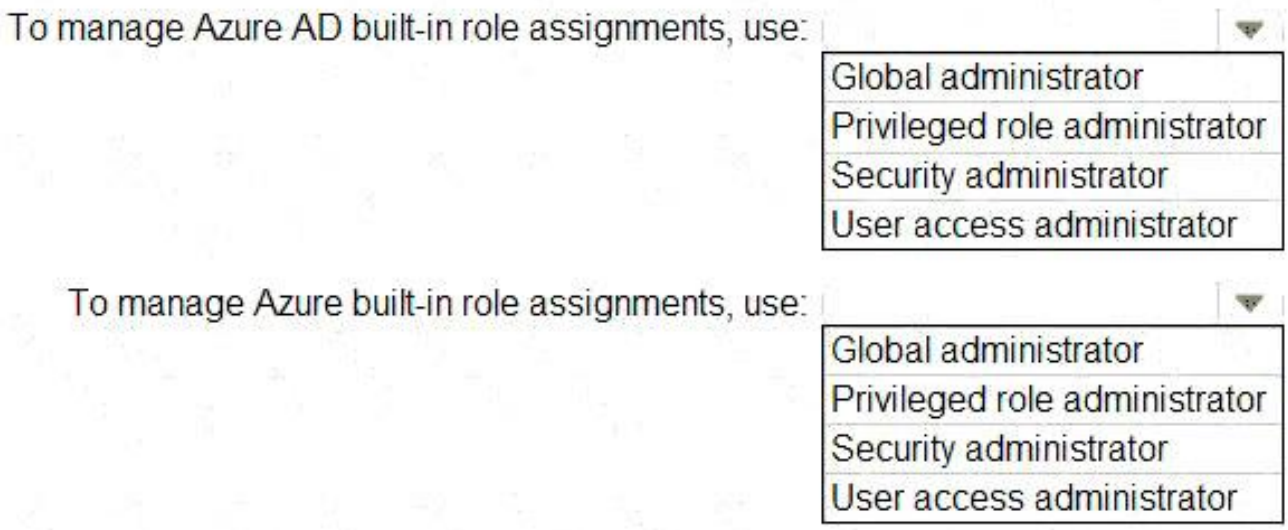
Azure Sentinel currently collects the Azure AD sign-ins logs and au dit logs.
On-premises Environment
The on-premises network contains the severs shown in the following table.

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

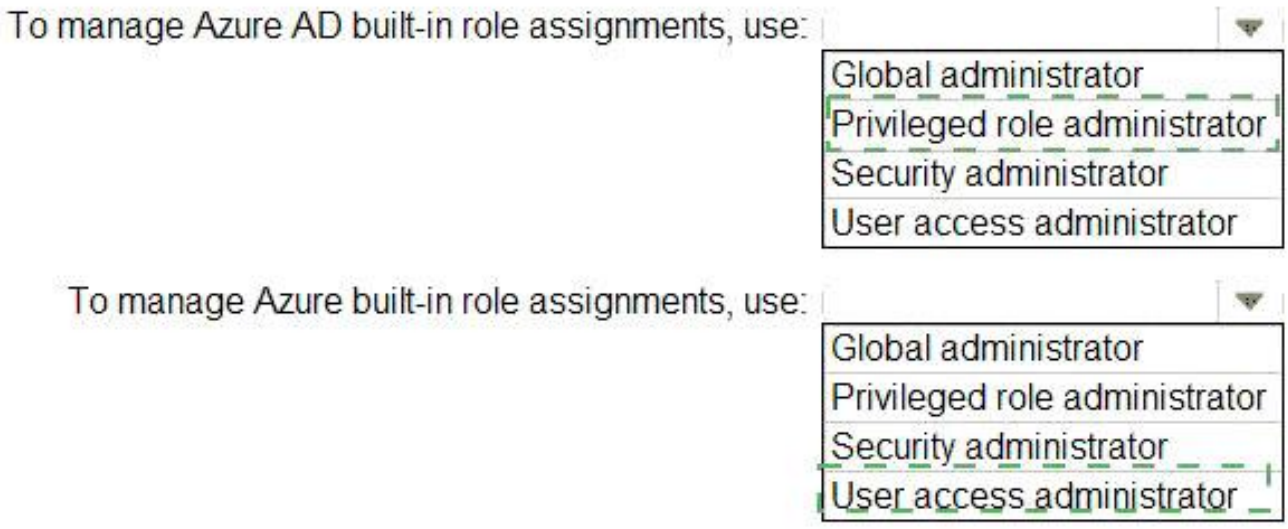
Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Delegation Requirements
Litware identifies the following delegation requirements:
* Delegate the management of privileged roles by using Azure AD Pri vileged Identity Management (PIM).
* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant-
* Use custom catalogs and custom programs for Identity Governance.
* Ensure that User1 can create enterprise applications in Azure AD. Use the principle of least privilege.
Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to Microsoft
365 group that he appropriate license assigned.
Management Requirement
Litware wants to create a group named LWGroup1 will conta in all the Azure AD user accountsfor Litware but exclude all the Azure AD guest accounts.
Authentication Requirements
Litware identifies the following authentication requirements:
* Implement multi-factor authentication (MFA) for all Litware users.
* Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
* Implement a banned password list for the litware.com forest.
* Enforce MFA when accessing on-premises applications.
* Automatically detect and remediate externally leaked credentials
Access Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

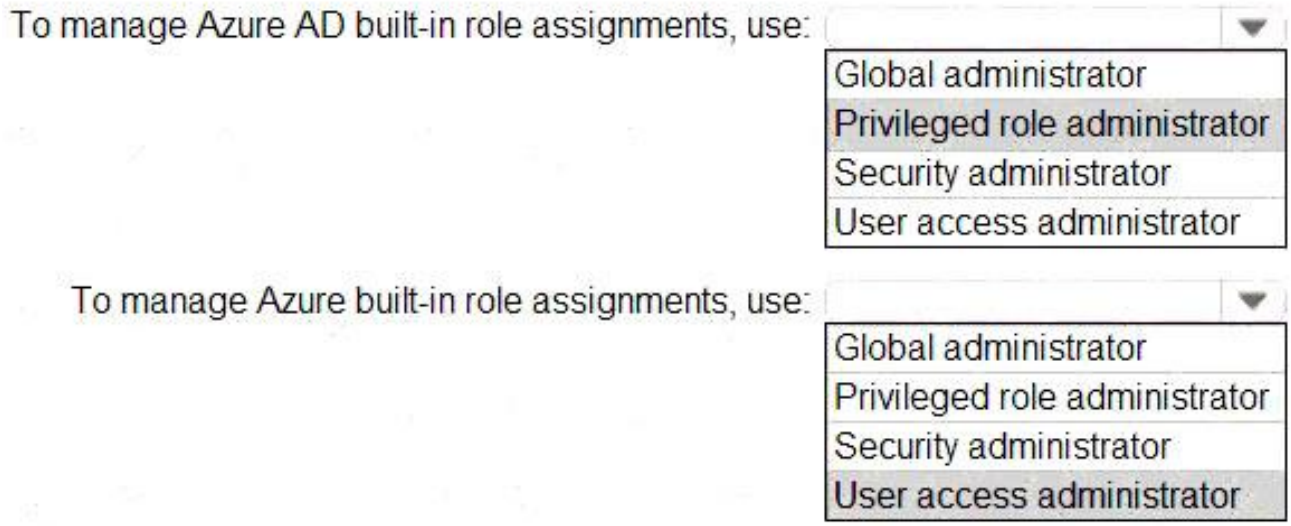
QUESTION NO: 11
役割の割り当てを管理するために使用する役割を特定する必要があります。ソリューションは委任要件を満たす必要があります。
どうすればいいでしょうか?
回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



