Microsoft 365 Certification MS-500 Exam

- **Vendor: Microsoft**
- **Exam Code: MS-500**
- **Exam Name: Microsoft 365 Security Administration**

Get Complete Version Exam MS-500 Dumps with VCE and PDF Here

https://www.passleader.com/ms-500.html

NEW QUESTION 107
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.
Solution: You use the Security event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION 108
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.
Solution: You use the Directory Service event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION 109
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.
Solution: You use the System event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION 110
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:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

NEW QUESTION 111
Several users in your Microsoft 365 subscription report that they received an email message without 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. Choose two.)

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

Answer: AD
Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files

NEW QUESTION 112
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.
Solution: You use the Application event log on Server1.
Does that meet the goal?

A. Yes
B. No

Answer: A
Explanation:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION 113
You have a Microsoft 365 E5 subscription without a Microsoft Azure 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 Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.
B. From Azure Log Analytics, query the logs.
C. From the Azure Active Directory admin center, view the audit logs.
D. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

Answer: D

NEW QUESTION 114
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

Answer: A
Explanation:
https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

NEW QUESTION 115
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: D
Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies

NEW QUESTION 116
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. 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. Choose two.)

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.

Answer: BD
Explanation:
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

NEW QUESTION 117
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

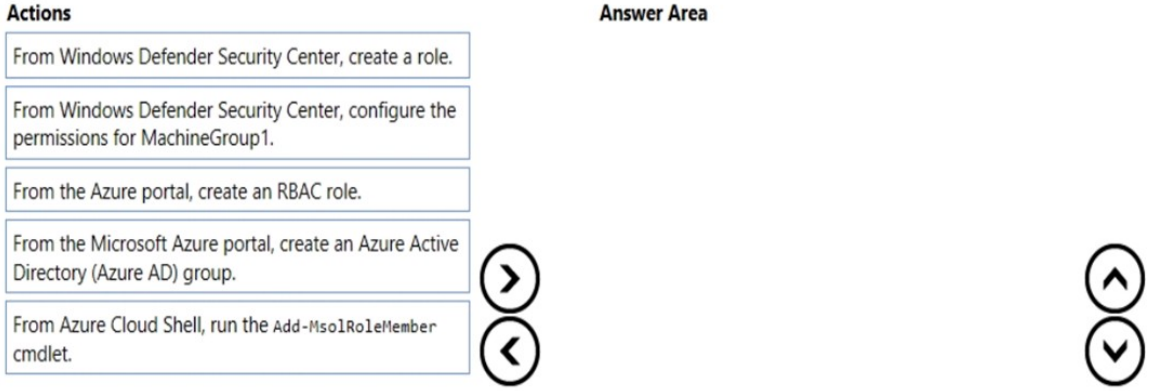
Answer: C
Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center

NEW QUESTION 118
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?

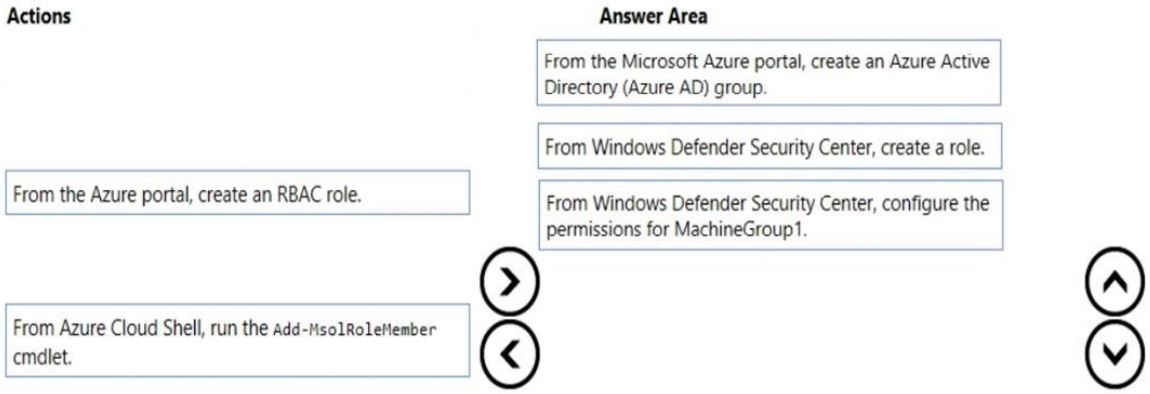
A. Get-UnifiedGroup
B. Get-MailUser
C. Get-TeamMessagingSettings
D. Get-TeamChannel

Answer: A

NEW QUESTION 119
Drag and Drop
You have a Microsoft 365 E5 subscription. All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP). You create a Windows Defender machine group named MachineGroup1. You need to enable delegation for the security settings of the computers in MachineGroup1. 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.)



