

Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator



NEW QUESTION 1

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



Exchange Administrator - Members

+ Add member X Remove member ✓- Access reviews ↓ Export ↻ Refresh

Assignment type

Search

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

What should you do to meet the security requirements?

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

Answer: D

NEW 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

Answer: A

Explanation:

References:

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

NEW 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

Answer: C

Explanation:

References:

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

NEW QUESTION 4

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.

Answer: AC

NEW QUESTION 5

You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

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

Answer: B

Explanation:

References:

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

Case Study: 2 Litware, Inc 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 range 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
Group 1	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

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
- Integrate Windows Defender and Windows Defender ATP on domain-joined servers
- 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 want to minimize the deployment of additional servers and services in the Active Directory forest.

NEW QUESTION 6

DRAG DROP

You need to configure threat detection for Active Directory. The solution must meet the security requirements.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Configure the Directory services setting in Azure ATP	
Download and install the ATA Gateway on DC1, DC2, and DC3	
Download and install the Azure ATP sensor package on DC1, DC2, and DC3	
Configure a site-to-site VPN	
Create a workspace in Azure ATP	
Download and install the ATA Center on Server1	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create a workspace in Azure ATP

Download and install the Azure ATP sensor package on DC1, DC2, and DC3

Configure the Directory services setting in Azure ATP

NEW QUESTION 7

You need to implement Windows 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

Answer: C

Explanation:

Case Study: 3 Contoso, Ltd Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktops 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 Intune Configuration

The devices enrolled in Intune 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	Not applicable	GroupA
Device6	Windows 10	Enabled	None

The device compliance policies in Intune 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	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

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 implement Azure AD Privileged Identity Management

NEW QUESTION 8

Which role should you assign to User1?

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

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim>

NEW QUESTION 9

HOTSPOT

Which policies apply to which devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

DevicePolicy1:

DevicePolicy2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

DevicePolicy1:

DevicePolicy2:

NEW 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 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

Answer: B

NEW 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 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

Answer: A

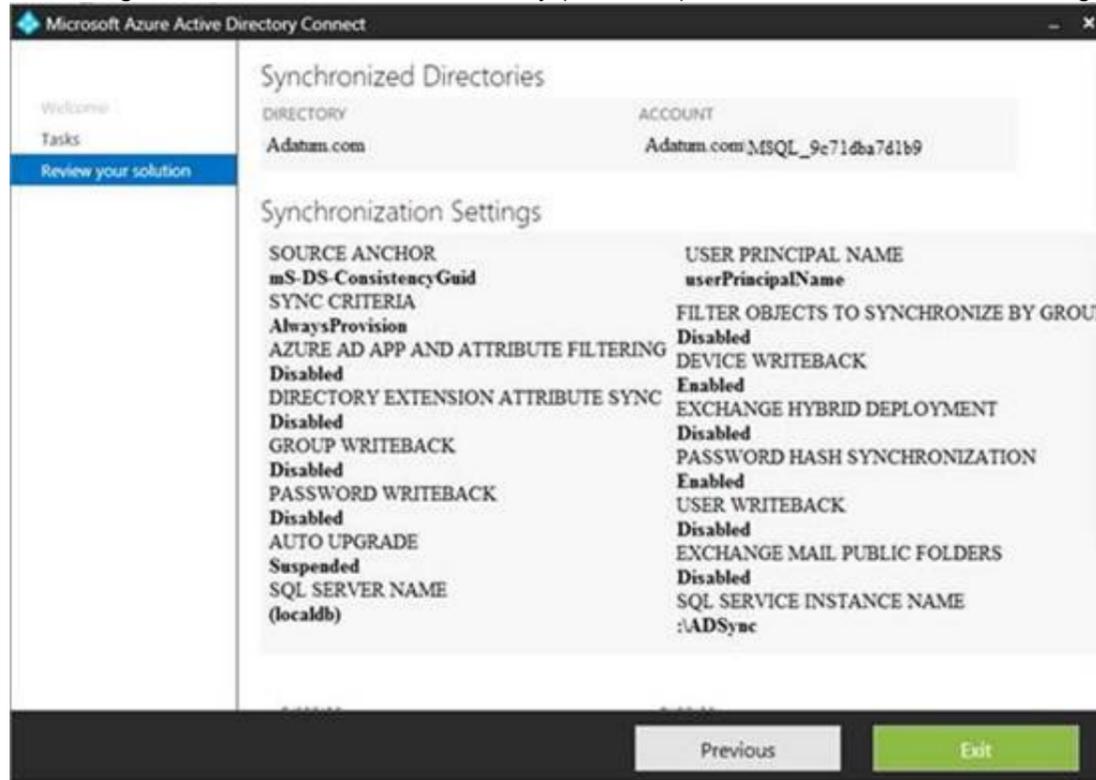
Explanation:

Case Study: 4 Mix Questions

NEW QUESTION 12

HOTSPOT

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

NEW QUESTION 17

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

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn- connectivitywindows10>

NEW QUESTION 18

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

Answer: A

Explanation:

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

NEW QUESTION 23

You have a Microsoft 365 Enterprise E5 subscription. You use Windows Defender Advanced Threat Protection (Windows 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 Advanced Threat Protection (ATP)
- C. Create a Conditional Access App Control policy for accessing Office 365
- D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Answer: A

Explanation:

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

NEW QUESTION 26

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 address that you intend to spoof belongs to the Executive group members. What should you do first?

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

Answer: C

Explanation:

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

NEW QUESTION 27

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed. You have a Microsoft Azure subscription. You are deploying Azure Advanced Threat Protection (ATP). You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016. You need to integrate the VPN and Azure ATP. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On VPN1:

Configure an authentication provider.	<input type="checkbox"/>
Configure an accounting provider.	<input type="checkbox"/>
Create a connection request policy.	<input type="checkbox"/>
Create a RADIUS client.	<input type="checkbox"/>

On Server1, enable the following inbound port:

443	<input type="checkbox"/>
1723	<input type="checkbox"/>
1813	<input type="checkbox"/>
8080	<input type="checkbox"/>
8531	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn>

NEW QUESTION 28

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

- Protected apps: App1
- Exempt apps: App2
- Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Yes No

- From Device1, User1 can copy data from App1 to App3.
- From Device2, User1 can copy data from App1 to App2.
- From Device2, User1 can copy data from App1 to App3.

<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Yes No

- From Device1, User1 can copy data from App1 to App3.
- From Device2, User1 can copy data from App1 to App2.
- From Device2, User1 can copy data from App1 to App3.

<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 32

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 34

Your company has 500 computers.

You plan to protect the computers by using Windows 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: Windows 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 Windows 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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 37

Note: This question is part of 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. Solution: You create a new label in the global policy and instruct the user to resend the email message.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 41

Note: This question is part of 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. Solution: You modify the encryption settings of the label.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 44

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1. You need to apply Policy1.

To which groups can you apply Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On-premises Active Directory groups:

Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	V
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12, Group13, and Group14 only	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 45

HOTSPOT

Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com. The company has the offices 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

The tenant contains the users shown in the following table.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

You create the Microsoft Cloud App Security policy shown in the following exhibit.

Create filters for the policy

Act on:

Single activity:
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

In a single app

Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR

equals

From group equals

as

Alerts

Create alert Use your organization's default settings
Daily alert limit 5

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

Statements

Yes	No
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements

Yes	No
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input checked="" type="radio"/>

In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

NEW QUESTION 48

HOTSPOT

You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain EU social security numbers
- Prevent any email messages that contain credit card numbers from being sent outside your organization
- Block the external sharing of Microsoft OneDrive content that contains EU passport numbers
- Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policies:

1	✓
2	
3	

Rules:

1	✓
2	
3	
4	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policies:

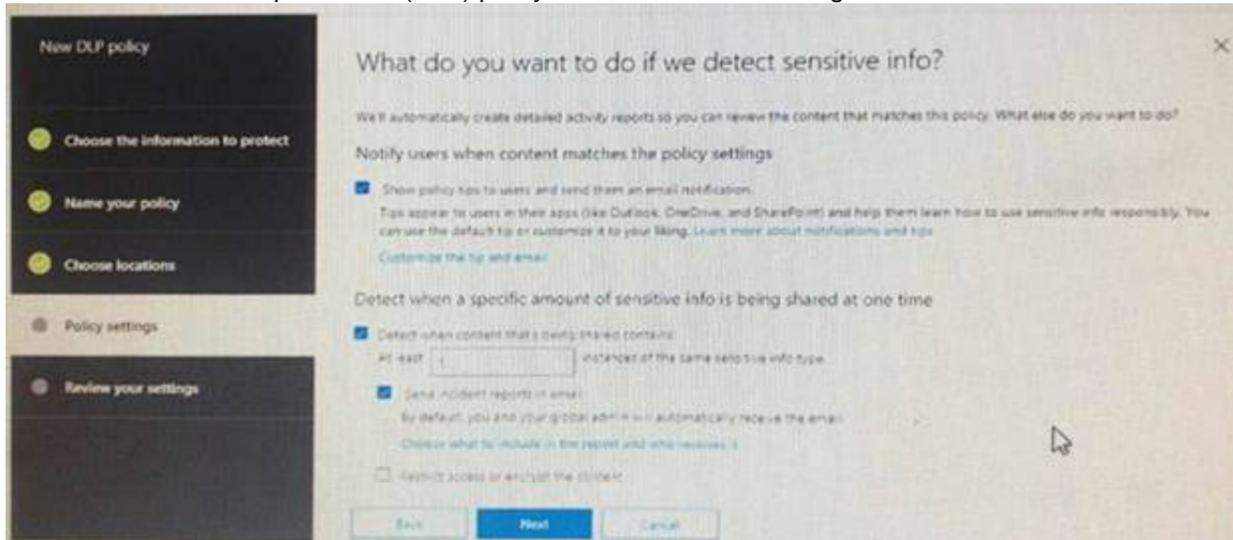
1	✓
2	
3	

Rules:

1	✓
2	
3	
4	

NEW QUESTION 49

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



What is the effect of the policy when a user attempts to send an email messages 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

Answer: A

Explanation:

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

NEW QUESTION 51

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. Compliance Policy Center
- C. eDiscovery Center
- D. Enterprise Search Center
- E. Document Center

Answer: C

Explanation:

Reference:

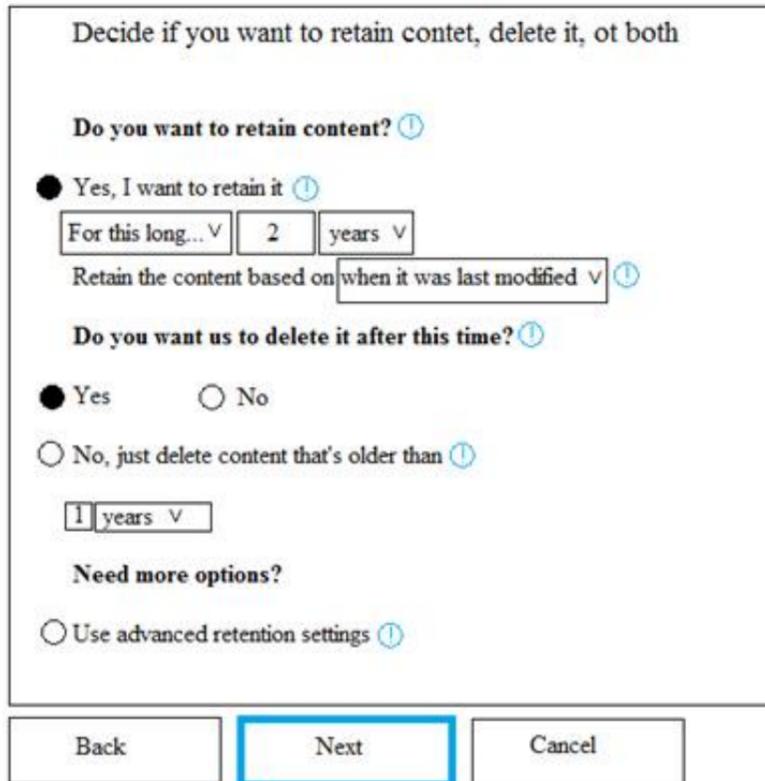
<https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bbb944-448d-b83d-8fec4abcc24c>