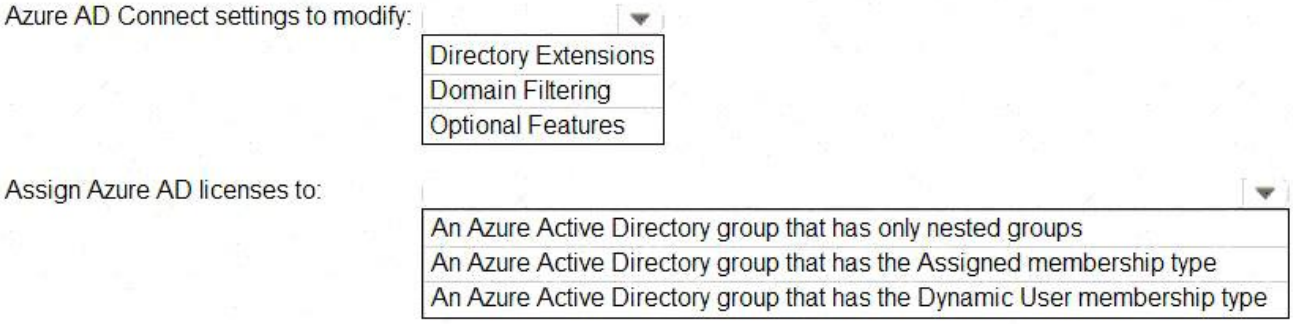
Explanation:



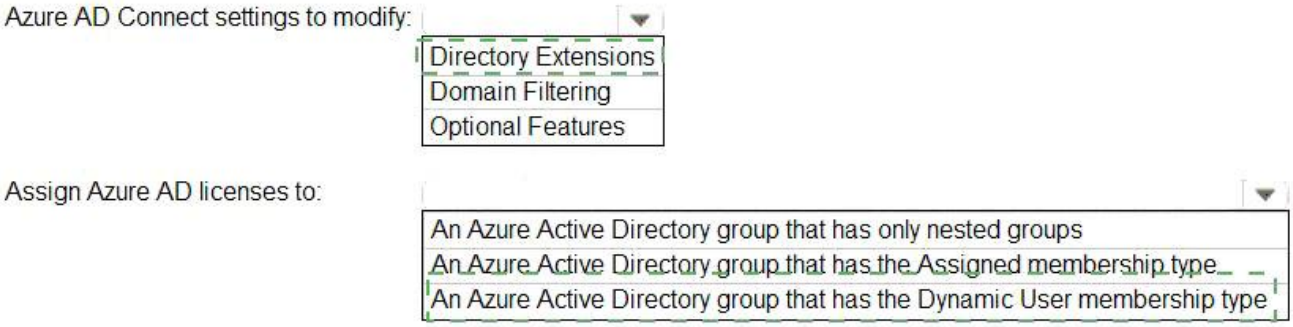
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn modules "Implement and manage Azure AD roles" and "Implement Privileged Identity Management (PIM)" , there is a clear distinction between Azure AD built-in roles and Azure (resource-based) built-in roles.
* Azure AD built-in roles govern directory-level access - such as managing users, groups, enterprise apps, or security settings in Azure Active Directory (Entra ID). The Privileged Role Administrator role allows the user to manage role assignments for directory roles in Azure AD, including activating roles through PIM. The Global Administrator also has this capability, but the Privileged Role Administrator is the least privilege role that meets the delegation requirement - aligning with the principle of least privilege stated in the scenario. As the documentation notes:
"Privileged Role Administrator manages role assignments in Azure AD, including the ability to activate and assign role s through Azure AD Privileged Identity Management."
* Azure built-in roles, on the other hand, are used to control access at the Azure resource level - for subscriptions, resource groups, and individual resources. The role responsible for managing these assignments is the User Access Administrator. This role can grant or revoke access to Azure resources by managing role assignments within Azure RBAC (Role-Based Access Control). The Microsoft documentation states:
"User Access Administrator allows management o f user access to Azure resources. It can assign roles in Azure RBAC for resources, subscriptions, and management groups."
Therefore:
To manage Azure AD built-in role assignments # Privileged role administrator
To manage Azure built-in role assignments # User access administrator This approach satisfies the delegation requirement mentioned in the scenario by assigning the least-privileged roles necessary for each type of role management task.

QUESTION NO: 12
Litware ユーザーへの Azure AD
ライセンスの割り当てを構成する必要があります。ソリューションはライセンス要件を満たしている必要があります。
どうすればいいでしょうか?
回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

In the SC-300 coverage of Azure AD Connect and Identity Governance, Microsoft explains that to surface a custom on-premises attribute in Azure AD you must enable Directory extensions in Azure AD Connect. The guide states that "Directory extensions lets you synchronize additional attributes from on-premises Active Directory to Azure AD so they are available in the cloud directory for apps and policy." This is the supported way to bring a custom attribute (here, LWLi censes) from the litware.com forest into Azure AD so it can be referenced by cloud features such as dynamic group rules. Domain filtering or optional features do not expose a new attribute to Azure AD; directory extensions does.
For license automation, the SC-300 materials on group-based licensing and dynamic groups emphasize that
"licenses can be assigned to Azure AD groups; group members then inherit the licenses, and when membership changes, licenses are added or removed automatically." They further note that "dynamic user groups evaluate rules against user attributes to add or remove users without manual effort," and that "nested groups are not supported for license inheritance-only direct members receive licenses." Using the synced LWLicenses attribute in a Dynamic User group rule (for example, user.extensionAttribute... -eq " E5 ") ensures users are automatically added to the correct group and therefore receive the specified licenses without

administrative intervention, fully meeting Litware's requirement t o "manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute."

QUESTION NO: 13
Identity Governance
を使用してアプリケーションアクセスの割り当てを追跡する必要があります。ソリューションは委任要件を満たす必要があります。
まず何をすべきでしょうか?
A. エンタープライズ アプリケーションのユーザー同意設定を変更します。
B. カタログを作成します。
C. プログラムを作成します。
D. エンタープライズ アプリケーションの管理者の同意要求設定を変更します。
Answer: B
Explanation:
In Azure AD Identity Governance, application access granted through Entitlement management is organized around catalogs and access packages. The SC-300 study materials explain that "a catalog is a container for resources and access packages" and that you must add your enterprise applications (or the groups tied to those apps) to a catalog before you can build access packages that users can request. Creating the catalog first enables you to place only the required resources in scope and to delegate day-to-day ownership: "catalog owners can manage the resources and access packages within their catalog without being tenant-wide admins," satisfying the delegation requirement to use custom catalogs and least privilege. After the catalog exists, you create one or more access packages that include the application (or groups) and policies that control who can request, how they are approved, and for how long. Identity Governance then lets you track access package assignments and review who has the app over time. By contrast, programs are used to group and report on governance initiatives (for example, collections of access reviews) rather than to onboard application resources; and modifying user/admin consent settings affects app consent behavior, not the lifecycle tracking of assignments. Therefore, the correct first step to track application access assignments while meeting the delegation requirements is to create a catalog.

QUESTION NO: 14
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。

For on-premises applications:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish an application by using Azure AD Application Proxy.

