# MICROSOFT SC-300 Exam Questions

**Total Questions: 300+**
**Demo Questions: 35**
**Version: Updated for 2025**

**Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner**

**For Access to the full set of Updated Questions – Visit:**
**Microsoft SC-300 Exam Questions by Cert Empire**

# Question: 1

You need to meet the authentication requirements for leaked credentials.
What should you do?

A. Enable federation with PingFederate in Azure AD Connect.

B. Configure Azure AD Password Protection.

C. Enable password hash synchronization in Azure AD Connect.

D. Configure an authentication method policy in Azure AD.

**Answer:**

C

**Explanation:**

To meet the requirements for leaked credentials for hybrid identities, you must enable password hash synchronization (PHS) in Azure AD Connect. PHS synchronizes a hash of the user's on-premises Active Directory password to Azure AD. This enables Azure AD Identity Protection to perform leaked credential detection by comparing the synchronized password hashes against a vast collection of credentials exposed in public data breaches. If a match is found, the user is flagged as high-risk, and automated remediation policies, such as forcing a password reset, can be triggered.



**Why Incorrect Options are Wrong:**

A. Enable federation with PingFederate in Azure AD Connect.
Federation offloads authentication to a third-party identity provider. This does not enable Azure AD's native leaked credential detection service.
B. Configure Azure AD Password Protection.
This feature prevents users from setting new passwords that are known to be weak or compromised. While related, it doesn't detect if a user's current password has been leaked, which is the primary function enabled by PHS for Identity Protection.
D. Configure an authentication method policy in Azure AD.
This policy manages which authentication methods (like MFA or FIDO2 keys) users can register and use. It is a response to risk, not the mechanism for detecting the risk of leaked credentials itself.
---

**References:**

1. Microsoft Learn, "What is Identity Protection?". Under the "Risk detections" section, for the "Leaked credentials" risk type, it states: "To detect leaked credentials for hybrid users that are synced from on-premises, you must enable password hash sync." This directly confirms that PHS is the required mechanism.
2. Microsoft Learn, "What is password hash synchronization with Azure AD?". In the section "Benefits of using password hash synchronization," one of the key benefits listed is "Leaked credential detection." It explains that PHS allows Azure AD to compare hashes against known compromised passwords.
3. Microsoft Learn, "Password protection for hybrid deployments". This document clarifies that Azure AD Password Protection is for blocking weak passwords, while Identity Protection's leaked credential detection (which requires PHS) is for identifying existing accounts that have been compromised.

## Question: 2

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements. What should you configure?

A. named locations that have a private IP address range

B. named locations that have a public IP address range

C. trusted IPs that have a public IP address range

D. trusted IPs that have a private IP address range

### Answer:

B

### Explanation:

To configure location-based access controls, such as for Multi-Factor Authentication (MFA), Azure Active Directory (Azure AD) uses the source public IP address of the user's connection. The recommended and most flexible method is to define the Boston office's public IP address range as a "Named Location." This named location can then be used as a condition within a Conditional Access policy to enforce or bypass MFA for users connecting from that trusted corporate network. Azure AD cannot see the internal private IP addresses of devices on the corporate network, as they are hidden by Network Address Translation (NAT).



### Why Incorrect Options are Wrong:

A. Azure AD evaluates the source IP of the connection, which is always a public IP address, not a private one from an internal network.
C. "Trusted IPs" is a legacy feature within the MFA service settings. The modern and recommended approach is to use Named Locations with Conditional Access policies.
D. The "Trusted IPs" feature, like Named Locations, relies on public IP addresses, as Azure AD has no visibility into an organization's private IP space.

### References:

1. Microsoft Learn, "Use the location condition in a Conditional Access policy": This document states, "With the location condition in Conditional Access, you can control access to your cloud apps based on the network location of a user... These locations can include public IPv4 or IPv6 network information". It explicitly details configuring named locations with public IP ranges. Section: "Define locations" and "Named locations"
2. Microsoft Learn, "Configure Azure AD Multi-Factor Authentication settings": This document describes the legacy "Trusted IPs" feature and recommends using Conditional Access instead. It notes, "If you're using Conditional Access, you don't need to configure trusted IPs... We

recommend you use Conditional Access to configure Named Locations instead of trusted IPs."
Section: "Trusted IPs"
3. Microsoft Learn, "What is Conditional Access in Azure Active Directory?": This document outlines the components of Conditional Access policies, listing "Locations" as a primary signal. It clarifies that this refers to the IP location from which a user is attempting to sign in.
Section: "Common signals"

## Question: 3

HOTSPOT You need to create the LWGroup1 group to meet the management requirements. How should you complete the dynamic membership rule? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You many need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

[image could not be rendered]

### Answer:

First Box: Null

Second Box: "Member"

### Explanation:

This dynamic membership rule is designed to automatically populate a group with all member users in the directory while excluding guests.

• (user.objectId -ne Null): This is the first condition. The objectId is a unique identifier that every object in Microsoft Entra ID possesses. By specifying that the objectId must not be equal (-ne) to Null, this clause effectively includes every user object in the directory. It's a standard way to create a rule that applies to all users as a starting point.



• (user.userType -eq "Member"): This is the second condition. The userType attribute distinguishes between internal members and external guests. This clause filters the initial set of all users down to only those whose userType is equal (-eq) to "Member".

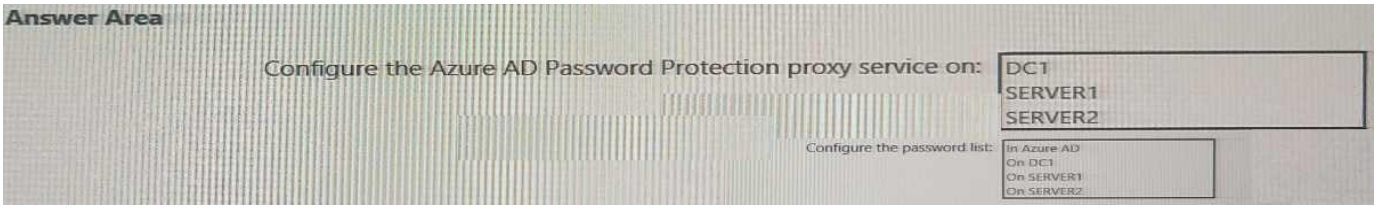
The and operator requires both conditions to be true. Therefore, the combined rule creates a group that contains all users who are specifically designated as members of the organization.

### References:

Microsoft Entra ID Documentation, Dynamic membership rules for groups in Microsoft Entra ID. Section: "Rule body" and "Supported properties". This document confirms that user.objectId and user.userType are valid properties for dynamic group rules. It also specifies that a simple rule to include all users is user.objectId -ne null and a rule to include all members is user.userType -eq "Member". The question combines these two valid clauses.
Microsoft Entra ID Documentation, Create or edit a dynamic group and get status.
Section: "Create a dynamic group rule". This guide provides examples of creating rules, including filtering based on the userType attribute to separate members from guests, which is a common administrative task matching the logic in the question.

## Question: 4

HOTSPOT You need to implement password restrictions to meet the authentication requirements. You install the Azure AD password Protection DC agent on DC1. What should you do next? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.




### Answer:

Configure the Azure AD Password Protection proxy service on: SERVER2

Configure the password list: In Azure AD

### Explanation:

The Azure AD Password Protection solution for an on-premises Active Directory environment consists of two key software components: the DC agent and the proxy service.



• Azure AD Password Protection Proxy Service: This service acts as the communication link between your on-premises domain controllers and Azure AD. It's responsible for fetching the latest password policies, which include both the global and your custom banned password lists. For security and performance best practices, the proxy service must be installed on a member server within the domain, not on a domain controller. In this scenario, SERVER2 is the appropriate choice.

• Password List Configuration: The custom banned password list is a core feature that you manage centrally. This list is configured and maintained exclusively within the Azure AD portal. After you define the list in Azure, the on-premises proxy service (on SERVER2) downloads it and makes it available to the DC agents. The agents then enforce these rules whenever a user changes their password.

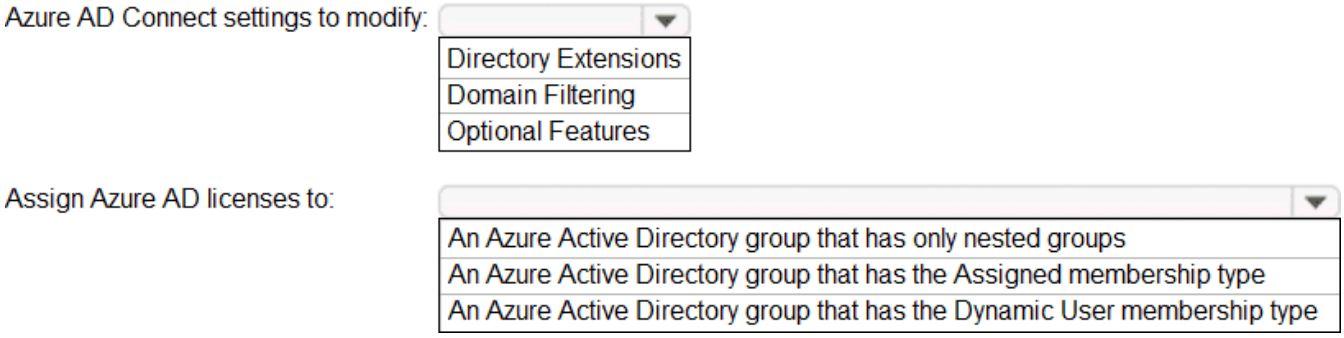
Therefore, after installing the DC agent on DC1, the correct subsequent steps are to install the proxy service on a member server like SERVER2 and configure the custom password list in Azure AD.

**References:**

Microsoft Documentation - "Deploy on-premises Azure AD Password Protection":
Proxy Service Location: "The Azure AD Password Protection proxy service is typically installed on a member server in your on-premises Active Directory domain... The Azure AD Password Protection proxy service is not supported to be installed on an Active Directory domain controller." This section validates the choice of a member server like SERVER2.
Password List Configuration: "You manage an on-premises deployment of Azure AD Password Protection by using the Azure portal... The primary configuration area is Custom smart lockout and the Custom banned password list." This statement confirms that the password list is always configured in Azure AD.
Deployment Steps: The official documentation details the deployment sequence, which involves configuring settings in the Azure portal, installing the proxy service on a member server, and then installing the DC agent on domain controllers. This reinforces the entire process.
(Source: Microsoft Learn, Deploy on-premises Azure AD Password Protection for Azure Active Directory)

## Question: 5

HOTSPOT You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE:Each correct selection is worth one point.




**Answer:**

Azure AD Connect settings to modify: Directory Extensions

Assign Azure AD licenses to: An Azure Active Directory group that has the Dynamic User membership type



**Explanation:**

To automate and efficiently manage license assignments at scale, the best practice is to use group-based licensing with dynamic groups.

Dynamic groups automatically manage membership based on user attributes (e.g., department, location). This ensures that users automatically receive the correct licenses when their roles or attributes change. To create these rules, the necessary attributes must be available in Azure AD. If custom attributes from an on-premises Active Directory are needed for these rules, you must configure Directory Extensions in Azure AD Connect to synchronize them to Azure AD.

