

MS-500

Number: MS-500
Passing Score: 800
Time Limit: 120 min
File Version: 1

MS-500.



Website: <https://vceplus.com>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

Implement and manage identity and access

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

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
All v

Search
Search by member's name

| 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?



<https://vceplus.com/>

- 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**

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 3

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

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 4

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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.

QUESTION 1

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

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

You need to create Group3.

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



Implement and manage identity and access

Testlet 3

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

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 offices shown in the following table.

| Location | Employees | Laptops | Desktop computers | 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 has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Montreal | 10.10.0.0/16 | 190.15.1.0/24 |
| Seattle | 172.16.0.0/16 | 194.25.2.0/24 |
| New York | 192.168.0.0/16 | 198.35.3.0/24 |

Named locations are defined in Azure AD as shown in the following table.

| Name | IP address range | Trusted |
|----------|------------------|---------|
| Montreal | 10.10.0.0/16 | Yes |
| New York | 192.168.0.0/16 | No |

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

| Name | User type | City | Role |
|-------|-----------|----------|----------------------------------|
| User1 | Member | Seattle | None |
| User2 | Member | Sea | Password administrator |
| User3 | Member | SEATTLE | None |
| User4 | Guest | SEA | None |
| User5 | Member | London | None |
| User6 | Member | London | Customer LockBox Access Approver |
| User7 | Member | Sydney | Reports reader |
| User8 | Member | Sydney | User administrator |
| User9 | Member | Montreal | None |

The tenant contains the groups shown in the following table.

| Name | Group type | Dynamic membership rule |
|----------|------------|---------------------------|
| ADGroup1 | Security | user.city -contains "SEA" |
| ADGroup2 | Office 365 | user.city -match "Sea**" |

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

| Name | Platform | Encryption | Member of |
|---------|------------|-----------------------|----------------|
| Device1 | Android | Disabled | GroupA, GroupC |
| Device2 | Windows 10 | Enabled | GroupB, GroupC |
| Device3 | Android | Disabled | GroupB, GroupC |
| Device4 | Windows 10 | Disabled | GroupB |
| Device5 | iOS | <i>Not applicable</i> | GroupA |
| Device6 | Windows 10 | Enabled | <i>None</i> |

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

| Name | Platform | Encryption | Assigned |
|---------------|------------|----------------|----------|
| DevicePolicy1 | Android | Not configured | Yes |
| DevicePolicy2 | Windows 10 | Required | Yes |
| DevicePolicy3 | Android | Required | Yes |

The device compliance policies have the assignments shown in the following table.

| Name | Include | Exclude |
|---------------|---------|-------------|
| DevicePolicy1 | GroupC | <i>None</i> |
| DevicePolicy2 | GroupB | GroupC |
| DevicePolicy3 | GroupA | <i>None</i> |

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management

QUESTION 1

Which user passwords will User2 be prevented from resetting?

- A. User6 and User7
- B. User4 and User6
- C. User4 only
- D. User7 and User8
- E. User8 only

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 2

You need to meet the technical requirements for User9. What should you do?

- A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
- B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
- C. Assign the Security administrator role to User9
- D. Assign the Global administrator role to User9

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Which role should you assign to User1?

- A. Global administrator
- B. User administrator
- C. Privileged role administrator
- D. Security administrator

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



Implement and manage identity and access

Question Set 4

QUESTION 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled ▪
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled



You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Azure AD app and attribute filtering settings.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps>

QUESTION 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
 - Password Hash Synchronization: Disabled
 - Password writeback: Disabled
 - Directory extension attribute sync: Disabled
 - Azure AD app and attribute filtering: Disabled
 - Exchange hybrid deployment: Disabled ▪
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 4

You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.

You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network.

What should you do first?

- A. From the Azure Active Directory admin center, create a new certificate
- B. Enable Application Proxy in Azure AD
- C. From Active Directory Administrative Center, create a Dynamic Access Control policy
- D. From the Azure Active Directory admin center, configure authentication methods

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10>

QUESTION 5

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user.

You plan to assign the Reports reader role to the user.

You need to view the permissions of the Reports reader role.

Which admin center should you use?

- A. Azure Active Directory
- B. Cloud App Security
- C. Security & Compliance
- D. Microsoft 365



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

You have a Microsoft 365 E5 subscription.