Answer:

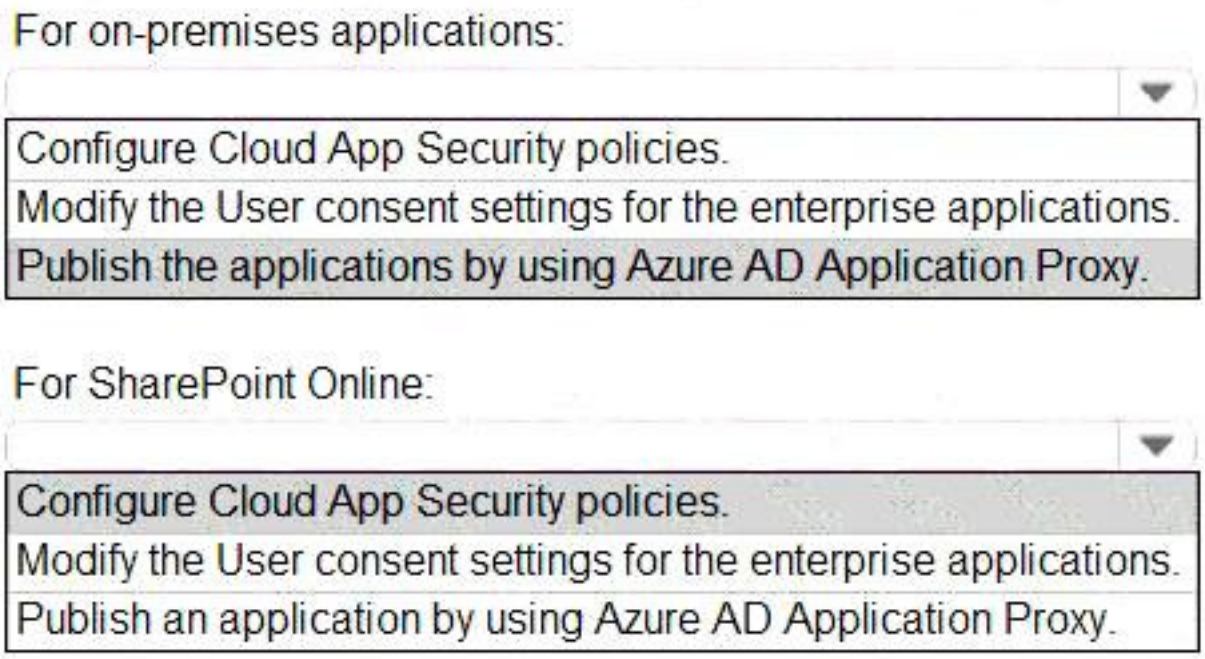
For on-premises applications:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

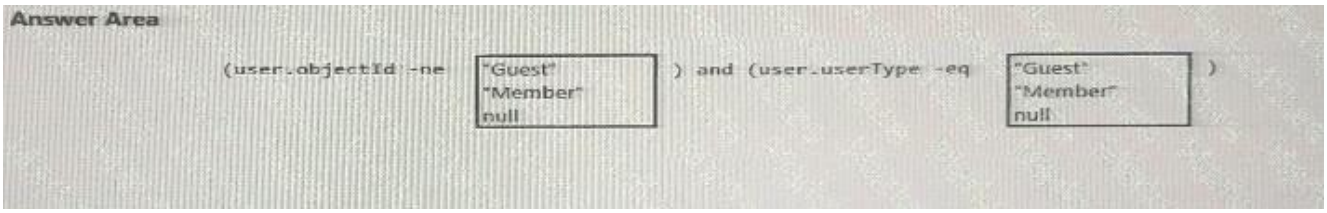
Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish an application by using Azure AD Application Proxy.

Explanation:

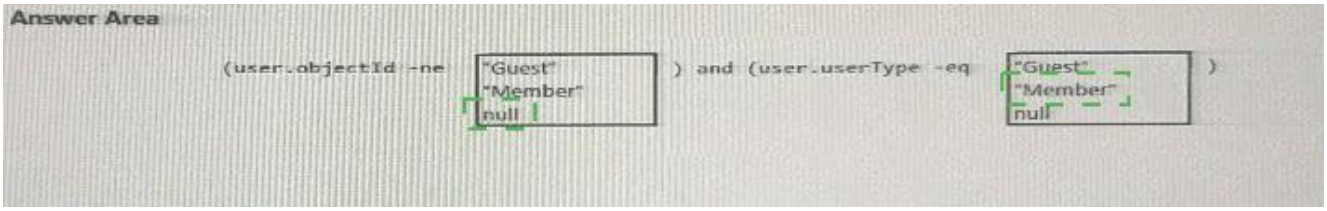


SC-300 materials stress that to enforce modern controls (like MFA) on on-premises apps, you must front them with Azure AD so Conditional Access can evaluate sign-ins. The documentation states that Azure AD Application Proxy " provides secure remote access to on-premises applications " and that apps published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

QUESTION NO: 15
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。

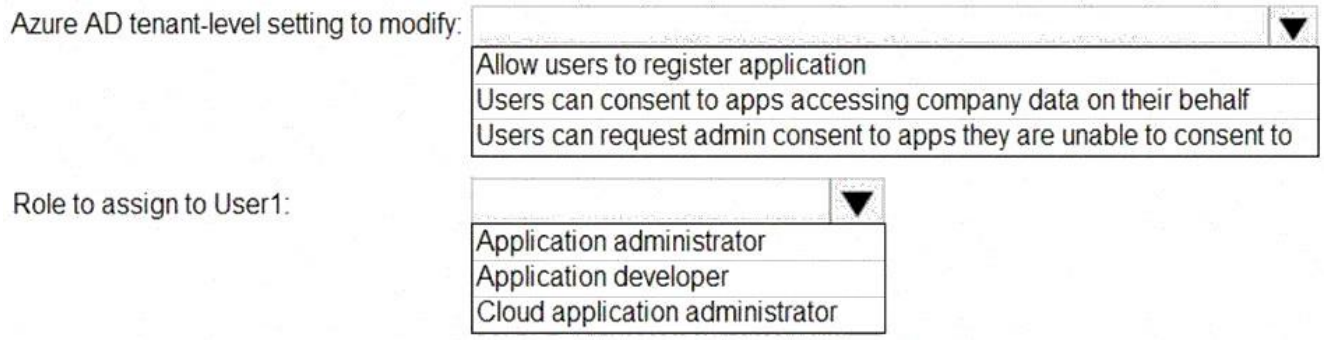


Answer:

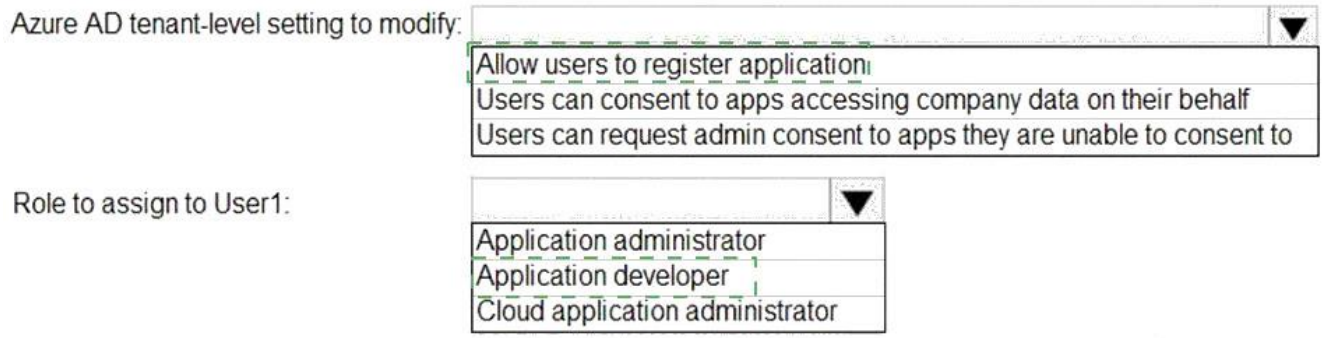


Explanation:
According to the Microsoft Identity and Access Administrator (SC-300) Exam Ref and the Azure AD Dynamic Membership Rul es documentation , when you create a dynamic group in Azure Active Directory (now Entra ID), you define rules that automatically add or remove users based on their attributes.
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.c om 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 rul es" , 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 ")

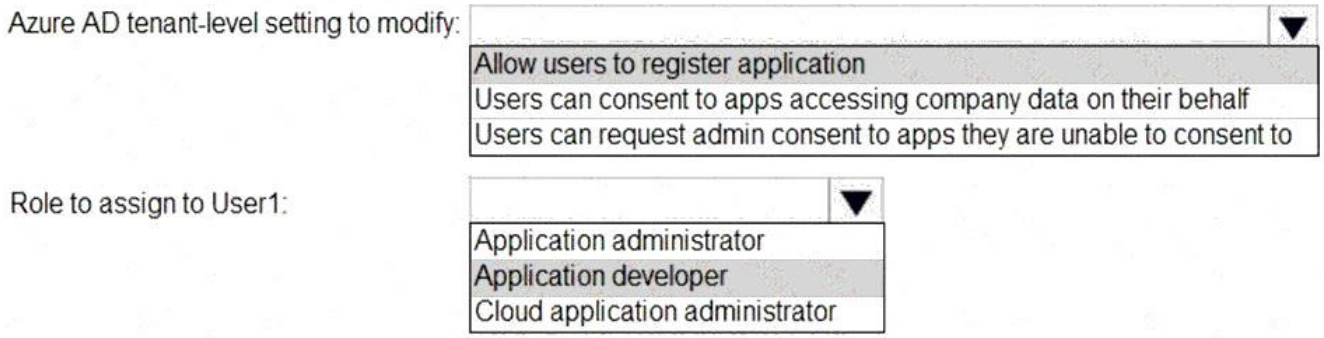
QUESTION NO: 16
委任要件を満たすには、Azure AD でアプリの登録を構成する必要があります。
どうすればいいでしょうか?
回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