Assigning licenses to a group with only nested groups is not supported, as members of the nested groups do not inherit licenses from the parent group.

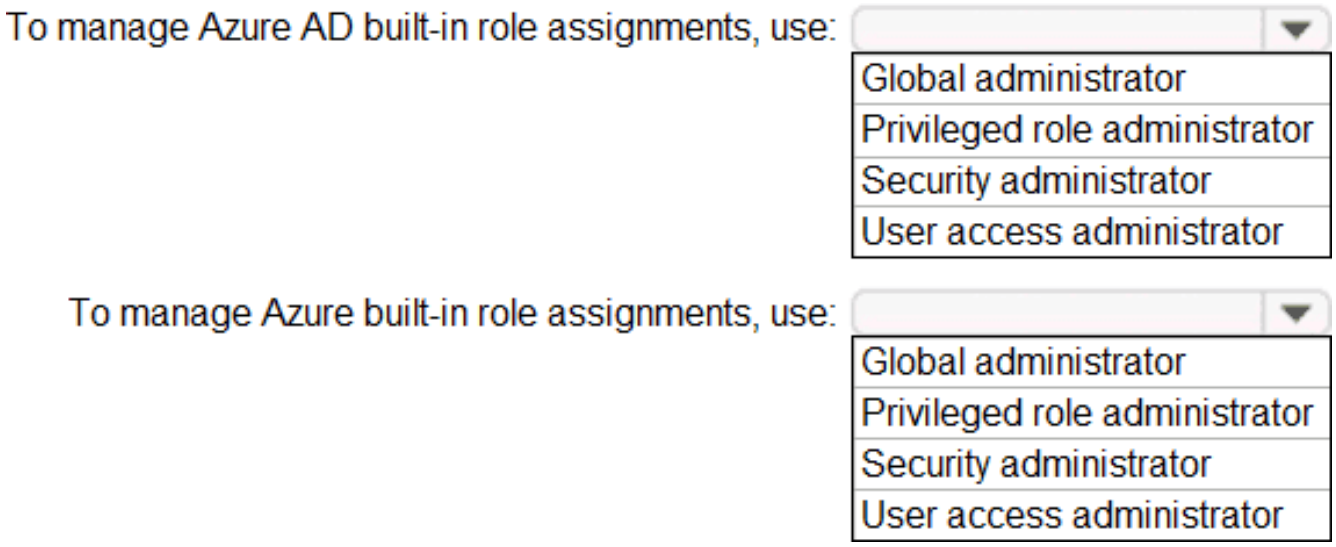
**References:**

Microsoft Learn, What is group-based licensing in Azure Active Directory?
Reference: Under the section "What is group-based licensing?", the documentation states, "You can use any security group for group-based licensing... You can use dynamic groups to make license management even easier. A group with dynamic membership rules where administrators can set rules to add and remove members automatically." This supports using dynamic groups for

license assignment.
Microsoft Learn, Azure AD Connect sync: Directory extensions
Reference: The article's introduction clearly states, "You can use directory extensions to extend the schema in Azure Active Directory (Azure AD) with your own attributes from on-premises Active Directory... You can use these attributes to build dynamic groups." This establishes the direct link between configuring Directory Extensions and enabling attribute-based dynamic groups.
Microsoft Learn, Assign licenses to a group in Azure Active Directory
Reference: Under the section "Limitations and known issues," the documentation notes, "Group-based licensing does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied." This confirms why the nested group option is incorrect.

## Question: 6

HOTSPOT You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE:Each correct selection is worth one point.




**Answer:**

Box 1: To manage Azure AD built-in role assignments, use: Privileged role administrator

Box 2: To manage Azure built-in role assignments, use: User access administrator

**Explanation:**

The two questions distinguish between managing roles for Azure Active Directory (Azure AD, now Microsoft Entra ID) and roles for Azure resources (subscriptions, resource groups, etc.).

• The Privileged Role Administrator is the specific Azure AD role designed for managing role assignments within Azure AD itself and in Azure AD Privileged Identity Management (PIM). While a Global Administrator can also perform these tasks, the Privileged Role Administrator is the most precise and appropriate choice that follows the principle of least privilege.

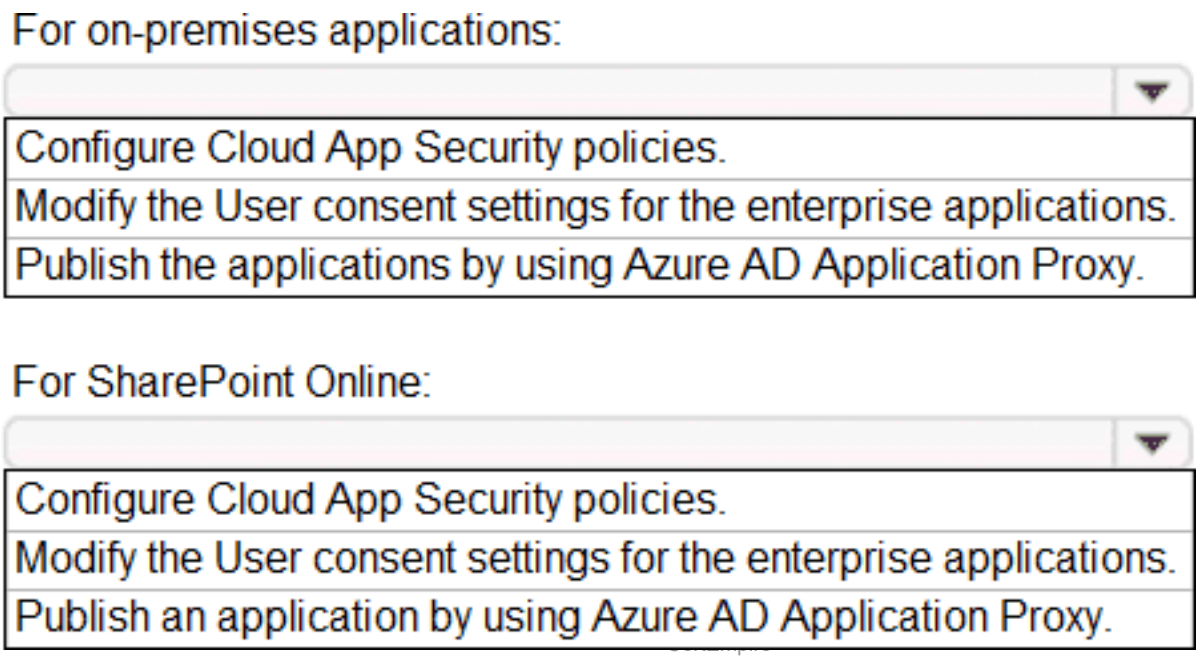
• The User Access Administrator is an Azure Role-Based Access Control (RBAC) role. Its purpose is to manage user permissions to Azure resources. This role grants the ability to assign other Azure roles (like Owner, Contributor, or Reader) to users, groups, and service principals at a specific scope, such as a subscription or resource group.

**References:**

Microsoft Entra Documentation, Microsoft Entra built-in roles: This document details the permissions for Azure AD roles. For the Privileged Role Administrator, it states, "Users with this role can manage role assignments in Microsoft Entra ID, as well as within Microsoft Entra Privileged Identity Management (PIM)." This directly supports the answer for the first box.
Microsoft Azure Documentation, Azure built-in roles: This source provides descriptions for Azure RBAC roles. For the User Access Administrator, it specifies the role "Lets you manage user access to Azure resources." This directly supports the answer for the second box.
Microsoft Azure Documentation, Classic subscription administrator roles, Azure roles, and Microsoft Entra roles: This document explicitly clarifies the distinction: "Azure AD roles are used to manage Azure AD resources... Azure roles are used to manage Azure resources such as virtual machines or storage." This foundational concept underlies the entire question, separating the two management planes.

## Question: 7

HOTSPOT You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE:Each correct selection is worth one point.




**Answer:**

Publish the applications by using Azure AD Application Proxy.

Configure Cloud App Security policies.

**Explanation:**

Azure AD Application Proxy is the specific service designed to provide secure remote access to on-premises web applications. By publishing an application with the Application Proxy, it becomes accessible to external users through Azure AD. This is the foundational step required before you can apply Azure AD's advanced security features, such as Conditional Access policies, to enforce authentication and access requirements for these internal resources.

Microsoft Defender for Cloud Apps (formerly Cloud App Security) provides visibility and granular control over data in cloud applications like SharePoint Online. To meet specific access requirements, you can create session policies in Defender for Cloud Apps. These policies can monitor and control user sessions in real-time, allowing you to take actions such as blocking downloads, preventing copy/paste, or requiring step-up authentication based on the user's context (e.g., location, device compliance), thereby enforcing security restrictions.

**References:**

Azure AD Application Proxy:
Microsoft Learn. (2023). Plan an Azure AD Application Proxy deployment. "Azure AD Application Proxy helps you support remote workers by publishing on-premises applications to be accessed over the internet. You can secure remote access to your on-premises applications because Application Proxy integrates with Azure AD." (Section: What is Application Proxy?)
Microsoft Learn. (2023). Tutorial: Add an on-premises application for remote access through Application Proxy in Azure Active Directory. This document provides the step-by-step process for publishing an on-premises application. (Section: Add an on-premises app to Azure AD)
Microsoft Defender for Cloud Apps (Cloud App Security):
Microsoft Learn. (2024). Deploy Conditional Access App Control for featured apps. "You can use session controls in Microsoft Defender for Cloud Apps to monitor and control sessions in real time... The session control allows you to monitor user activities and to allow/block downloads." SharePoint Online is listed as a featured app. (Section: How session control works)
Microsoft Learn. (2024). Session policies. "With Microsoft Defender for Cloud Apps session policies, you can... Monitor and control sessions in real-time... and Block and protect downloads on unmanaged devices." (Section: What are session policies?)

## Question: 8

You need to configure the detection of multi-staged attacks to meet the monitoring requirements. What should you do?

A. Customize the Azure Sentinel rule logic.

B. Create a workbook.

C. Add Azure Sentinel data connectors.

D. Add an Azure Sentinel playbook.

**Answer:**

A

**Explanation:**

Microsoft Sentinel (formerly Azure Sentinel) uses analytics rules to detect threats and generate alerts. Detecting a multi-staged attack requires correlating various events and activities across different data sources over time. This is achieved by defining or customizing the query logic within an analytics rule. By tailoring the rule logic using Kusto Query Language (KQL), you can create specific conditions that identify the sequence of events characteristic of a complex, multi-staged attack, thereby meeting the monitoring requirement for advanced threat detection.