NEW QUESTION 54

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the following exhibit.



You apply Retention1 to SharePoint sites and OneDrive accounts.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained
deleted on January 1, 2021
deleted on July 1, 2021

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file
can recover the file until January 1, 2020
can recover the file until March 1, 2020
can recover the file until May 1, 2020

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained
deleted on January 1, 2021
deleted on July 1, 2021

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file
can recover the file until January 1, 2020
can recover the file until March 1, 2020
can recover the file until May 1, 2020

NEW QUESTION 58

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 SharePoint & Compliance admin center, create a label.
- D. From the SharePoint admin center, modify the records management settings.
- E. From the Security & Compliance admin center, publish a label.

Answer: CE

Explanation:

Reference:

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

NEW QUESTION 61

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 Security & Compliance admin center, assign a role group to Admin1.

Answer: C

Explanation:

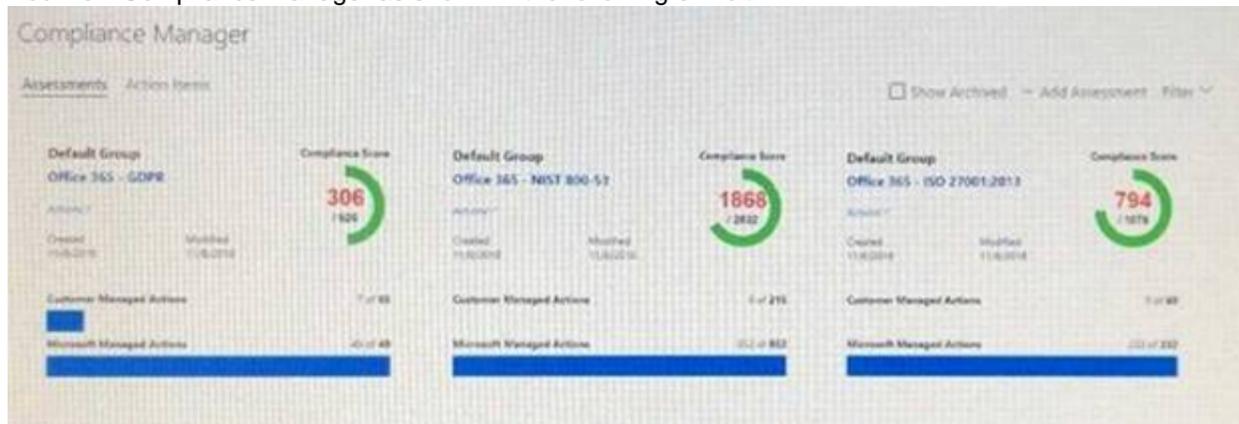
Reference:

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

NEW QUESTION 62

HOTSPOT

You view Compliance Manager as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
 NOTE: Each correct selection is worth one point.

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	▼
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	▼
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud>

NEW QUESTION 63

You have a Microsoft 365 subscription.

All computers run Windows 10 Enterprise and are managed by using Microsoft Intune. You plan to view only security-related Windows telemetry data. You need to ensure that only Windows security data is sent to Microsoft. What should you create from the Intune admin center?