You need to ensure that users who are assigned the Exchange administrator role have time-limited permissions and must use multi-factor authentication (MFA) to request the permissions.

What should you use to achieve the goal?

- A. Security & Compliance permissions

- B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- C. Microsoft Azure AD group management
- D. Microsoft Office 365 user management

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Your company has a Microsoft 365 subscription.

The company does not permit users to enroll personal devices in mobile device management (MDM).

Users in the sales department have personal iOS devices.

You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.

The users must be prevented from backing up the app's data to iCloud.

What should you create?

- A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
- B. an app protection policy in Microsoft Endpoint Manager
- C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
- D. a device compliance policy in Microsoft Endpoint Manager

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Your company has a main office and a Microsoft 365 subscription.

You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.

What should you include in the configuration?

- A. a user risk policy
- B. a sign-in risk policy
- C. a named location in Azure Active Directory (Azure AD)
- D. an Azure MFA Server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

QUESTION 9

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the Security event log on Server1.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

QUESTION 10

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the Directory Service event log on Server1.

Does that meet the goal?

A. Yes

B. No



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

QUESTION 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the System event log on Server1.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

QUESTION 12

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the Application event log on Server1.

Does that meet the goal?

A. Yes

B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

QUESTION 13

You have a Microsoft 365 E5 subscription.

Some users are required to use an authenticator app to access Microsoft SharePoint Online.

You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.

What should you do?

- A. From the Security & Compliance admin center, download a report.
- B. From Azure Log Analytics, query the logs.
- C. From the Security & Compliance admin center, perform an audit log search.
- D. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

QUESTION 14

You have a Microsoft 365 E5 subscription.

Some users are required to use an authenticator app to access Microsoft SharePoint Online.

You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.

What should you do?

- A. From the Azure Active Directory admin center, view the sign-ins.
- B. From the Security & Compliance admin center, download a report.
- C. From the Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.
- D. From the Azure Active Directory admin center, view the audit logs.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

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



Implement and manage threat protection

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



Implement and manage threat protection

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.

QUESTION 1

You need to enable and configure Microsoft Defender ATP to meet the security requirements. What should you do?

- A. Configure port mirroring
- B. Create the `ForceDefenderPassiveMode` registry setting
- C. Download and install the Microsoft Monitoring Agent
- D. Run `WindowsDefenderATPOnboardingScript.cmd`

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>

Implement and manage threat protection

Testlet 3

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

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 offices shown in the following table.

| Location | Employees | Laptops | Desktop computers | 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 has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Montreal | 10.10.0.0/16 | 190.15.1.0/24 |
| Seattle | 172.16.0.0/16 | 194.25.2.0/24 |
| New York | 192.168.0.0/16 | 198.35.3.0/24 |

Named locations are defined in Azure AD as shown in the following table.

| Name | IP address range | Trusted |
|----------|------------------|---------|
| Montreal | 10.10.0.0/16 | Yes |
| New York | 192.168.0.0/16 | No |

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

| Name | User type | City | Role |
|-------|-----------|----------|----------------------------------|
| User1 | Member | Seattle | None |
| User2 | Member | Sea | Password administrator |
| User3 | Member | SEATTLE | None |
| User4 | Guest | SEA | None |
| User5 | Member | London | None |
| User6 | Member | London | Customer LockBox Access Approver |
| User7 | Member | Sydney | Reports reader |
| User8 | Member | Sydney | User administrator |
| User9 | Member | Montreal | None |

The tenant contains the groups shown in the following table.

| Name | Group type | Dynamic membership rule |
|----------|------------|---------------------------|
| ADGroup1 | Security | user.city -contains "SEA" |
| ADGroup2 | Office 365 | user.city -match "Sea**" |

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

| Name | Platform | Encryption | Member of |
|---------|------------|-----------------------|----------------|
| Device1 | Android | Disabled | GroupA, GroupC |
| Device2 | Windows 10 | Enabled | GroupB, GroupC |
| Device3 | Android | Disabled | GroupB, GroupC |
| Device4 | Windows 10 | Disabled | GroupB |
| Device5 | iOS | <i>Not applicable</i> | GroupA |
| Device6 | Windows 10 | Enabled | <i>None</i> |

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

| Name | Platform | Encryption | Assigned |
|---------------|------------|----------------|----------|
| DevicePolicy1 | Android | Not configured | Yes |
| DevicePolicy2 | Windows 10 | Required | Yes |
| DevicePolicy3 | Android | Required | Yes |

The device compliance policies have the assignments shown in the following table.

| Name | Include | Exclude |
|---------------|---------|-------------|
| DevicePolicy1 | GroupC | <i>None</i> |
| DevicePolicy2 | GroupB | GroupC |
| DevicePolicy3 | GroupA | <i>None</i> |

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management



Implement and manage threat protection

Question Set 4

QUESTION 1

Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1.