**Why Incorrect Options are Wrong:**

B. Create a workbook.
Workbooks are used for data visualization and creating interactive reports; they do not actively detect threats or generate alerts.
C. Add Azure Sentinel data connectors.
Data connectors are necessary to ingest data into Sentinel, but they do not contain the logic required to analyze that data for threats.
D. Add an Azure Sentinel playbook.
Playbooks are used for automating responses and orchestration after an alert has been triggered by an analytics rule; they are not used for detection.
---

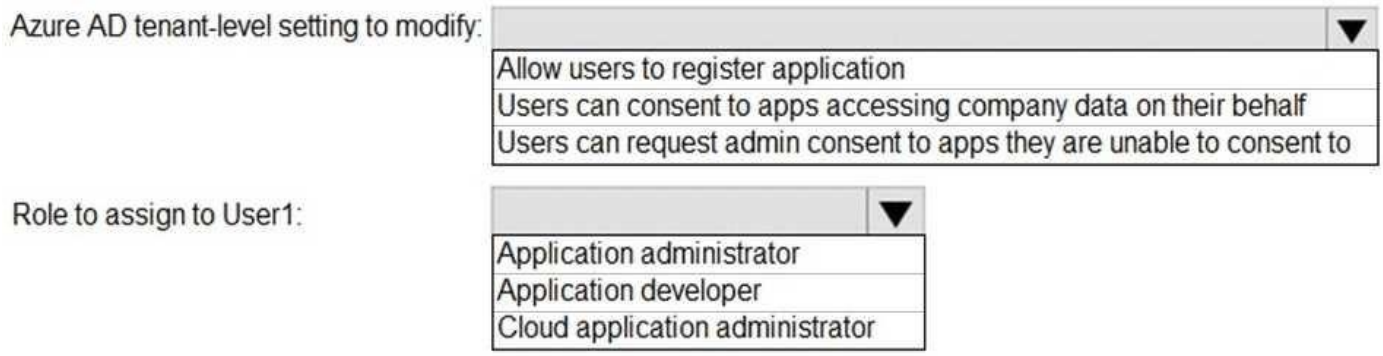
**References:**

1. Microsoft Documentation Create custom analytics rules to detect threats: "To help you detect threats and anomalous behaviors in your environment, you can create custom analytics rules. These rules search for specific events or sets of events across your environment, alert you when certain event thresholds or conditions are reached, generate incidents for your SOC to triage and investigate..." This directly supports that rule logic is for detection.
Source: Microsoft. (2023). Create custom analytics rules to detect threats. Microsoft Learn.

Retrieved from https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom
2. Microsoft Documentation Detect threats with built-in analytics rules in Microsoft Sentinel: "Microsoft Sentinel provides built-in rule templates to help you create threat detection rules... The rule logic is a query that is run on Log Analytics." This confirms that the core of detection is the rule's logic/query.
Source: Microsoft. (2023). Detect threats with built-in analytics rules in Microsoft Sentinel. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-built-in
3. Microsoft Documentation Visualize and monitor your data: "After you've connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks... Workbooks are intended for SOC engineers and analysts of all tiers to visualize data." This clarifies the role of workbooks as visualization tools, not detection mechanisms.
Source: Microsoft. (2023). Visualize and monitor your data. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data
4. Microsoft Documentation Automate threat response with playbooks in Microsoft Sentinel: "A playbook is a collection of procedures that can be run from Microsoft Sentinel in response to an alert or incident... Playbooks can help you automate and orchestrate your response..." This establishes playbooks as a response tool, not a detection tool.
Source: Microsoft. (2023). Automate threat response with playbooks in Microsoft Sentinel. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

## Question: 9

HOTSPOT You need to configure app registration in Azure AD to meet the delegation requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE:Each correct selection is worth one point.




**Answer:**

Azure AD tenant-level setting to modify: Allow users to register application

Role to assign to User1: Application developer

**Explanation:**



To meet the delegation requirements using the principle of least privilege, you should first restrict the general ability of non-administrative users to create applications. This is done by configuring the Allow users to register application tenant-wide setting to 'No'.

Next, to grant this specific capability only to User1, you assign them the Application developer role. This role is specifically designed to allow a user to create and manage the application registrations they own, even when the general tenant setting prohibits it for other users. The Application administrator and Cloud application administrator roles would grant excessive permissions, including the ability to manage all applications in the tenant, which violates the principle of least privilege for this scenario.

**References:**

Microsoft Entra ID Documentation, Microsoft Entra built-in roles.
Reference: Under the "Application Developer" role description.
Content: "Users in this role can create application registrations when the 'Users can register applications' setting is set to No. This role also grants permission to consent to permissions on behalf of the current user." This directly supports assigning the Application developer role as the correct method for delegation when the general setting is restricted.
Microsoft Entra ID Documentation, Configure user settings in Microsoft Entra ID.
Reference: Section on "Restrict app registration to administrators."

Content: This documentation explains that setting "Users can register applications" to 'No' prevents non-admin users from creating app registrations. It specifies that for a user to register an app in this case, they must be assigned a role that grants the microsoft.directory/applications/create permission, such as Application developer.

## Question: 10

You need to track application access assignments by using Identity Governance. The solution must
meet the delegation requirements.
What should you do first?

A. Modify the User consent settings for the enterprise applications.

B. Create a catalog.

C. Create a program.

D. Modify the Admin consent requests settings for the enterprise applications.

**Answer:**

B

**Explanation:**

In Azure AD Identity Governance, Entitlement Management is the feature used to manage and track application access. The core component for enabling delegation is the catalog. A catalog is a container for resources (such as applications and groups) and access packages. Creating a catalog is the essential first step because it allows an administrator to group related resources and then delegate control over that catalog to non-administrators (e.g., business owners). These delegated "catalog owners" can then manage the resources, create access packages, and approve requests for access within their designated catalog, fulfilling the delegation requirement.



**Why Incorrect Options are Wrong:**

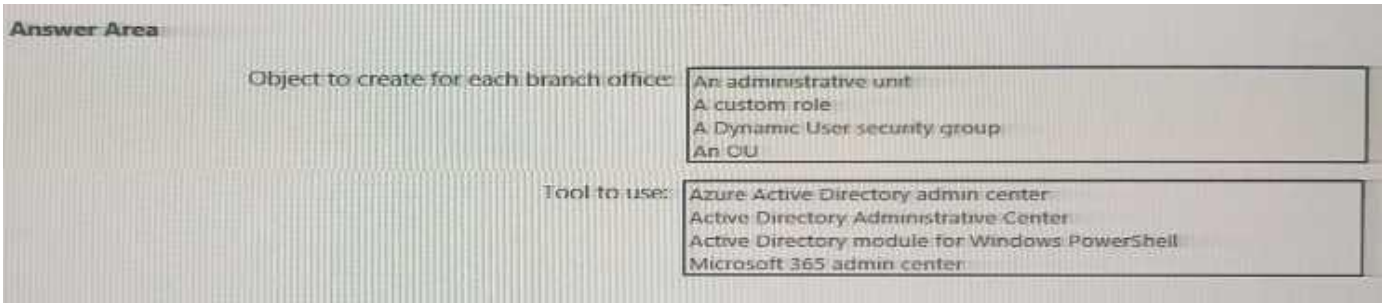
A. Modify the User consent settings for the enterprise applications.
This setting controls whether users can grant applications access to their data. It is a tenant-wide application governance policy, not the first step in creating a delegated access management structure.
C. Create a program.
The "program" concept was used in older versions of Identity Governance, primarily for grouping Access Reviews. In modern Entitlement Management, catalogs are the correct construct for grouping resources and delegating administration.
D. Modify the Admin consent requests settings for the enterprise applications.
This configures a workflow for applications requiring high-privilege permissions. It is an important security control but is not the foundational step for delegating the management of access assignments.
---

**References:**

1. Microsoft Learn What are catalogs in Azure AD entitlement management?
Section: "What are catalogs?" and "Delegation"
Quote/Content: "A catalog is a container of resources and access packages. You create a catalog when you want to group related resources and access packages... The primary way to delegate in entitlement management is to create a catalog and make a user a catalog owner. A catalog owner can then add resources, create access packages, and manage access policies." This establishes the catalog as the primary tool for delegation.
2. Microsoft Learn Delegate access governance in Azure AD entitlement management
Section: "Delegate from IT administrator to catalog creator"
Quote/Content: The article outlines the delegation model and its common scenarios. The process invariably begins with the creation and configuration of a catalog to which management can be delegated. For example, in the "Departmental delegation" scenario, the first step described is: "IT administrator creates a new catalog for the Marketing department."
3. Microsoft Learn Tutorial: Manage access to resources in Azure AD entitlement management
Section: "Prerequisites" and "Step 2: Create a new catalog"
Quote/Content: This official tutorial demonstrates the end-to-end process. After the initial one-time role assignment, the first operational step for the delegated user (the catalog creator) is to "create a new catalog." This confirms that creating the catalog is the foundational action in the delegated workflow.

# Question: 11

HOTSPOT You need to meet the technical requirements for license management by the helpdesk administrators. What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.




**Answer:**

Object to create for each branch office: An administrative unit

Tool to use: Azure Active Directory admin center

**Explanation:**

To delegate administrative permissions with a limited scope, such as managing licenses for users in a specific branch office, the correct object to create in Azure Active Directory (Azure AD) is an Administrative Unit (AU). AUs act as containers to which you can assign users and then assign administrative roles (like License Administrator) that are restricted to managing only the members of that AU. This fulfills the requirement of scoping the helpdesk's permissions.

The primary management interface for creating and managing Azure AD objects, including Administrative Units and scoped role assignments, is the Azure Active Directory admin center (now part of the Microsoft Entra admin center). The other tools listed, such as the Active Directory Administrative Center, are used for on-premises Active Directory Domain Services, not for cloud-based Azure AD.

**References:**

Microsoft Entra Documentation, Administrative units in Microsoft Entra ID. This document states, "This article describes administrative units in Microsoft Entra ID. An administrative unit is a Microsoft Entra resource that can be a container for other Microsoft Entra resources... You can use administrative units to delegate permissions to regional administrators or to set policy at a granular level."
Microsoft Entra Documentation, Create, manage, and use administrative units in Microsoft Entra ID. This guide details the process and prerequisites. Under the "Create an administrative unit" section, it specifies using the "Azure portal" which directs to the Azure AD/Microsoft Entra admin

center.

Microsoft Entra Documentation, Assign Microsoft Entra roles with administrative unit scope. This page confirms the exact scenario: "In Microsoft Entra ID, you can assign a Microsoft Entra role with a scope that's limited to one or more administrative units. This is known as scoped role assignment." It further illustrates how to perform this action within the Azure portal.

# Question: 12

You need to allocate licenses to the new users from ADatum. The solution must meet the technical requirements. Which type of object should you create?

A. A Dynamo User security group

B. An OU

C. A distribution group

D. An administrative unit

**Answer:**

D

**Explanation:**

The most suitable object for meeting the technical requirements of managing resources for a specific subset of users (new users from ADatum) is an Administrative Unit (AU). AUs are Microsoft Entra ID containers that allow for the delegation of administrative permissions over a defined set of users, groups, or devices. By creating an AU for ADatum users, you can then assign a scoped "License Administrator" role to a designated administrator. This empowers them to allocate and manage licenses exclusively for the users within that AU, fulfilling the requirement for delegated and granular control without granting tenant-wide permissions.