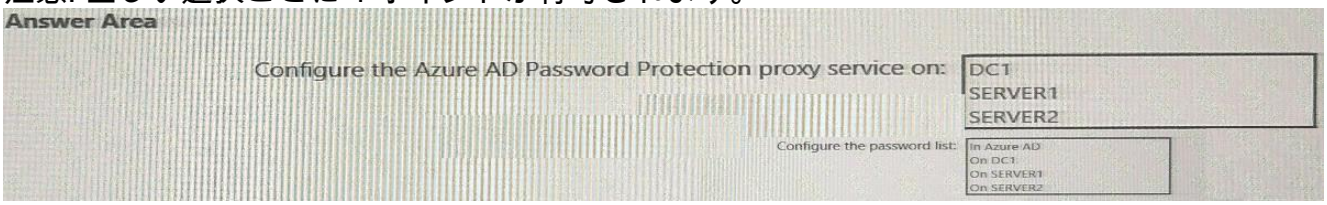


Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

QUESTION NO: 17
認証要件を満たすには、パスワード制限を実装する必要があります。
DC1 に Azure AD パスワード保護 DC エージェントをインストールします。
次に何をすべきでしょうか?
回答するには、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:

Explanation:
Server1
On DC1
Azure AD Password Protection has two components: the DC agent (installed on domain controllers) and the proxy service (installed on one or more member servers). The SC-300 materials and Microsoft Identity Governance guidance explain that the proxy service is required when domain controllers do not have direct internet access. The proxy retrieves the password protection policy and custom banned password list from Azure AD over outbound HTTPS and makes it available to DC agents. The documentation further states that you should deploy at least one proxy per forest and two for high availability, and that domain controllers do not need internet connectivity when a proxy is deployed. In this scenario, DCs are explicitly blocked from internet access, so the proxy must be placed on member servers. Both SERVER1 (Application Proxy connector) and SERVER2 (Azure AD Connect) are domain-joined member servers with internet connectivity and are appropriate locations for the AzureADPasswordProtectionProxy service; selecting both provides the recommended redundancy. The custom banned password list is configured in Azure AD at the tenant level (as part of Azure AD Password Protection settings), not on individual servers. Once configured, the policy and list are downloaded by the proxy and enforced by the DC agent during password set or change operations, satisfying the requirement to implement a banned password list for the litware.com forest.

QUESTION NO: 18
漏洩した資格情報に対する認証要件を満たす必要があります。
何をすべきでしょうか?
A. Azure AD Connect で PingFederate とのフェデレーションを有効にします。
B. Azure AD パスワード保護を構成します。
C. Azure AD Connect でパスワード ハッシュ同期を有効にします。
D. Azure AD で認証方法ポリシーを構成します。
Answer: C
Explanation:
In SC-300, Azure AD Identity Protection is the prescribed control to "automatically detect and remediate externally leaked credentials." That specific user risk-Leaked credentials-relies on Microsoft comparing known breached username/password pairs with what Azure AD can evaluate. The study materials explain that Identity Protection "detects leaked credentials when Microsoft finds a match with the user's current credentials," and also note that password hash synchronization (PHS) can be enabled even if your sign-in method is Pass-through Authentication or federation. A common exam call-out is that without PHS, Azure AD has no hash to compare, so the leaked-credential signal is unavailable. Enabling PHS (you can keep PTA as the active sign-in method) allows Identity Protection to raise user risk and enforce policy actions such as require password change or block access. By contrast, Azure

AD Password Protection addresses banned/weak passwords at change time, not breached-credential telemetry; federation choices (e.g., PingFederate) don't deliver the leaked-credential signal; and authentication method policy controls how users perform MFA (e.g., methods) rather than whether leaked credentials are detected. Therefore, to meet the requirement to
"automatically detect and remediate externally leaked credentials," the minimum correct step is to enable password hash synchronization while retaining PTA-exactly as recommended in SC-300 guidance.

QUESTION NO: 19
監視要件を満たすには、多段階攻撃の検出を構成する必要があります。
何をすべきでしょうか?
A. Azure Sentinel ルールのロジックをカスタマイズします。
B. ワークブックを作成します。
C. Azure Sentinel データ コネクタを追加します。
D. Azure Sentinel プレイブックを追加します。
Answer: A
Explanation:
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "M onitor and respond to Azure AD events with Azure Sentinel" , multi-staged attacks are advanced threat scenarios that require correlation of multiple events - for example, a suspicious sign-in followed by abnormal Office 365 activity.
The scenario in the question states:
"Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity." Azure Sentinel's Fusion rule is a built-in, machine-learning-driven correlation rule that automatically detects multi-stage attacks by analyzing anomalies across multiple data sources such as Azure AD sign-in logs, Office 365 activity, and security alerts. However, to fine-tune detection or meet specific organizational monitoring requirements, administrators can customize the rule logic in Sentinel analytics. This allows you to define how different signals and events are correlated, what thresholds trigger an alert, and how Sentinel interprets combined anomalies.
Microsoft documentation states:
"Fusion uses correlation logic in analytics rules to detect complex multi-stage attacks. Administrators can customize rule logic to meet specific detection requirements and fine-tune alert sensitivity ." The other options do not meet the requirement:
* B. Create a workbook # Used for visualization and reporting, not detection.
* C. Add data connectors # Used to ingest data sources; this is already configured.
* D. Add a playbook # Used for automated response, not for detection logic configuration.
# Correct Answer: A. Customize the Azure Sentinel rule logic

QUESTION NO: 20
ボストンオフィスから接続するユーザーに対して、MFA設定を構成する必要があります。ソリューションは、認証要件とアクセス要件を満たす必要があります。
何を設定すればよいでしょうか?

A. プライベートIPアドレス範囲を持つ名前付き場所
B. パブリックIPアドレス範囲を持つ名前付き場所
C. パブリックIPアドレス範囲を持つ信頼できるIP
D. プライベートIPアドレス範囲を持つ信頼できるIP
Answer: B
Explanation:
SC-300 emphasizes using Conditional Access with named locations to scope MFA-especially to exclude trusted corporate egress IPs . The materials state that administrators can define named locations by public IP ranges and "mark them as trusted" for policy exceptions. This aligns with the requirement: enforce MFA for all users, but exempt users authenticating from the Boston office. Because Azure AD evaluates the client's public egress address, private RFC1918 ranges are never seen by Azure AD on the internet, so defining private IP ranges would not work. Likewise, the legacy "Trusted IPs" setting belongs to the old per-user MFA service settings; SC-300 guidance prefers Conditional Access named locations for modern MFA deployments and for combining with other conditions (apps, platforms, user risk, locations). Implementing the Boston office as a named location using its public egress IP range(s), and marking it trusted, lets you exclude that location from the tenant-wide MFA policy while still meeting the broader requirement to enforce MFA for everyone else and for on-prem apps published via Azure AD Application Proxy. In short: define Boston's public IP as a named location and use it in your Conditional Access policy exclusion to satisfy the exemption precisely and securely.
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 dom ain 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 foll owing 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 li mit.
* 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 th e 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 rol e 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 method s 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.

