



Vendor: Microsoft

Exam Code: MS-500

Exam Name: Microsoft 365 Security Administration

Version: 13.02

Q & As: 116

Topic 1, Fabrikam inc.

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

QUESTION 1

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

Exchange Administrator - Members

+ Add member X Remove member  Access reviews  Export  Refresh

Assignment type

Search

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

- Change the Assignment Type for Admin2 to Permanent
- From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
- From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
- Change the Assignment Type for Admin1 to Eligible

Correct Answer: D

QUESTION 2

You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.

What should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- Create an access review.
- Assign the Global administrator role to User1.
- Assign the Guest inviter role to User1.
- Modify the External collaboration settings in the Azure Active Directory admin center.

Correct Answer: CD

QUESTION 3

You need to resolve the issue that targets 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

Correct Answer: B

Explanation:

<https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization>

QUESTION 4

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

Correct Answer: C

Explanation:

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

QUESTION 5

HOTSPOT

You need to recommend an email malware solution that meets the security requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policy to create:

ATP safe attachments	v
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	v
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	