**Why Incorrect Options are Wrong:**

A. A Dynamic User security group: While a dynamic security group is effective for automating license assignment via group-based licensing, it does not provide the capability to delegate the administration of those licenses to a specific administrator with a restricted scope.
B. An OU: Organizational Units (OUs) are a construct for on-premises Active Directory Domain Services (AD DS) to organize objects and delegate control. They are not the native object used for delegating administration in Microsoft Entra ID.
C. A distribution group: A distribution group's primary purpose is to manage email distribution lists. It cannot be used to assign licenses or delegate administrative permissions.

**References:**

1. Microsoft Entra ID Documentation, "Administrative units in Microsoft Entra ID": This document states, "An administrative unit is a Microsoft Entra ID resource that can be a container for other Microsoft Entra ID resources... You can use administrative units to delegate administrative permissions over subsets of users and groups." This directly supports the use of AUs for delegated management of a user subset.
2. Microsoft Entra ID Documentation, "Assign Microsoft Entra roles with administrative unit scope": This guide details the process and purpose of scoped roles. It explains, "In Microsoft

Entra ID, for more granular administrative control, you can assign a Microsoft Entra role with a scope that's limited to one or more administrative units." This confirms that roles like License Administrator can be scoped to an AU.
3. Microsoft Learn, SC-300 Learning Path, "Delegate administrator roles by using administrative units": This official courseware for the SC-300 exam explicitly covers the scenario of using AUs to restrict administrative permissions. The module "Create and use administrative units" demonstrates how to create an AU to group users for delegated management tasks, including license allocation.

## Question: 13

HOTSPOT You need to meet the technical requirements for the probability that user identifies were compromised. What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

[image could not be rendered]

### Answer:

The users must first: Register for multi-factor authentication (MFA).

You must configure: A user risk policy

### Explanation:

The scenario addresses a situation where there's a "probability that user identities were compromised." This directly relates to the capabilities of Azure AD Identity Protection.

• A user risk policy is the specific Azure AD Identity Protection policy designed to detect and respond to threats associated with a user account itself, rather than a single sign-in attempt. It calculates the probability that an identity has been compromised based on threat intelligence signals, such as leaked credentials found on the dark web. This perfectly matches the requirement.



• For a user risk policy to automatically remediate a compromised account (e.g., by forcing a secure password reset), the user must first be able to securely verify their identity. Registering for multi-factor authentication (MFA) is a fundamental prerequisite for this self-remediation process. Without a registered MFA method, the user cannot complete the required security challenges to prove their identity and reset their password safely.

### References:

Microsoft Documentation (Microsoft Entra ID): In the section on Identity Protection policies, it is stated that "User risk represents the probability that a given identity or account is compromised." The user risk policy is the tool used to enforce controls based on this calculated probability. Source: Microsoft Learn, "What are Identity Protection policies?", Section: "User risk policy". Microsoft Documentation (Microsoft Entra ID): The documentation on configuring risk policies specifies user requirements for self-remediation. "To allow users to self-remediate from risks, users must be registered for both Azure AD Multi-Factor Authentication and self-service password reset (SSPR)." Registering for MFA is the essential first step that enables these secure actions. Source: Microsoft Learn, "Configure and enable risk policies", Section: "User experience".

## Question: 14

You need to meet the planned changes for the User administrator role.
What should you do?

A. Create an access review.

B. Modify Role settings

C. Create an administrator unit.

D. Modify Active Assignments.

**Answer:**

D

**Explanation:**

To implement planned changes for the User administrator role, the most direct action is to modify its active assignments. This involves adding or removing users or groups from the role to align with the new requirements. This action directly alters who currently holds the permissions associated with the User administrator role. While other options are related to role management, modifying active assignments is the specific task for changing the membership of a role.

**Why Incorrect Options are Wrong:**



A. Create an access review: This is a governance tool used to periodically review and certify who has access, not to directly implement a planned change to role membership.
B. Modify Role settings: This action, typically within Privileged Identity Management (PIM), changes the activation parameters for a role (e.g., MFA requirements, duration), not who is assigned to it.
C. Create an administrative unit: This creates a container to scope role assignments to a subset of users, but it does not, by itself, change any role assignments. It is a preparatory step for a scoped assignment.
---

**References:**

1. Assign Microsoft Entra roles in the Microsoft Entra admin center. Microsoft Learn. This document details the process of managing role assignments. Under the section "Assign a role," it outlines the steps to add a user to a role, and under "Remove a role assignment," it shows how to remove a user. This directly corresponds to modifying active assignments.
Reference:
learn.microsoft.com/en-us/entra/identity/role-based-access-control/manage-roles-portal, Sections: "Assign a role" and "Remove a role assignment".
2. Configure Microsoft Entra role settings in Privileged Identity Management. Microsoft Learn.

This document explains that role settings define the properties for PIM activations, such as requiring MFA, justification, or setting activation duration. This confirms that modifying role settings does not change the role's membership.
Reference: learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings, Section: "Role settings".
3. Administrative units in Microsoft Entra ID. Microsoft Learn. This source clarifies that an administrative unit is a resource that acts as a container for scoping administrative permissions. Creating an AU is a prerequisite for delegating administration over a specific set of users, but the act of assigning the role with that scope is a separate step.
Reference:
learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units, Section: "What are administrative units?".
4. What are Microsoft Entra access reviews? Microsoft Learn. This overview explains that access reviews are a feature for managing and reviewing user access to resources to ensure only the right people have continued access. The outcome of a review might lead to a change, but the review itself is not the implementation of that change.
Reference: learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview, Section: "Why are access reviews important?".

## Question: 15

You need to sync the ADatum users. The solution must meet the technical requirements.
What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.

B. From PowerShell, run Set-ADSyncScheduler.

C. From PowerShell, run Start-ADSyncSyncCycle.

D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

**Answer:**

A

**Explanation:**

To change which users are synchronized from an on-premises Active Directory to Azure AD, you must modify the synchronization scope. The "Customize synchronization options" task in the Azure AD Connect wizard is the designated method for this configuration. This task allows an administrator to access the "Domain and OU filtering" page, where they can select or deselect specific Organizational Units (OUs). To sync the "ADatum users," the administrator would use this option to ensure the OU containing these users is selected for synchronization, thereby meeting the technical requirement to include them in the sync scope.



**Why Incorrect Options are Wrong:**

B. Set-ADSyncScheduler is a PowerShell cmdlet used to modify the frequency of the synchronization cycle, not to define which objects are synchronized.
C. Start-ADSyncSyncCycle is a PowerShell cmdlet that manually initiates a synchronization cycle. It only syncs objects already within the configured scope.
D. "Change user sign-in" is a wizard task used to alter the user authentication method (e.g., Password Hash Synchronization, Pass-through Authentication), not the scope of users being synced.
---

**References:**

1. Microsoft Learn. "Azure AD Connect sync: Configure filtering." Under the section "Organizational unit-based filtering," the documentation states, "To configure OU-based filtering, you must run the Azure AD Connect installation wizard... On the Domain and OU filtering page, clear the OUs you don't want to synchronize with Azure AD." The wizard is accessed by selecting the "Customize synchronization options" task.
2. Microsoft Learn. "Azure AD Connect: Tasks and customization." In the table under "Additional

tasks available in Azure AD Connect," the task "Customize synchronization options" is described as the method to "configure OU filtering or attribute filtering."
3. Microsoft Learn. "Azure AD Connect sync: Scheduler." The section "Start the scheduler" explains that the Start-ADSyncSyncCycle cmdlet is used to "manually trigger a cycle." The section "Customize the synchronization schedule" details using Set-ADSyncScheduler to change the schedule. Neither function alters the synchronization scope.

## Question: 16

You need to meet the planned changes and technical requirements for App1.
What should you implement?

A. a policy set in Microsoft Endpoint Manager

B. an app configuratifon policy in Microsoft Endpoint Manager

C. an app registration in Azure AD

D. Azure AD Application Proxy

**Answer:**

C

**Explanation:**

Registering an application in Azure AD is the foundational step to integrate it with the Microsoft identity platform. This process creates a globally unique application object and a corresponding service principal in your tenant. This identity allows the application to authenticate with Azure AD, enabling scenarios like user sign-on (SSO) and authorizing the application to access protected resources, such as Microsoft Graph or other APIs. This is the primary mechanism for establishing a trust relationship between an application and Azure AD.



**Why Incorrect Options are Wrong:**

A. A policy set in Microsoft Endpoint Manager is used to bundle and assign existing management objects like apps and policies to users or devices, not for application identity integration.
B. An app configuration policy in Microsoft Endpoint Manager is used to customize and deploy settings to managed mobile applications (MAM), not to register an application for authentication.
D. Azure AD Application Proxy is a specific feature used to publish on-premises web applications for secure remote access, not for the general registration of any application with Azure AD.
---

**References:**

1. Microsoft identity platform documentation. "Quickstart: Register an application with the Microsoft identity platform." Microsoft Learn. This document states, "To delegate identity and access management functions to Azure AD, an application must be registered with an Azure AD tenant... Registering your application establishes a trust relationship between your app and the Microsoft identity platform."
2. Microsoft identity platform documentation. "Application and service principal objects in Azure Active Directory." Microsoft Learn. This article explains that registering an application automatically creates an application object and a service principal object in the home tenant, which are essential for an application to be authenticated and authorized for resources.

3. Microsoft Endpoint Manager documentation. "Use policy sets to group collections of management objects." Microsoft Learn. This source details the function of policy sets, confirming they are for grouping existing configurations, not for creating application identities.
4. Microsoft Endpoint Manager documentation. "App configuration policies for Microsoft Intune." Microsoft Learn. This document describes how app configuration policies deliver settings to apps on managed devices, a distinct function from Azure AD app registration.

# Question: 17

You create a Log Analytics workspace.
You need to implement the technical requirements for auditing.
What should you configure in Azure AD?

A. Company branding

B. Diagnostics settings

C. External Identities

D. App registrations

**Answer:**

B

**Explanation:**

To send Azure AD audit logs to a Log Analytics workspace, you must configure Diagnostic settings within Azure AD. This is the designated feature for streaming platform logs and metrics, including audit logs, sign-in logs, and provisioning logs, to various destinations. These destinations include Log Analytics for advanced querying and analysis, Azure Storage for long-term archival, or Azure Event Hubs for integration with external SIEM tools. Configuring these settings is the direct and required step to meet the auditing requirements described.