QUESTION NO: 21
App1 という名前の Web アプリが含まれる Microsoft 365 E5
サブスクリプションがあります。
ゲストユーザーには、App1 へのアクセスが定期的に許可されます。
過去 30 日間に App1 にアクセスしていないゲスト
ユーザーのアクセスが削除されるようにする必要があります。ソリューションでは管理の労力を最小限に抑える必要があります。
何を設定すればよいでしょうか?
A. コンプライアンスポリシー
B. アプリケーションアクセスのアクセスレビュー
C. ゲストアクセスレビュー
D. 条件付きアクセスポリシー
Answer: B
Explanation:
According to Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn - Manage access reviews in Azure AD Identity Governance , administrators can configure acc ess reviews for users who have access to specific applications. Access reviews are ideal when you need to regularly validate user access and automatically remove inactive

or unnecessary accounts, including guest users.
For guest access to applications like App1 , Azure AD allows you to configure an access review for application access with recurrence (for example, every 30 days). In the review settings, you can enable the option "Automatically remove access for users who do not respond" or "Remove access if user has not signed in within 30 days." This automation fulfills the requirement to remove access for guest users who haven't used the app in 30 days while minimizing administrative effort-no manual intervention needed.
Correct Answer: B. an access revie w for application access

QUESTION NO: 22
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
Answer: C
Explanation:
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:

QUESTION NO: 23
contoso.comという名前のAzureActive Directory（Azure AD）テナントがあり、Azure AD IdentityProtectionポリシーが適用されています。
Azure Sentinelインスタンスを作成し、Azure ActiveDirectoryコネクタを構成します。
Azure Sentinelが、Azure AD IdentityProtectionによって発生したリスクアラートに基づいてインシデントを生成できることを確認する必要があります。
あなたは最初に何をすべきですか？
A. AzureSentinelデータコネクタを追加します。
B. Azure AD IdentityProtectionで通知設定を構成します。
C. AzureSentinelプレイブックを作成します。
D. AzureADの診断設定を変更します。
Answer: D
Explanation:
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn module "Integrate Azure AD Identity Protection with Azure Sentinel" , Azure Sentinel (now part of Microsoft Defender XDR) can collect and analyze Azure AD Identity Protection (AIP) alerts to generate incidents and automated responses. However, Sentinel cannot directly pull these alerts until diagnostic logging is enabled in Azure AD.
By default, Azure AD does not send Identity Protection data (such as User risk detections , Sign-in risk detections , and Risky users) to Sentinel. To integrate them, you must first enable diagnostic settings to send these logs to a Log Analytics workspace that Sentinel uses. Once logs are being streamed, Sentinel can correlate and generate incidents from these risk alerts using its built-in analytics rules or custom playbooks.
The official Microsoft documentation states:
"To surface Azure AD Identity Protection alerts in Azure Sentinel, you must first enable Azure AD diagnostic logs and send them to a Log Analytics workspace connected to Sentinel."
* Modify Azure AD diagnostic settings # Enable log categories:
* AuditLogs
* SignInLogs
* RiskyUsers
* RiskDetections
* Stream these logs to the Log Analytics workspace linked to Azure Sentinel.
* Azure Sentinel can now use data connectors and analytic rules to trigger incidents or automation playbooks based on risk events.
* A. Add an Azure Sentinel data connector: You do that after diagnostic settings are

configured and logs are available in Log Analytics.
* B. Configure Notify settings in Azure AD Identity Protection: This only controls email notifications to administrators - it does not forward alerts to Sentinel.
* C. Create an Azure Sentinel playbook: Playbooks are for automated responses, not for collecting data.
Step-by-step reasoning: Why not the other options:

QUESTION NO: 24
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
Answer: B
Explanation:
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.

QUESTION NO: 25
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
Answer: B
Explanation:
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.

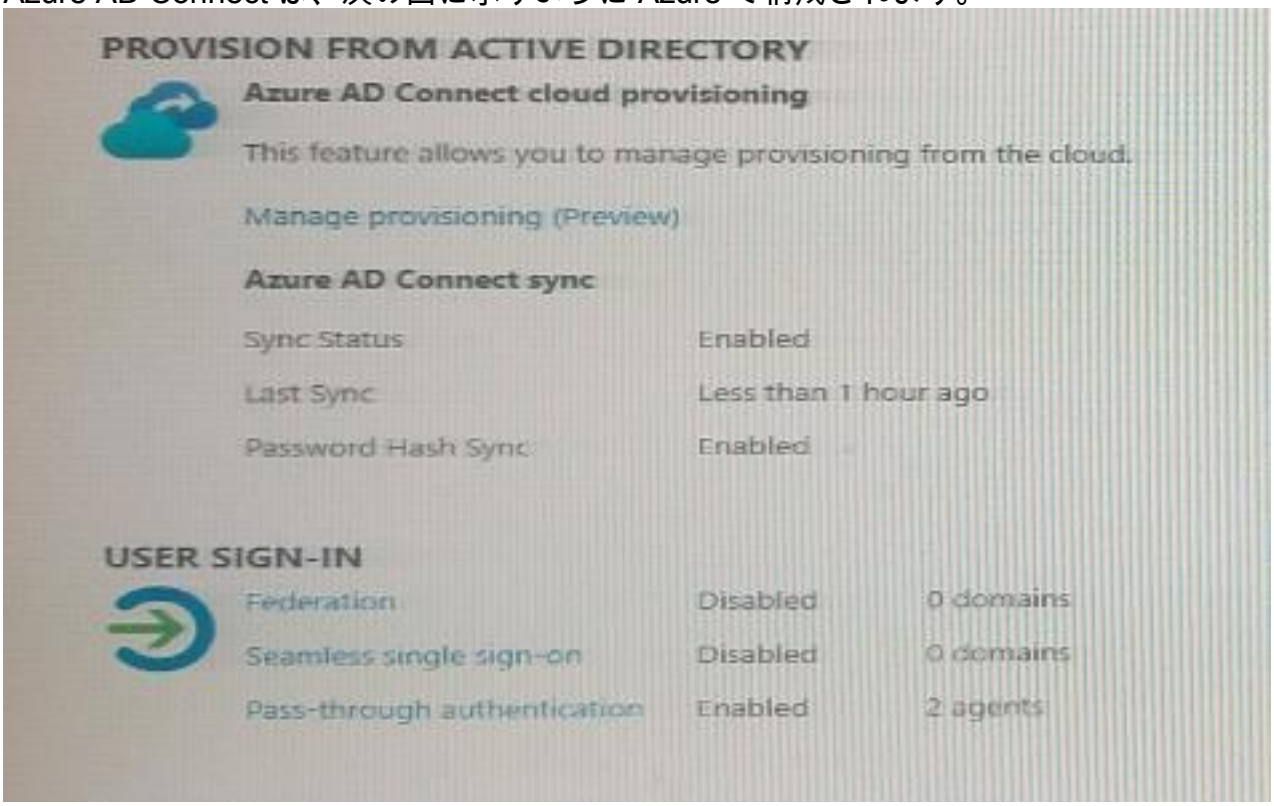
QUESTION NO: 26
Microsoft 365 テナントがあります。
Azure Monitor を使用して、Azure Active Directory (Azure AD)
監査ログ情報を表示できるようにする必要があります。
まず何をすべきでしょうか?
A. Get-AzureADAuditDirectoryLogs コマンドレットを実行します。
B. Azure AD ブックを作成します。
C. Set-AzureADTenantDetail コマンドレットを実行します。
D. Azure AD の診断設定を変更します。
Answer: D
Explanation:
According 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 A D 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.

QUESTION NO: 27
ネットワークには、Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory

ドメインが含まれています。テナントには、次の表に示すものが含まれています。

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

すべてのユーザーはリモートで作業します。
Azure AD Connect は、次の図に示すように Azure で構成されます。



オンプレミス ドメインからインターネットへの接続が失われます。
どのユーザーが Azure AD にサインインできますか?

