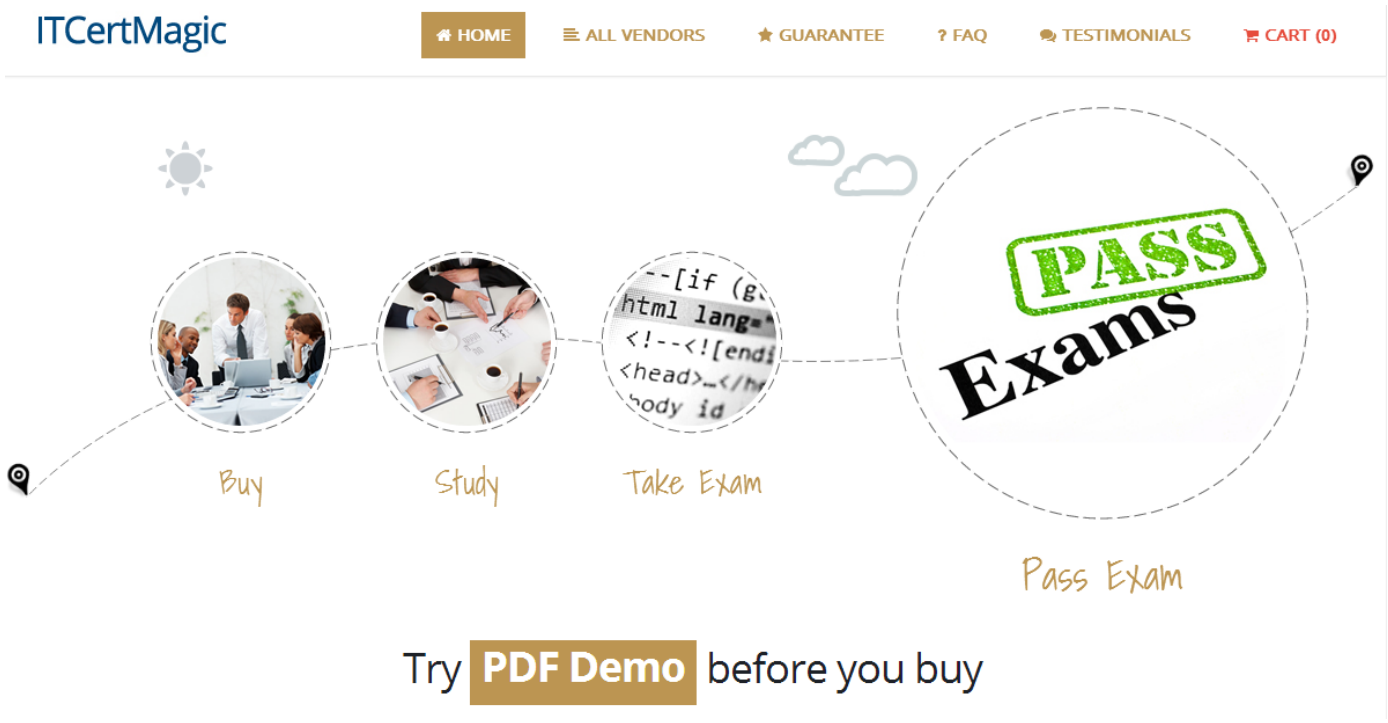
ITCertMagic



http://www.itcertmagic.com/

Pass-Guaranteed Certification Exam Questions | Exam Dumps - ITCertMagic

Exam : **MS-102-KR**

Title : Microsoft 365 Administrator (MS-102 Korean Version)

Vendor : Microsoft

Version : DEMO

QUESTION NO: 1
Intune에 대한 기술적 요구 사항과 계획된 변경 사항을 충족해야 합니다.
어떻게 해야 하나요? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.
Answer Area

Settings to configure in Azure AD:	Device settings Mobility (MDM and MAM) Organizational relationships User settings
Settings to configure in Intune:	Device compliance Device configuration Device enrollment Mobile Device Management Authority

Answer:
Answer Area

Settings to configure in Azure AD:	Device settings Mobility (MDM and MAM) Organizational relationships User settings
Settings to configure in Intune:	Device compliance Device configuration Device enrollment Mobile Device Management Authority

Explanation:

Settings to configure in Azure AD:	**Device settings** **Mobility (MDM and MAM)** **Organizational relationships** **User settings**
Settings to configure in Intune:	**Device compliance** **Device configuration** **Device enrollment** **Mobile Device Management Authority**

Reference:
https://docs.microsoft.com/en-us/intune/windows-enroll
Topic 1, Contoso, LtdOverview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 ES subscription.
Existing Environment
Requirement
The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.
The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.
The domain is synced to Microsoft Entra ID (Microsoft Entra ID) and includes the users shown in the following table.

Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.
Planned Changes
Contoso plans to implement the following changes:
*Implement Microsoft 365.
*Manage devices by using Microsoft Intune.
*Implement Microsoft Entra IDvanced Threat Protection (ATP).
*Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements
Contoso identifies the following technical requirements:
*When a Windows 10 device is joined to Microsoft Entra ID, the device must enroll in Intune automaticity.
*Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
*User1 must be able to enroll all the New York office mobile devices in Intune.
*Azure ATP sensors must be installed and must NOT use port mirroring.
*Whenever possible, the principle of least privilege must be used.

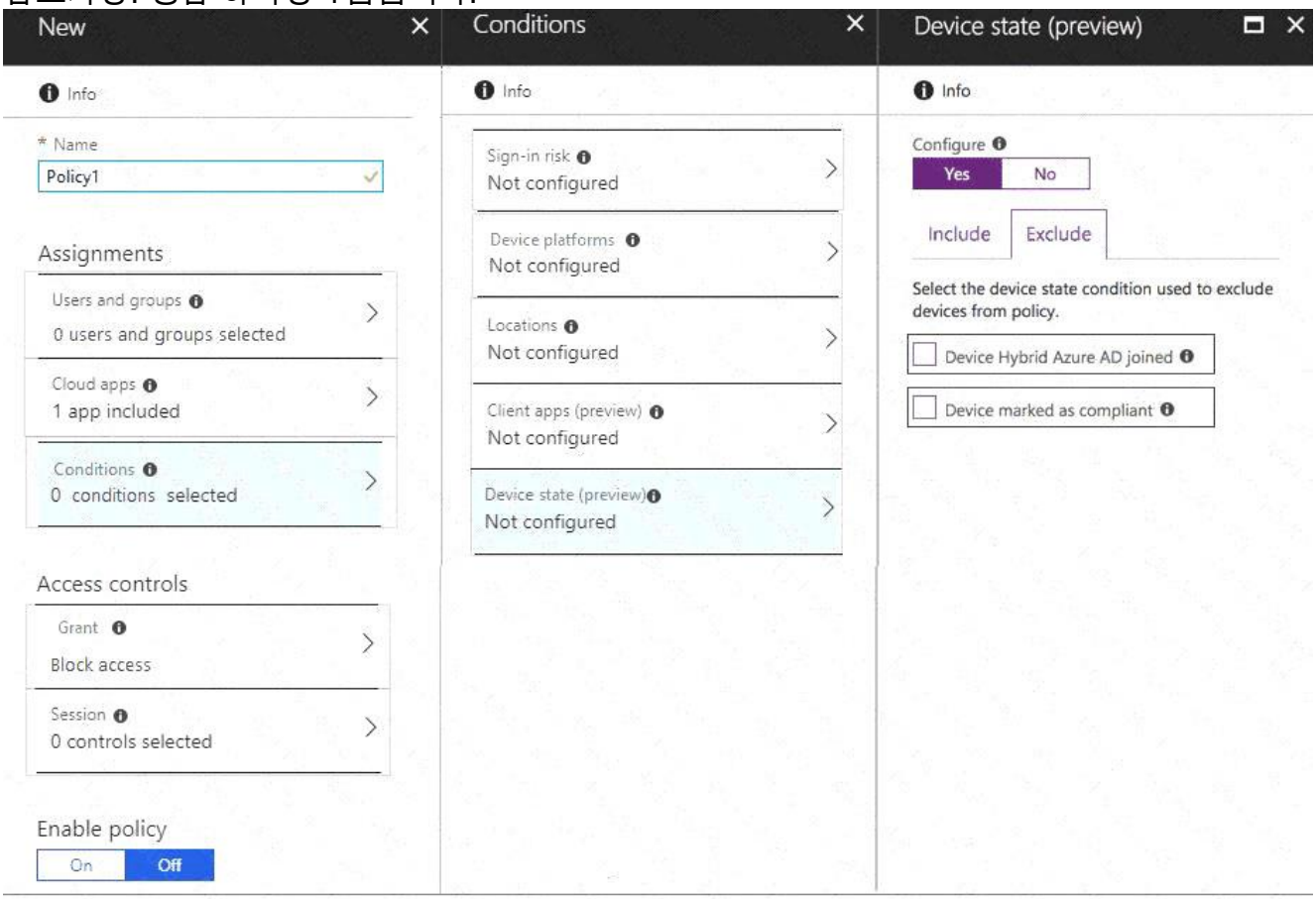
*A Microsoft Store for Business must be created.
Compliance Requirements
Contoso identifies the following compliance requirements:
*Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
*Configure Windows Information Protection (W1P) for the Windows 10 devices.

QUESTION NO: 2
어떤 서버에 Azure ATP 센서를 설치해야 합니까?
A. 서버 1
B. 서버 2
C. 서버 3
D. 서버 4
E. 서버 5
Answer: A
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning
However, if the case study had required that the DCs can ' t have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