**Why Incorrect Options are Wrong:**

A. Company branding: This feature is for customizing the appearance of your organization's sign-in pages and is unrelated to log collection or auditing.
C. External Identities: This section is for managing how your organization collaborates with external users (B2B) and customers (B2C), not for configuring log exports.
D. App registrations: This is used to integrate applications with Azure AD for authentication and authorization purposes, not for streaming tenant-level audit logs.
---

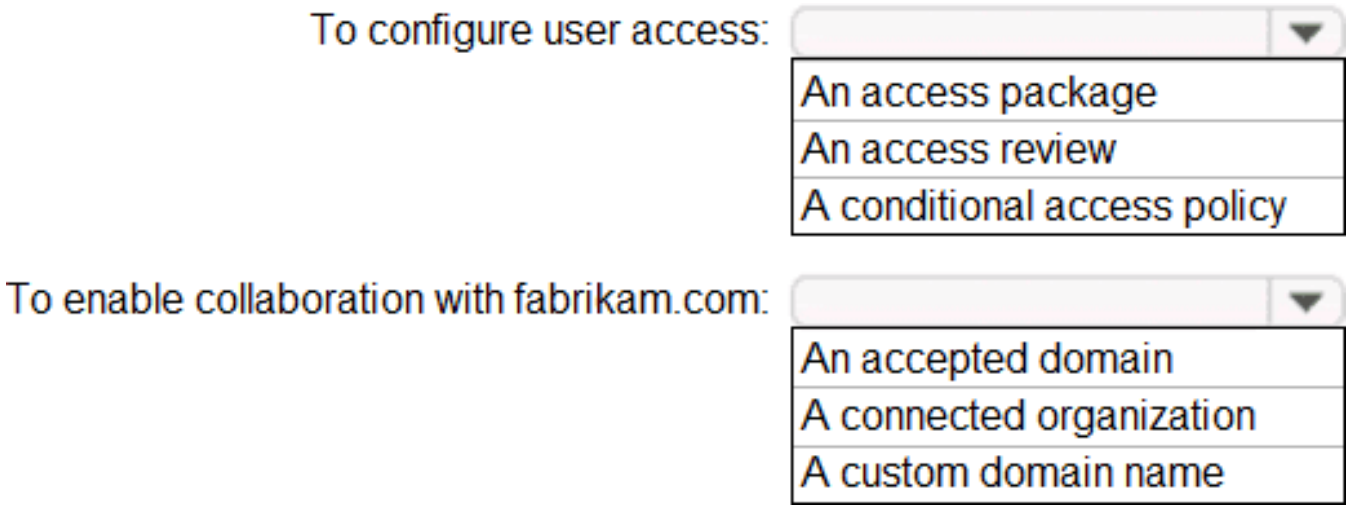
**References:**

1. Microsoft Learn. "Integrate Azure AD logs with Azure Monitor logs." Microsoft Entra documentation. In the "Prerequisites" section, it explicitly lists a Log Analytics workspace. The section "Send logs to Log Analytics workspace" details the procedure, stating, "Use the following steps to send the Azure Active Directory (Azure AD) activity logs to a Log Analytics workspace... 1. Sign in to the Microsoft Entra admin center....2. Browse to Identity Monitoring & health Diagnostic settings."
2. Microsoft Learn. "Diagnostic settings in Azure Monitor." Azure Monitor documentation. The "Overview" section explains, "Diagnostic settings are used to configure streaming export of

platform logs and metrics for a particular resource to the destination of your choice." Azure AD is treated as a tenant-level resource for this purpose.
3. Microsoft Learn. "Audit logs in Azure Active Directory." Microsoft Entra documentation. Under the "Route audit logs to other endpoints for reporting and monitoring" section, it states, "You can route the Activity logs to several endpoints... This routing is configured in the Diagnostic Settings in Azure AD."

## Question: 18

HOTSPOT You need to implement the planned changes and technical requirements for the marketing department. What should you do? To answer, select the appropriate options in the answer area. NOTE:Each correct selection is worth one point.




**Answer:**

To configure user access: An access package



To enable collaboration with fabrikam.com: A connected organization

**Explanation:**

An access package is the most precise tool for this scenario because it is a feature within Azure AD Entitlement Management designed to bundle resources like group memberships, application roles, and SharePoint site access. This allows administrators to govern access for specific groups, such as the marketing department, by creating a single requestable package. It simplifies managing who has access to what, for how long, and with what approval process.

To collaborate with an external partner like fabrikam.com, you must first define that partner within your tenant. A connected organization is the specific Azure AD Entitlement Management object for an external Azure AD tenant or domain you have a relationship with. Adding fabrikam.com as a connected organization enables its users to be granted access to your resources via access packages, thereby facilitating secure external collaboration.

**References:**

Microsoft Entra documentation What is entitlement management?
Reference: Under the "What can I do with entitlement management?" section, it states, "Delegate to non-administrators the ability to create access packages. These access packages contain resources that users can request." This directly supports using access packages to configure user access to a bundle of resources.
Microsoft Entra documentation Add a connected organization in entitlement management
Reference: In the introduction, it states, "With Azure AD entitlement management, you can collaborate with people outside your organization... If you want to provide an access path for all users in an external directory or domain, you can set up a connection with that directory or domain by adding it as a connected organization." This confirms its role in enabling collaboration with external domains like fabrikam.com.
Microsoft Entra documentation What is Conditional Access?
Reference: The overview explains that "Conditional Access policies at their simplest are if-then statements... if a user wants to access a resource, then they must complete an action." This shows Conditional Access is for enforcing policies on how access occurs, not for bundling the resources themselves, making "access package" more precise for the task.
Microsoft Entra documentation What are Microsoft Entra access reviews?
Reference: The documentation states, "Microsoft Entra access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments." This clarifies that access reviews are for periodic validation of existing access, not for the initial configuration.

## Question: 19

You need to allocate licenses to the new users from ADatum. The solution must meet the technical requirements. Which type of object should you create?

A. a distribution group

B. a Dynamic User security group

C. an administrative unit

D. an OU

**Answer:**

C

**Explanation:**

An Azure AD Administrative Unit (AU) lets you place a subset of directory objects-such as all users from the newly-acquired ADatum-into a logical container. You can then delegate the License Administrator role scoped to that AU, so license assignments can be performed for only those users, exactly meeting the requirement to "allocate licenses to the new users from ADatum" while satisfying the technical constraint that licensing privileges be limited to that population.

**Why Incorrect Options are Wrong:**



A. Distribution groups are mail-enabled only; Azure AD does not allow license assignment or scoped admin delegation through them.
B. A Dynamic User security group can auto-assign licenses, but it cannot restrict the licensing admin's scope; admins would still have tenant-wide rights, violating the requirement.
D. Organizational Units exist only in on-premises AD; Azure AD ignores OUs for licensing or role-scoping purposes.

**References:**

1. Microsoft, "Administrative units in Azure Active Directory," Learn Doc ID: roles/administrative-units, Sec. "Scope Azure AD roles," para. 3-4 (accessed 2025-09-22).
2. Microsoft, "Assign licenses to users with Azure AD administrative units," Learn Doc ID: licenses/assign-licenses-admin-units, Steps 1-3 (accessed 2025-09-22).
3. Microsoft, "Group-based licensing in Azure Active Directory," Learn Doc ID: licenses/group-based-licensing, Limitations section, bullet "No delegation of licensing scope" (accessed 2025-09-22).

## Question: 20

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

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

ADatum 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.

ADatum 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.

[image could not be rendered]

The tenant contains the groups shown in the following table.

[image could not be rendered]

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum 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 ITGroup1, 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. Planned Changes -

ADatum 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 groups of litware.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.

Requirements. Technical Requirements

ADatum 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.

You need to implement the planned changes for litware.com.

What should you configure?

A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com



B. Azure AD Connect to include the litware.com domain

C. staging mode in Azure AD Connect for the litware.com domain

**Answer:**

B

**Explanation:**

The requirement is to synchronize a new, separate Active Directory forest (litware.com) into an Azure AD tenant that is already synchronizing an existing forest (adatum.com) via Azure AD Connect. The supported and standard topology for this scenario is "Multiple forests, single Azure AD tenant." This is achieved by modifying the configuration of the existing Azure AD Connect server to include the litware.com forest as an additional source directory. This consolidates identity synchronization management onto the single, existing server.

**Why Incorrect Options are Wrong:**

A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com
While technically possible to run cloud sync for one forest and Azure AD Connect for another, modifying the existing server is the more direct and standard method for adding a connected forest.

C. staging mode in Azure AD Connect for the litware.com domain
Staging mode applies to an entire Azure AD Connect server, making it a passive standby for testing or disaster recovery. It does not perform active synchronization to Azure AD.
---

**References:**

1. Microsoft Entra Documentation (formerly Azure AD). Topologies for Microsoft Entra Connect. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/plan-connect-topologies#multiple-forests-single-azure-ad-tenant.
Reference Details: The section "Multiple forests, single Azure AD tenant" explicitly states, "It's a supported topology to have all forests in a single Microsoft Entra Connect sync server... The Microsoft Entra Connect installation wizard offers several options to consolidate users represented in multiple forests." This directly supports adding the new forest to the existing server (Option B).
2. Microsoft Entra Documentation (formerly Azure AD). Microsoft Entra Connect: Staging server and disaster recovery. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-staging-server.
Reference Details: The "Staging mode" section clarifies, "A server in staging mode reads data from all connected directories but does not write anything to connected directories." This confirms that a staging server does not perform the required active synchronization, making Option C incorrect.
3. Microsoft Entra Documentation (formerly Azure AD). Microsoft Entra Connect: Customize synchronization options. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-customize-sync-options.
Reference Details: The section "Connect your directories" describes the step in the configuration wizard where you can add directories (forests). This is the process used to implement the solution described in Option B.

## Question: 21

HOTSPOT -

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

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

ADatum 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.

ADatum 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.

[image could not be rendered]

The tenant contains the groups shown in the following table.

[image could not be rendered]

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum 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 ITGroup1, 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. Planned Changes -

ADatum 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 groups of litware.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.

Requirements. Technical Requirements

ADatum 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.

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.



NOTE: Each correct selection is worth one point.

[image could not be rendered]

**Answer:**

Number of authentication methods required: 2

Authentication methods that can be used: Email, phone, and Microsoft Authenticator only

**Explanation:**

The correct configuration is determined by Azure Active Directory's built-in policies for administrator accounts, which override general user policies.

• Number of Methods: User3 holds the User administrator role. For security reasons, Azure AD enforces a non-configurable, two-method password reset policy for all administrator roles. Even though the technical requirement specifies one method for users, this built-in policy for administrators cannot be changed and takes precedence. Therefore, User3 will be required to provide 2 authentication methods.

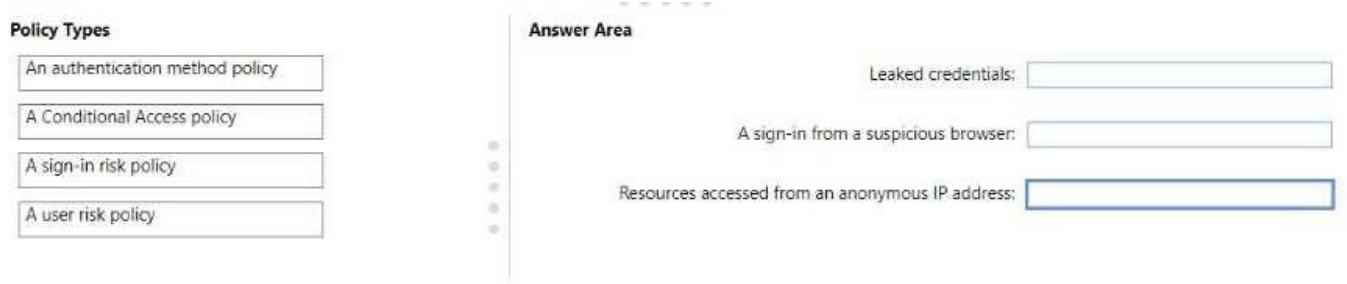
• Available Methods: The same mandatory administrator policy also prohibits the use of security questions as a valid authentication method for password resets. While the plan was to make Email, Phone, Security Questions, and the Microsoft Authenticator app available, User3 will only be able to use the methods permitted for administrators. This excludes security questions, leaving Email, phone, and Microsoft Authenticator as the only available options for User3.

