

- **Vendor: Microsoft**
- **Exam Code: SC-300**
- **Exam Name: Microsoft Identity and Access Administrator**
- **New Updated Questions from [Braindump2go](#)**
- **(Updated in [December/2021](#))**

Visit Braindump2go and Download Full Version SC-300 Exam Dumps

QUESTION 1

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

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

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

[SC-300 Exam Dumps](#) **[SC-300 Exam Questions](#)** **[SC-300 PDF Dumps](#)** **[SC-300 VCE Dumps](#)**

<https://www.braindump2go.com/sc-300.html>

- The users in the London office have the Microsoft 365 Phone System license unassigned.
 - The users in the Seattle office have the Yammer Enterprise license unassigned.
- Security defaults are disabled for contoso.com.
Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

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:

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

QUESTION 2**Case Study 1 - Contoso, Ltd****Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

[SC-300 Exam Dumps](#) [SC-300 Exam Questions](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#)

<https://www.braindump2go.com/sc-300.html>

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

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

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.

- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

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 configuration policy in Microsoft Endpoint Manager
- C. an app registration in Azure AD
- D. Azure AD Application Proxy

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

QUESTION 3

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

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

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

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:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

QUESTION 4

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

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

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

Hotspot Question

You need to meet the technical requirements for the probability that user identities 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.

Answer Area

The users must first:

<input type="checkbox"/>	Provide consent for any app to access the data of Contoso.
<input type="checkbox"/>	Register for multi-factor authentication (MFA).
<input type="checkbox"/>	Register for self-service password reset (SSPR).

You must configure:

<input type="checkbox"/>	A sign-in risk policy
<input type="checkbox"/>	A user risk policy
<input type="checkbox"/>	An Azure AD Password Protection policy

Answer:

Answer Area

The users must first:

▼

Provide consent for any app to access the data of Contoso.

Register for multi-factor authentication (MFA).

Register for self-service password reset (SSPR).

You must configure:

▼

A sign-in risk policy

A user risk policy

An Azure AD Password Protection policy

Explanation:

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

QUESTION 5

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.

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

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

Hotspot Question

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 Area

To configure user access:

An access package
An access review
A conditional access policy

To enable collaboration with fabrikam.com:

An accepted domain
A connected organization
A custom domain name

Answer:**Answer Area**

To configure user access:

An access package
An access review
A conditional access policy

To enable collaboration with fabrikam.com:

An accepted domain
A connected organization
A custom domain name

Explanation:<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>**QUESTION 6****Case Study 2 - Litware, Inc****Overview**

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

[SC-300 Exam Dumps](#) [SC-300 Exam Questions](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#)

<https://www.braindump2go.com/sc-300.html>

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `LWLicenses` to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the `LWLicenses` attribute. Users who have the appropriate value for `LWLicenses` must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named `LWGroup1` that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

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

You need to meet the authentication requirements for leaked credentials.

What should you do?

- A. Enable password hash synchronization in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Configure an authentication method policy in Azure AD.
- D. Enable federation with PingFederate in Azure AD Connect.

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>

QUESTION 7

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `LWLicenses` to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the `LWLicenses` attribute. Users who have the appropriate value for `LWLicenses` must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named `LWGroup1` that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

[SC-300 Exam Dumps](#) [SC-300 Exam Questions](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#)

<https://www.braindump2go.com/sc-300.html>

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

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

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

QUESTION 8

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `LWLicenses` to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the `LWLicenses` attribute. Users who have the appropriate value for `LWLicenses` must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named `LWGroup1` that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

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

Hotspot Question

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 Area

Azure AD Connect settings to modify:

▼
Directory Extensions
Domain Filtering
Optional Features

Assign Azure AD licenses to:

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

Answer:

Answer Area

Azure AD Connect settings to modify:

Assign Azure AD licenses to:

Explanation:

Litware recently added a custom user attribute named LWWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the attribute. Users who have the appropriate value for LWWLicenses must be added LWWLicenses automatically to a Microsoft 365 group that has the appropriate licenses assigned.