How long after the Azure ATP cloud service is updated will Sensor1 be updated?

- A. 7 days
- B. 24 hours
- C. 1 hour
- D. 48 hours
- E. 12 hours

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

QUESTION 2

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create?

- A. ATP anti-phishing
- B. DKIM
- C. Anti-spam
- D. Anti-malware



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files#BKMK_ModQuarantineTime

QUESTION 3

Your company has 500 computers.

You plan to protect the computers by using Microsoft Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.

You need to recommend a remediation solution that meets the following requirements:

- Microsoft Defender ATP administrators must manually approve all remediation for the executives ▪
- Remediation must occur automatically for all other users

What should you recommend doing from Microsoft Defender Security Center?

- A. Configure 20 system exclusions on automation allowed/block lists
- B. Configure two alert notification rules
- C. Download an offboarding package for the computers of the 20 executives
- D. Create two machine groups

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groups-windows-defender-advanced-threat-protection>

QUESTION 4

You have a Microsoft 365 Enterprise E5 subscription.

You use Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You need to integrate Microsoft Office 365 Threat Intelligence and Microsoft Defender ATP.

Where should you configure the integration?

- A. From the Microsoft 365 admin center, select **Settings**, and then select **Services & add-ins**.
- B. From the Security & Compliance admin center, select **Threat management**, and then select **Explorer**.
- C. From the Microsoft 365 admin center, select **Reports**, and then select **Security & Compliance**.
- D. From the Security & Compliance admin center, select **Threat management** and then select **Threat tracker**.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-office-365-ti-with-wdatp>

QUESTION 5

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.

The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.

What should you do?

- A. Configure auditing in the Office 365 Security & Compliance center.
- B. Turn off Delayed updates for the Azure ATP sensors.
- C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
- D. Integrate SIEM and Azure ATP.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>

QUESTION 6

You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com.

You create a safe links policy, as shown in the following exhibit.

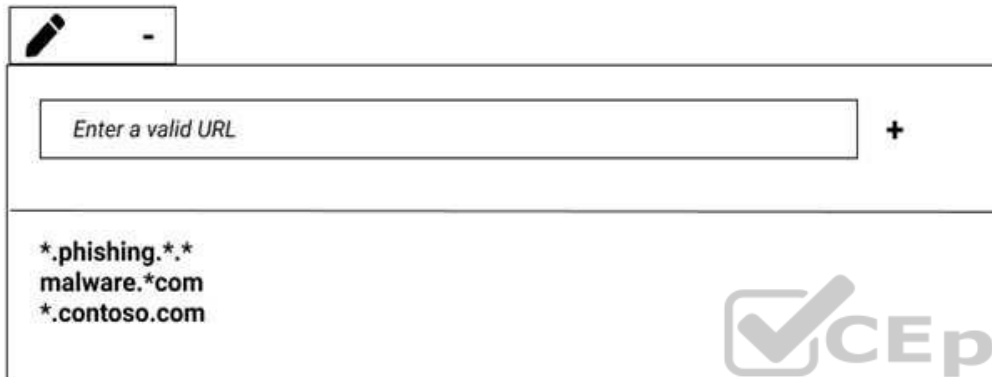


Safe links policy for your organization

Settings that apply to content across Office 365

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.

Block the following URLs:



Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- ☒ Office 365 ProPlus, Office for iOS and Android
- ☒ Office Online of above applications

For the locations selected above:

- ☒ Do not track when users click safe links:
- ☒ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

- A. fabrikam.phishing.fabrikam.com
- B. malware.fabrikam.com
- C. fabrikam.contoso.com
- D. www.malware.fabrikam.com

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list-with-atp>

QUESTION 7

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.

The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Advanced Threat Protection (ATP) by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.

What should you do?

- A. Configure Event Forwarding on the domain controllers
- B. Configure auditing in the Office 365 Security & Compliance center.
- C. Turn on Delayed updates for the Azure ATP sensors.
- D. Enable the Audit account management Group Policy setting for the servers.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding>

QUESTION 8

Several users in your Microsoft 365 subscription report that they received an email message without the attachment.