**References:**

Microsoft Azure Documentation: In the "Administrator password policy differences" section, the official documentation states: "Microsoft enforces a strong, default, two-gate password reset policy for any Azure administrator role... This policy can't be changed. For password reset, the administrator must have at least two methods registered... For security reasons, security questions are not permitted as a reset method for administrators."
Source: Microsoft Learn, "Self-service password reset policies and restrictions in Azure Active Directory", Section: Administrator password policy differences.

## Question: 22

DRAG DROP You need to resolve the recent security incident issues. What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.




**Answer:**

Leaked credentials: A user risk policy

A sign-in from a suspicious browser: A sign-in risk policy

Resources accessed from an anonymous IP address: A sign-in risk policy



**Explanation:**

Microsoft Entra ID Protection uses distinct policies to address different types of threats. The key is to differentiate between risks associated with a user's identity versus risks tied to a specific sign-in attempt.

• User Risk Policy: This policy addresses threats that suggest a user's identity has been compromised. Leaked credentials are a prime example, as the compromise is persistent to the user account, not just a single login. The user risk policy is designed to trigger remediation actions, like forcing a password reset, when a user's cumulative risk score reaches a certain level.

• Sign-in Risk Policy: This policy evaluates the risk of individual, real-time sign-in attempts. An attempted sign-in from a suspicious browser (detected as unfamiliar sign-in properties) or from an anonymous IP address (like a Tor browser) are events specific to that login session. A sign-in risk policy can enforce controls in real-time for that specific attempt, such as blocking access or requiring multi-factor authentication (MFA).

**References:**

Microsoft Learn, Identity Protection and risk: This document defines the two primary types of risk. It states, "User risk is the probability that a given identity or account is compromised." It lists leaked credentials as a key indicator for user risk. It also defines, "Sign-in risk is the probability that a given authentication request isn't authorized by the identity owner," listing anonymous IP address and unfamiliar sign-in properties as real-time detections.

Microsoft Learn, Configure and enable risk policies: This documentation details how to configure the two main Identity Protection policies. It explains, "The Identity Protection user risk policy detects the probability that a user account is compromised... The Identity Protection sign-in risk policy detects the probability a sign-in is compromised in real-time." This directly supports mapping leaked credentials to the user risk policy and session-specific threats to the sign-in risk policy.

## Question: 23

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

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

ADatum 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.

ADatum 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.

[image could not be rendered]

The tenant contains the groups shown in the following table.

[image could not be rendered]

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum 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 ITGroup1, 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. Planned Changes -

ADatum 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 groups of litware.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.

Requirements. Technical Requirements

ADatum 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.

You need to resolve the issue of the sales department users.

What should you configure for the Azure AD tenant?

A. the User settings



B. the Device settings

C. the Access reviews settings

D. Security defaults

**Answer:**

B

**Explanation:**

The case study identifies an issue where sales department users are unable to join new devices because they have reached their limit. A planned change is to increase this limit to 10. The setting that controls the "Maximum number of devices per user" for Azure AD join and Azure AD registration is located within the Device settings blade in the Azure Active Directory portal. Modifying this specific setting directly resolves the problem described in the scenario.

**Why Incorrect Options are Wrong:**

A. the User settings: This section is for configuring settings related to user features, such as application registrations and external collaboration, not for managing tenant-wide device limits.
C. the Access reviews settings: Access reviews are a feature for reviewing user access to groups, applications, and privileged roles to ensure only appropriate access is maintained, which is

unrelated to device limits.

D. Security defaults: Security defaults provide a baseline level of security by enforcing policies like multi-factor authentication but do not include configurations for the number of devices a user can register.

**References:**

1. Microsoft Learn. (2023). Configure device settings. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal.
Reference Details: In the section "Configure device settings in the Azure portal," the documentation explicitly lists "Maximum number of devices per user" as a configurable setting on the Device settings page. This directly confirms that option B is the correct location to resolve the issue.

2. Microsoft Learn. (2023). How to: Manage device registration and join in Azure AD. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/devices/manage-device-identities.
Reference Details: This document states, "You can manage the Azure AD device settings in the Azure portal under Azure Active Directory Devices Device settings." This reinforces that device-specific configurations are managed under "Device settings."

## Question: 24

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

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

ADatum 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.

ADatum 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.

[image could not be rendered]

The tenant contains the groups shown in the following table.

[image could not be rendered]

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum 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 ITGroup1, 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. Planned Changes -

ADatum 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 groups of litware.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.

Requirements. Technical Requirements

ADatum 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.

You need to resolve the issue of ITGroup1.

What should you do first?

A. Recreate the IT-Group 1 group.



B. Change Membership type of IT-Group1 to Dynamic Device

C. Add an owner to ITGroup1.

D. Change Membership type of IT-Group1 to Dynamic User

**Answer:**

A

**Explanation:**

To assign an Azure AD role, such as Device Administrators, to a group, the group must be a "role-assignable" group. This is a specific property (isAssignableToRole) that must be enabled when the group is created. This property is immutable, meaning it cannot be changed after the group has been created.
The problem states that ITGroup1 does not appear in the selection list for role assignment, which indicates it was created without this property enabled. Therefore, the existing group cannot be modified to accept the role assignment. The only solution is to delete the old group and recreate it with the "Azure AD roles can be assigned to the group" setting enabled.

**Why Incorrect Options are Wrong:**

B. Azure AD roles cannot be assigned to groups with a membership type of Dynamic Device. This change would make the group ineligible.

C. Adding an owner to a group is a management function and does not affect the group's eligibility for Azure AD role assignments.

D. While role-assignable groups can be Dynamic User, simply changing the membership type will not fix the underlying immutable isAssignableToRole property.

**References:**

1. Microsoft Learn, "Use Azure AD groups to manage role assignments": Under the "How do role-assignable groups work?" section, it states, "To assign a role to a group, you must create a new security or Microsoft 365 group with the isAssignableToRole property set to true... This setting is immutable. Once a group is created with this property set, it can't be changed."
2. Microsoft Learn, "Create a role-assignable group in Azure Active Directory": In the "Create a role-assignable group" section, step 6 shows the setting "Azure AD roles can be assigned to the group (Preview)". A note in this section clarifies, "This setting can't be changed later."
3. Microsoft Learn, "Troubleshoot Azure AD roles assigned to groups": Under the "Why can't I assign an Azure AD role to a group?" section, it lists potential reasons, including "The group is not a role-assignable group." It further explains, "You can't change the isAssignableToRole property on an existing group. You must create a new role-assignable group." This section also confirms that Dynamic Device groups are not supported for role assignments.

## Question: 25

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

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

ADatum 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.

ADatum 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.

[image could not be rendered]

The tenant contains the groups shown in the following table.

[image could not be rendered]

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum 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 ITGroup1, 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. Planned Changes -

ADatum 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 groups of litware.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.

Requirements. Technical Requirements

ADatum 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.

You need to implement the planned changes for Package1.

Which users can create and manage the access review?

A. User3 only



B. User4 only

C. User5 only

D. User3 and User4

E. User3 and User5

F. User4and User5

**Answer:**

E

**Explanation:**

To create and manage access reviews in Azure AD, a user must be assigned one of the following roles: Global Administrator, User Administrator, or Identity Governance Administrator.
User5 (Identity Governance Administrator): This is the most specific, least-privilege role designed for managing Identity Governance features, including access reviews for access packages.
User3 (User Administrator): This role is explicitly granted the permission to create and manage all types of access reviews.
User4 (Global Administrator): While this role has the technical capability, the case study's technical requirements state, "The principle of least privilege must be used." Using a Global

Administrator account for routine governance tasks violates this principle. Therefore, in the context of the stated requirements, the appropriate operational roles are User Administrator and Identity Governance Administrator.

**Why Incorrect Options are Wrong:**

A, B, C: These options are incorrect because more than one user has the necessary permissions to perform the task according to the specified principles.
D: This option is incorrect as it omits User5, who holds the Identity Governance Administrator role, the most appropriate role for this task.
F: This option incorrectly omits User3 (User Administrator), whose role is explicitly permitted to manage access reviews, and incorrectly includes User4 (Global Administrator) whose use would violate the stated principle of least privilege.

**References:**

1. Microsoft Learn. (2023). Azure AD built-in roles. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference.
User administrator: "Users with this role can... create and manage all aspects of users and groups... This administrator can also create and manage access reviews."
Identity Governance administrator: "Users with this role can manage Azure AD Identity Governance features... including access reviews, entitlement management..."

2. Microsoft Learn. (2023). Create an access review of groups and applications in Azure AD access reviews. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review.
Under the "Prerequisites" section, it states: "To create an access review, you must have one of the following roles: Global administrator, User administrator, or Identity Governance administrator."
3. Microsoft. (2021). Principle of least privilege. Microsoft Security Best Practices. Retrieved from https://learn.microsoft.com/en-us/security/compass/privileged-access-least-privilege.
This document outlines the importance of limiting administrative access to only the permissions required for a specific task, which supports excluding the Global Administrator for routine operational duties.

## Question: 26

You need to resolve the issue of the guest user invitations. What should you do for the Azure AD tenant?

A. Configure the Continuous access evaluation settings.

B. Modify the External collaboration settings.

C. Configure the Access reviews settings.

D. Configure a Conditional Access policy.

### Answer:

B

### Explanation:

The External collaboration settings in Azure Active Directory are the central control plane for managing how your organization interacts with guest users (B2B collaboration). These settings directly govern the invitation process, including who is allowed to invite guests, which domains guests can be invited from (allow/deny lists), and other collaboration restrictions. To resolve an issue with guest user invitations, such as users being unable to send them or invitations being blocked, an administrator must review and modify these specific settings.



### Why Incorrect Options are Wrong:

A. Configure the Continuous access evaluation settings.
Continuous access evaluation (CAE) revokes access tokens in near real-time based on critical events. It does not control the initial process of sending or accepting guest invitations.
C. Configure the Access reviews settings.
Access reviews are a governance feature used to periodically review and recertify existing user access to resources. They manage the lifecycle of guest access, not the initial invitation.
D. Configure a Conditional Access policy.
Conditional Access policies apply controls during the sign-in process, after a guest has accepted an invitation. While a policy could block a guest from signing in, it does not control the invitation itself.

### References:

1. Microsoft Learn. "Configure external collaboration settings." Microsoft Entra documentation. Accessed May 20, 2024. This document details the settings available for B2B collaboration, stating, "With Azure AD B2B collaboration, a tenant admin can set the following invitation policies: Turn off invitations, Only admins and users in the guest inviter role can invite, Admins, the guest inviter role, and members can invite, All users, including guests, can invite." This directly addresses the control of the invitation process.