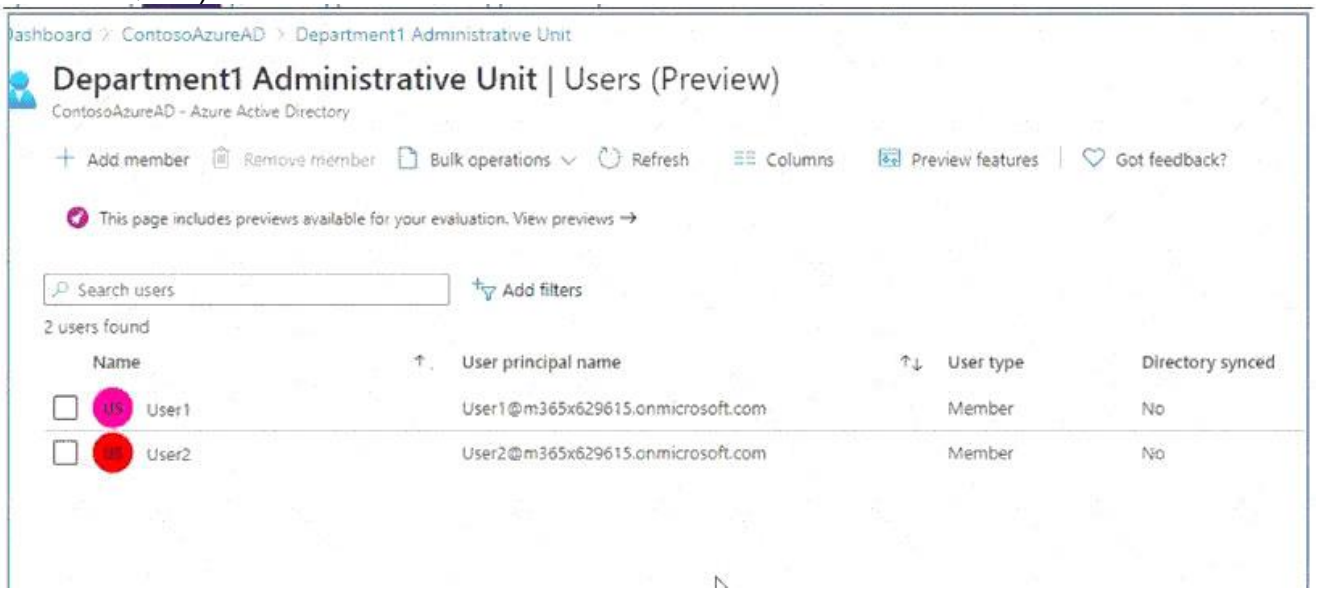
A. ユーザー1のみ
B. ユーザー1とユーザー3のみ
C. ユーザー1とユーザー2のみ
D. ユーザー1、ユーザー2、ユーザー3

Answer: C

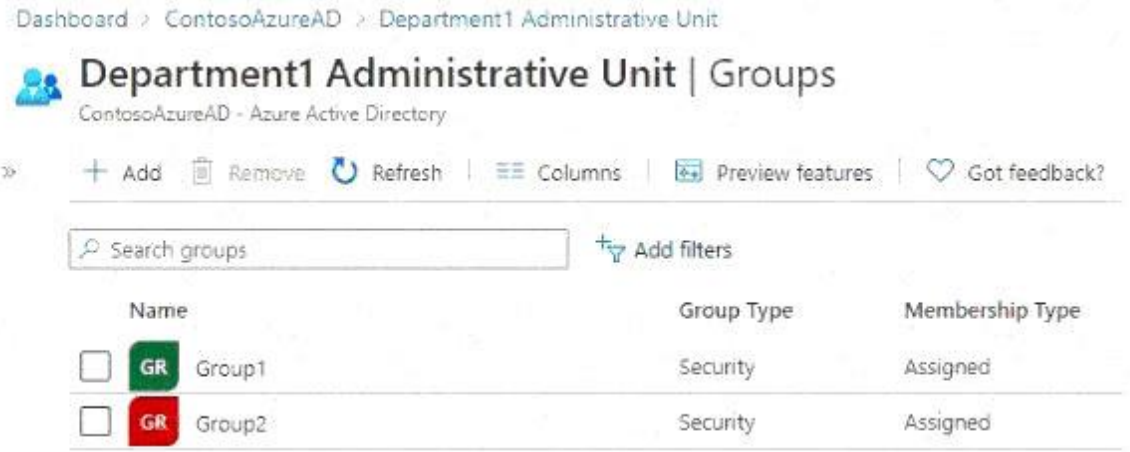
Explanation:
The exhibit shows Pass-through authentication (PTA) enabled with two agents and Password Hash Sync (PHS) enabled. SC-300 materials state that when both PTA and PHS are enabled, Azure AD can fall back to password hash verification if PTA agents are unavailable. With connectivity from on-premises to the Internet lost , PTA agents cannot validate passwords; however, PHS continues to allow cloud authentication for synchronized users. Therefore:
* User1 (cloud-only) authenticates in Azure AD directly, unaffected by on-prem connectivity.
* User2 (directory-synced) can still sign in because PHS is enabled and provides backup authentication when PTA is unreachable.
* User3 (guest) authenticates in the home tenant, which is independent of your on-prem

connectivity; the host tenant simply relies on the external identity.
SC-300 explicitly teaches that enabling PHS alongside PTA provides resiliency for sign-in and is a recommended best practice. Consequently, all three users can sign in under the described outage.

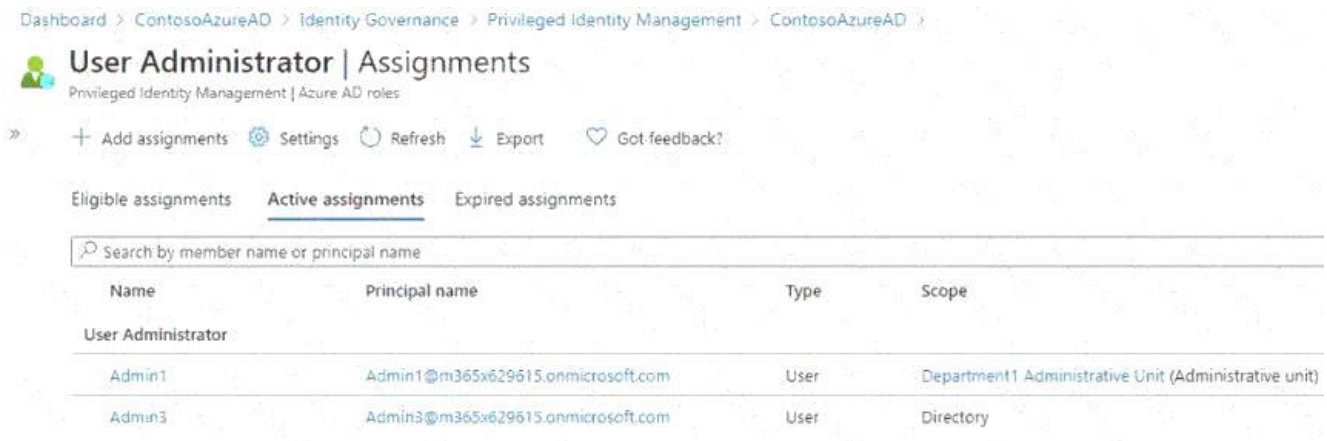
QUESTION NO: 28
Group3 というグループと Department1 という管理単位を含む Microsoft Entra テナントがあります。
部門には、「ユーザー」展示に示されているユーザーがいます。 (「ユーザー」タブをクリックします。)