Answer:



NEW QUESTION 120
Hotspot
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. Four Windows 10 devices are joined to the tenant as shown in the following table:

Name	Has TPM	BitLocker Drive Encryption (BitLocker) -protected C drive	BitLocker Drive Encryption (BitLocker) -protected D drive
Device1	Yes	Yes	No
Device2	Yes	No	Yes
Device3	No	Yes	Yes
Device4	No	No	No

On which devices can you use BitLocker To Go and on which devices can you turn on auto-unlock? (To answer, select the appropriate options in the answer area.)

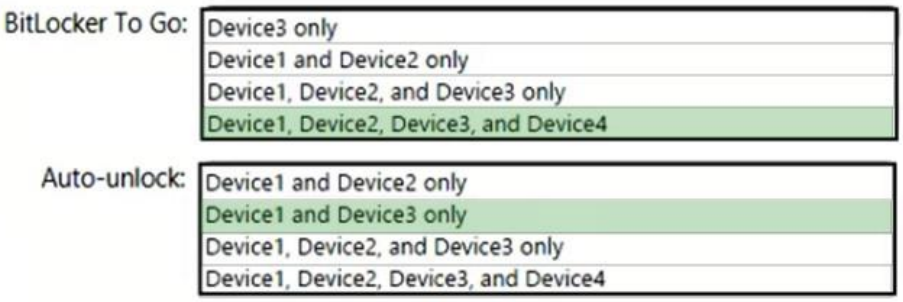
Answer Area

BitLocker To Go:
- Device3 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Auto-unlock:
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Answer:

Answer Area



NEW QUESTION 121
.....

NEW QUESTION 150
Your organization has an Azure Active Directory (Azure AD) tenant with a Microsoft 365 E5 plan. Your on premises AD is federated with Azure AD using Active Directory Federation Services (AD FS) and synchronized using the Azure AD Connect sync service. Azure AD Connect has the following settings:
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- User writeback: Disabled
You want to identify the users with leaked credentials in Azure AD. What should you do?

A. Enable password hash synchronization (PHS).
B. Enable password writeback.
C. Implement Azure AD's dynamic banned password feature.
D. Enable and require Azure multi-factor authentication (MFA) for all users.
E. Implement Azure AD access reviews.

Answer: A

NEW QUESTION 151
Hotspot
Your network has an Active Directory Domain Services (AD DS) domain named company.com. You have an Azure Active Directory (Azure AD) tenant configured as a hybrid organization. Your company has a Microsoft 365 Enterprise E5 subscription. You enable Office 365 Advanced Threat Protection (ATP). Your company uses an Exchange Online email solution. You are configuring security for incoming email. If a message attachment is infected with malware, the message should be delivered without the attachment. You need to configure the policy to support this. How should you configure the policy? (To answer, select the appropriate options from the drop-down menus.)
.....

NEW QUESTION 152
Hotspot
You are an Office 365 Global Administrator in an organization with an Office 365 Enterprise E5 subscription. As per the compliance team's request, you auto-apply two-year retention labels to all emails in your organization's Exchange Online mailboxes received from Company2, your organization's supplier. Jane, the Finance manager, manually assigns a five-year retention label to the new email she received from Company2 after you assigned the auto-reply retention labels. Eduardo, an accounts payable clerk, manually assigns a one-year retention label to a new invoice

email from Company2 before you assigned the auto-apply retention labels. You need to determine which retention labels take precedence. (For each of the following statements, select Yes if the statement is true. Otherwise, select No.)
.....

NEW QUESTION 153
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 User5.
Solution: You start a message trace, and then create a Data Subject request (DSR) case.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019

NEW QUESTION 154
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 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

Answer: A

NEW QUESTION 155
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 User5.
Solution: You assign the eDiscovery Manager role to Admin1, and then create an eDiscovery case.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019

NEW QUESTION 156
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 permissions of the mailbox of User5, and then create an eDiscovery case. Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019

NEW QUESTION 157
Drag and Drop
You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. All the devices in the tenant are managed by using Microsoft Intune. You purchase a cloud app named App1 that supports session controls. You need to ensure that access to App can be reviewed in real time. 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.)
.....

NEW QUESTION 158
You have a Microsoft 365 E5 subscription and 5,000 users. You create several alert policies that are triggered every time activities match rules. You need to create an alert policy that is triggered when the volume of matched activities becomes unusual. What should you do first?

A. Enable Microsoft Office 365 auditing.
B. Enable Microsoft Office 365 analytics.
C. Enable Microsoft Office 365 Cloud App Security.
D. Deploy a Microsoft Office 365 add-in to all the users.

Answer: B

NEW QUESTION 159
You have a Microsoft 365 subscription that contains the users shown in the following table:
.....
You enable self-service password reset for Group1 and configure security questions as the only authentication method for self-service password reset. You need to identify which user must answer security questions to reset his password. Which user should you identify?

A. User1
B. User2
C. User3
D. User4

Answer: C

NEW QUESTION 160
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table:
.....
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. User1 and User3 only.
B. User1, User2, User3, and User4.

C. User3 only.
D. User3 and User4 only.

Answer: D

NEW QUESTION 161
.....