

MS-101 Dumps

Microsoft 365 Mobility and Security (beta)

<https://www.certleader.com/MS-101-dumps.html>



NEW QUESTION 1

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

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

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 2

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

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

You have a Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the SharePoint admin center, you modify the sharing settings.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 3

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

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft

Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management

You add a new device named Device 1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to a Configuration Manager device collection. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription.

You are configuring permissions for Security & Compliance.

You need to ensure that the users can perform the tasks shown in the following table.

Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.

To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:

- Records Management
- Security Administrator
- Security Reader
- Supervisory Review

User2:

- Compliance Administrator
- Organization Management
- Security Administrator
- Security Reader
- Supervisory Review

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles>

NEW QUESTION 5

HOTSPOT

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	None
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	None

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

User1 can view Device1 in Windows Defender Security Center.

User2 can sign in to Windows Defender Security Center.

User3 can view Device1 in Windows Defender Security Center.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements

Yes

No

User1 can view Device1 in Windows Defender Security Center.

User2 can sign in to Windows Defender Security Center.

User3 can view Device1 in Windows Defender Security Center.

NEW QUESTION 6

HOTSPOT

You have a Microsoft 365 subscription.

You need to implement Windows Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Platform:

Android
iOS
Windows 10 and later
Windows 8.1 and later

Settings:

Offboard package
Onboard package
Windows Defender Application Guard
Windows Defender Firewall

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 7

You have a Microsoft 365 tenant
You have a line-of-business application named App1 that users access by using the My Apps portal. After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control, You need to be alerted by email if impossible travel is detected for a user of Appl. The solution must ensure that alerts are generated for App1 only. What should you do?

- A. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.
- B. From Microsoft Cloud App Security, modify the impossible travel alert policy.
- C. From Microsoft Cloud App Security, create an app discovery policy.
- D. From the Azure Active Directory admin center, modify the conditional access policy.

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-anomaly-detection-policy>

NEW QUESTION 8

HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	Not applicable

You onboard computers to Windows Defender ATP as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Computer1:

Group1 only
Group2 only
Group1 and Group2
Ungrouped machines

Computer2:

Group1 only
Group3 only
Group1 and Group3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Computer1:

Computer2:

NEW QUESTION 9

DRAG DROP

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Windows Defender Advanced Threat Protection (ATP). The solution must avoid installing software on the devices whenever possible.

Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method 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.

NOTE: Each correct selection is worth one point.

Methods	Answer Area
A Microsoft Azure ATP sensor	Windows 8.1: <input type="text"/>
A local script	Windows 10: <input type="text"/>
Microsoft Monitoring Agent	Windows Server 2016: <input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection> <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection> <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection>

NEW QUESTION 10

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices. You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices. You need to recommend a Windows 10 deployment method. What should you recommend?

- A. a provisioning package
- B. an in place upgrade
- C. wipe and load refresh
- D. Windows Autopilot

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure>

NEW QUESTION 10

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices. Your company uses the following types of devices:

- Windows 10
- Windows 8.1
- Android
- iOS

Which devices can be managed by using co-management?

- A. Windows 10 and Windows 8.1 only
- B. Windows 10, Android, and iOS only
- C. Windows 10 only
- D. Windows 10, Windows 8.1, Android, and iOS

Answer: D

Explanation:

References:

https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-management-solution#bkmk_intune

NEW QUESTION 15

HOTSPOT

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

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

Name	Assigned to
Policy1	Group3
Policy2	Group2

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	
Device1 is compliant.	<input type="radio"/>	<input type="radio"/>	
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>	
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area			
Statements	Yes	No	
Device1 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>	
Device2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>	
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>	

NEW QUESTION 17

Your company has a Microsoft 365 E3 subscription.

All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).

You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.

What should you use?

- A. Windows Autopilot
- B. Windows Update
- C. Subscription Activation
- D. an in-place upgrade

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot>

NEW QUESTION 19

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content. What should you do?

- A. From the AADRM PowerShell module, run the set-AadrmonboardingControlPolicy cmdlet.
- B. From Azure Information Protection, create a policy.
- C. From the AAORM PowerShell module, run the Add-AadrmRoleBasedAdministrator cmdlet.
- D. From Azure Information Protection, configure the protection activation status.

Answer: B

Explanation:

References:

<https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information-protection/>

NEW QUESTION 24

Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

- Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
 - Opened a mailbox of which the user was not the owner
 - Reset a user password
- What should you use?

- A. Microsoft Azure Active Directory (Azure AD) audit logs
- B. Security & Compliance content search
- C. Microsoft Azure Active Directory (Azure AD) sign-ins
- D. Security & Compliance audit tag search

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview>

NEW QUESTION 29

You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that User1 can place a hold on all mailbox content. Which role should you assign to User1?

