

KTest

更に上のクオリティ 更に上のサービス



問題集

<http://www.ktest.jp>

1年で無料進級することに提供する

Exam : **MS-500**

Title : Microsoft 365 Security
Administration

Version : DEMO

1. Testlet 1

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

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?

- 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

2.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

Explanation:

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

3.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.

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	

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

Answer: D

Explanation:

Reference:

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

5. 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

Explanation:

References:

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