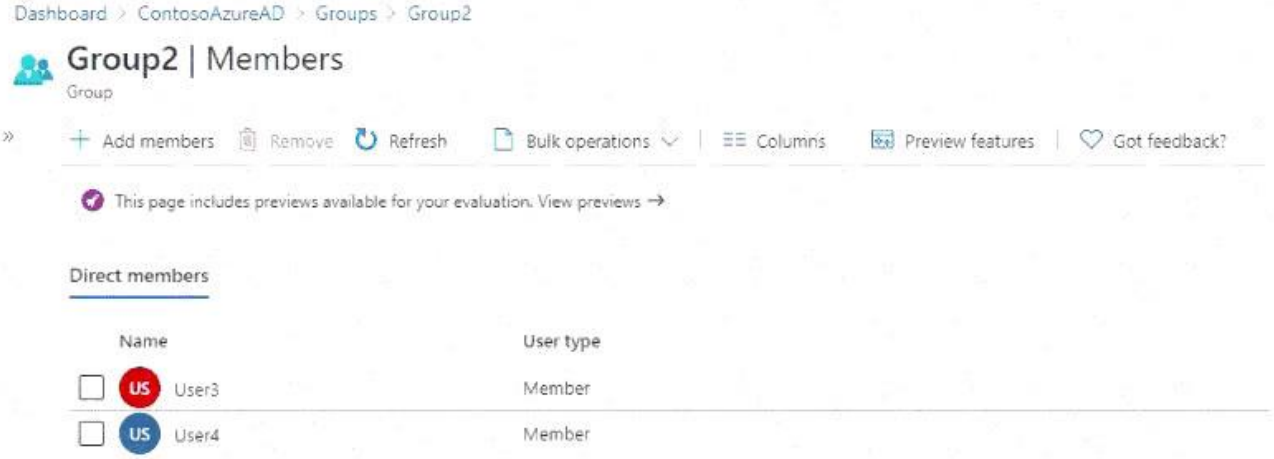
Department1 には、[グループ] 展示に表示されるグループがあります ([グループ] タブをクリックします)。



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。

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group3.	○	○
Admin3 can reset the password of User1.	○	○

Answer:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group3.	○	○
Admin3 can reset the password of User1.	○	○

Explanation:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	●
Admin1 can add User1 to Group3.	○	●
Admin3 can reset the password of User1.	●	○

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."

QUESTION NO: 29
contoso.com という名前の Microsoft Entra テナントがあり、その中に User1 という名前のユーザーがいます。User1 は、次の表に示すデバイスを所有しています。

Name	Platform	Registered in contoso.com
Device1	Windows 11	Yes
Device2	Windows 11	No
Device3	iOS	Yes

2025年11月5日、あなたはcontoso.comで以下の設定を含む利用規約を作成し、施行します。
* 名前: 用語 1
* 表示名: Contoso利用規約
* ユーザーに利用規約の展開を要求する: オン
* すべてのデバイスでユーザーに同意を求める: オン
* 同意の有効期限:
* 有効期限開始日：2025年12月10日
* 頻度：月1回
2025年11月15日、ユーザー1はデバイス3上で利用規約1に同意した。
2025年11月15日、ユーザー1はデバイス3上で利用規約1に同意した。
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
On November 20, 2025, User1 can accept Terms1 on Device1.	●	○
On December 11, 2025, User1 can accept Terms1 on Device2.	●	○
On December 7, 2025, User1 can accept Terms1 on Device3.	○	●

Answer:

Answer Area

Statements	Yes	No
On November 20, 2025, User1 can accept Terms1 on Device1.	●	○
On December 11, 2025, User1 can accept Terms1 on Device2.	●	○
On December 7, 2025, User1 can accept Terms1 on Device3.	○	●

Explanation:

Answer Area

Statements	Yes	No
On November 20, 2025, User1 can accept Terms1 on Device1.	●	○
On December 11, 2025, User1 can accept Terms1 on Device2.	●	○
On December 7, 2025, User1 can accept Terms1 on Device3.	○	●

QUESTION NO: 30
デフォルトのアプリ登録設定を持つ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	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

App1 と App2 という 2 つのクラウド アプリを購入します。グローバル管理者は、App1 を Azure AD に登録します。
App1 にユーザーを割り当てることができるユーザーと、Azure AD に App2 を登録できるユーザーを特定する必要があります。
何を特定する必要がありますか?
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 ポイントが加算されます。

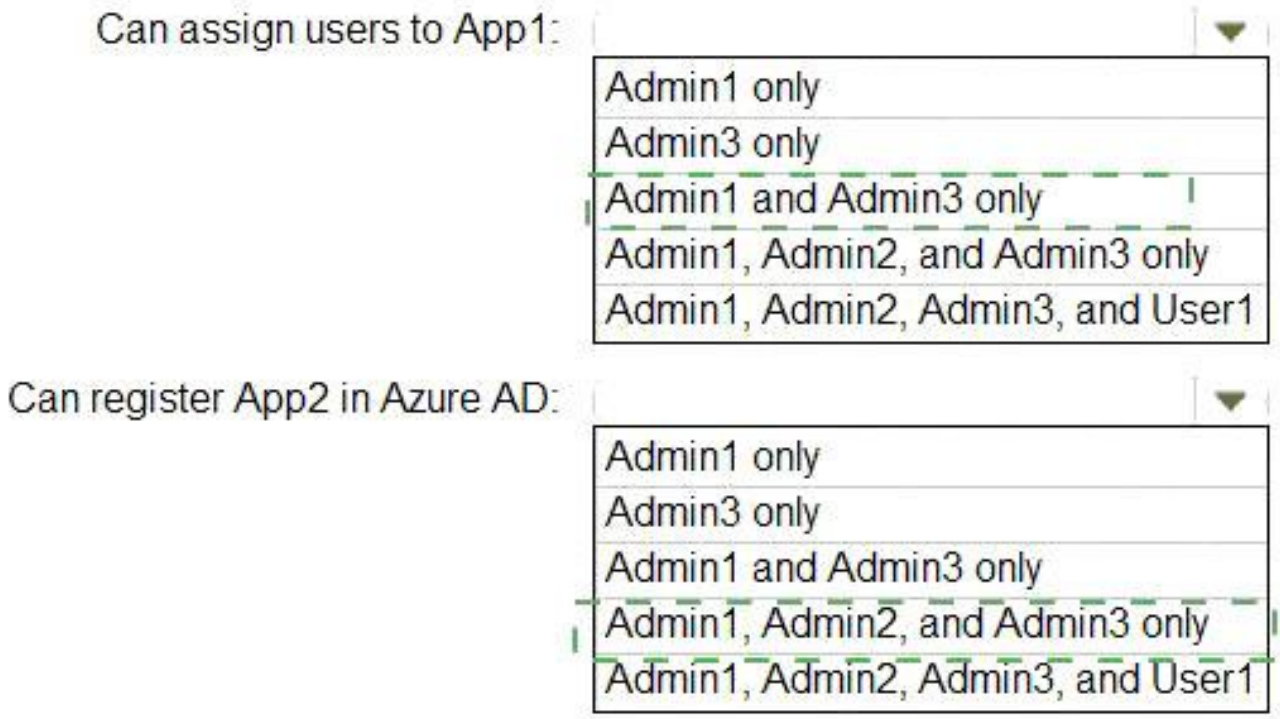
Can assign users to App1:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Answer:



Explanation:
* Can assign users to App1: Admin1 and Admin3 only
* Can register App2 in Azure AD: Admin1, Admin2, and Admin3 only
According to the Microsoft Identity and Access Adminis trator (SC-300) Study Guide and Microsoft Learn module "Manage enterprise applications and app registrations" , role-based access control (RBAC) in Azure Active Directory defines what administrative actions each role can perform for applications.
1# # Assign ing users to an enterprise application (App1):
The ability to assign users to enterprise apps (service principals) in Azure AD is granted to two specific roles:
* Application Administrator
* Cloud Application Administrator
These roles allow administrators to a dd and remove users or groups from the Users and Groups section of an enterprise app, manage application properties, and control assignments.
The Application Developer role is designed only to create and manage own app registrations , not to assign users to enterprise apps.
The User role has no administrative privileges related to app assignments.
Therefore, only Admin1 (Application Administrator) and Admin3 (Cloud Application Administrator) can assign users to App1.
2# # Registering applications in Azure AD (App2):
By default, the App registrations setting in Azure AD allows all users to register applications. However, if the question specifies that the default settings apply (which means users can register applications), then both admins and developers ca n register apps.
Microsoft documentation clarifies:
"By default, all users can register app registrations in Azure AD. Roles such as Application Developer, Application Administrator, and Cloud Application Administrator also have this

capability regardless of tenant-wide settings." Therefore, the following users can register new apps:
* Admin1 (Application Administrator)
* Admin2 (Application Developer)
* Admin3 (Cloud Application Administrator)
# Correct answer for registration: Admin1, Admin2, and Admin3 only
# Final Correct Answers:
* Can assign users to App1: Admin1 and Admin3 only
* Can register App2 in Azure AD: Admin1, Admin2, and Admin3 only