- A. e Discovery Manager from the Security & Compliance admin center
- B. compliance management from the Exchange admin center
- C. User management administrator from the Microsoft 365 admin center
- D. Information Protection administrator from the Azure Active Directory admin center

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019>

NEW QUESTION 32

HOTSPOT

You have a Microsoft 365 subscription that contains all the user data.

You plan to create the retention policy shown in the Locations exhibit. (Click the Locations tab.)

Choose locations

The policy will apply to content that's stored in the locations you choose.

Apply policy only to content in Exchange email, public folders, Office 365 groups, OneDrive and SharePoint documents.
 Let me choose specific locations. [?](#)

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	Exchange email	1 recipient Choose recipients	- Exclude recipients
<input type="checkbox"/>	SharePoint sites		
<input type="checkbox"/>	OneDrive accounts		
<input checked="" type="checkbox"/>	Office 365 groups	1 group Choose groups	- Exclude groups

You configure the Advanced retention settings as shown in the Retention exhibit. (Click the Retention tab.)

Advanced retention

Keyword query editor

merger
 acquisition
 takeover

Actions

When content matches the conditions, perform the following actions.

Retention actions

Retain the content [?](#)

For this long... years

Do you want us to delete it after this time?

Yes No

Don't retain the content. Just delete it if it's older than [?](#)

years

Retain or delete the content based on [?](#)

The locations specified in the policy include the groups shown in the following table.

Location	Include
Exchange email	A distribution group named LegalTeam
Office 365 groups	A security group named Legal365

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
Any file stored in Microsoft SharePoint group library by a user in the Legal365 group will be stored for five years, and then deleted.	<input type="radio"/>	<input type="radio"/>
An email message that contains the word takeover and is sent by a user in the LegalTeam group will be deleted automatically after five years.	<input type="radio"/>	<input type="radio"/>
If a new user is added to the LegalTeam group next week, and the user sends an email message that contains the word takeover, the message will be deleted automatically after five years.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 34

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

Exempt apps: App2

Protected apps: App1

Windows Information Protection mode: Block

Network boundary: IPv4 range of: 192.168.1.1-192.168-1.255

You need to identify the apps from which you can open File1.abc.

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
You can open File1.abc in App1.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

NEW QUESTION 35

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User 1. You need to preserve a copy of all the email messages that contain the word Project X.

WDM should you do?

- A. From the Security & Compliance admin center, create an eDiscovery case.
- B. From the Exchange admin center, create a mail now rule.
- C. From the Security fit Compliance adman center, start a message trace.
- D. From Microsoft Cloud App Security, create an access policy.

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case>

NEW QUESTION 37

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the word Project X.

You need to export the results of the content search. What do you need to download the report?

- A. a certification authority (CA) certificate
- B. an export key
- C. a password
- D. a user certificate

Answer: B

Explanation:

References:

[https://docs.HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results"microsoft.com/en-us/office365/securitycompliance/export-search-results](https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results)

NEW QUESTION 42

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You have three applications named App1, App2, and App3 that have the same file format.

Your company uses Windows Information Protection (WIP). WIP has the following configurations: Windows Information Protection mode: Silent

Protected apps: App1 Exempt apps: App2

From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

NEW QUESTION 46

HOTSPOT

You have a new Microsoft 365 subscription.

A user named User1 has a mailbox in Microsoft Exchange Online.

You need to log any changes to the mailbox folder permissions of User1.

Which command should you run? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

▼	User1	▼	\$true
Set-AdminAuditLogConfig		-AdminAuditLogEnabled	
Set-Mailbox		-AuditEnabled	
Set-UnifiedAuditSetting		-UnifiedAuditLogIngestionEnabled	

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

<https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins> <https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

NEW QUESTION 47

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune.

Solution: You add your user account as a device enrollment manager. Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 49

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to an Active Directory group. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

References:

<https://www.sccconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/>

NEW QUESTION 54

Your company has a Microsoft 365 subscription.

You implement Microsoft Azure Information Protection.

You need to automatically protect email messages that contain the word Confidential in the subject line.

What should you create?

A. a mail flow rule from the Exchange admin center

B. a message trace from the Security & Compliance admin center

C. a supervision policy from the Security & Compliance admin center

D. a sharing policy from the Exchange admin center

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-exo-rules>

NEW QUESTION 57

You have a Microsoft 365 subscription.

You need to investigate user activity in Microsoft 365, including from where users signed in, which applications were used, and increases in activity during the past month. The solution must minimize administrative effort.

Which admin center should you use?

A. Azure ATP

B. Security & Compliance

C. Cloud App Security

D. Flow

Answer: B

Explanation:

References:

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

NEW QUESTION 62

HOTSPOT

You have a Microsoft Office 365 subscription.

You need to delegate eDiscovery tasks as shown in the following table.