You need to review the attachments that were removed from the messages.

Which two tools can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. the Exchange admin center
- B. the Azure ATP admin center
- C. Outlook on the web
- D. the Security & Compliance admin center
- E. Microsoft Azure Security Center

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files>

QUESTION 9

You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Intune.

You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.

Which type of device configuration profile should you use?

- A. Endpoint protection
- B. Device restrictions
- C. Identity protection
- D. Windows Defender ATP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

QUESTION 10

You have a hybrid Microsoft Exchange Server organization. All users have Microsoft 365 E5 licenses.

You plan to implement an Advanced Threat Protection (ATP) anti-phishing policy.

You need to enable mailbox intelligence for all users.

What should you do first?

- A. Configure attribute filtering in Microsoft Azure Active Directory Connect (Azure AD Connect)
- B. Purchase the ATP add-on
- C. Select **Directory extension attribute sync** in Microsoft Azure Active Directory Connect (Azure AD Connect)
- D. Migrate the on-premises mailboxes to Exchange Online

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies>

QUESTION 11

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view ATP reports in the Threat management dashboard.

Which role provides User1 with the required role permissions?

- A. Security reader
- B. Message center reader
- C. Compliance administrator
- D. Information Protection administrator
- E. Service administrator
- F. Exchange administrator

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are-needed-to-view-the-atp-reports>

QUESTION 12

You have a Microsoft 365 Enterprise E5 subscription.

You use Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). You plan to use Microsoft Office 365 Attack simulator.

What is a prerequisite for running Attack simulator?

- A. Enable multi-factor authentication (MFA)
- B. Configure Office 365 Advanced Threat Protection (ATP)
- C. Create a Conditional Access App Control policy for accessing Office 365
- D. Integrate Office 365 Threat Intelligence and Microsoft Defender ATP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

QUESTION 13

You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.

Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.

You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.

The email addresses that you intend to spoof belong to the Executive group members.

What should you do first?

- A. From the Azure ATP admin center, configure the primary workspace settings
- B. From the Microsoft Azure portal, configure the user risk policy settings in Azure AD Identity Protection
- C. Enable MFA for the Research group members



D. Migrate the Executive group members to Exchange Online

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

QUESTION 14

You have a Microsoft 365 E5 subscription.

You implement Advanced Threat Protection (ATP) safe attachments policies for all users.

User reports that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.

What should you do from ATP?

- A. Set the action to **Block**
- B. Add an exception
- C. Add a condition
- D. Set the action to **Dynamic Delivery**

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing>

QUESTION 15

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

| Name | Configuration |
|---------|-------------------|
| DC1 | Domain controller |
| Server1 | Member server |

You plan to implement Azure Advanced Threat Protection (ATP) for the domain.

You install an Azure ATP standalone sensor on Server1.

You need to monitor the domain by using Azure ATP.

What should you do?

- A. Configure port mirroring for Server1.
- B. Install the Microsoft Monitoring Agent on DC1.
- C. Install the Microsoft Monitoring Agent on Server1.
- D. Configure port mirroring for DC1.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-port-mirroring>

QUESTION 16

An administrator plans to deploy several Azure Advanced Threat Protection (ATP) sensors.

You need to provide the administrator with the Azure information required to deploy the sensors.

What information should you provide?

- A. an Azure Active Directory Authentication Library (ADAL) token
- B. the public key
- C. the access key
- D. the URL of the Azure ATP admin center

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/workspace-portal>

QUESTION 17

You have a Microsoft 365 tenant.

You have 500 computers that run Windows 10.

You plan to monitor the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP) after the computers are enrolled in Microsoft Intune.

You need to ensure that the computers connect to Windows Defender ATP.

How should you prepare Intune for Windows Defender ATP?

- A. Configure an enrollment restriction
- B. Create a device configuration profile
- C. Create a conditional access policy
- D. Create a Windows Autopilot deployment profile



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/intune/advanced-threat-protection>

QUESTION 18

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

| Name | User mailbox | Multi-factor authentication (MFA) |
|-------|---------------------------------------|-----------------------------------|
| User1 | On-premises Microsoft Exchange Server | Required |
| User2 | On-premises Microsoft Exchange Server | Disabled |
| User3 | Microsoft Exchange Online | Required |
| User4 | Microsoft Exchange Online | Disabled |

You plan to use Microsoft 365 Attack Simulator.