2. Microsoft Learn. "What are Azure AD access reviews?" Microsoft Entra documentation. Accessed May 20, 2024. This source clarifies the purpose of access reviews: "Azure Active Directory (Azure AD) access reviews help organizations efficiently manage group memberships, access to enterprise applications, and role assignments." This confirms they are for reviewing existing access, not for managing invitations.
3. Microsoft Learn. "What is Conditional Access?" Microsoft Entra documentation. Accessed May 20, 2024. This document explains, "Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action." This shows its focus is on the sign-in event, not the pre-authentication invitation step.

## Question: 27

You need to modify the settings of the User administrator role to meet the technical requirements. Which two actions should you perform for the role? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Select Require justification on activation

B. Set all assignments to Active

C. Set all assignments to Eligible

D. Modify the Expire eligible assignments after setting.

E. Select Require ticket information on activation.

**Answer:**

C, D

**Explanation:**

To meet the technical requirements of securing a privileged role like User Administrator, the principle of least privilege and Just-In-Time (JIT) access must be implemented using Azure AD Privileged Identity Management (PIM).
The first essential action is to change assignments from "Active" (permanent) to "Eligible" (C). This ensures that users do not have standing privileges but must activate the role when needed.
The second action is to configure the role settings to enforce a lifecycle on these assignments. Modifying the "Expire eligible assignments after" setting (D) ensures that a user's eligibility for the role is not permanent and must be periodically reviewed and renewed. This prevents "privilege creep" and strengthens the security posture.

**Why Incorrect Options are Wrong:**

A. While requiring justification is a valuable security control for auditing, it governs the activation event, not the more fundamental lifecycle of the role eligibility itself.
B. Setting assignments to "Active" grants permanent, standing privileges, which is directly contrary to the security goals of implementing PIM and the principle of least privilege.
E. Requiring ticket information, similar to justification, is an important audit control for the activation process but does not manage the duration or lifecycle of the user's eligibility.

**References:**

1. Microsoft Learn Assign Azure AD roles in Privileged Identity Management: This document distinguishes between the two assignment types. It states, "Eligible assignments require the member of the role to perform an action to use the role... Microsoft recommends a 'principle of least privilege' by making users eligible for a role..." This supports choosing option C.

Source: Microsoft Documentation, learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-member, Section: "Assignment type".
2. Microsoft Learn Configure Azure AD role settings in Privileged Identity Management: This document details the specific settings available for roles managed by PIM. Under the "Assignment" tab settings, it lists "Expire eligible assignments after" and explains its function is to set the default duration for an eligible assignment. This directly supports option D as a key configuration for managing the assignment lifecycle.
Source: Microsoft Documentation, learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure, Section: "Role settings", Sub-section: "Assignment".

## Question: 28

Your company has an Azure Active Directory (Azure AD) tenant named contosri.com. The company
has the business partners shown in the following table.

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

users can request access by using package 1.
Users at Fabrikam and Litware use ail then respective domain names for email addresses.
You plan to create an access package named packaqe1 that will be accessible only to the Fabrikam
and Litware users.
You need to configure connected organizations for Fabrikam and litware so that any of their users can
request access by using package1.
What is the minimum of connected organization that you should create.



A. 1

B. 2

C. 3

D. 4

**Answer:**

B

**Explanation:**

In Azure AD Entitlement Management, a "connected organization" is an object that represents a single external Azure AD directory or domain with which you have a collaborative relationship. The purpose is to group all users from an external organization under a single identifier for easier access management.
The scenario requires providing access to users from two distinct business partners: Fabrikam and Litware. Since these are separate organizations, they will have their own respective Azure AD tenants. Therefore, to manage access for users from both companies, you must create a minimum of two connected organizations: one representing the Fabrikam tenant and another representing the Litware tenant. A single connected organization cannot represent more than one

external Azure AD tenant.

### Why Incorrect Options are Wrong:

A: A single connected organization can only be linked to one external Azure AD tenant. It cannot represent both Fabrikam and Litware simultaneously.
C: The scenario only identifies two external partner organizations (Fabrikam and Litware). There is no information provided that would justify the need for a third connected organization.
D: This is incorrect for the same reason as C. Creating four connected organizations would be unnecessary as there are only two specified partner companies.
---

### References:

1. Microsoft Learn, Azure Active Directory Documentation. "Add a connected organization in Azure AD entitlement management." This document defines a connected organization and outlines the creation process. It states, "A connected organization is an external Azure AD directory or domain that you have a relationship with." The process described involves specifying a single directory for each connected organization, confirming that one object represents one external tenant.
Reference: https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization, Section: "What is a connected organization?".

2. Microsoft Learn, Azure Active Directory Documentation. "What is entitlement management?" This overview document defines the core terminology used in Entitlement Management.
Reference: https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview, Section: "Terminology", Definition of "Connected organization".

## Question: 29

You have an Azure subscription that contains the resources shown in the following table.

| 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 |

For which resources can you create an access review?

A. Group1, App1, Contributor, and Role1

B. Hotel and Contributor only

C. Group1, Role1, and Contributor only

D. Group1 only

### Answer:

A

### Explanation:



Azure AD access reviews are a feature of Azure AD Identity Governance used to manage and attest to user access rights. Access reviews can be created for several types of resources to ensure that only appropriate individuals have continued access. The supported resources for review include memberships in security groups and Microsoft 365 groups (like Group1), user assignments to enterprise applications (like App1), assignments to Azure AD roles (like Role1), and assignments to Azure resource roles (like Contributor). A resource group itself (Hotel) is not a direct target for an access review; rather, the role assignments on the resource group are reviewed.

### Why Incorrect Options are Wrong:

B. Hotel and Contributor only: A resource group (Hotel) is not a directly reviewable entity. You review the role assignments to it. This option also incorrectly omits groups, applications, and Azure AD roles.
C. Group1, Role1, and Contributor only: This option is incorrect because it omits enterprise applications (App1), which are a valid target for access reviews.
D. Group1 only: This option is incorrect as it omits enterprise applications (App1), Azure AD roles (Role1), and Azure resource roles (Contributor), all of which can be reviewed.

**References:**

1. Microsoft Learn. "What are access reviews?". Microsoft Entra documentation. Accessed October 10, 2023. In the "What can you review?" section, it explicitly lists: "Membership in a group," "Access to an enterprise application," "Assignment to an Azure AD role," and "Assignment to an Azure resource role." This directly supports that Group1, App1, Role1, and Contributor are all valid targets.
2. Microsoft Learn. "Create an access review of groups and applications in Azure AD access reviews". Microsoft Entra documentation. Accessed October 10, 2023. Step 4 of the "Create an access review" procedure shows the options to review "Teams + Groups" or "Applications," confirming Group1 and App1 as valid.
3. Microsoft Learn. "Create an access review of Azure resource roles in Privileged Identity Management (PIM)". Microsoft Entra documentation. Accessed October 10, 2023. This document details the process for creating access reviews for Azure resource roles like "Contributor."
4. Microsoft Learn. "Create an access review of Azure AD roles in Privileged Identity Management (PIM)". Microsoft Entra documentation. Accessed October 10, 2023. This document outlines the procedure for creating access reviews for Azure AD roles, such as Role1.

## Question: 30

You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.
You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.
You need to download the Azure AD log that contains conditional access policy data.
What should you export from Azure AD?

A. sign-ins in JSON format

B. sign-ins in CSV format

C. audit logs in JSON format

D. audit logs in CSV format

### Answer:

A

### Explanation:

To analyze Conditional Access usage, you need data on how policies are evaluated and applied during user sign-in events. The Azure AD sign-in logs provide this specific information. Each sign-in event record contains a detailed breakdown of the Conditional Access policies that were triggered, the conditions that were met, and the resulting outcome (e.g., success, failure, MFA required).

For integration with a third-party SIEM, JSON is the standard and most effective format. It preserves the complex, nested structure of the log data, which is crucial for accurately parsing the multiple policies and conditions that can apply to a single sign-in.

### Why Incorrect Options are Wrong:

B. sign-ins in CSV format: While sign-in logs are the correct data source, the CSV format flattens the hierarchical data, making it difficult for a SIEM to parse the nested details of Conditional Access policy results.
C. audit logs in JSON format: Audit logs record administrative activities, such as when a Conditional Access policy is created, updated, or deleted. They do not contain information about the application of these policies during user sign-ins.
D. audit logs in CSV format: This option is incorrect because audit logs do not contain the required usage data, and CSV is a less suitable format for SIEM ingestion compared to JSON.
---

**References:**

1. Microsoft Learn Sign-in logs in Azure Active Directory: This document details the contents of the sign-in logs. Under the "Conditional Access" section, it states, "If a Conditional Access policy was applied on the sign-in, you can select the Conditional Access tab to view the policies that were applied and the result." This confirms sign-in logs are the source for CA usage data.
Source: Microsoft Corporation. (2023). Sign-in logs in Azure Active Directory. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins#conditional-access
2. Microsoft Learn Audit logs in Azure Active Directory: This document explains that audit logs provide traceability for activities performed in Azure AD. It lists "Update policy" under the "Policy" category, confirming that audit logs track changes to policies, not their application on users.
Source: Microsoft Corporation. (2023). Audit logs in Azure Active Directory. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs
3. Microsoft Learn Stream Azure AD logs to an Azure event hub: This documentation describes the primary method for exporting logs to a SIEM. It explicitly shows the log data schema, which is in JSON format. The signInLogs schema includes the conditionalAccessPolicies property, an array of objects detailing the applied policies.
Source: Microsoft Corporation. (2023). Tutorial: Stream Azure Active Directory logs to an Azure event hub. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-stream-logs-to-event-hub (See the "Log schemas" section).

## Question: 31

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User2, and User3.

You create a group named Group1. You add User2 and User3 to Group1.

You configure a role in Azure AD Privileged Identity Management (PIM) as shown in the Application Administrator exhibit. (Click the Application Administrator tab.)

[image could not be rendered]

Group1 is configured as the approver for the Application administrator role.

You configure User2 to be eligible for the Application administrator role.

For User1 you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click the Assignment tab.)

[image could not be rendered]



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

[image could not be rendered]

**Answer:**

Statement 1: No

Statement 2: Yes

Statement 3: Yes

**Explanation:**

Statement 1: No. User1 has an Eligible assignment, not an Active one. An eligible assignment means the user must first request and complete an activation process (which in this case requires justification and approval) before they can use the role's permissions. The permissions are not granted automatically.

Statement 2: Yes. The designated approver is Group1, which contains both User2 and User3. A fundamental rule in Privileged Identity Management (PIM) is that a user cannot approve their own activation request. Therefore, when User2 requests the role, they cannot approve it themselves, leaving User3 as the only member of the group who can grant approval.

Statement 3: Yes. User1's eligibility ends on January 31, 2021. The request to activate is made at 23:00 on that day, which is within the eligibility period. The role settings specify an Activation maximum duration of 5 hours. The clock for this duration starts upon approval. Therefore, if the role is approved and activated at 23:00, it will expire 5 hours later, which is 04:00 on February 1, 2021.