User	Task
User1	<ul style="list-style-type: none"> Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content. View the eDiscovery cases created by User1. Configure case settings. Place content on hold.
User2	<ul style="list-style-type: none"> View the eDiscovery cases created by User1. Export data from Advanced eDiscovery.

The solution must follow the principle of the least privilege.

To which role group should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:

▼
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

User2:

▼
eDiscovery Administrator
eDiscovery Manager
Records Management
Reviewer
Security Administrator

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 65

You plan to use the Security & Compliance admin center to import several PST files into Microsoft 365 mailboxes.

Which three actions should you perform before you import the data? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the Exchange admin center, create a public folder.
- B. Copy the PST files by using AzCopy.
- C. From the Exchange admin center, assign admin roles.
- D. From the Microsoft Azure portal, create a storage account that has a blob container.
- E. From the Microsoft 365 admin center, deploy an add-in.
- F. Create a mapping file that uses the CSV file format.

Answer: BCF

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files>

NEW QUESTION 70

You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS).

What should you do?

- A. From the Security & Compliance admin center, add User1 to the eDiscovery Manager role group.
- B. From the Azure Active Directory admin center, add User1 to the Security Reader role group.
- C. From the Security & Compliance admin center, add User1 to the Compliance Administrator role group.
- D. From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users>

NEW QUESTION 74

HOTSPOT

From the Security & Compliance admin center, you create a retention policy named Policy1. You need to prevent all users from disabling the policy or reducing the retention period.

Which command should you run? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Set-ComplianceTag	<code>-Identity "Policy1"</code>	-enabled	<code>\$true</code>
Set-HoldCompliancePolicy		-Force	
Set-RetentionCompliancePolicy		-RestrictiveRetention	
Set-RetentionPolicy		-RetentionPolicyTagLinks	
Set-RetentionPolicyTag		-SystemTag	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-pHYPERLINK>
"https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps"s

NEW QUESTION 76

Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender Advanced Threat Protection (ATP). You need to view which Windows Defender ATP alert events have a high severity and occurred during the last seven days. What should you use in Windows Defender ATP?

- A. the threat intelligence API
- B. Automated investigations
- C. Threat analytics
- D. Advanced hunting

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alertswindows-defender-advanced-threat-protection>
<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automatedinvestigations-windows-defender-advanced-threat-protection>

NEW QUESTION 78

Your company has a Microsoft 365 tenant. The company sells products online and processes credit card information. You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents. What should you use?

- A. a Security & Compliance data loss prevention (DLP) policy
- B. a Microsoft Cloud App Security access policy
- C. a Security & Compliance retention policy
- D. a Microsoft Cloud App Security file policy

Answer: A

Explanation:

References:

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

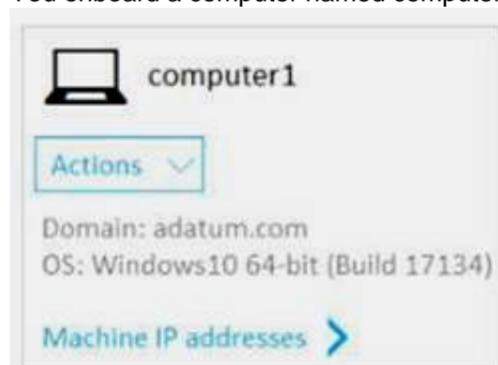
NEW QUESTION 79

HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP includes the machine groups shown in the following table.

Rank	Machine group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped machines (default)	Not applicable

You onboard a computer named computer1 to Windows Defender ATP 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.

Computer1 will be a member of [answer choice].

▼
Group3 only
Group4 only
Group3 and Group4 only
Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

▼
Group1 only
Group1 and Group2 only
Group1, Group2, Group3, and Group4
Ungrouped machines

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Computer1 will be a member of [answer choice].

▼
Group3 only
Group4 only
Group3 and Group4 only
Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

▼
Group1 only
Group1 and Group2 only
Group1, Group2, Group3, and Group4
Ungrouped machines

NEW QUESTION 81

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices. You perform a proof of concept (PoC) deployment of Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP- related data to be stored in the United States. You plan to onboard all the devices to Windows Defender ATP. You need to store the Windows Defender ATP data in Europe. What should you first?

- A. Create a workspace.
- B. Onboard a new device.
- C. Delete the workspace.
- D. Offboard the test devices.

Answer: D

NEW QUESTION 84

You have a Microsoft 365 subscription. You need to be notified if users receive email containing a file that has a virus. What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a data governance event.
- C. From the Exchange admin center, create an anti-malware policy.
- D. From the Security & Compliance admin center, create a safe attachments policy.

