

Question: 461

CertyIQ

Introductory Info Case Study -
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 relevant 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

Contoso also includes a marketing department that has users in each office.

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 E5

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.

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. Question 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. Configure a Conditional Access policy.
- C. Configure the Access reviews settings.
- D. Modify the External collaboration settings.

Question: 462

CertyIQ

Introductory Info Case Study -
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 relevant 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

Contoso also includes a marketing department that has users in each office.

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 E5

- 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

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. Question 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.

Question: 463

CertyIQ

Introductory Info Case Study -

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. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash 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 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 by using conditional access policies.

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:

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. Question You need to configure the detection of multi-staged attacks to meet the monitoring requirements.

What should you do?

- A. Customize the Microsoft Sentinel rule logic.
- B. Create a workbook.
- C. Add Microsoft Sentinel data connectors.
- D. Add an Microsoft Sentinel playbook.

Question: 464

CertyIQ

Introductory Info Case Study -

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. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash 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 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 by using conditional access policies.

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:

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. Question 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.