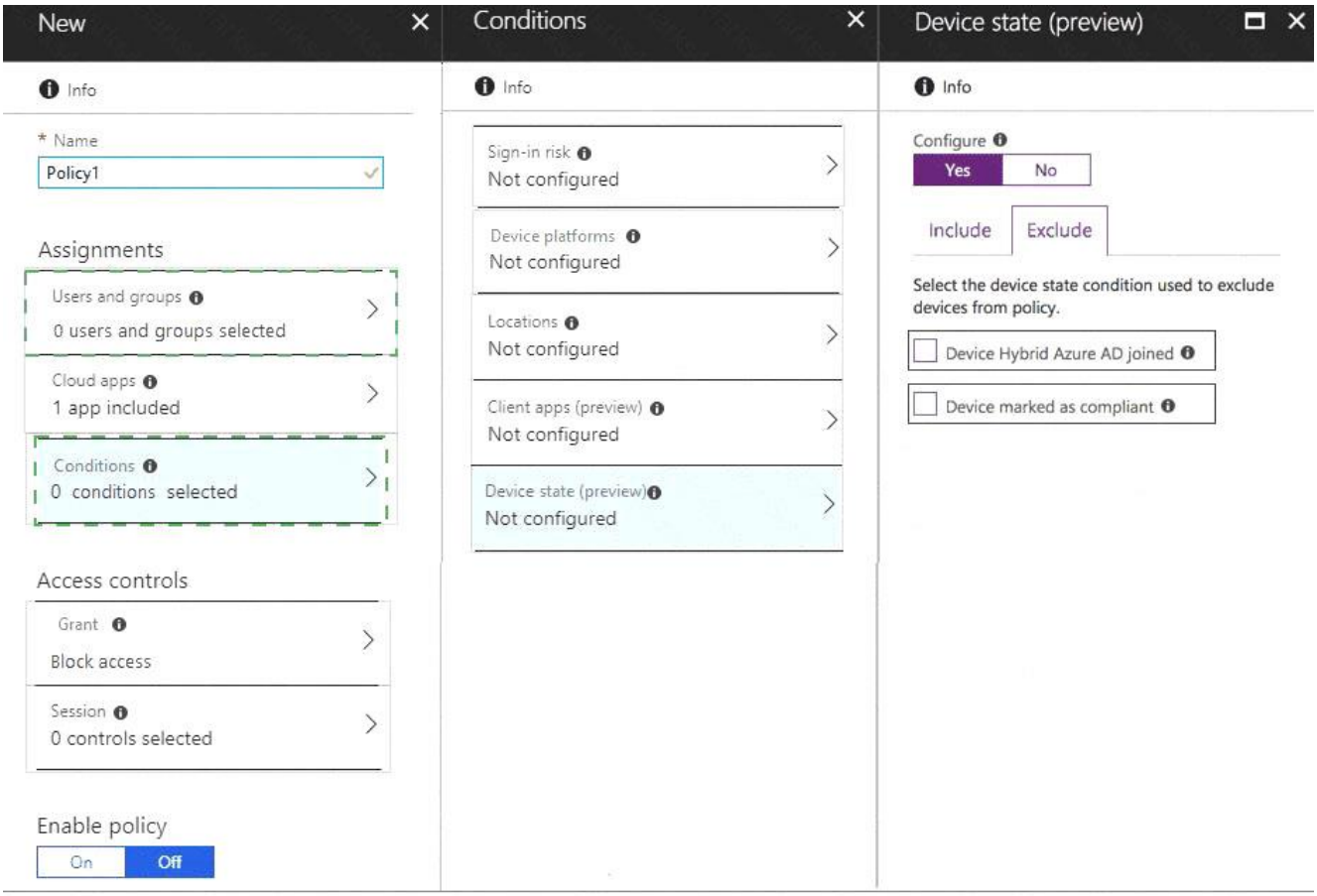
QUESTION NO: 3
참고: 이 문제는 동일한 시나리오를 제시하는 일련의 문제 중 하나입니다. 각 문제에는 제시된 목표를 달성할 수 있는 고유한 해결책이 포함되어 있습니다. 일부 문제 세트에는 정답이 두 개 이상일 수 있으며, 정답이 없는 문제 세트도 있습니다.
이 섹션에서 질문에 답변한 후에는 해당 질문으로 돌아갈 수 없습니다. 따라서 이 질문들은 검토 화면에 나타나지 않습니다.
네트워크에는 Microsoft Entra ID(Microsoft Entra ID)와 동기화된 contoso.com이라는 Active Directory 도메인이 있습니다.
Windows 10 장치는 Microsoft System Center Configuration Manager(현재 분기)를 사용하여 관리할 수 있습니다.
공동 관리를 위한 파일럿 프로그램을 구성합니다.
도메인에 Device1이라는 새 장치를 추가합니다. Device1에 Configuration Manager 클라이언트를 설치합니다.
Microsoft Intune 및 Configuration Manager를 사용하여 Device1을 관리할 수 있는지 확인해야 합니다.
해결 방법: Configuration Manager 장치 컬렉션을 파일럿 컬렉션으로 정의합니다. 해당 컬렉션에 Device1을 추가합니다.
이것이 목표를 달성합니까?
A. 예
B. 아니요
Answer: A
Explanation:
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be

enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

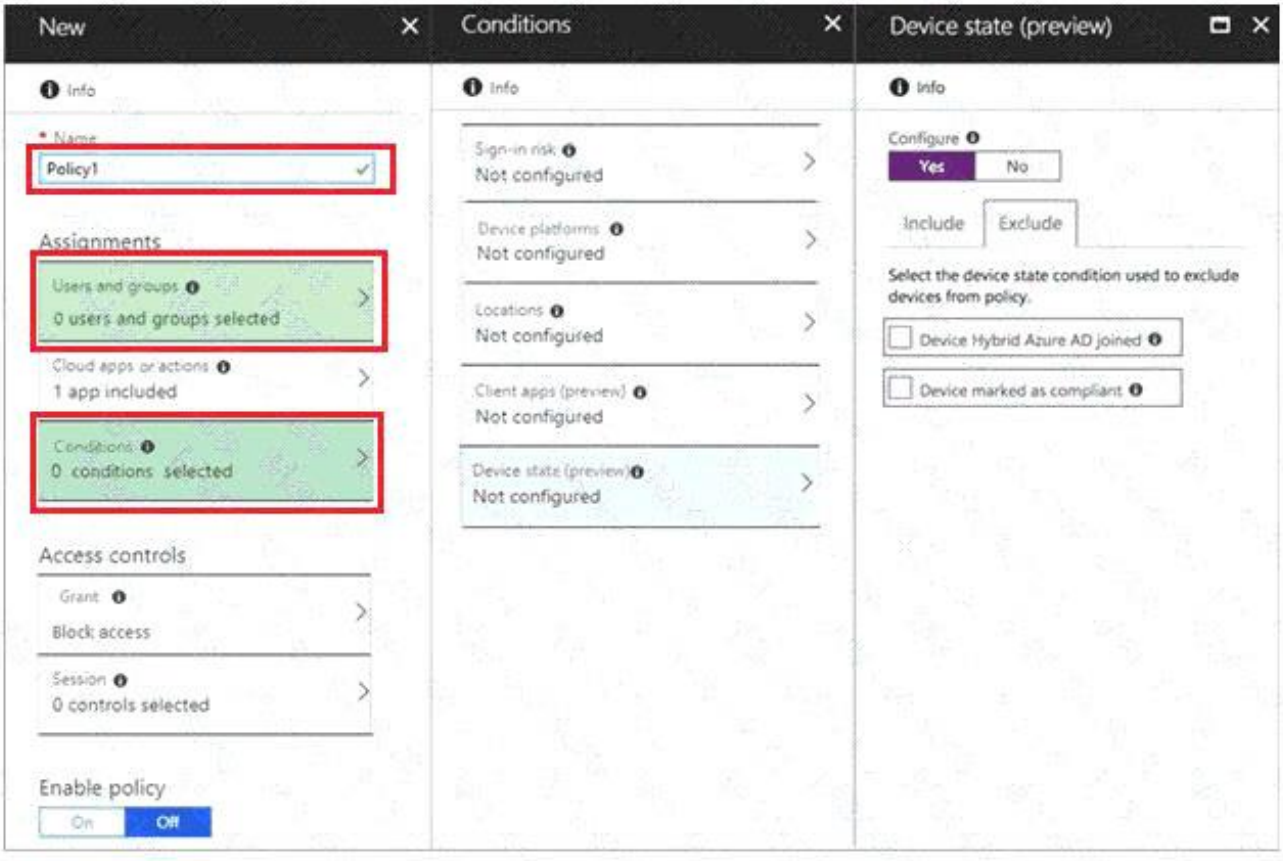
QUESTION NO: 4
규정 준수 요구 사항을 충족하려면 조건부 액세스 정책을 구성해야 합니다.
Exchange Online을 클라우드 앱으로 추가합니다.
Policy1에서 어떤 두 가지 추가 설정을 구성해야 합니까? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.



Answer:



Explanation:
Suggested answer:



References:https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

QUESTION NO: 5
User1이 기술 요구 사항을 충족하도록 장치를 등록할 수 있도록 해야 합니다. 어떻게 해야 할까요?
A. Microsoft Entra ID 관리 센터에서 User1에게 클라우드 장치 관리자 권한을 부여합니다.
B. Microsoft Entra ID 관리 센터에서 사용자당 최대 장치 수 설정을 구성합니다.
C. Intune 관리 센터에서 User1을 장치 등록 관리자로 추가합니다.
D. Intune 관리 센터에서 등록 제한을 구성합니다.
Answer: C
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

QUESTION NO: 6
어떤 서버에서 Defender for ID 센서를 사용해야 합니까?
A. 서버1
B. 서버2
C. 서버3
D. 서버4
E. 서버5
Answer: A
Explanation:
However, if the case study had required that the DCs can ' t have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

QUESTION NO: 7
참고: 이 문제는 동일한 시나리오를 제시하는 일련의 문제 중 하나입니다. 각 문제에는 제시된 목표를 달성할 수 있는 고유한 해결책이 포함되어 있습니다. 일부 문제 세트에는 정답이 두 개 이상일 수 있으며, 정답이 없는 문제 세트도 있습니다.
이 섹션에서 질문에 답변한 후에는 해당 질문으로 돌아갈 수 없습니다. 따라서 이 질문들은 검토 화면에 나타나지 않습니다.
네트워크에는 Microsoft Entra ID(Microsoft Entra ID)와 동기화된 contoso.com이라는 Active Directory 도메인이 있습니다.
Windows 10 장치는 Microsoft System Center Configuration Manager(현재 분기)를 사용하여 관리할 수 있습니다.
공동 관리를 위한 파일럿 프로그램을 구성합니다.
도메인에 Device1이라는 새 장치를 추가합니다. Device1에 Configuration Manager 클라이언트를 설치합니다.
Microsoft Intune 및 Configuration Manager를 사용하여 Device1을 관리할 수 있는지 확인해야 합니다.
해결 방법: 장치 관리 관리 센터에서 장치 구성 프로필을 생성합니다.
이것이 목표를 달성합니까?
A. 예

B. 아니요

Answer: B

Explanation:

It looks like the given answer is correct. There is an on-premises Active Directory synced to Microsoft Entra ID (Microsoft Entra ID) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Microsoft Entra ID 2. Client agent setting for hybrid Microsoft Entra ID-join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager https://docs.microsoft.com/en-us/mem/configmgr /comanage/tutorial-co-manage-client

QUESTION NO: 8

3월부터 각 사무실의 컴퓨터는 얼마 동안 Microsoft에서 지원됩니까? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.