Answer: C

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spamand-anti-malware-protection>

NEW QUESTION 85

HOTSPOT
You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	Policy name Description Applied to	Managers
		If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com
Impersonation	Users to protect Protect all domains I own Protect specific domains Action > User impersonation Action > Domain impersonation Safety tips > User impersonation Safety tips > Domain impersonation Safety tips > Unusual characters Mailbox intelligence	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off
Spoof	Enable antispoofting protection Action	On Quarantine the message
Advanced settings	Advanced phishing thresholds	3 - More Aggressive

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 message is identified as a domain impersonation, [answer choice].

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages are moved to the Junk Email folder

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

- Advanced phishing thresholds
- Domain impersonation
- Enable antispoofting protection
- Mailbox intelligence

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

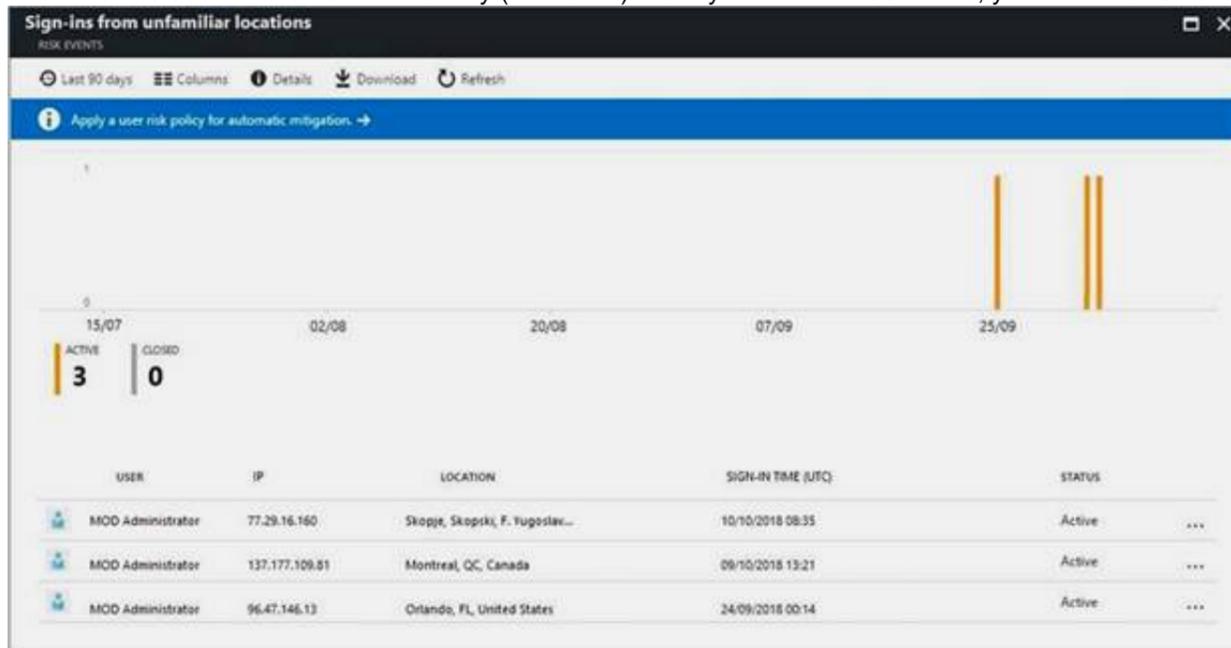
References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-HYPERLINK> "https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-anti-phishing-policy-options"atp-anti-phishing-policy-options

NEW QUESTION 88

HOTSPOT

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events 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 require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

- named location in Azure AD
- sign-in risk policy
- user risk policy

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

- a named location in Azure AD
- a sign-in risk policy
- a user risk policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations

NEW QUESTION 92

HOTSPOT

Your network contains an Active Directory forest named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