You need to identify the users against which you can use Attack Simulator.

Which users should you identify?

- A. User3 only
- B. User1, User2, User3, and User4
- C. User3 and User4 only
- D. User1 and User3 only



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Each targeted recipient must have an Exchange Online mailbox.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide>

QUESTION 19

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view ATP reports in the Threat management dashboard.

Which role provides User1 with the required role permissions?

- A. Security administrators B. Exchange administrator
- C. Compliance administrator
- D. Message center reader

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are-needed-to-view-the-atp-reports>



Implement and manage information protection

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

QUESTION 1

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.

- A. Create an access review
- B. Assign the Global administrator role to User1

- C. Assign the Guest inviter role to User1
- D. Modify the External collaboration settings in the Azure Active Directory admin center

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:



Implement and manage information protection

Question Set 2

QUESTION 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them.

You modify the encryption settings of the label.

Does that meet the goal?

- A. Yes
- B. No



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them.

You modify the content expiration settings of the label.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

You have a Microsoft 365 subscription for a company named Contoso, Ltd. All data is in Microsoft 365.

Contoso works with a partner company named Litware, Inc. Litware has a Microsoft 365 subscription. Microsoft OneDrive has the default settings.

You need to allow users at Contoso to share files from Microsoft OneDrive to specific users at Litware.

Which two actions should you perform from the OneDrive admin center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Increase the permission level for OneDrive External sharing
- B. Modify the Links settings
- C. Change the permissions for OneDrive External sharing to the least permissive level
- D. Decrease the permission level for OneDrive External sharing
- E. Modify the Device access settings
- F. Modify the Sync settings

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

QUESTION 4

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

- A. Run the `Set-SPOTenant` cmdlet and specify the `-ConditionalAccessPolicy` parameter.
- B. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
- D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps> <https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

QUESTION 5

A user stores the following files in Microsoft OneDrive:

- File.docx
- ImportantFile.docx
- File_Important.docx

You create a Microsoft Cloud App Security file policy Policy1 that has the filter shown in the following exhibit.

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING 👁 Edit and preview results

✕

File name ▼

contains words ▼

File ▼



Apply to:

all files ▼

Apply to:

all file owners ▼

To which files does Policy1 apply?

- A. File_Important.docx only
- B. File.docx, ImportantFile.docx, and File_Important.docx
- C. File.docx only
- D. ImportantFile.docx only
- E. File.docx and File_Important.docx only

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/file-filters>

QUESTION 6

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them.

You create a new label in the global policy and instruct the user to resend the email message.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 7

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

- A. Run the `Set-SPODataConnectionSetting` cmdlet and specify the `AssignmentCollection` parameter
- B. From the SharePoint admin center, configure the Access control settings
- C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
- D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy **Correct Answer:** B

Section: (none)

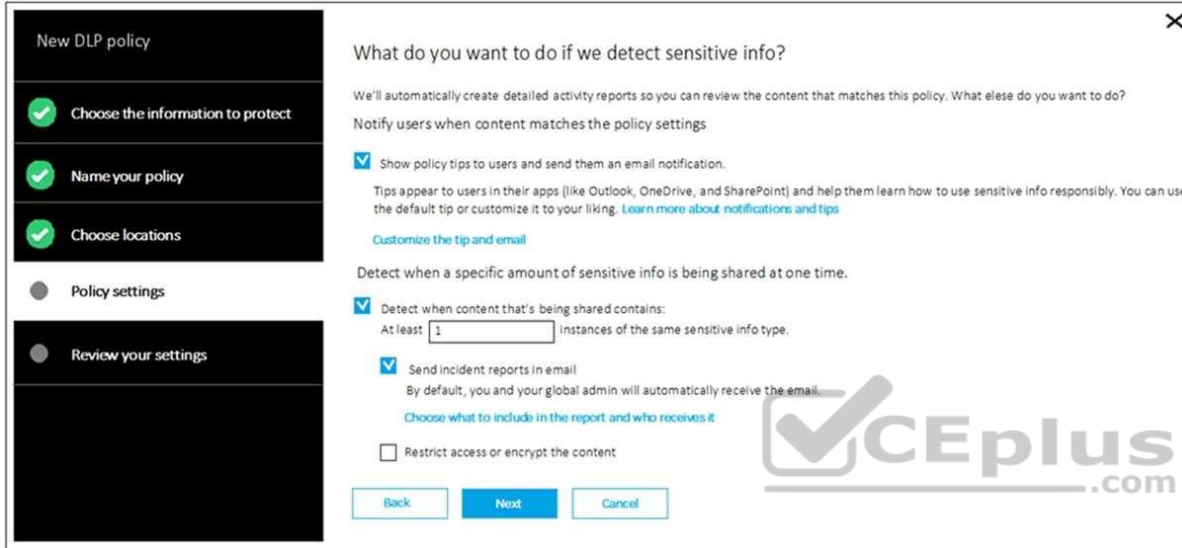
Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