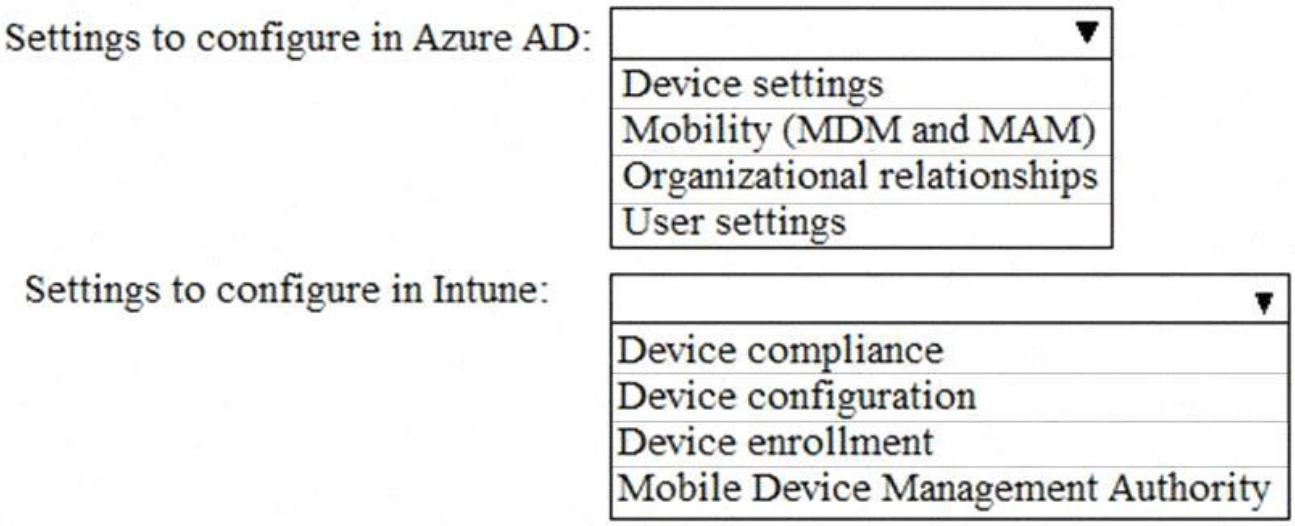
참고사항: 정답 하나당 1점입니다.

Answer:

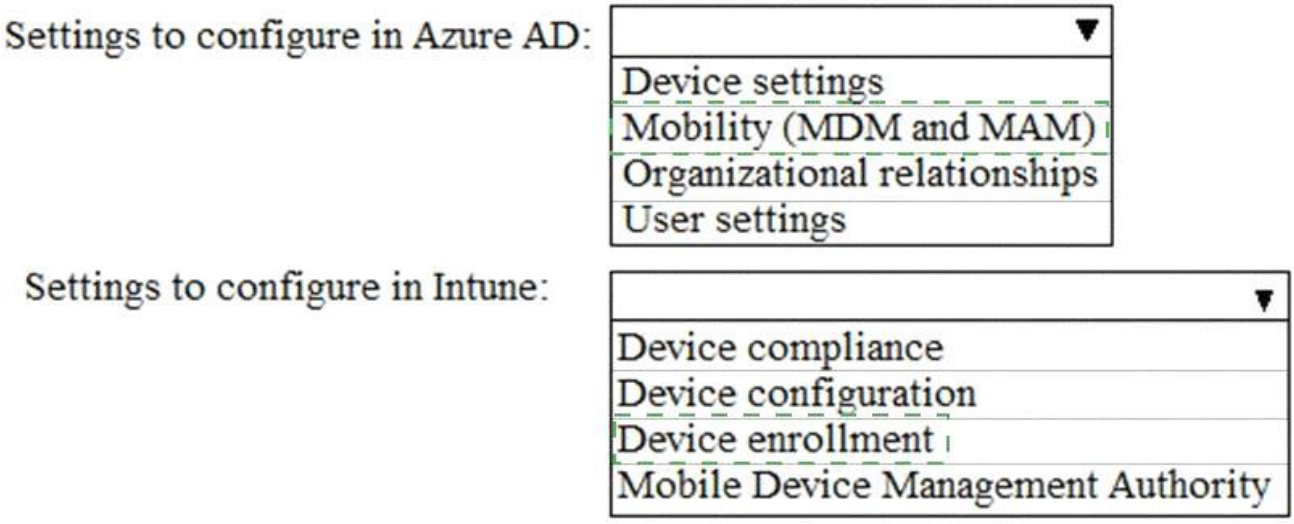
Explanation:

https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates:
Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date References:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

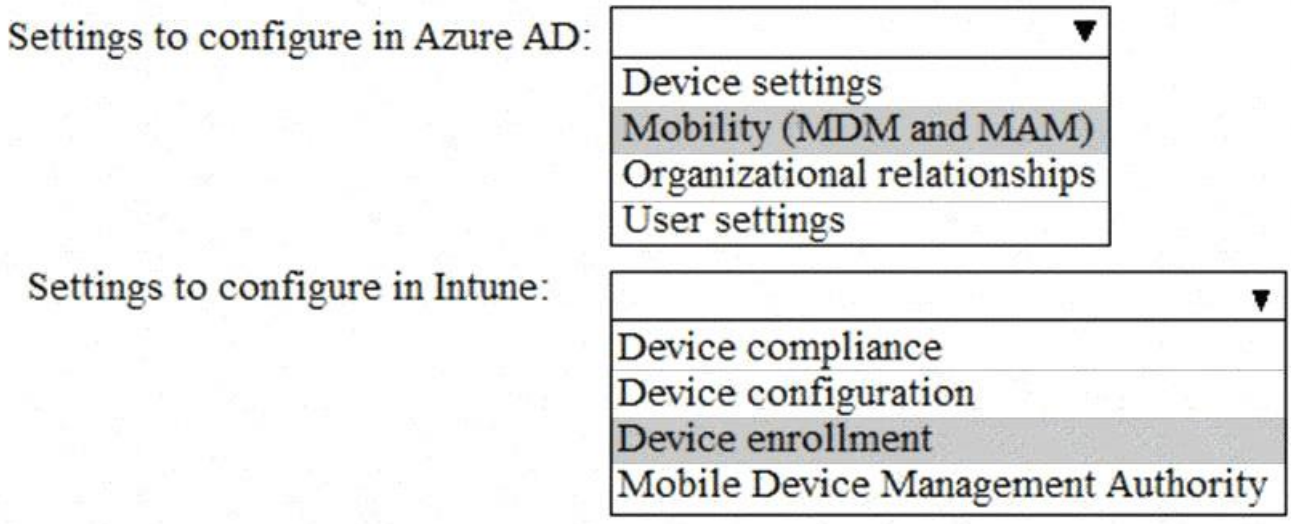
QUESTION NO: 9
Windows 10 장치에 대한 Intune 요구 사항을 충족해야 합니다.
어떻게 해야 하나요? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.



Answer:



Explanation:



References:
https://docs.microsoft.com/en-us/intune/windows-enroll

QUESTION NO: 10

Microsoft Store for Business를 만들어야 합니다. 어떤 사용자가 스토어를 만들 수 있나요?
A. 사용자2
B. 사용자3
C. 사용자4
D. 사용자5
Answer: C
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

QUESTION NO: 11
지원 기술자가 몬트리올 사무실 모바일 기기에 대한 기술 요구 사항을 충족할 수 있는지 확인해야 합니다.
최소한 필요한 전담 지원 기술자는 몇 명입니까?
A. 1
B. 4
C. 7
D. 31
Answer: B
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

QUESTION NO: 12
Windows 10 장치에 대한 규정 준수 요구 사항을 충족해야 합니다.
Intune 관리 센터에서 무엇을 만들어야 합니까?
A. 장치 준수 정책
B. 장치 구성 프로필
C. 응용 프로그램 정책
D. 앱 구성 정책
Answer: C
Topic 2, A. DatumCase Study:
Overview
Existing Environment
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. When you are ready to answer a question, click the Question button to return to the question.
Current Infrastructure
A). Datum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
A). Datum uses and processes Personally Identifiable Information (PII).
Problem Statements
Requirements
A). Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.
Business Goals
A). Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.
A). Datum wants to minimize the cost of hardware and software whenever possible.
Technical Requirements
A). Datum identifies the following technical requirements:
Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office
365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user ' s user account.
A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

QUESTION NO: 13

EU PII 데이터에 대한 기술적 요구 사항을 충족해야 합니다.
무엇을 만들어야 할까요?

A. 보안 및 규정 준수 관리 센터의 보존 정책입니다.
B. Exchange 관리 센터의 보존 정책
C. Exchange 관리 센터의 데이터 손실 방지(DLP) 정책
D. 보안 및 규정 준수 관리 센터의 데이터 유출 방지(DLP) 정책

Answer: A

References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies EU PII wants both documents and email message to be preserved so S & C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

QUESTION NO: 14

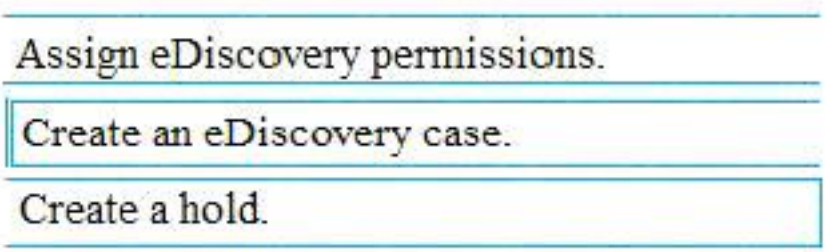
법무부의 요구 사항을 충족해야 합니다.
보안 및 규정 준수 관리 센터에서 순서대로 수행해야 하는 세 가지 작업은 무엇입니까?
대답하려면 작업 목록에서 해당 작업을 답변 영역으로 이동하고 올바른 순서로 정렬합니다.

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Answer:

Actions	Answer Area
Create a data loss prevention (DLP) policy.	Assign eDiscovery permissions.
Create an eDiscovery case.	Create an eDiscovery case.
Create a label.	Create a hold.
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Explanation:

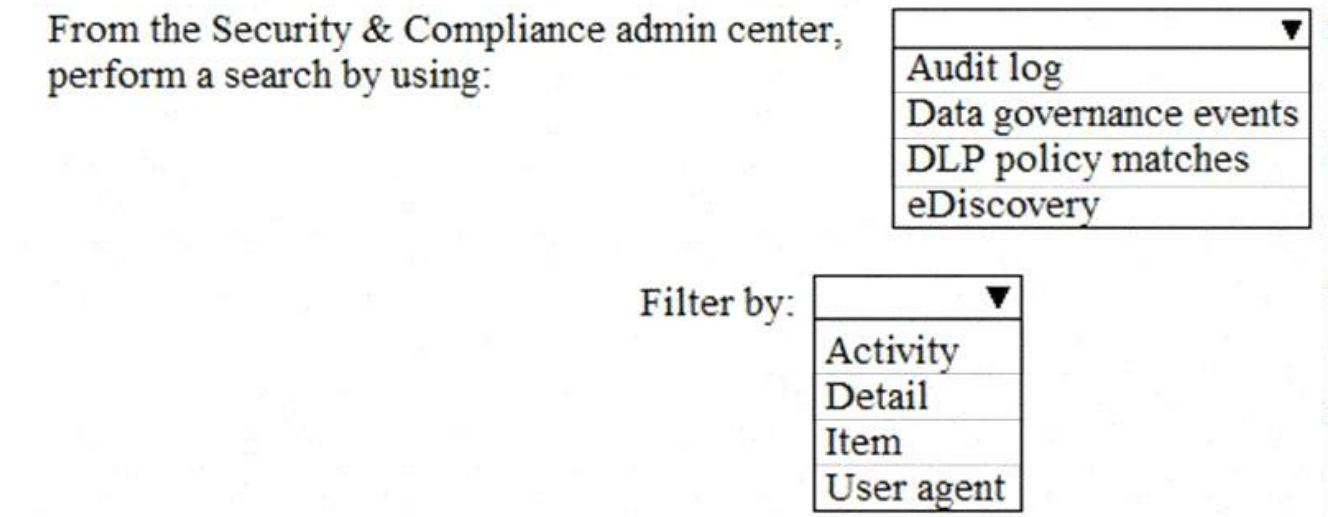


References:
https://www.sherweb.com/blog/ediscovery-office-365/

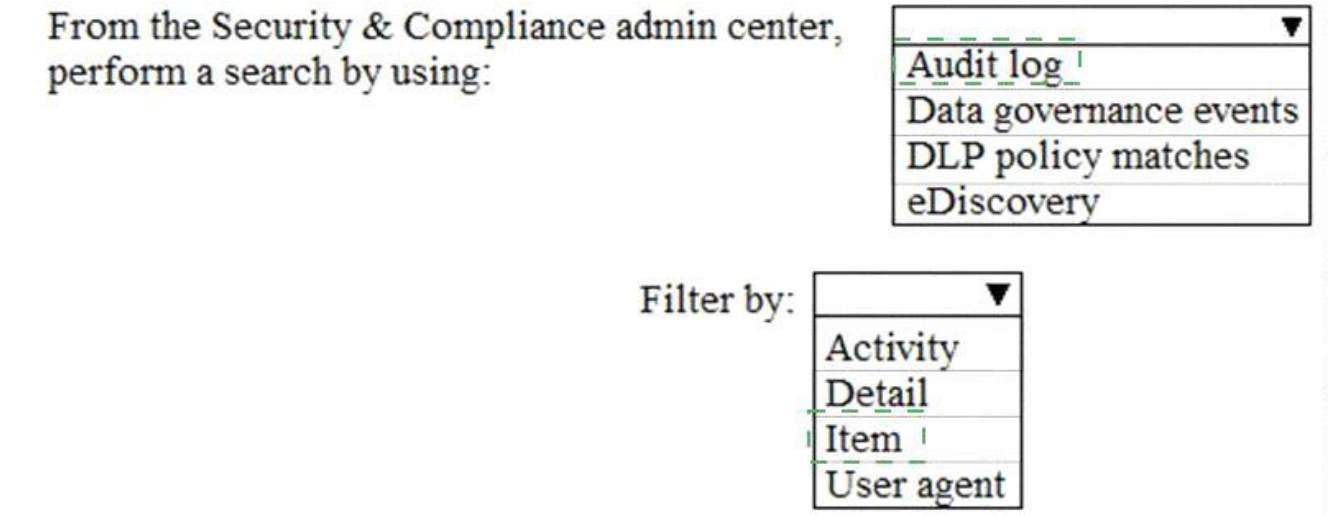
QUESTION NO: 15
기술적 요구 사항을 충족하려면 미국 PII 데이터를 보호해야 합니다.
무엇을 만들어야 할까요?
A. 도메인 예외를 포함하는 데이터 손실 방지(DLP) 정책
B. 민감한 데이터가 포함된 콘텐츠를 감지하는 보안 및 규정 준수 보존 정책
C. 활동을 포함하는 보안 및 규정 준수 경고 정책
D. 사용자 재정의를 포함하는 데이터 손실 방지(DLP) 정책
Answer: A

QUESTION NO: 16
보안 관리자에게 해결책을 제시해야 합니다. 해당 해결책은 기술적 요구 사항을 충족해야 합니다.
추천 사항에 무엇을 포함해야 할까요?
A. Microsoft Entra ID(Microsoft Entra ID) 권한 있는 ID 관리
B. 마이크로소프트 엔트라 ID(Microsoft Entra ID) 신원 보호
C. Microsoft Entra ID(Microsoft Entra ID) 조건부 액세스 정책
D. Microsoft Entra ID(Microsoft Entra ID) 인증 방법
Answer: B
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access- conditions#sign-in-risk states clearly that Sign-in risk

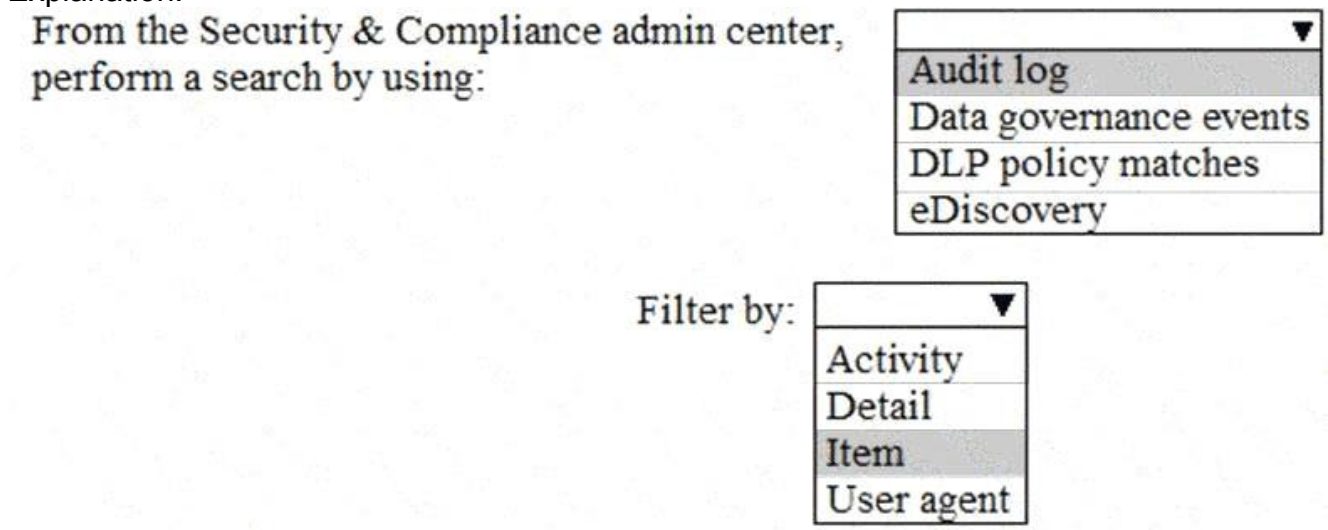
QUESTION NO: 17
SharePoint 관리자의 기술 요구 사항을 충족해야 합니다. 어떻게 해야 합니까? 답하려면 답에서 적절한 옵션을 선택하십시오. 참고: 각 정답은 1점입니다.



Answer:



Explanation:

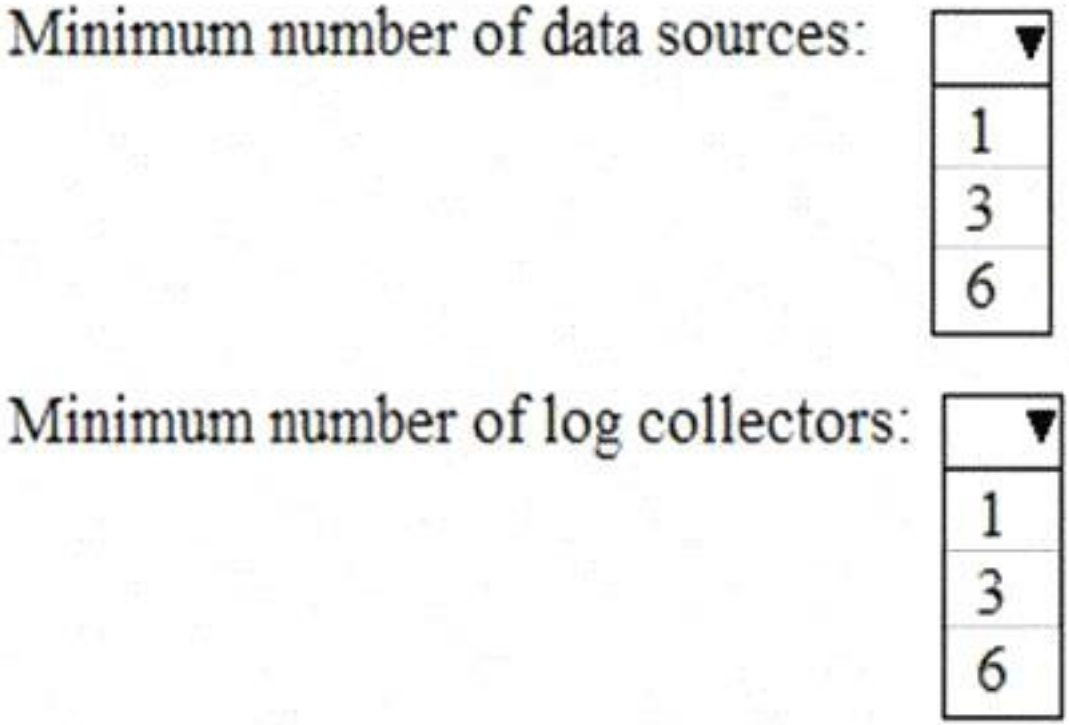


References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and- compliance#step-3-filter-the-search-results

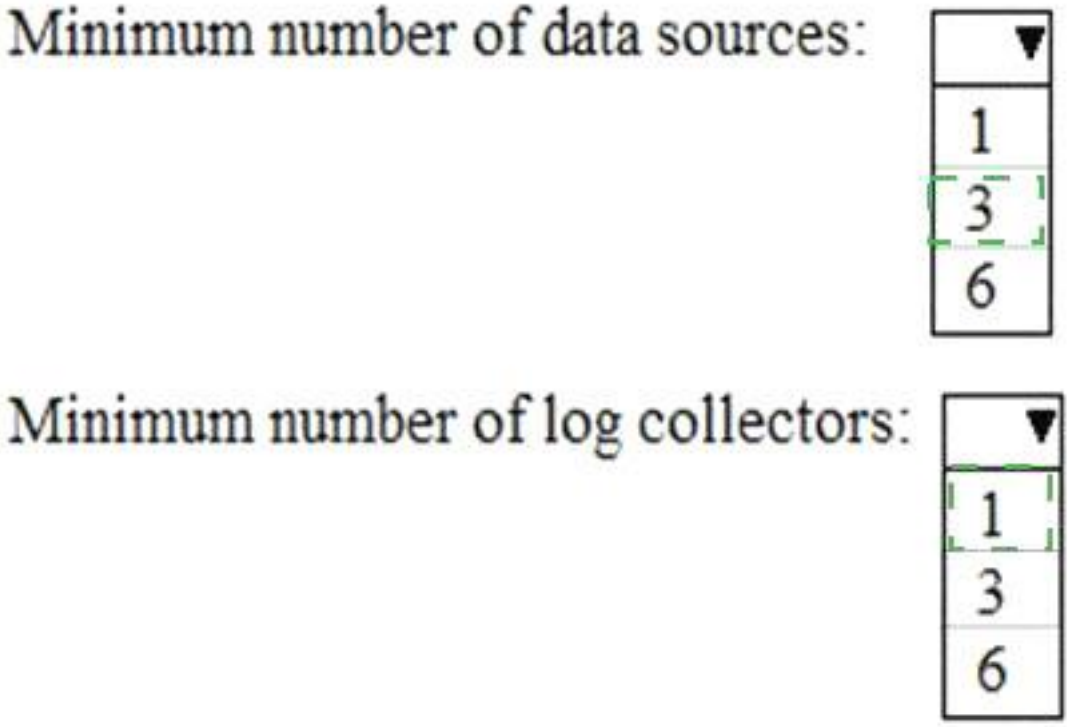
QUESTION NO: 18

뉴욕 사무소 감사원은 어떤 보고서를 살펴봐야 합니까?
A. DLP 정책이 일치합니다.
B. DLP 오탐지 및 재정의
C. DLP 사건
D. 상위 발신자 및 수신자
Answer: C
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies
This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