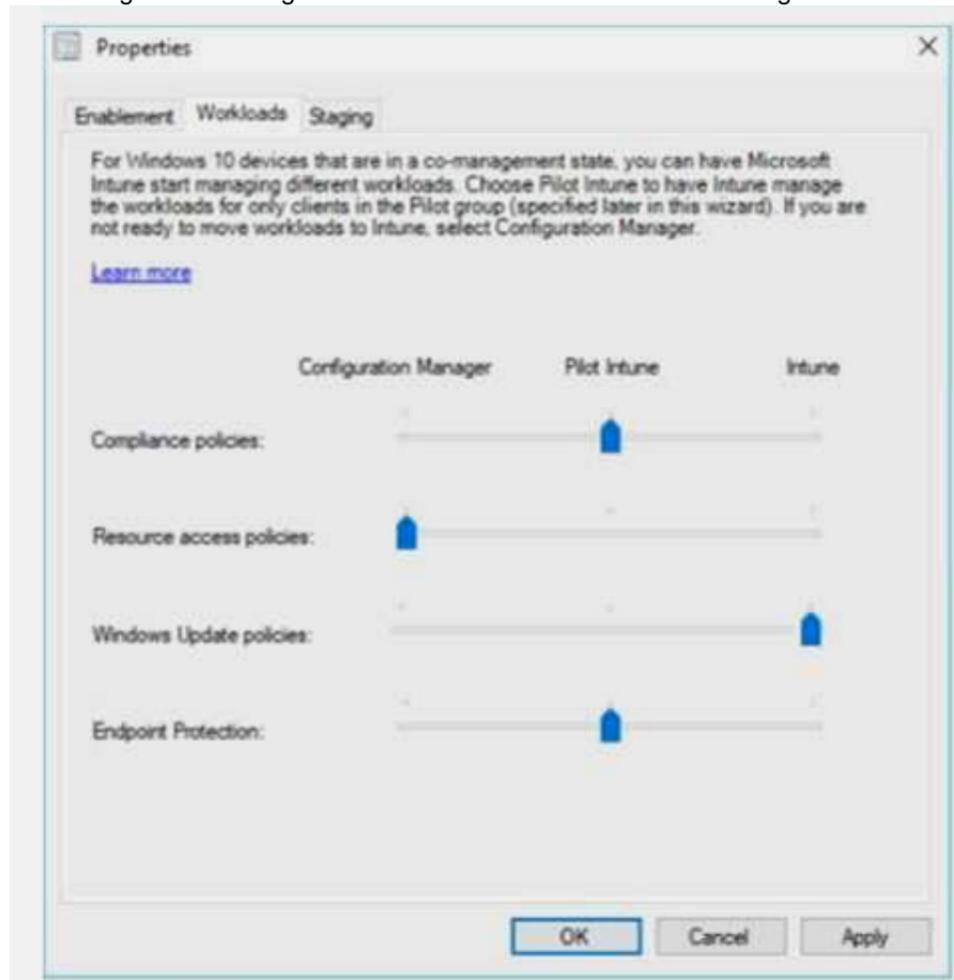
You use Microsoft System Center Configuration Manager (Current Branch) for device management. You have the Windows 10 devices shown in the following table.

Name	Collection
Device1	Collection1
Device2	Collection2

You configure Configuration Manager co-management as follows: Automatic enrollment in Intune: Pilot

Pilot collection: Collection2

You configure co-management workloads as shown in the following exhibit.



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
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 93

You have a Microsoft 365 tenant.
All users are assigned the Enterprise Mobility + Security license.
You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Intune automatically.
What should you configure?

- A. Enrollment restrictions from the Intune admin center
- B. device enrollment managers from the Intune admin center
- C. MAM User scope from the Azure Active Directory admin center
- D. MDM User scope from the Azure Active Directory admin center

Answer: D

Explanation:

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

NEW QUESTION 95

Your company uses Microsoft System Center Configuration Manager (Current Branch) and Microsoft Intune to co-manage devices.
Which two actions can be performed only from Intune? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. Deploy applications to Windows 10 devices.
- B. Deploy VPN profiles to iOS devices.
- C. Deploy VPN profiles to Windows 10 devices.
- D. Publish applications to Android devices.

Answer: BD

Explanation:

References:
<https://docs.microsoft.com/en-us/sccm/comanage/overview>
<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles>

NEW QUESTION 96

HOTSPOT
Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).
You have Windows 10 and Windows 8.1 devices.
You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

First action to perform:

- | |
|---|
| ▼ |
| Enroll the devices in Microsoft Intune. |
| Configure device compliance in Microsoft Intune. |
| Create a Microsoft Azure Log Analytics workspace. |
| Add an alias (CNAME) record to the DNS zone of contoso.com. |

Second action to perform:

- | |
|--|
| ▼ |
| Configure all the devices to have a commercial ID. |
| Configure software inventory in Configuration Manager. |
| Configure all the devices to join the Windows Insider Program. |
| Configure and restart the Windows Update service on all the devices. |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started> <https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started>

NEW QUESTION 98

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. You have a Microsoft 365 subscription.
You need to ensure that users can manage the configuration settings for all the Windows 10 devices in your organization.
What should you configure?

- A. the Enrollment restrictions
- B. the mobile device management (MDM) authority
- C. the Exchange on-premises access settings
- D. the Windows enrollment settings

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/intune/mdm-authority-set>

NEW QUESTION 103

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune. Solution: You create the Mobility (MDM and MAM) settings. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 105

Your company has 10 offices.

The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.

You discover that one of the offices has the following:

- Computers that have several preinstalled applications
- Computers that use nonstandard computer names
- Computers that have Windows 10 preinstalled
- Computers that are in a workgroup

You must configure the computers to meet the following corporate requirements:

- All the computers must be joined to the domain.
- All the computers must have computer names that use a prefix of CONTOSO.
- All the computers must only have approved corporate applications installed.

You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.

What should you recommend?