QUESTION 8

You create a data loss prevention (DLP) policy as shown in the following exhibit:



What is the effect of the policy when a user attempts to send an email message that contains sensitive information?

- A. The user receives a notification and can send the email message
- B. The user receives a notification and cannot send the email message
- C. The email message is sent without a notification
- D. The email message is blocked silently

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

QUESTION 9

You have a Microsoft 365 subscription.

You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.

Which type of site collection should you create first?

- A. Records Center
- B. eDiscovery Center
- C. Enterprise Search Center
- D. Document Center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bb-b944-448d-b83d-8fec4abcc24c>

QUESTION 10

You have a Microsoft 365 subscription that includes a user named User1.

You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.

You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.

Which type of Cloud App Security policy should you create?

- A. an app permission policy
- B. an activity policy
- C. a Cloud Discovery anomaly detection policy
- D. a session policy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad>



Manage governance and compliance features in Microsoft 365

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

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 offices shown in the following table.

| Location | Employees | Laptops | Desktop computers | 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 has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

| Location | IP address space | Public NAT segment |
|----------|------------------|--------------------|
| Montreal | 10.10.0.0/16 | 190.15.1.0/24 |
| Seattle | 172.16.0.0/16 | 194.25.2.0/24 |
| New York | 192.168.0.0/16 | 198.35.3.0/24 |

Named locations are defined in Azure AD as shown in the following table.

| Name | IP address range | Trusted |
|----------|------------------|---------|
| Montreal | 10.10.0.0/16 | Yes |
| New York | 192.168.0.0/16 | No |



From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

| Name | User type | City | Role |
|-------|-----------|----------|----------------------------------|
| User1 | Member | Seattle | None |
| User2 | Member | Sea | Password administrator |
| User3 | Member | SEATTLE | None |
| User4 | Guest | SEA | None |
| User5 | Member | London | None |
| User6 | Member | London | Customer LockBox Access Approver |
| User7 | Member | Sydney | Reports reader |
| User8 | Member | Sydney | User administrator |
| User9 | Member | Montreal | None |

The tenant contains the groups shown in the following table.

| Name | Group type | Dynamic membership rule |
|----------|------------|---------------------------|
| ADGroup1 | Security | user.city -contains "SEA" |
| ADGroup2 | Office 365 | user.city -match "Sea**" |

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

| Name | Platform | Encryption | Member of |
|---------|------------|-----------------------|----------------|
| Device1 | Android | Disabled | GroupA, GroupC |
| Device2 | Windows 10 | Enabled | GroupB, GroupC |
| Device3 | Android | Disabled | GroupB, GroupC |
| Device4 | Windows 10 | Disabled | GroupB |
| Device5 | iOS | <i>Not applicable</i> | GroupA |
| Device6 | Windows 10 | Enabled | <i>None</i> |

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

| Name | Platform | Encryption | Assigned |
|---------------|------------|----------------|----------|
| DevicePolicy1 | Android | Not configured | Yes |
| DevicePolicy2 | Windows 10 | Required | Yes |
| DevicePolicy3 | Android | Required | Yes |

The device compliance policies have the assignments shown in the following table.

| Name | Include | Exclude |
|---------------|---------|-------------|
| DevicePolicy1 | GroupC | <i>None</i> |
| DevicePolicy2 | GroupB | GroupC |
| DevicePolicy3 | GroupA | <i>None</i> |

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
 - Ensure that User9 can enable and configure Azure AD Privileged Identity Management

QUESTION 1

What should User6 use to meet the technical requirements?