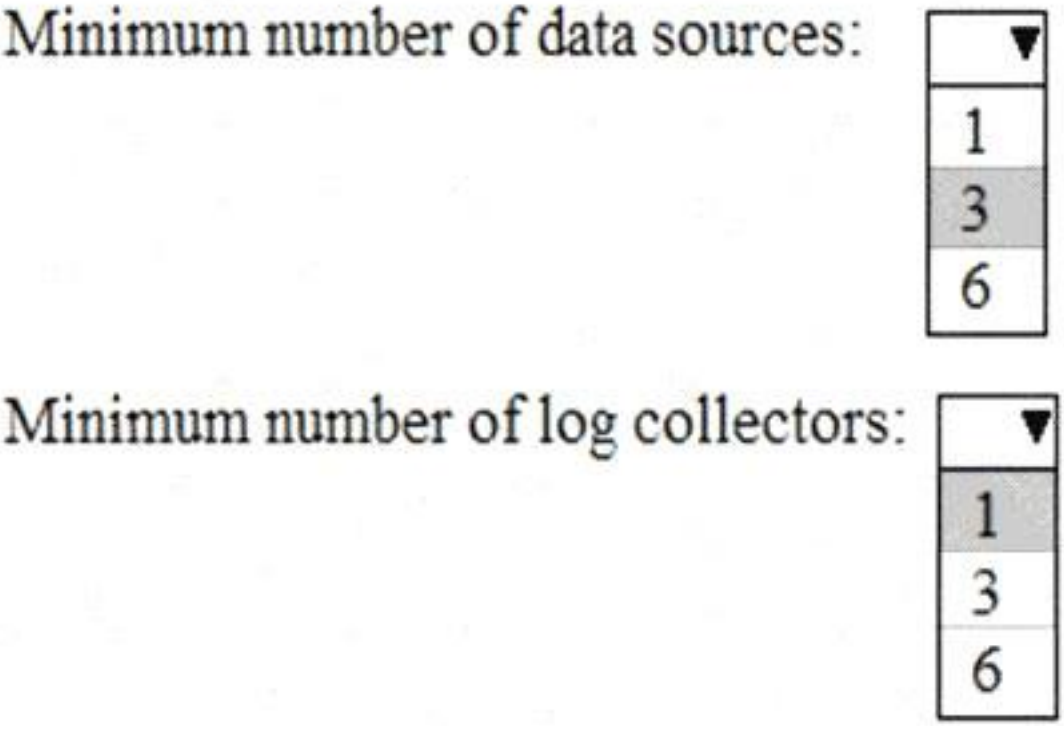
QUESTION NO: 19
로그 분석을 위해서는 기술적 요구 사항을 충족해야 합니다.
Microsoft Cloud App Security에서 만들어야 하는 최소 데이터 소스 및 로그 수집기 수는 얼마입니까? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.



Answer:



Explanation:



References:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

QUESTION NO: 20
대량 문서 검색을 위한 기술적 요구 사항을 충족해야 합니다. 무엇을 만들어야 합니까?
A. 보안 및 규정 준수 관리 센터의 데이터 유출 방지(DLP) 정책
B. 보안 및 규정 준수 관리 센터의 경고 정책
C. Microsoft Cloud App Security의 파일 정책

D. Microsoft Cloud App Security의 활동 정책

Answer: D

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

Topic 3, Litware Inc.Case Study

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

General Overviews

Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment

Existing Environment

The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in

the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.

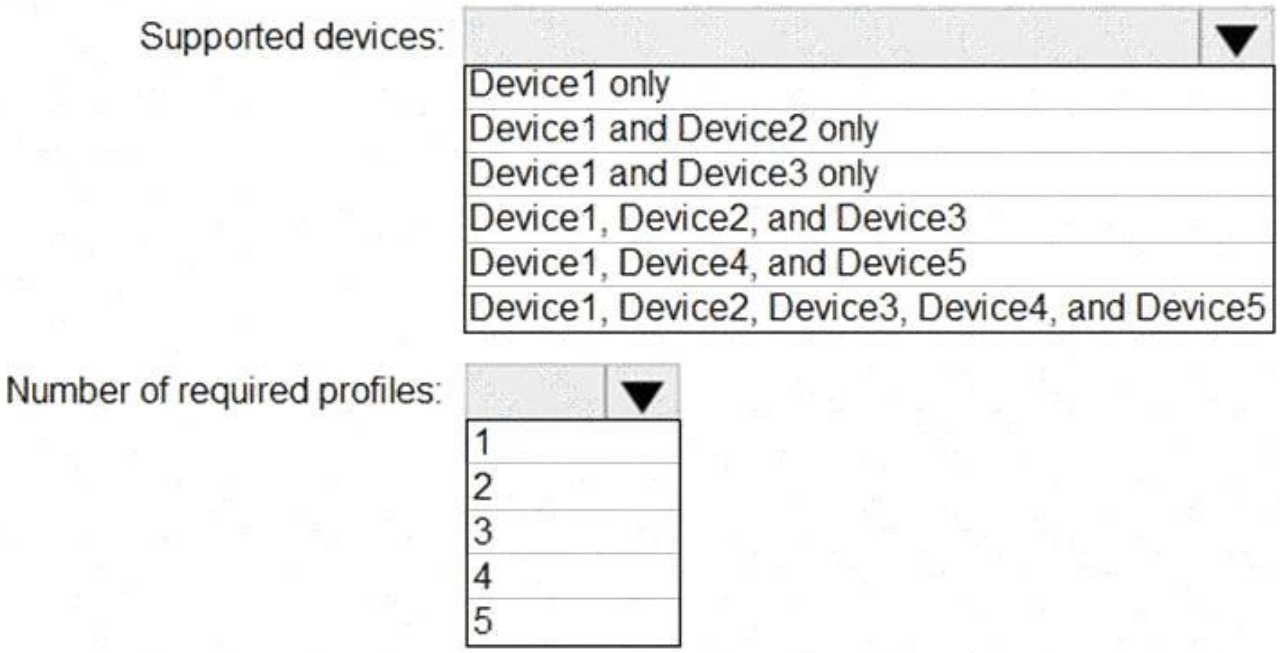
Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.
The verified domain is linked to an Microsoft Entra ID (Microsoft Entra ID) tenant named litware.com. Audit log search is turned on for the litware.com tenant.
Problem Statements
Litware identifies the following issues:
Users open email attachments that contain malicious content.
Devices without an assigned compliance policy show a status of Compliant.
User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.
Requirements
Planned Changes
Litware plans to implement the following changes:
Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
Implement data loss prevention (DLP) policies to protect confidential information.
Grant User2 permissions to review the audit logs of he litware.com tenant.
Deploy new devices to the Seattle office as shown in the following table.

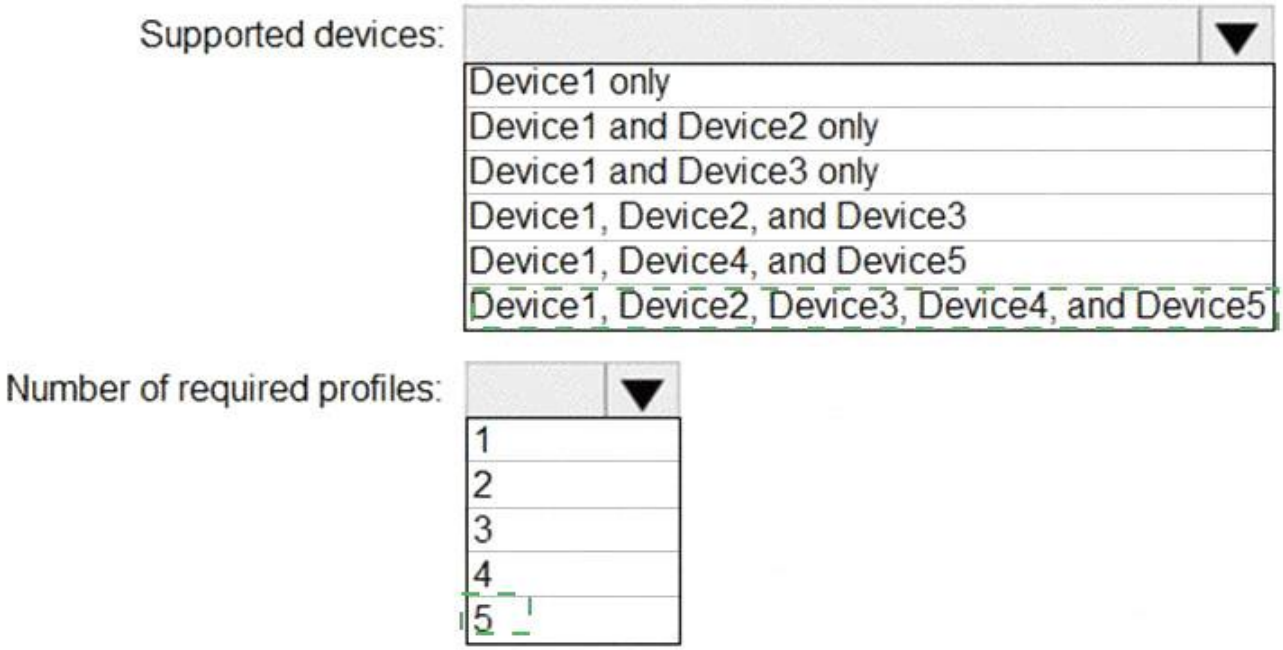
Name	Platform
Device6	Windows 10
Device7	Windows 10
Device8	iOS
Device9	Android
Device10	Android

Implement a notification system for when DLP policies are triggered.
Configure a Safe Attachments policy for the litware.com tenant.
Technical Requirements
Litware identifies the following technical requirements:
Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Microsoft Entra ID.
Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
User2 must be granted the permissions to review audit logs for the following activities:
- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Microsoft Entra ID
Users must be able to apply sensitivity labels to documents by using Office for the web.
Windows Autopilot must be used for device provisioning, whenever possible.
A DLP policy must be created to meet the following requirements:
- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
The principle of least privilege must be used.