- A. a provisioning package
- B. wipe and load refresh
- C. Windows Autopilot
- D. an in-place upgrade

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios> <https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot>

NEW QUESTION 107

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

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

You have a Microsoft 365 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition> <https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlineand-OneDrive-for/ba-p/46678>

NEW QUESTION 111

You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription. You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.

What should you do first?

- A. Enable Microsoft Office 365 Cloud App Security.
- B. Deploy Windows Defender Advanced Threat Protection (Windows Defender ATP)
- C. Enable Microsoft Office 365 Analytics.

Answer: B

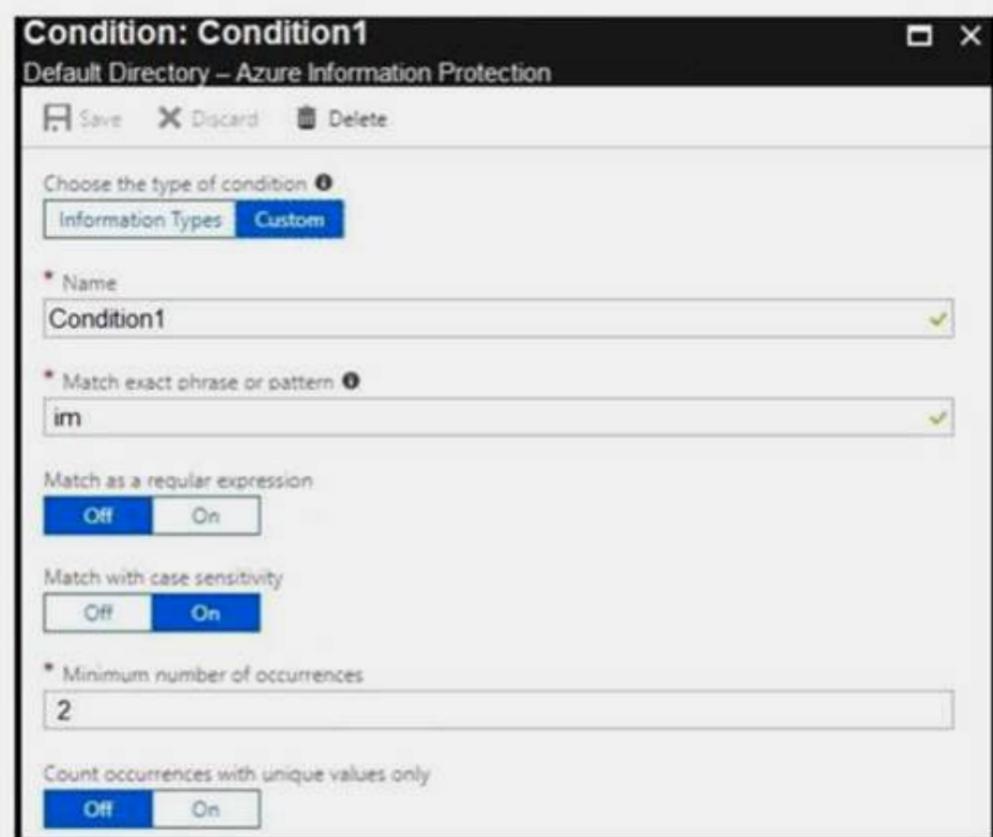
NEW QUESTION 112

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. A user named User1 has files on a Windows 10 device as shown in the following table.

Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination.
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.



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
Label1 applies to File1.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File2.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION 117

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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-AzureRmRoleAssignment cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:
<https://docs.microsoft.com/en-us/powershell/module/azurerms/resources/new-azurermroleassignment?view=azurermps-6.13.0>

NEW QUESTION 119

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. From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group. You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States. Solution: From the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 122

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. You sign for Microsoft Store for Business. The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator
User5	None	None

Microsoft Store for Business has the following Shopping behavior settings: Allow users to shop is set to On. Make everyone a Basic Purchaser is set to Off. You need to identify which users can install apps from the Microsoft for Business private store. Which users should you identify?

- A. User1, User2, User3, User4, and User5
- B. User1 only
- C. User1 and User2 only
- D. User3 and User4 only
- E. User1, User2, User3, and User4 only

Answer: C

Explanation:

References:
<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business>

NEW QUESTION 126

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 Azure Active Directory (Azure AD) tenant named contoso.com. You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1. The tenant contains users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors. Solution: You instruct User1 to modify the Azure ATP sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 130

You have a Microsoft 365 subscription that uses a default domain named contoso.com. You have two users named User 1 and User2. From the Security & Compliance admin center, you add User1 to the ediscovery Manager role group. From the Security & Compliance admin center, User1 creates a case named Case1. You need to ensure that User1 can add User2 as a case member. The solution must use the principle of least privilege. To which role group should you add User2?

