Prüfungsnummer:MS-500

Prüfungsname: Microsoft 365 Security Administration

Version:demo

https://www.it-exams.fr/

Testlet 1

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure
The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements
Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy

▪

Identity Synchronization Notification" in the subject line. Several users recently opened email

attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes
Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration
Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange

Online only

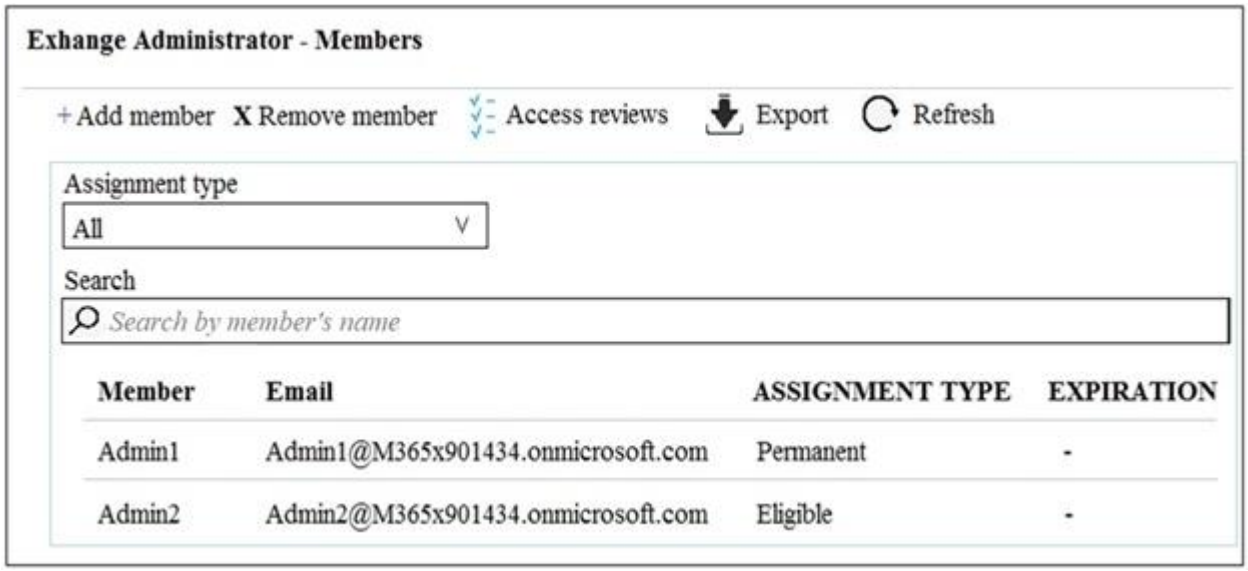
Security Requirements
Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Q1
An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.



What should you do to meet the security requirements?

A. Change the Assignment Type for Admin2 to Permanent
B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
D. Change the Assignment Type for Admin1 to Eligible

Answer: D

Q2
You need to recommend a solution for the user administrators that meets the security requirements for auditing.

Which blade should you recommend using from the Azure Active Directory admin center?

A. Sign-ins
B. Azure AD Identity Protection
C. Authentication methods

D. Access review

Answer: A

References:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Q3
HOTSPOT

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Set the frequency to:

One time	V
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	V
Advanced settings	
Programs	
Reviewers	

Answer:

Set the frequency to:

One time	V
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	V
Advanced settings	
Programs	
Reviewers	

Q4
You need to recommend a solution to protect the sign-ins of Admin1 and Admin2.

What should you include in the recommendation?

A. a device compliance policy
B. an access review
C. a user risk policy
D. a sign-in risk policy

Answer: C

References:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy

Q5
You need to resolve the issue that generates the automated email messages to the IT team.

Which tool should you run first?

A. Synchronization Service Manager
B. Azure AD Connect wizard
C. Synchronization Rules Editor
D. IdFix

Answer: B

References:
https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization
Implement and manage identity and access

Testlet 2
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.
Existing Environment
Internal Network Infrastructure
The network contains a single domain forest. The forest functional level is Windows Server 2016.
Users are subject to sign-in hour restrictions as defined in Active Directory.
The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).
The following operating systems are used on the network:
Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.
Cloud Infrastructure
Litware recently purchased Microsoft 365 subscription licenses for all users.
Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings.
User accounts are not yet synced to Azure AD.
You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements
Planned Changes
Litware plans to implement the following changes:
Migrate the email system to Microsoft Exchange Online

▪

Implement Azure AD Privileged Identity Management

▪

Security Requirements
Litware identifies the following security requirements:
Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest

▪

Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory

▪

Implement a permanent eligible assignment of the Compliance administrator role for User1

▪

Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP

▪

Prevent access to Azure resources for the guest user accounts by default

▪

Ensure that all domain-joined computers are registered to Azure AD

▪

Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.
You identify the following requirements for testing MFA:
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location.

▪

Any disruption of legitimate authentication attempts must be minimized.

▪

General Requirements
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Q6
You need to create Group2.

What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center
B. a mail-enabled security group in the Microsoft 365 admin center
C. a security group in the Microsoft 365 admin center
D. a distribution list in the Microsoft 365 admin center
E. a security group in the Azure AD admin center

Answer: CE

Q7
Which IP address space should you include in the Trusted IP MFA configuration?

A. 131.107.83.0/28
B. 192.168.16.0/20
C. 172.16.0.0/24
D. 192.168.0.0/20

Answer: B

Q8
HOTSPOT

How should you configure Group3? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Group type:
- An Office 365 group in the Microsoft 365 admin center
- A security group in Active Directory Users and Computers
- A security group in the Azure Active Directory admin center

Group membership criteria:
- A dynamic distribution list
- A dynamic membership rule set to accountEnabled Equals true
- A dynamic membership rule set to userType Equals Member

Answer:

Answer Area

Group type:

- An Office 365 group in the Microsoft 365 admin center
- A security group in Active Directory Users and Computers
- A security group in the Azure Active Directory admin center

Group membership criteria:

- A dynamic distribution list
- A dynamic membership rule set to accountEnabled Equals true
- A dynamic membership rule set to userType Equals Member

Reference:
https://docs.microsoft.com/en-us/azure/information-protection/prepare

Q9
HOTSPOT

How should you configure Azure AD Connect? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User sign-in settings:

- Password Synchronization with single-sign on
- Pass-through authentication with single sign-on
- Federation with Active Directory Federation Services (AD FS)

Device options:

- Hybrid Azure AD Join
- Enable Device writeback
- Disable Device writeback

Answer:

Answer Area