- A. a device configuration profile that has device restrictions configured
- B. a device configuration profile that has the Endpoint Protection settings configured
- C. a device configuration policy that has the System Security settings configured
- D. a device compliance policy that has the Device Health settings configured

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry>

NEW QUESTION 67

You have a Microsoft 365 subscription that includes a user named Admin1.
 You need to ensure that Admin1 can preserve 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 Discovery Management admin 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.

Answer: B

NEW QUESTION 70

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 on Server1
- C. Configure a registry on the computers
- D. On the computers, run tdadm.exe

Answer: C

NEW QUESTION 75

HOTSPOT
 You have a Microsoft 365 E5 subscription.
 Users and device objects are added and removed daily. Users in the sales department frequently change their device.
 You need to create three following groups:

Group	Requirement
1	All the devices of users where the Department attributes is set to Sales
2	All the devices where the Department attribute is set to Sales
3	All the devices where the deviceOwnership attribute is set to Company

The solution must minimize administrative effort.
 What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md>

NEW QUESTION 78

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.

Answer: C

Explanation:

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

NEW QUESTION 80

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.



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

Answer: D

Explanation:

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

NEW QUESTION 83

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 questions 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-Mailbox -Identity "User1" -AuditEnabled \$true command. Does that meet the goal?

- A. Yes

B. No

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

NEW QUESTION 84

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 questions 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

Answer: B

Explanation:

References:

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

NEW QUESTION 86

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 questions 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

Answer: B

Explanation:

References:

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

NEW QUESTION 91

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.

Answer: D

Explanation:

References:

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

NEW QUESTION 93

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.

Answer: C

Explanation:

References:

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

NEW QUESTION 96

HOTSPOT

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1. You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two actions should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

Search Clear **Results**

Activities

Show results for all activities

User administration activities

- Added user
- Deleted user
- Set license properties
- Reset user password
- Changed user password
- Changed user license
- Updated user
- Set property that forces user to change password

Azure AD group administration activities

- Added group
- Updated group
- Deleted group
- Added member to group
- Removed member from group

Application administration activities

- Added service principal
- Removed a service principal from the directory
- Set delegation entry
- Removed credentials from a service principal
- Added delegation entity
- Added credentials to a service principal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 100

HOTSPOT

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.

Create a label to help users classify their content.

- Name your label
- Label settings
- Review your settings

Review your settings

Name: Label1 Edit

Descriptions for admins Edit

Description for users Edit

Retention Edit

2 years
 Retain and Delete
 Based on when it was created
 Use Label to classify content as a "Record"

Back Create this label Cancel

You publish Label1 to SharePoint sites.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

	▼
never delete the file.	
delete the file before January 1, 2021.	
delete the file after January 1, 2021.	

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

	▼
always remain in the library.	
remain in the library until you delete the file.	
be deleted automatically on March 15, 2021.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 101

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

Answer: D

Explanation:

References:

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

NEW QUESTION 104

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

Answer: C

Explanation:

References:

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

NEW QUESTION 105

You have a Microsoft 365 subscription.

You have a team named Team1 in Microsoft Teams. You plan to place all the content in Team1 on hold.

You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.

Which cmdlet should you use?

- A. Get-UnifiedGroup
- B. Get-MailUser
- C. Get-TeamMessagingSettings
- D. Get-TeamChannel

Answer: A

NEW QUESTION 110

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. Anti-malware
- B. DKIM

- C. Anti-spam
- D. ATP anti-phishing

Answer: A

NEW QUESTION 114

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.

Answer: B

NEW QUESTION 118

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 questions 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

Answer: B

Explanation:

References:

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

NEW QUESTION 121

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 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.

Answer: A

Explanation:

Reference:

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

NEW QUESTION 124

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 questions 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-MailboxFolderPermission -Identity "User1"

-User User1@contoso.com -AccessRights Owner command. Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

NEW QUESTION 129

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

MS-500 Practice Exam Features:

- * MS-500 Questions and Answers Updated Frequently
- * MS-500 Practice Questions Verified by Expert Senior Certified Staff
- * MS-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * MS-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The MS-500 Practice Test Here](#)