QUESTION 9
Case Study 2 - Litware, Inc
Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.

[SC-300 Exam Dumps](#) [SC-300 Exam Questions](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#)

<https://www.braindump2go.com/sc-300.html>

- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `LWLicenses` to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the `LWLicenses` attribute. Users who have the appropriate value for `LWLicenses` must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named `LWGroup1` that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

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

Hotspot Question

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 Area

To manage Azure AD built-in role assignments, use:

<input type="checkbox"/>
Global administrator
Privileged role administrator
Security administrator
User access administrator

To manage Azure built-in role assignments, use:

<input type="checkbox"/>
Global administrator
Privileged role administrator
Security administrator
User access administrator

Answer:

Answer Area

To manage Azure AD built-in role assignments, use:

 Global administrator
 Privileged role administrator
 Security administrator
 User access administrator

To manage Azure built-in role assignments, use:

 Global administrator
 Privileged role administrator
 Security administrator
 User access administrator

Explanation:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

QUESTION 10

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

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

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

[SC-300 Exam Dumps](#) [SC-300 Exam Questions](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#)

<https://www.braindump2go.com/sc-300.html>

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD.
- Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named `LWLicenses` to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the `LWLicenses` attribute. Users who have the appropriate value for `LWLicenses` must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named `LWGroup1` that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

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

Hotspot Question

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 Area

For on-premises applications:

<input type="checkbox"/>	Configure Cloud App Security policies.
<input type="checkbox"/>	Modify the User consent settings for the enterprise applications.
<input type="checkbox"/>	Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

<input type="checkbox"/>	Configure Cloud App Security policies.
<input type="checkbox"/>	Modify the User consent settings for the enterprise applications.
<input type="checkbox"/>	Publish an application by using Azure AD Application Proxy.

Answer:

[SC-300 Exam Dumps](#) [SC-300 Exam Questions](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#)

<https://www.braindump2go.com/sc-300.html>

Answer Area

For on-premises applications:

▼

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

For SharePoint Online:

▼

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

QUESTION 11

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

Users sign in to computers that run Windows 10 and are joined to the domain.

You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).

You need to configure the computers for Azure AD Seamless SSO.

What should you do?

- A. Configure Sign-in options.
- B. Enable Enterprise State Roaming.
- C. Modify the Intranet Zone settings.
- D. Install the Azure AD Connect Authentication Agent.

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ssso-quick-start>

QUESTION 12

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

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

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

- A. Group1 and Group4 only
- B. Group1, Group2, Group3, Group4, and Group5
- C. Group1 and Group2 only
- D. Group1 only

E. Group1, Group2, Group4, and Group5 only

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

QUESTION 13

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Azure Active Directory (Azure AD).

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Set-MsolCompanySettings
- B. Set-MsolDomainFederationSettings
- C. Update-MsolFederatedDomain
- D. Set-MsolDomain

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup>

QUESTION 14

You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click the **Exhibit** tab.)

Guest user access

Guest user access restrictions (Preview) ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☒ Guest users have limited access to properties and memberships of directory objects
- ☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Admins and users in the guest inviter role can invite ⓘ

☒ Yes ☐ No

Members can invite ⓘ

☒ Yes ☐ No

Guests can invite ⓘ

☐ Yes ☒ No

Email One-Time Passcode for guests ⓘ

[Learn more](#)

☒ Yes ☐ No

Enable guest self-service sign up via user flows (Preview) ⓘ

[Learn more](#)

☒ Yes ☐ No

Collaboration restrictions

- ☒ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive)

A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

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

Which users will be emailed a passcode?

- A. User2 only
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

QUESTION 15

[SC-300 Exam Dumps](#) [SC-300 Exam Questions](#) [SC-300 PDF Dumps](#) [SC-300 VCE Dumps](#)

<https://www.braindump2go.com/sc-300.html>

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Identity Governance blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Licenses blade in the Azure Active Directory admin center
- D. the Set-WindowsProductKey cmdlet

Answer: C