- A. Supervision in the Security & Compliance admin center
- B. Service requests in the Microsoft 365 admin center
- C. Security & privacy in the Microsoft 365 admin center
- D. Data subject requests in the Security & Compliance admin center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



Manage governance and compliance features in Microsoft 365

Question Set 2

QUESTION 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-AuditConfig -Workload Exchange` command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps>

QUESTION 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox*` command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-adminauditlogconfig?view=exchange-ps>

QUESTION 3

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security & Compliance admin center, you create a label that designates personal data.

You need to auto-apply the new label to all the content in Site1.

What should you do first?

- A. From PowerShell, run `Set-ManagedContentSettings`.
- B. From PowerShell, run `Set-ComplianceTag`.



C. From the Security & Compliance admin center, create a Data Subject Request (DSR).

D. Remove Azure Information Protection from the Site1 files.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in-office-365>

QUESTION 4

You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search.

What should you do from the Security & Compliance admin center?

A. From Search & investigation, create a guided search.

B. From Events, create an event.

C. From Alerts, create an alert policy.

D. From Search & investigation, create an eDiscovery case.



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

QUESTION 5

You have a Microsoft 365 E5 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

- A. From the Security & Compliance admin center, modify the Policy Tips settings of a DLP policy.
- B. From the Cloud App Security admin center, apply a filter to the alerts.
- C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
- D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

QUESTION 6

You have a Microsoft 365 subscription.

You create and run a content search from the Security & Compliance admin center.

You need to download the results of the content search.

What should you obtain first?

- A. an export key
- B. a password
- C. a certificate
- D. a pin

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results>

QUESTION 7

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E5 license.

How long will auditing data be retained?

- A. 30 days
- B. 90 days
- C. 365 days
- D. 5 years

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

QUESTION 8

You have a Microsoft 365 subscription.

You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

- A. From Exchange Online PowerShell, run `Start-RetentionAutoTagLearning`
- B. From Exchange Online PowerShell, run `Start-ManagedFolderAssistant`
- C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy
- D. From the Security & Compliance admin center, create a label policy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/labels>

QUESTION 9

You have a Microsoft 365 subscription.

You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.

What should you create first?

- A. A retention label in Microsoft Office 365
- B. A custom sensitive information type
- C. A Data Subject Request (DSR)
- D. A safe attachments policy in Microsoft Office 365

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool#more-information-about-using-the-dsrcase-tool>

QUESTION 10

You have a Microsoft 365 subscription.

A user reports that changes were made to several files in Microsoft OneDrive.

You need to identify which files were modified by which users in the user's OneDrive.

What should you do?



<https://vceplus.com/>

- A. From the Azure Active Directory admin center, open the audit log
- B. From the OneDrive admin center, select **Device access**
- C. From Security & Compliance, perform an eDiscovery search
- D. From Microsoft Cloud App Security, open the activity log

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/activity-filters>

QUESTION 11

You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the Cloud App Security admin center, create a file policy.
- B. From the SharePoint admin center, modify the Site Settings.
- C. From the Security admin center, create a label.
- D. From the SharePoint admin center, modify the records management settings.
- E. From the Security admin center, publish a label.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp>

QUESTION 12

You recently created and published several label policies in a Microsoft 365 subscription.

You need to view which labels were applied by users manually and which labels were applied automatically.

What should you do from the Security & Compliance admin center?

- A. From Search & investigation, select **Content search**
- B. From Data governance, select **Events**
- C. From Search & investigation, select **eDiscovery**
- D. From Reports, select **Dashboard**

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains the users shown in the following table.

| Name | Role |
|-------|----------------------------------|
| User1 | Compliance Manager Contributor |
| User2 | Compliance Manager Assessor |
| User3 | Compliance Manager Administrator |
| User4 | Portal Admin |

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 14

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains the users shown in the following table.

| Name | Role |
|-------|----------------------------------|
| User1 | Compliance Manager Contributor |
| User2 | Compliance Manager Assessor |
| User3 | Compliance Manager Administrator |
| User4 | Portal Admin |



You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend modifying the licenses assigned to User5.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 15

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains the users shown in the following table.

| Name | Role |
|-------|----------------------------------|
| User1 | Compliance Manager Contributor |
| User2 | Compliance Manager Assessor |
| User3 | Compliance Manager Administrator |
| User4 | Portal Admin |



You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User5.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 16

You have a Microsoft 365 subscription.