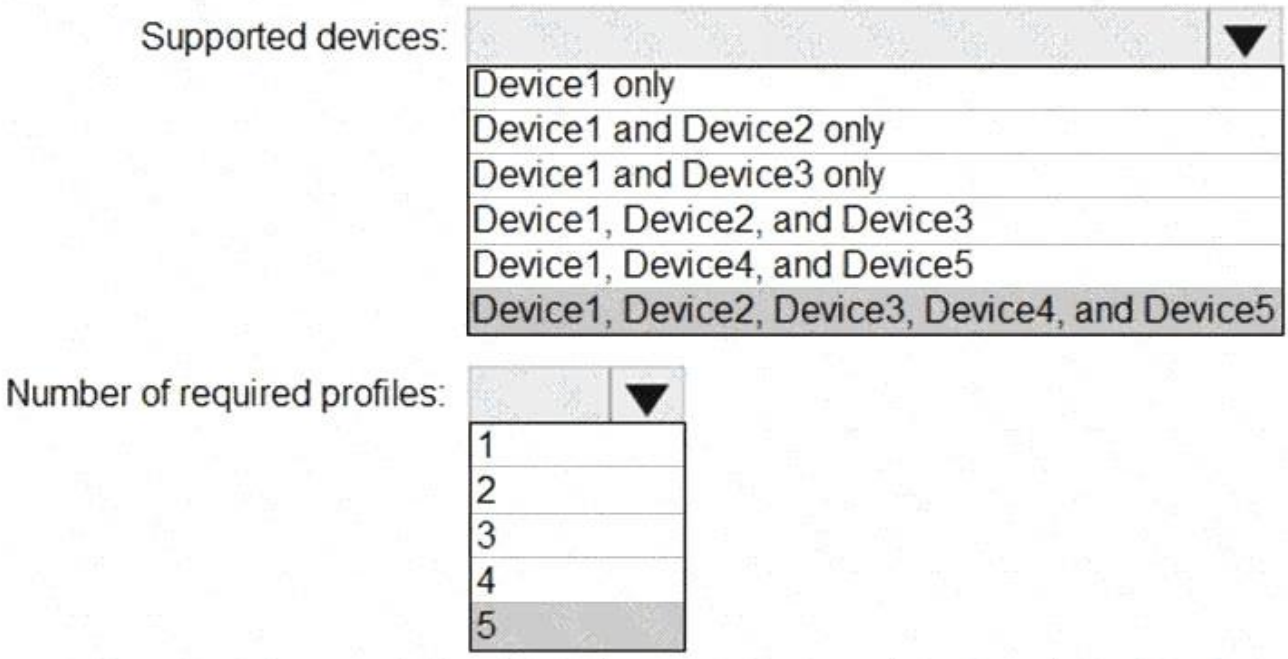
QUESTION NO: 21
계획된 변경 사항을 지원하기 위해 엔드포인트 보호 장치 구성 프로필을 구현할 계획입니다.
어떤 장치가 지원될지, 그리고 얼마나 많은 프로필을 구현해야 할지를 식별해야 합니다.
무엇을 식별해야 합니까? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.



Answer:



Explanation:



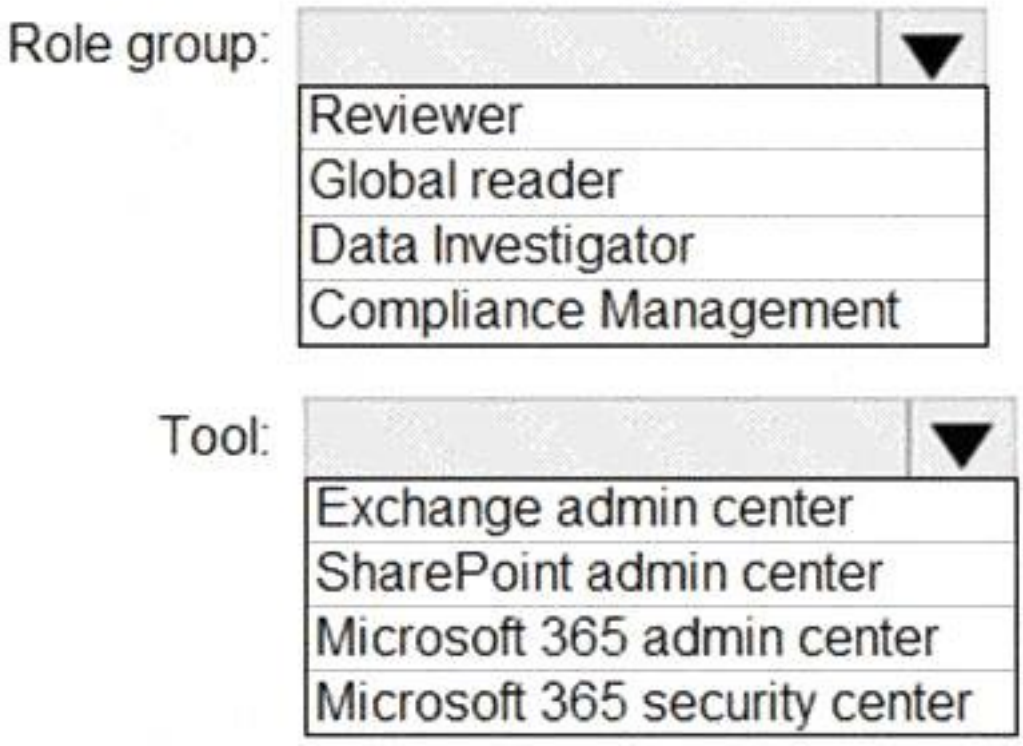
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

QUESTION NO: 22
기술적 요구 사항을 충족하려면 DLP 정책을 만들어야 합니다.
먼저 무엇을 구성해야 하나요?
A. 민감한 정보 유형
B. Insider 위험 관리 설정
C. 이벤트 유형
D. 민감도 레이블
Answer: A
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

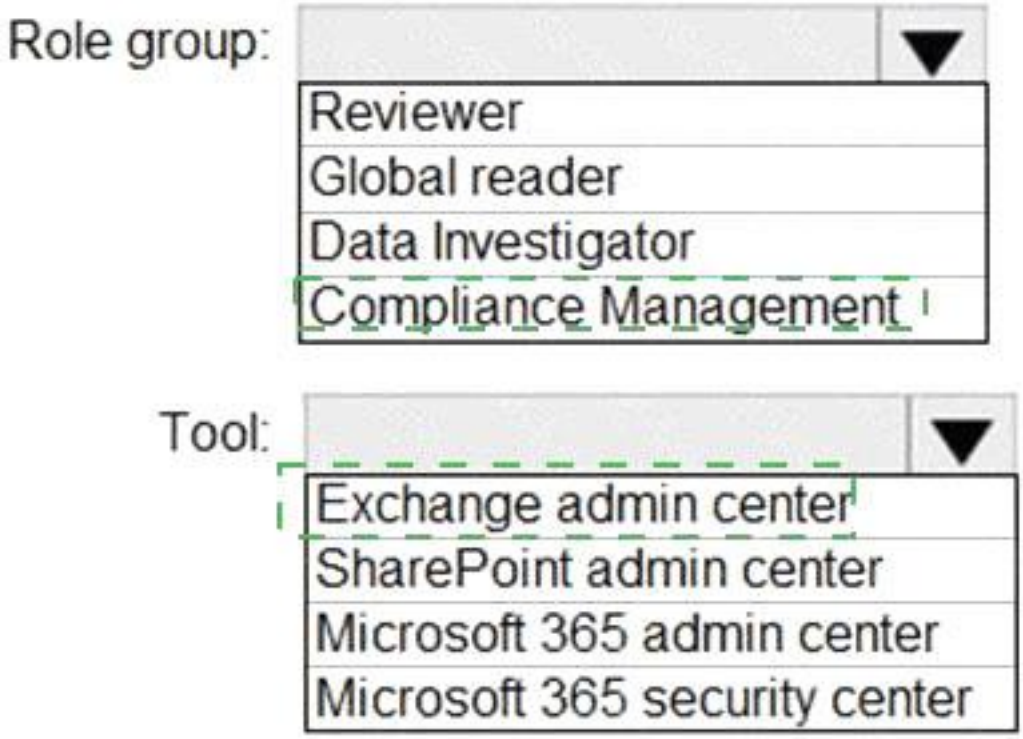
QUESTION NO: 23
계획된 DLP 정책을 만듭니다.
기술적 요구 사항을 충족하도록 알림을 구성해야 합니다.
어떻게 해야 할까요?
A. Microsoft 365 보안 센터에서 경고 정책을 구성합니다.
B. Microsoft Endpoint Manager 관리 센터에서 사용자 지정 알림을 구성합니다.
C. Microsoft 365 관리 센터에서 브리핑 이메일을 구성합니다.
D. Microsoft 365 규정 준수 센터에서 Endpoint DLP 설정을 구성합니다.
Answer: D
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365- worldwide

QUESTION NO: 24
기술적 요구 사항을 충족하려면 안전한 첨부 파일 정책을 만들어야 합니다.
어떤 옵션을 선택해야 할까요?
A. 바꾸기
B. 리디렉션 활성화
C. 블록
D. 동적 배달
Answer: D
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security
/safe-attachments.md

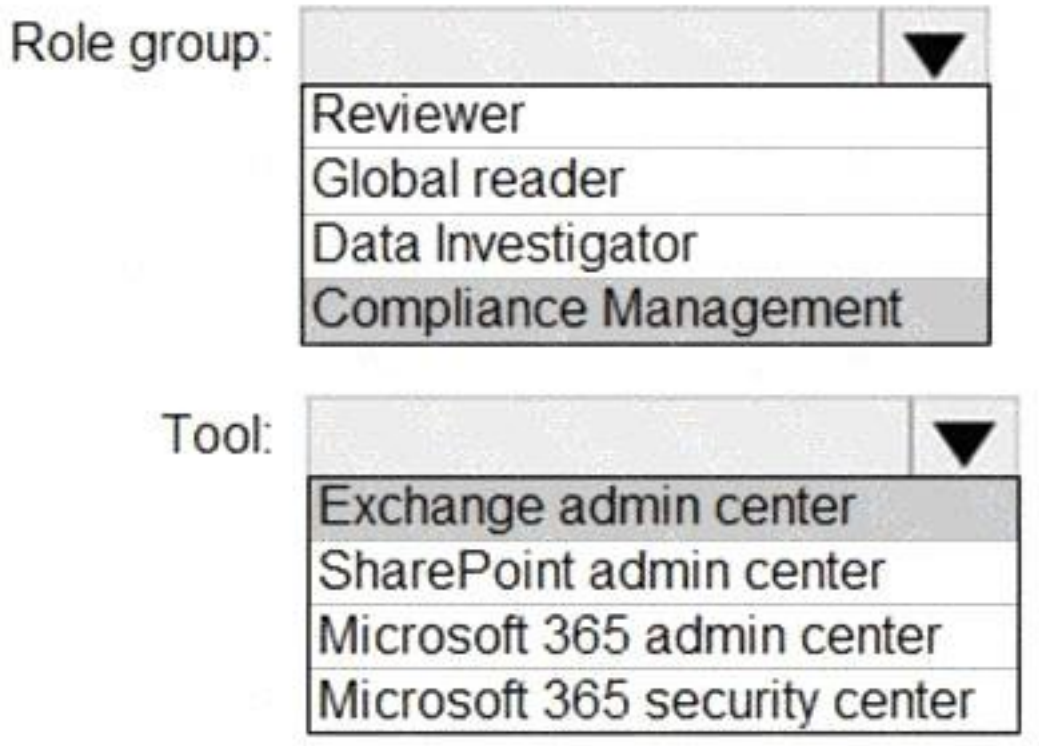
QUESTION NO: 25
User2가 감사 로그를 검토할 수 있는지 확인해야 합니다. 솔루션은 기술 요구 사항을 충족해야 합니다.
User2를 어떤 역할 그룹에 추가해야 하며, 무엇을 사용해야 합니까? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.