- A. eDiscovery Manager
- B. eDiscovery Administrator
- C. Security Administrator

Answer: C

Explanation:

Case Study: 1 Contoso, Ltd Overview

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

The company has the employees and devices shown in the following table.

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

Contoso recently purchased a Microsoft 365 ES subscription.

Existing Environment Requirement

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

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

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

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

The domain also includes a group named Group1.

Planned Changes

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must NOT use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- Configure Windows Information Protection (WIP) for the Windows 10 devices.

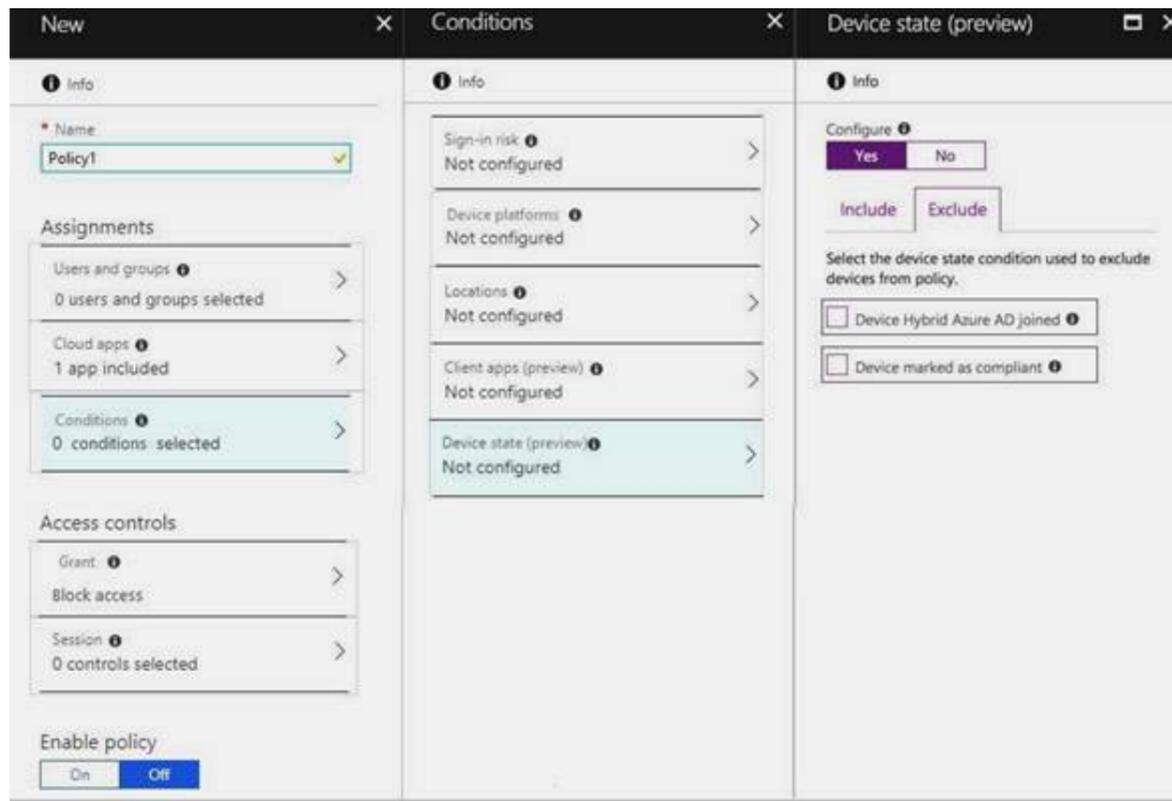
NEW QUESTION 131

HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

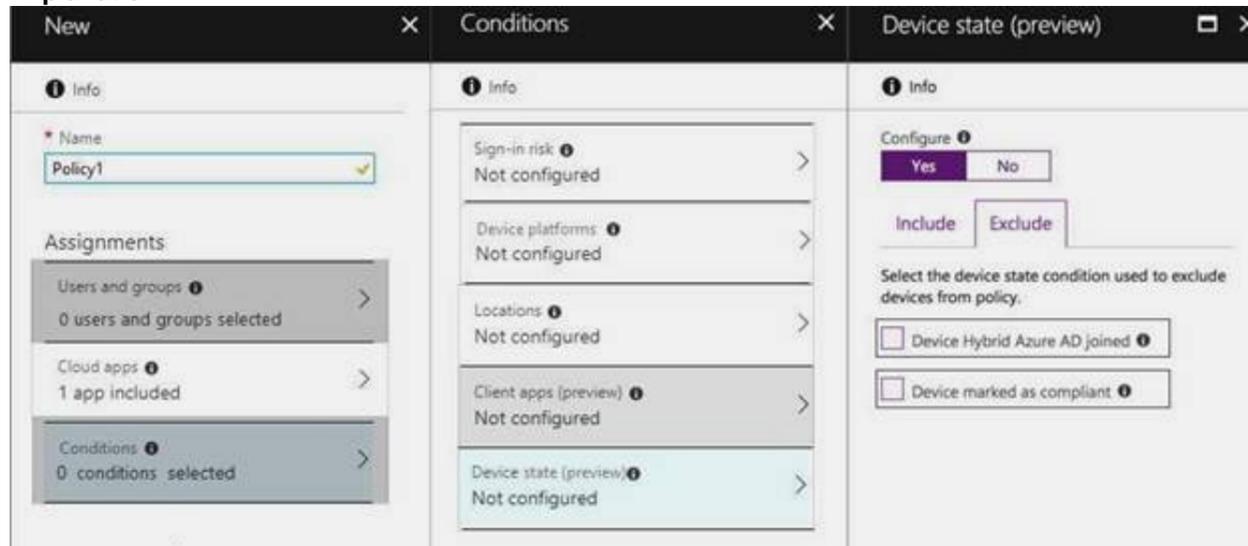
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 136