**References:**

Assignment Types (Eligible vs. Active): Microsoft Learn, Assign Azure AD roles in Privileged Identity Management. "Eligible assignments require the member of the role to perform an action to use the role...Active assignments don't require the member to perform any action to use the role."

Approval Workflow and Self-Approval: Microsoft Learn, Approve or deny requests for Azure AD roles in Privileged Identity Management. Under the "Approve requests" section, it states, "If you are a designated approver, you'll receive an email notification...You can't approve your own requests."



Activation Settings: Microsoft Learn, Configure Azure AD role settings in Privileged Identity Management. The "Activation maximum duration (hours)" setting is defined as the "maximum time, in hours, that a role stays active before it expires."

# Question: 32

You have an Azure Active Directory (Azure AD) tenant.
You need to review the Azure AD sign-ins log to investigate sign ins that occurred in the past.
For how long does Azure AD store events in the sign-in log?

A. 14 days

B. 30 days

C. 90 days

D. 365 days

**Answer:**

B

**Explanation:**

The retention period for Azure Active Directory (Azure AD) sign-in logs depends on the Azure AD license. For tenants with Azure AD Premium P1 or Azure AD Premium P2 licenses, the sign-in activity reports are retained for 30 days. For tenants with an Azure AD Free license, the retention period is 7 days. Given the options and the context of the SC-300 certification, which covers premium features, the 30-day retention period is the correct answer. You can also archive the logs to Azure Storage or integrate them with Azure Monitor for longer retention.



**Why Incorrect Options are Wrong:**

A. 14 days is not a standard retention period for any Azure AD activity logs.
C. 90 days is the default retention for Azure Activity Logs sent to a Log Analytics workspace, not the native retention within Azure AD sign-in reports.
D. 365 days is a common custom retention period when archiving logs to Azure Storage or a Log Analytics workspace, but it is not the default retention in Azure AD.

**References:**

1. Microsoft Learn. (2023). How long does Azure AD store reporting data? Azure Active Directory documentation. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention. (See the table under the "How long does Azure AD store the data?" section, which specifies "30 Days" for Sign-ins with an Azure AD Premium P1 or P2 license).
2. Microsoft Learn. (2023). Azure Active Directory reporting and monitoring deployment dependencies. Azure Active Directory documentation. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/plan-monitoring-and-reporting#reporting-and-monitoring-dependencies. (See the "Data retention" row in the table, which confirms the 30-day retention for Premium licenses).

# Question: 33

HOTSPOT

-

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)

[image could not be rendered]

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)

[image could not be rendered]

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

[image could not be rendered]

For each of the following statements, select Yes if the statement is true. Otherwise, select No.



NOTE: Each correct selection is worth one point.

[image could not be rendered]

## Answer:

Yes

Yes

Yes

## Explanation:

Statement 1: Yes

The Privileged Identity Management (PIM) "Role setting details" for the User Administrator role clearly show that the setting "Require approval to activate" is set to "Yes". Since Admin1 is an eligible member for this role, they must request activation and get approval from a designated approver before the role becomes active.

Statement 2: Yes

The PIM role settings indicate an "Activation maximum duration" of 8 hours. This defines the maximum time the role can be active, but a user can request activation for any duration up to this maximum. Therefore, Admin2 requesting activation for two hours is a valid request.

Statement 3: Yes

Admin3 will be prompted for MFA twice due to two distinct security policies:

• Sign-in MFA: The Conditional Access policy, "Policy1," is enabled for "All users" and "All cloud apps" and requires multi-factor authentication to grant access. This policy will trigger when Admin3 first signs in to the Azure AD admin center.

• Activation MFA: The PIM role settings for the User Administrator role have the setting "On activation, require Azure MFA" set to "Yes." This triggers a second, separate MFA prompt specifically for the role activation process itself.

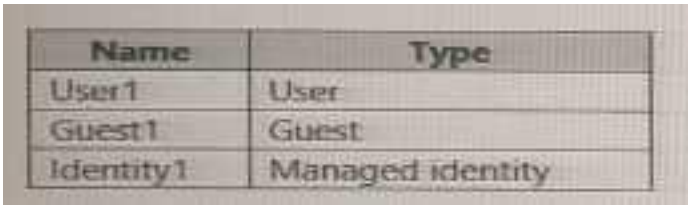
**References:**

Microsoft Learn, Approve or deny requests for Azure AD roles in Privileged Identity Management: This document confirms that if "Require approval" is enabled in a role's settings, an approver must grant the request before the user can activate the role. (See the "Approve requests" section).

Microsoft Learn, Configure Azure AD role settings in Privileged Identity Management: This documentation explains the activation settings for PIM roles, including "Activation maximum duration." It clarifies this setting is the maximum allowed time for an activation. (See the "Activation" settings table).
Microsoft Learn, Conditional Access and Privileged Identity Management: "You can also choose to enforce Azure AD Multi-Factor Authentication on activation for a specific role in PIM settings... PIM will ask users for Azure AD Multi-Factor Authentication during activation, regardless of what other policies are in place." This explicitly states that PIM's MFA on activation is a distinct check from MFA required by Conditional Access policies.

## Question: 34

You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.



| Name | Type |
|---|---|
| User1 | User |
| Guest1 | Guest |
| Identity1 | Managed identity |

Which objects can you add as eligible in Azure Privileged identity Management (PIM) for an Azure AD
role?

A. User1 only

B. User1 and Identity1 only

C. User1. Guest1, and Identity

D. User1 and Guest1 only

**Answer:**

D



**Explanation:**

Azure Privileged Identity Management (PIM) for Azure AD roles allows for eligible assignments to be made to users and specific types of groups. Both member users (User1) and guest users (Guest1) are supported principals that can be made eligible for Azure AD roles through PIM. While role-assignable groups can be used in PIM, the object 'Group1' is only described as a "Security group," not a "role-assignable group," making it ineligible. Managed identities (Identity1), which are a type of service principal, are not supported for eligible assignments in PIM for Azure AD roles. PIM for Azure resource roles supports managed identities, but the question specifically concerns Azure AD roles.

**Why Incorrect Options are Wrong:**

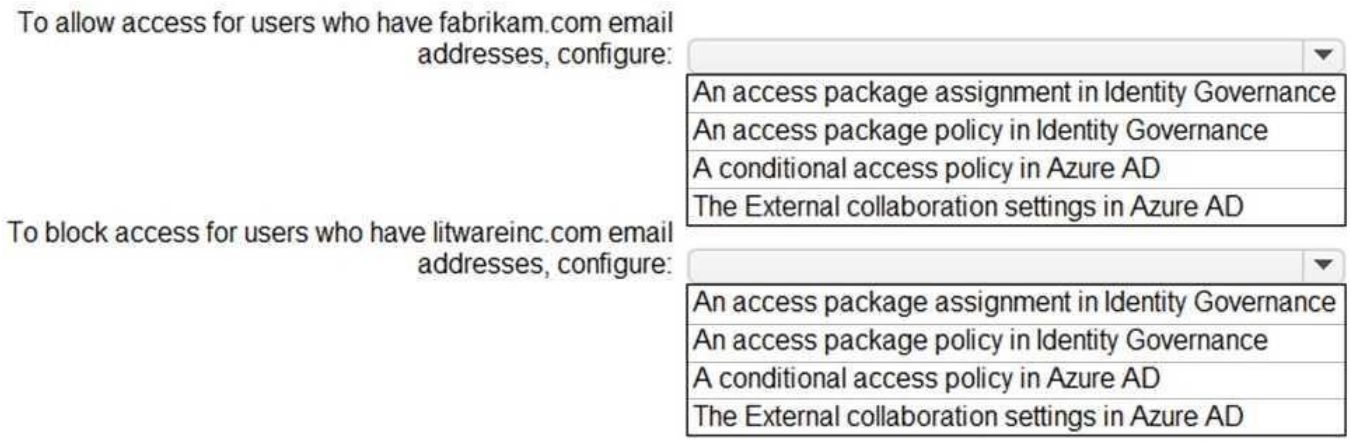
A. User1 only: This is incorrect because guest users (Guest1) can also be made eligible for Azure AD roles in PIM.
B. User1 and Identity1 only: This is incorrect because user-assigned managed identities (Identity1) cannot be made eligible for Azure AD roles in PIM.
C. User1, Guest1, and Identity1: This is incorrect because user-assigned managed identities (Identity1) are not supported for PIM for Azure AD roles.

**References:**

1. Microsoft Learn, "Assign Azure AD roles in Privileged Identity Management." This document outlines the process for assigning roles and specifies the types of principals that can be assigned. Under the "Assign eligibility" section, it states, "You can assign users (both member and guest) and groups to Azure AD roles." It does not mention service principals or managed identities.
2. Microsoft Learn, "Use Azure AD groups to manage role assignments." This document clarifies the requirement for groups. Under the "Prerequisites" section, it states, "To assign a role to a group, you must create a new security or Microsoft 365 group with the isAssignableToRole property set to true." This confirms that a standard security group, as described in the question, is not eligible.
3. Microsoft Learn, "Assign Azure resource roles in Privileged Identity Management." This document contrasts with the capabilities for Azure AD roles. In the "Assign a resource role" section, the documentation shows that for Azure resources, you can assign roles to "users, groups, service principals, and managed identities," explicitly highlighting that this capability is for resource roles, not Azure AD roles.

## Question: 35

HOTSPOT Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc. Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses. You plan to create an access package named package1 that will be accessible only to the users at Fabrikam. You create a connected organization for Fabrikam. You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses. What should you do? To answer, select the appropriate options in the answer area. NOTE:Each correct selection is worth one point.




**Answer:**

An access package policy in Identity Governance.

The External collaboration settings in Azure AD

**Explanation:**

Access package policies are the core component of Microsoft Entra Identity Governance for defining who is eligible to request access to a specific package. To grant access to fabrikam.com users, you create a policy for package1 that allows requests from the connected organization representing Fabrikam. This policy explicitly establishes the rules and lifecycle for how users from that partner organization can obtain access.

The most direct and definitive method to block B2B collaboration with an entire domain is through the tenant-wide External collaboration settings in Microsoft Entra ID. By adding litwareinc.com to the "deny" list under collaboration restrictions, you prevent any user from that domain from being invited as a guest. This global setting effectively blocks them from accessing any resources in your tenant, including package1.

**References:**

Microsoft Entra documentation Create a new access package in entitlement management: This document details the process of creating access packages and their associated policies. It states, "On the Requests tab, you specify a policy to define who can request the access package... For example, you can specify that only users in your directory, or users from connected organizations, can request the access package." This supports using a policy to allow access. (See section: "Create an initial policy for users in your directory").

Microsoft Entra documentation Allow or block invitations to B2B users from specific organizations: This source explicitly describes the function of collaboration restrictions. It confirms, "You can use an allowlist or a denylist to... Deny invitations to the specified domains. If you set up a denylist, you can send invitations to any domain except the ones you block." This validates using External collaboration settings to block specific domains at the tenant level. (See section: "Set collaboration restrictions in the portal").