You enable auditing for the subscription.

You plan to provide a user named Auditor with the ability to review audit logs.

You add Auditor to the Global administrator role group.

Several days later, you discover that Auditor disabled auditing.

You remove Auditor from the Global administrator role group and enable auditing.

You need to modify Auditor to meet the following requirements:

- Be prevented from disabling auditing
- Use the principle of least privilege ▪
- Be able to review the audit log



To which role group should you add Auditor?

- A. Security reader
- B. Compliance administrator
- C. Security operator
- D. Security administrator

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center>

QUESTION 17

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains the users shown in the following table.

| Name | Role |
|-------|----------------------------------|
| User1 | Compliance Manager Contributor |
| User2 | Compliance Manager Assessor |
| User3 | Compliance Manager Administrator |
| User4 | Portal Admin |

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend removing User1 from the Compliance Manager Contributor role.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 18

You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1.

You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1.

What should you do first?

- A. From the Azure Active Directory admin center, assign a role group to Admin1.
- B. From the Microsoft 365 admin center, assign a role to Admin1.
- C. From the Security & Compliance admin center, assign a role group to Admin1.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

QUESTION 19

You have a Microsoft 365 subscription.

You need to enable auditing for all Microsoft Exchange Online users.

What should you do?

- A. From the Exchange admin center, create a journal rule
- B. Run the `Set-MailboxDatabase cmdlet`
- C. Run the `Set-Mailbox cmdlet`
- D. From the Exchange admin center, create a mail flow message trace rule.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

QUESTION 20

You have a Microsoft 365 subscription.

You create a supervision policy named Policy1, and you designate a user named User1 as the reviewer.

What should User1 use to view supervised communications?

- A. a team in Microsoft Teams
- B. the Security & Compliance admin center
- C. Outlook on the web
- D. the Exchange admin center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/supervision-policies?view=o365-worldwide>

QUESTION 21

You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

You need to ensure that the users can use the new label to protect their email.

What should you do?

- A. Modify the priority order of label policies
- B. Wait six hours and ask the users to try again
- C. Create a label policy
- D. Create a new sensitive information type

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

You have a Microsoft 365 subscription that includes a user named Admin1.

You need to ensure that Admin1 can retain all the mailbox content of users, including their deleted items.

The solution must use the principle of least privilege.

What should you do?

- A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.
- B. From the Exchange admin center, assign the Security Administrator role to Admin1.
- C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.
- D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 23**

You have a hybrid Microsoft 365 environment.

All computers run Windows 10 Enterprise and have Microsoft Office 365 ProPlus installed. All the computers are joined to Active Directory.

You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft.

What should you do?

- A. On Server1, run `readinessreportcreator.exe`
- B. Configure a registry entry on Server1
- C. Configure a registry entry on the computers
- D. On the computers, run `tdadm.exe`

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Your company has a Microsoft 365 subscription that includes a user named User1.

You suspect that User1 sent email messages to a competitor detailing company secrets.

You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.

What should you include in the recommendation?

- A. Enable In-Place Archiving for the mailbox of User1
- B. From the Security & Compliance, perform a content search of the mailbox of User1
- C. Place a Litigation Hold on the mailbox of User1
- D. Configure message delivery restrictions for the mailbox of User1

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 25

You have a Microsoft 365 subscription.

Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.

You need to ensure that the labels will be available for manual assignment as soon as possible.

What should you do?

- A. From the Security & Compliance admin center, create a label policy
- B. From Exchange Online PowerShell, run `Start-RetentionAutoTagLearning`
- C. From Exchange Online PowerShell, run `Start-ManagedFolderAssistant`
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

You have a Microsoft 365 subscription.

Your company uses Jamf Pro to manage macOS devices.

You plan to create device compliance policies for the macOS devices based on the Jamf Pro data.

You need to connect Microsoft Endpoint Manager to Jamf Pro.

What should you do first?

- A. From the Azure Active Directory admin center, add a Mobility (MDM and MAM) application.
- B. From the Endpoint Management admin center, add the Mobile Threat Defense connector.
- C. From the Endpoint Management admin center, configure Partner device management.
- D. From the Azure Active Directory admin center, register an application.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf>

QUESTION 27

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains 1,000 user mailboxes.

An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.

You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.

Solution: You modify the privacy profile, and then create a Data Subject Request (DSR) case.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>