Answer:



Explanation:



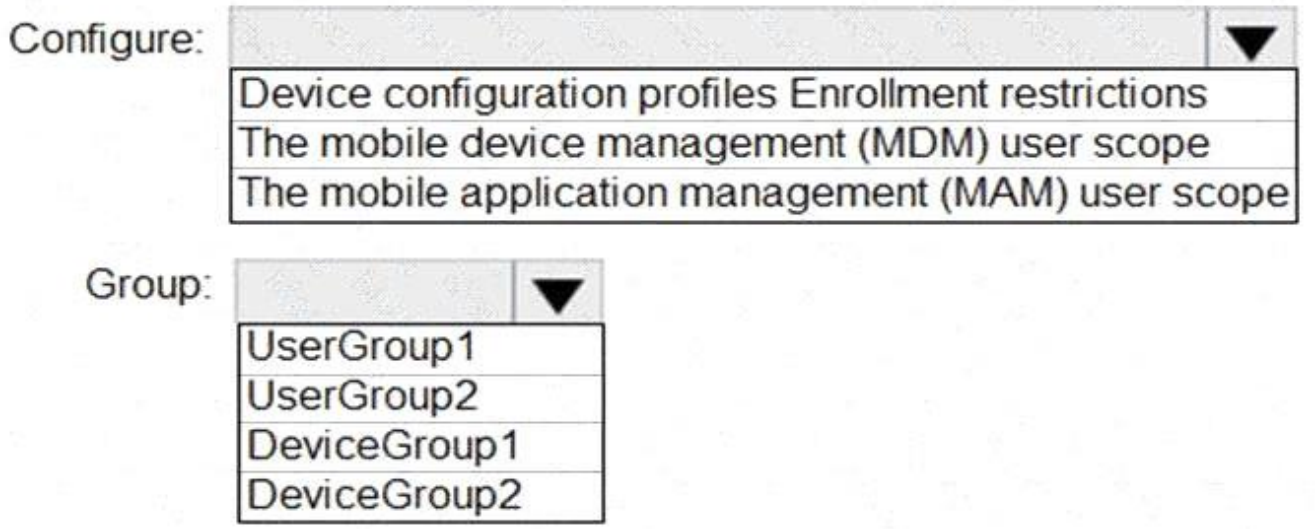
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?
view=o365-worldwide

QUESTION NO: 26

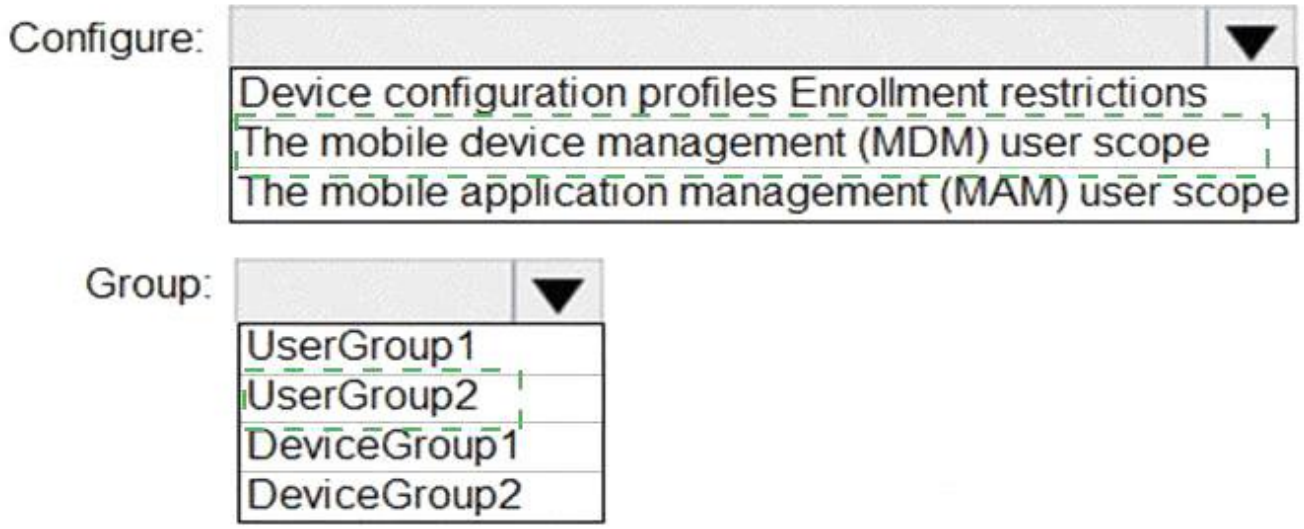
기술적 요구 사항을 충족하도록 규정 준수 설정을 구성해야 합니다.
Microsoft Endpoint Manager 관리 센터에서 무엇을 해야 하나요?
A. 규정 준수 정책에서 알림 설정을 수정합니다.
B. 위치에서 비준수 장치에 대한 새 위치를 만듭니다.
C. 비준수 장치 폐기에서 모든 장치 폐기 상태 지우기를 선택합니다.
D. 규정 준수 정책 설정을 수정합니다.
Answer: D
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION NO: 27
기술적 요구 사항을 충족하도록 웹에서 Office를 구성해야 합니다.
어떻게 해야 할까요?
A. User1에게 글로벌 독자 역할을 할당합니다.
B. SharePoint Online 및 OneDrive에서 Office 파일에 대한 민감도 레이블을 사용하도록 설정합니다.
C. 민감도 레이블을 적용하기 위한 자동 레이블 지정 정책을 구성합니다.
D. User1에게 Office 앱 관리자 역할을 할당합니다.
Answer: B
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?
view=o365-worldwide

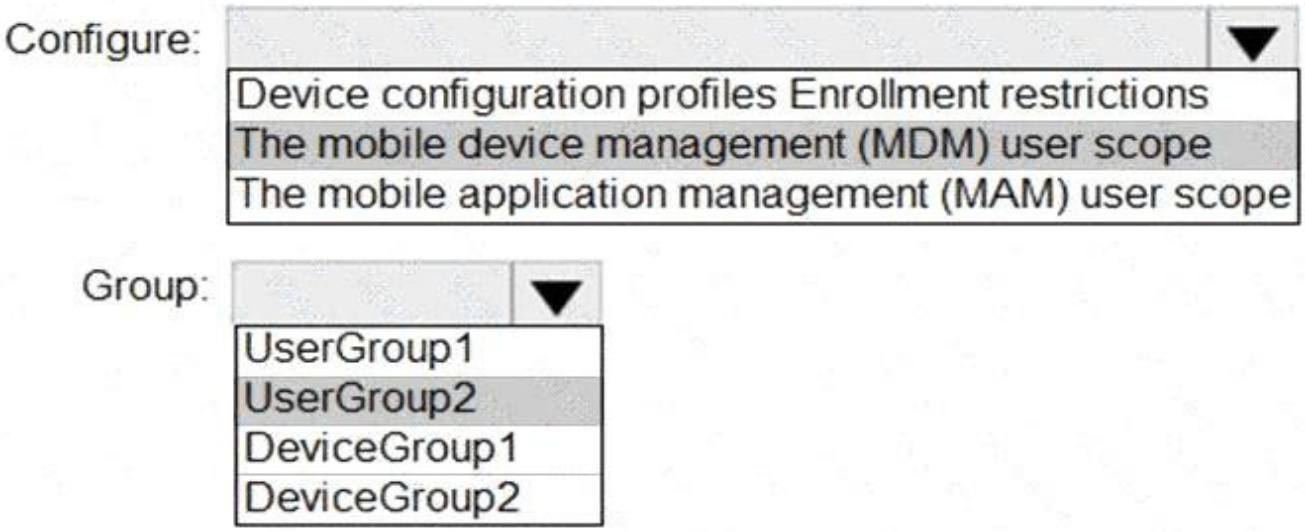
QUESTION NO: 28
Intune에서 자동 등록을 구성해야 합니다. 솔루션은 기술 요구 사항을 충족해야 합니다.
무엇을 구성해야 하며, 어떤 그룹에 구성을 할당해야 합니까? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.



Answer:



Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

QUESTION NO: 29
기술적 요구 사항을 충족하도록 정보 거버넌스 설정을 구성해야 합니다.
어떤 유형의 정책을 구성해야 하며, 몇 개의 정책을 구성해야 합니까? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

Topic 4, FabrikamOverview

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment

Active Directory Environment

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

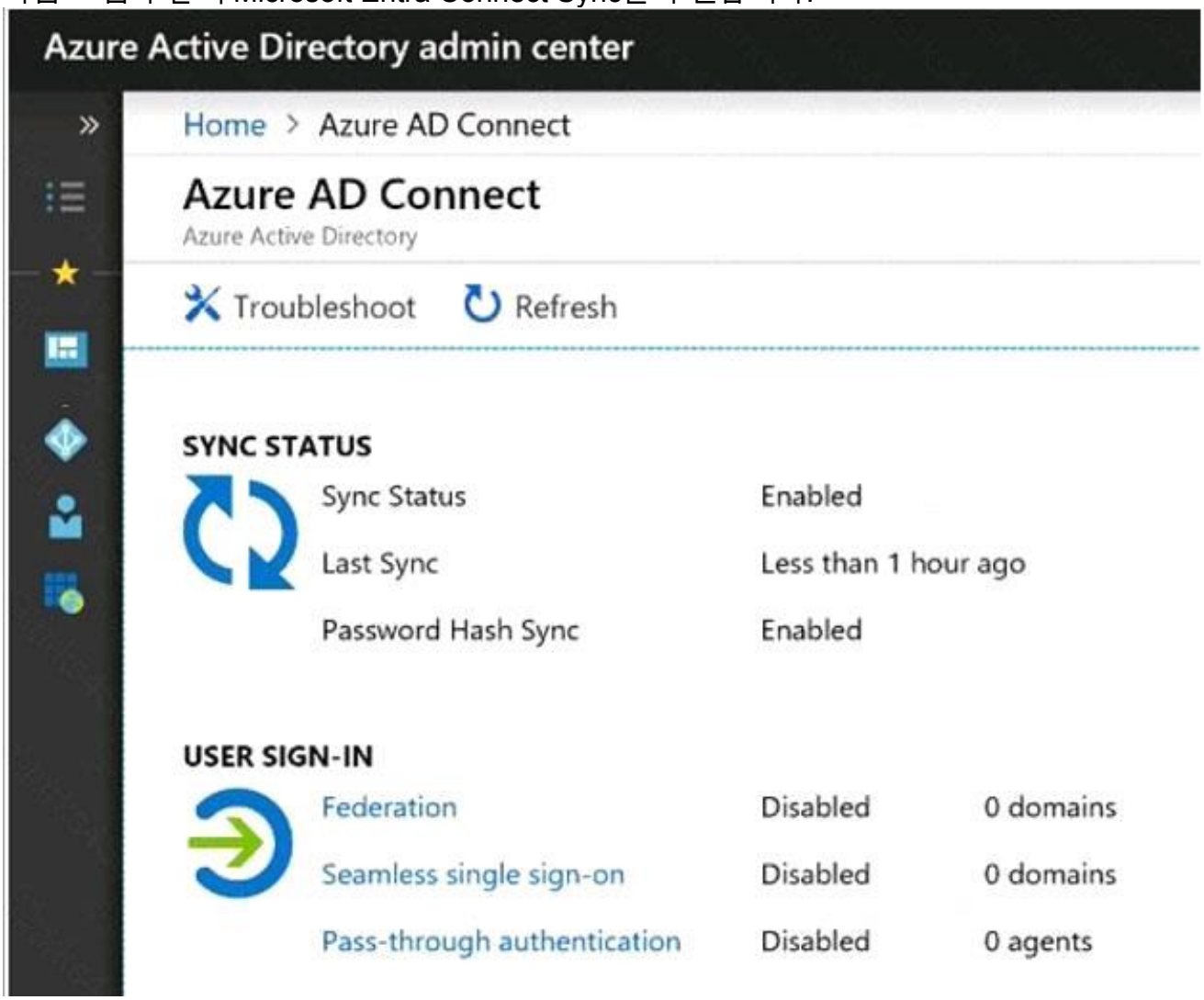
Network Infrastructure
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.
Requirements
Planned Changes
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.
Technical Requirements
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.
Application Requirements
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online.
App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.
Security Requirements
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