QUESTION NO: 31
Microsoft 365 ES サブスクリプションがあり、その中に User1 というユーザーがいます。User1 はアプリケーション管理者ロールの対象です。
User1 は、アプリケーション プロキシの新しいコネクタ グループを構成する必要があります。
User1 のロールをアクティブ化するにはどうすればよいですか?
A. Microsoft Defender for Cloud Apps ポータル
B. Microsoft 365 管理センター
C. Azure Active Directory 管理センター
D. Microsoft 365 Defender ポータル
Answer: C
Explanation:
User1 is eligible for the Application Administrator role and needs to configure an Application Proxy connector group. Application Proxy is an Azure AD feature used to publish on-premises applications securely.
To activate the eligible role, User1 must perform a Privileged Identity Management (PIM) activation within the Azure AD admin center.
From Microsoft Documentation:
"Privileged Identity Management (PIM) role activations are performed in the Azure AD admin center under Azure AD # Privileged Identity Management # My roles." Activation steps are not available through Microsoft 365 or Defender portals.

QUESTION NO: 32
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
Answer: B
Explanation:
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.

QUESTION NO: 33
「Terms1」という名前の使用条件 (ToU) を含む Microsoft Entra テナントがあります。
Policy1 という名前の条件付きアクセス ポリシーを作成して、Terms1
を展開します。ユーザーにTerms1への同意を要求するようにPolicy1を構成する必要があります。 Policy1 にはどの設定を構成する必要がありますか?
A. 条件
B. セッション
C. 許可
D. ターゲットリソース
Answer: B
Explanation:
Conditional Access policies evaluate Assignments (users, cloud apps), optional Conditions , and then enforce Access controls . In SC-300, Terms of use (ToU) is enforced via Grant controls : the policy must " require terms of use " so that users must accept a specified ToU before access is granted. The documentation states that the ToU experience is applied when a policy includes the control to " require terms of use ," and this control lives under the Grant section (alongside controls like require MFA, require compliant device, etc.
). Therefore, to deploy Terms1 with Policy1 , configure the Grant controls and select Require terms of use and choose Terms1 . Conditions or Session settings do not trigger ToU acceptance; they refine when or how access is permitted. Target resources select apps, but the enforcement of acceptance is strictly a Grant control.

QUESTION NO: 34
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
Answer: D
Explanation:
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.

QUESTION NO: 35
Microsoft Entra テナントには、Group1 というグループと、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 Group1 のメンバーです。
App1 という名前のエンタープライズ アプリケーションを登録します。
App1 のセルフサービス アプリケーション アクセスを有効にし、次の設定を構成します。
ユーザーがこのアプリケーションへのアクセスをリクエストできるようにする: はい
割り当てられたユーザーをどのグループに追加するか: Group1
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: はい
このアプリケーションへのアクセスを承認できるユーザー: User2
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
User1 must request access to App1 before they can use the app.	○	○
If User2 requests access to App1, they will be added to Group1 automatically.	○	○
User2 can approve App1 requests by using the Microsoft Entra admin center.	○	○

Answer:

Statements	Yes	No
User1 must request access to App1 before they can use the app.	○	○
If User2 requests access to App1, they will be added to Group1 automatically.	○	○
User2 can approve App1 requests by using the Microsoft Entra admin center.	○	○

Explanation:
User1 must request access to App1 before they can use the app: No
If User2 requests access to App1, they will be added to Gro up1 automatically: Yes User2 can approve App1 requests by using the Microsoft Entra admin center: Yes Let's break this down step by step based on Microsoft Entra ID self-service application access and the configured settings, as outlined in Microsoft Iden tity and Access Administrator documentation.
Understanding Self-Service Application Access in Microsoft Entra ID:
Self-service application access in Microsoft Entra ID allows users to request access to applications without needing an administrator to manua lly assign them. This is configured on a per-application basis.
The settings for App1 are:
Allow users to request access to this application: Yes- Users can request access to App1.
To which group should assigned users be added: Group1- Users who are grante d access will be added to Group1, which provides the necessary permissions to use App1.
Require approval before granting access to this application: Yes- Access requests must be approved before the user is added to Group1.
Who is allowed to approve access to this application: User2- User2 is the designated approver for access requests to App1.
Statement 1: User1 must request access to App1 before they can use the app.
Analysis:
User1 is already a member of Group1, as stated in the question.
The self-service settings specify that users who are granted access to App1 will be added to Group1. This implies that membership in Group1 is what grants access to App1.
Since User1 is already a member of Group1, they already have access to App1. In Microsoft Entra ID, i f a user is already assigned to an application (either directly or via group membership), they do not need to request access through the self-service process-they can simply use the app.
The self-service access request process is for users who are not yet assigned to the app (i.e., not in Group1).
Since User1 is already in Group1, they do not need to request access.
Conclusion:This statement isNo. User1 does not need to request access because they are already a member of Group1 and can use App1 immediately.
Statement 2: If User2 requests access to App1, they will be added to Group1 automatically.
Analysis:
User2 is not a member of Group1 (the question does not state that User2 is in Group1).
The self-service settings allow users to request access to App1, an d the setting " To which group should assigned users be added: Group1 " means that users who are granted access

will be added to Group1.
However, the setting " Require approval before granting access to this application: Yes " means that User2's request must be approved before they are added to Group1. The approver for App1 requests is User2 themselves, which introduces a potential conflict.
In Microsoft Entra ID, if a user is both the requester and the approver, the system typicallyallows them to approve thei r own request (unless additional policies prevent this, which is not specified in the question).
Therefore, User2 can request access and approve their own request.
Once the request is approved, User2 will be added to Group1 automatically as per the self-se rvice settings.
The term " automatically " in the statement refers to the process after approval-once approved, the addition to Group1 happens without further manual intervention.
Conclusion:This statement isYes. If User2 requests access to App1 and approves their own request, they will be added to Group1 automatically.
Statement 3: User2 can approve App1 requests by using the Microsoft Entra admin center.
Analysis:
The self-service settings specify that User2 is the designated approver for access requests to App1.
In Microsoft Entra ID, approvers can manage access requests through the Microsoft Entra admin center (via the " My Access " portal or the " Access Requests " section, depending on their role and permissions).
User2, as the designated approver, will rece ive a notification (via email or the My Access portal) when a request is made. They can then log into the Microsoft Entra admin center, navigate to the access requests section, and approve or deny the request.
Even though User2 is not explicitly an admin, the fact that they are designated as the approver for App1 requests grants them the ability to approve requests through the Microsoft Entra admin center.
Conclusion:This statement isYes. User2 can approve App1 requests using the Microsoft Entra admin cente r.
Additional Considerations:
If User2 were not allowed to approve their own request (e.g., due to a separation of duties policy), Statement
2 might be affected. However, Microsoft Entra ID does not enforce such a restriction by default, and the question d oes not specify any additional policies.
The Microsoft Entra admin center is the primary interface for managing access requests, but users can also approve requests via email links or the My Access portal. The statement specifically mentions the admin cent er, which is a valid method.
Conclusion:
Statement 1:No- User1 does not need to request access since they are already in Group1.
Statement 2:Yes- User2 will be added to Group1 automatically after their request is approved (by themselves).
Statement 3:Yes- User2 can approve requests using the Microsoft Entra admin center.
References:
Microsoft Entra ID documentation: " Configure self-service application access " (Microsoft Learn:

https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-self-se rvice)
Microsoft Entra ID documentation: " Manage access requests " (Microsoft Learn:https://learn.microsoft.com /en-us/entra/identity/governance/access-reviews-overview)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers self - service application access and approval workflows in Microsoft Entra ID.