

Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator



NEW QUESTION 1

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 2

HOTSPOT

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Set the frequency to:

One time	v
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Set the frequency to:

One time	v
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

NEW QUESTION 3

HOTSPOT

You install Azure ATP sensors on domain controllers. You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing. You need to meet the security requirements for Azure ATP reporting. What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Policy to edit:

▼

Default Domain Controllers Policy

Default Domain Policy

A local policy on one domain controller

Audit setting to configure:

▼

Audit User Account Management

Audit Computer Account Management

Audit Other Account Management Events

Audit Security Group Management

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 4

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

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

Answer Area

- 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 5

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 6

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

Answer: A

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

NEW QUESTION 7

HOTSPOT
You are evaluating which devices are compliant in Intune.
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
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input type="radio"/>
Device6 is compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device2 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device6 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 8

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 9

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 see 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

Answer: A

NEW QUESTION 10

DRAG DROP

You have a Microsoft 365 subscription. All users use Microsoft Exchange Online. Microsoft 365 is configured to use the default policy settings without any custom rules. You manage message hygiene.

Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each location may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Locations		Answer Area
ATP quarantine	Messages that contain word-filtered content:	Location
The Junk Email folder of a user's mailbox	Messages that are classified as phishing:	Location
The Clutter folder a user's mailbox		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

	Answer Area
Messages that contain word-filtered content:	The Junk Email folder of a user's mailbox
Messages that are classified as phishing:	The Junk Email folder of a user's mailbox

NEW QUESTION 10

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-groupswindows-defender-advanced-threat-protection>

NEW QUESTION 12

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 15

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 19

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

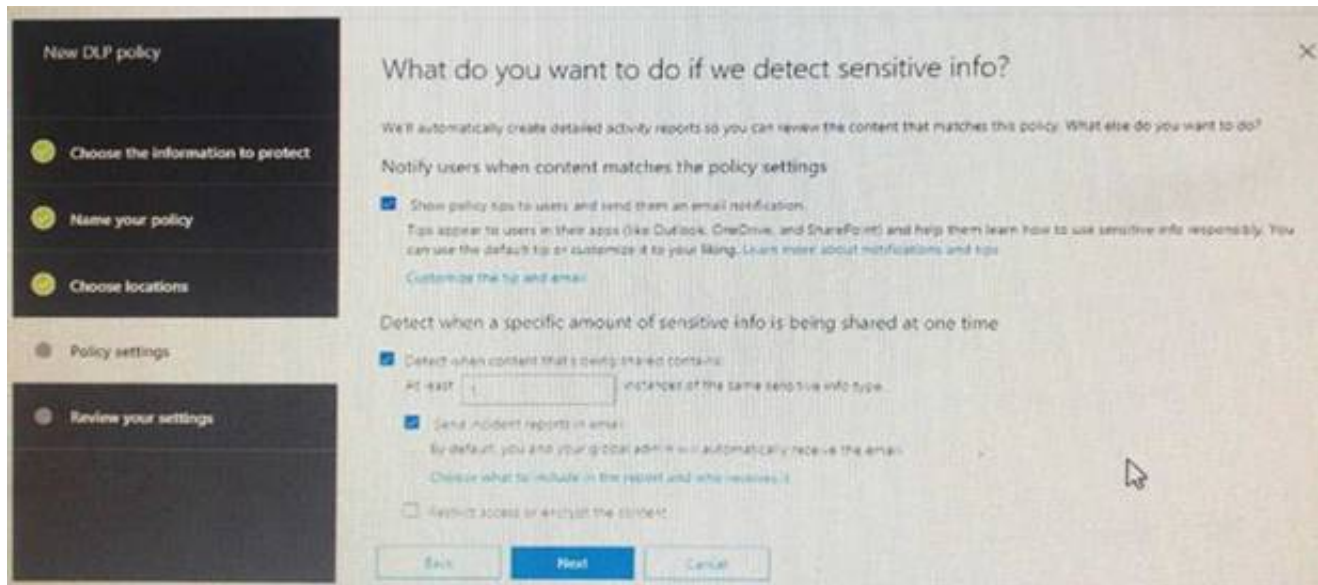
Explanation:

Reference:

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

NEW QUESTION 23

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 26

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 28

HOTSPOT

You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 1 years ▾

☐ No, just delete content that's older than ⓘ

1 years ▾

Delete the content based on when it was created ▾ ⓘ

Need more options?

☐ Use advanced retention settings ⓘ

Back Next Cancel

Policy2 is configured as shown in the following exhibit.

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 3 years ▾

Retain the content based on when it was created ▾ ⓘ

Do you want us to delete it after this time?

☐ Yes ☒ No

☐ No, just delete content that's older than ⓘ

1 years ▾

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence>

NEW QUESTION 32

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 36

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 40

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

Answer: C

NEW QUESTION 42

HOTSPOT
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
•Assignments: Include Group1, Exclude Group2
•Conditions: Sign in risk of Low and above
•Access: Allow access, Require password multi-factor authentication
You need to identify how the policy affects User1 and User2. What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:

Blocked

Can sign in without MFA

Prompted for MFA

User2:

Blocked

Can sign in without MFA

Prompted for MFA

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1:

Blocked

Can sign in without MFA

Prompted for MFA

User2:

Blocked

Can sign in without MFA

Prompted for MFA

NEW QUESTION 44

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 45

HOTSPOT

You have a Microsoft 365 subscription.
 You create a retention label named Label1 as shown in the following exhibit.

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].	<div>▼</div> <div> never delete the file. delete the file before January 1, 2021. delete the file after January 1, 2021. </div>
If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].	<div>▼</div> <div> always remain in the library. remain in the library until you delete the file. be deleted automatically on March 15, 2021. </div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 50

HOTSPOT

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

- You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:
- Rule1:
 - Conditions: Label 1, Detect content that's shared with people outside my organization
 - Actions: Restrict access to the content for external users
 - User notifications: Notify the user who last modified the content
 - User overrides: On
 - Priority: 0
 - Rule2:
 - Conditions: Label 1 or Label2
 - Actions: Restrict access to the content

- Priority: 1
- Rule3:
- Conditions: Label2, Detect content that's shared with people outside my organization
- Actions: Restrict access to the content for external users
- User notifications: Notify the user who last modified the content
- User overrides: On
- Priority: 2

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

Statements	Yes	No
External users can access File1.	<input type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input type="radio"/>
External users can access File3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
External users can access File1.	<input checked="" type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input checked="" type="radio"/>	<input type="radio"/>
External users can access File3.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 55

DRAG 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.

Actions

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Azure portal, create an RBAC role.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Azure Cloud Shell, run the Add-IsolRoleMember cmdlet.

➤

➡

Answer Area

⬆

⬇

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Azure portal, create an RBAC role.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Azure Cloud Shell, run the Add-Hso1RoleMember cmdlet.

Answer Area

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From the Azure portal, create an RBAC role.

>

<

↶

↷

NEW QUESTION 56

.....

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](#)