QUESTION NO: 30

Project1과 Project2에서 모든 영업 부서 사용자가 성공적으로 인증할 수 있는지 확인해야 합니다.
시범 프로젝트에는 어떤 인증 전략을 구현해야 합니까?
A. 패스스루 인증
B. 패스스루 인증 및 원활한 SSO
C. 비밀번호 해시 동기화 및 원활한 SSO
D. 비밀번호 해시 동기화
Answer: C
Explanation:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

QUESTION NO: 31
User1에게 어떤 역할을 할당해야 할까요?
사용 가능한 선택 사항 (올바른 모든 선택 사항을 선택하세요)
A. 위생관리
B. 보안 리더
C. 보안 관리자
D. 기록 관리
Answer: C
Explanation:
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Microsoft Entra ID, Identity Protection, Privileged Identity Management, as well as the ability to read Microsoft Entra ID sign-in reports and audit logs, and in Office
365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

QUESTION NO: 32
핫스팟
Microsoft 365 테넌트를 생성합니다.
다음 그림과 같이 Microsoft Entra Connect Sync를 구현합니다.



아래 그림에 제시된 정보를 바탕으로 각 문장을 완성하는 답을 드롭다운 메뉴에서 선택하세요.
참고: 정답 하나당 1점입니다.

Answer Area

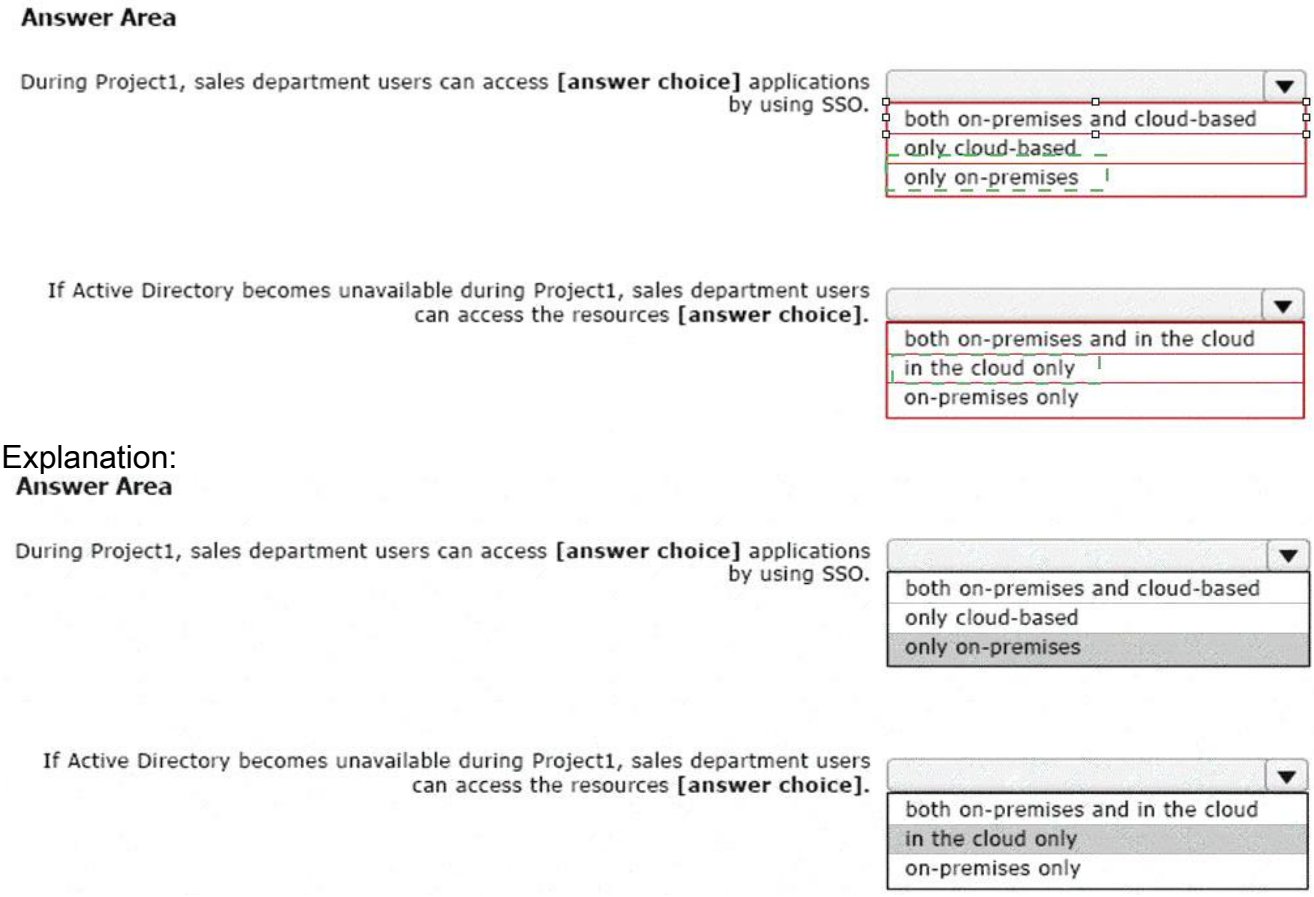
During Project1, sales department users can access **[answer choice]** applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources **[answer choice]**.

- both on-premises and in the cloud
- in the cloud only
- on-premises only

Answer:



Explanation:

Box 1: only on-premises
In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.
In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Microsoft Entra ID user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Microsoft Entra ID. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.
Box 2: in the cloud only

QUESTION NO: 33
Project1에 필요한 프로세스를 평가하고 있습니다.
프로젝트에 도메인 이름을 추가하는 동안 어떤 DNS 레코드를 생성해야 하는지 추천해야 합니다.
어떤 DNS 레코드를 추천해야 하나요?
A. 호스트(A)
B. 호스트 정보
C. 텍스트(TXT)
D. 별칭(CNAME)
Answer: C
Explanation:

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
Text (TXT)
Mail exchanger (MX)
incorrect answer options you may see on the exam include the following:
alias (CNAME)
Host (A)
host (AAA)
Pointer (PTR)
Name Server (NS)
host information (HINFO)
pointer (PTR)
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns- hosting-provider
Topic 5, Litware, IrkLitware, Irk. is a consulting company that has a
main office in Montreal and a branch office in Seattle?
Ltware collaborates with a third-party company named A. Datum Corporation.
The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.
Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Microsoft Entra ID Premium P2 licenses.
The subscription contains a verified DNS domain named litware.com.
Microsoft Entra Connect Sync is installed and has the following configurations:
* Password hash synchronization is enabled.
* Synchronization is enabled for the UtwareAdmins OU only.
Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Microsoft Entra tenant has Security defaults enabled.
Litware identifies the following issues:
* Admin1 cannot create conditional access policies.
* Admin4 receives an error when attempting to use SSPR.
* Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.
Litware plans to implement the following changes:
* Implement Microsoft Intune.
* Implement Microsoft Teams.
* Implement Microsoft Defender for Office 365.
* Ensure that users can install Office 365 apps on their device.
* Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
* Configure Microsoft Entra Connect Sync to sync the Montreal Users OU and the Seattle Users OU.
Litware identifies the following technical requirements:
* Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
* Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
* Litware users must be able to invite A. Datum users to participate in the following activities:
o Join Microsoft Teams channels,
o Join Microsoft Teams chats,
o Access shared files.
* Just in time access to critical administrative roles must be required.
* Microsoft 365 incidents and advisories must be reviewed monthly.
* Office 365 service status notifications must be sent to Admin2.
* The principle of least privilege must be used.

QUESTION NO: 34
몬트리올 사용자 및 시애틀 사용자 OU에 대한 계획된 변경 사항을 지원하도록 Microsoft Entra Connect Sync를 구성해야 합니다.
어떻게 해야 할까요?
A. Microsoft Entra Connect 동기화 마법사에서 동기화 옵션 사용자 지정을 선택합니다.
B. PowerShell에서 Add-ADSyncConnectorAttnbuteinclusion cmdlet을 실행합니다.

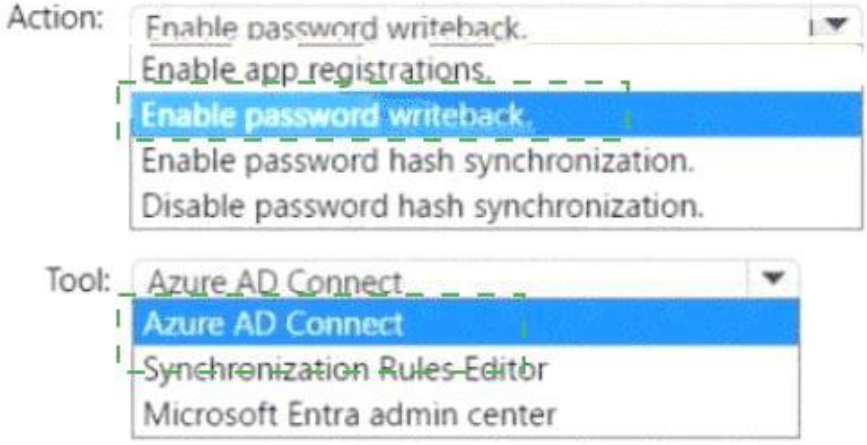
C. PowerShell에서 start-ADSyncSyncCycle cmdlet을 실행합니다.
D. Microsoft Entra Connect 동기화 마법사에서 페더레이션 관리를 선택합니다.
Answer: A

QUESTION NO: 35
Admin4가 SSPR을 사용할 수 있는지 확인해야 합니다.
어떤 도구를 사용해야 할까요? 그리고 어떤 작업을 수행해야 할까요? 대답하려면 답변 영역에서 적절한 옵션을 선택하세요.
참고사항: 정답 하나당 1점입니다.

Answer Area

Answer:

Answer Area



Explanation:

Answer Area