On which server should you install the Azure ATP sensor?

- A. Server 1
- B. Server 2
- C. Server 3
- D. Server 4
- E. Server 5

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning>

NEW QUESTION 139

You need to meet the compliance requirements for the Windows 10 devices. What should you create from the Intune admin center?

- A. a device compliance policy
- B. a device configuration profile
- C. an application policy
- D. an app configuration policy

Answer: D

NEW QUESTION 143

You need to create the Microsoft Store for Business. Which user can create the store?

- A. User2
- B. User3
- C. User4
- D. User5

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business>

Case Study: 2

A. Datum Case Study: Overview

Existing Environment

This is a case study Case studies are not timed separately. You can use as much exam time as you

would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is

provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question. Current Infrastructure

A. Datum recently purchased a Microsoft 365 subscription. All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

A. Datum uses and processes Personally Identifiable Information (PII).

Problem Statements Requirements

A. Datum entered into litigation. The legal department must place a hold on all the documents of a

user named User1 that are in Microsoft 365. Business Goals

A. Datum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

A. Datum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

A. Datum identifies the following technical requirements:

- Centrally perform log analysis for all offices.
- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
- A security administrator requires a report that shows which Microsoft 365 users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.
- Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

NEW QUESTION 148

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

Answer: C

Explanation:

References:

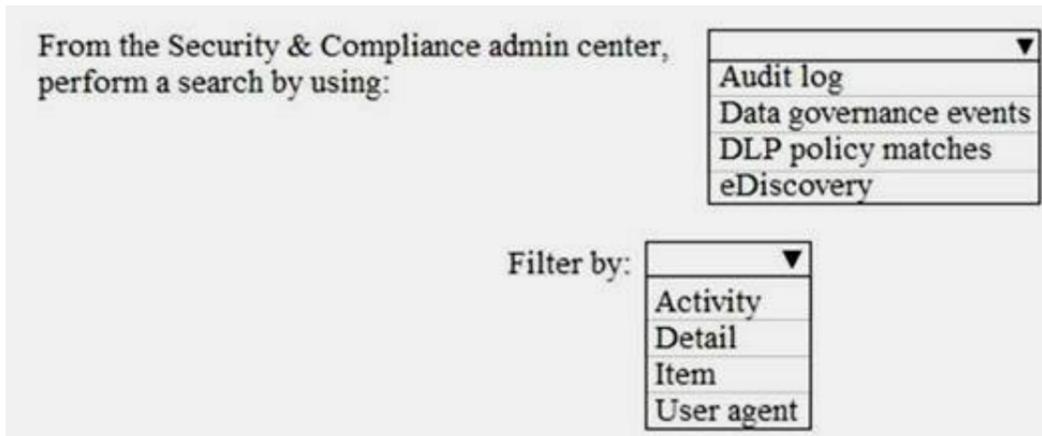
[https://docs.microsoft.com/en-us/office365/SHYPERLINK \"https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies\" securitycompliance/data-loss- prevention-policies](https://docs.microsoft.com/en-us/office365/SHYPERLINK \)

NEW QUESTION 153

HOTSPOT

You need to meet the technical requirement for the SharePoint administrator. What should you do?

To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- 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#step-3-filter-the-search-results>

NEW QUESTION 154

You need to protect the U.S. PII data to meet the technical requirements. What should you create?

- A. a data loss prevention (DLP) policy that contains a domain exception
- B. a Security & Compliance retention policy that detects content containing sensitive data
- C. a Security & Compliance alert policy that contains an activity
- D. a data loss prevention (DLP) policy that contains a user override

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts>

NEW QUESTION 156

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your MS-101 Exam with Our Prep Materials Via below:

<https://www.certleader.com/MS-101-dumps.html>