

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.

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 2

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 3

You have a Microsoft 365 subscription.

Your company purchases a new financial application named App1.

From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.

You need to prevent the missing information from affecting the score. What should you configure from the Cloud Discover settings?

A. Organization details

B. Default behavior

C. Score metrics

D. App tags

Answer: D

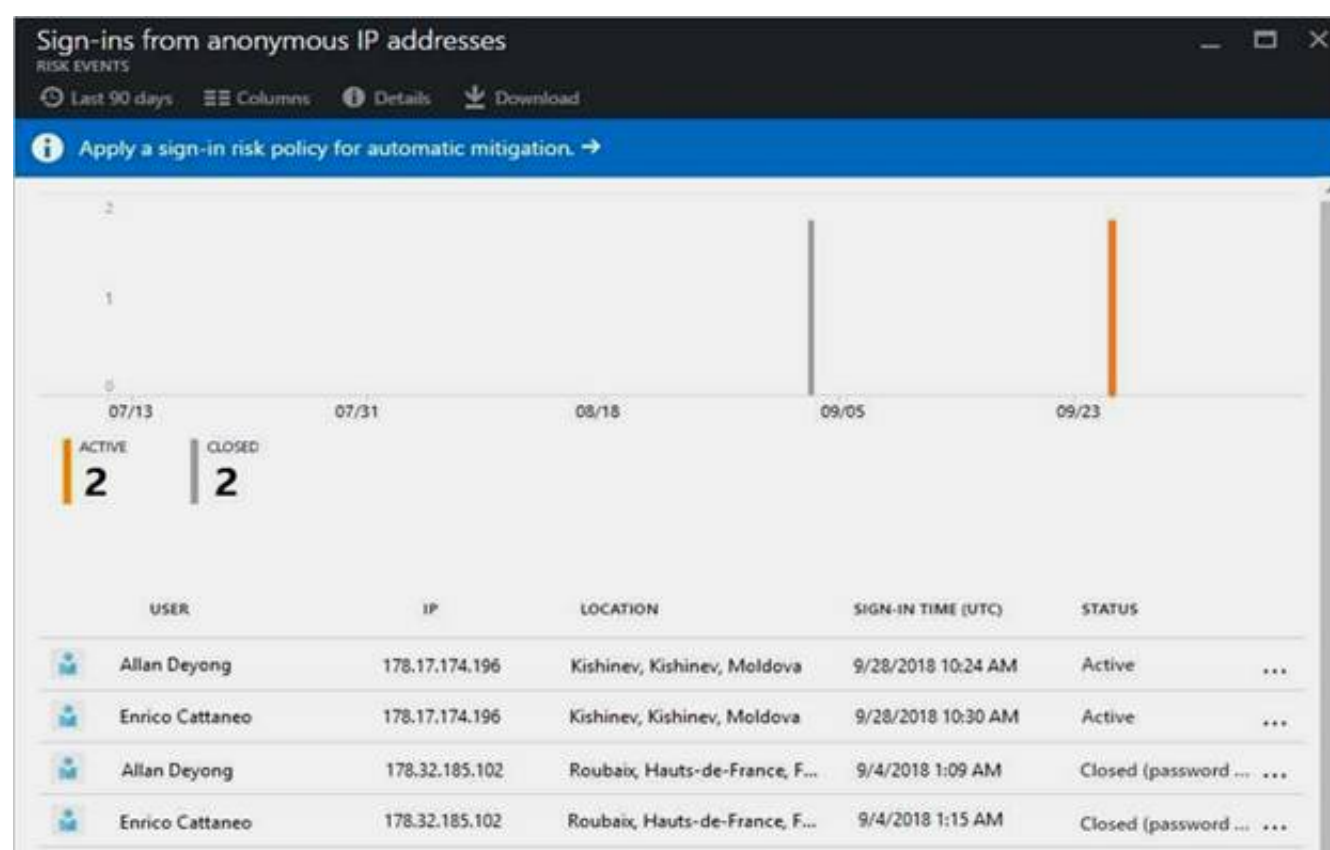
Explanation:

References:

<https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries>

NEW QUESTION 4

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)



You need to reduce the likelihood that the sign-ins are identified as risky. What should you do?

- A. From the Security & Compliance admin center, create a classification label.
- B. From the Security & Compliance admin center, add the users to the Security Readers role group.
- C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
- D. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

Answer: D

Explanation:

References:

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

NEW QUESTION 5

DRAG DROP

You create a Microsoft 365 subscription.

You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).

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

Actions	Answer Area
Download the Azure ATP sensor setup package.	
Create a Security & Compliance threat management policy.	
Create an Azure Active Directory (Azure AD) conditional access policy.	
Install sensors.	
Create a workspace.	
Enter credentials.	
Configure the sensor settings.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/>

NEW QUESTION 6

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.

Users in other departments must not be restricted.

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

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the default safe links policy.
- C. Create a data loss prevention (DLP) policy that has a Content contains condition.

D. Create a new safe links policy.

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients>

NEW QUESTION 7

HOTSPOT

You have several devices enrolled in Microsoft Intune.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	Group1
User2	Intune administrator	Group2
User3	None	None

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	Group2
2	Policy2	10	Group1
Default	All users	5	All users

You add User3 as a device enrollment manager 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
User1 can enroll a maximum of 10 devices in Intune.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Intune.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

[https://docs.microsoft.com/en-us/sHYPERLINK "https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager"ccm/mdm/deploy- use/enroll-devices-with-device-enrollment-manager](https://docs.microsoft.com/en-us/sHYPERLINK)

NEW QUESTION 8

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 9

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. Your company implements Windows Information Protection (WIP).

You need to modify which users and applications are affected by WIP.

What should you do? To answer, select the appropriate options m the answer area.

NOTE: Each correct selection is worth one point.

To modify which users are affected by WIP, configure:

▼
The Azure AD app registration
The Azure AD device settings
The MAM User scope
The mobile device management (MDM) authority

To modify which applications are affected by WIP, configure:

▼
App configuration policies
App protection policies
Compliance policies
Device configuration profiles

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 10

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 10

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 12

HOTSPOT

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.

New DLP policy

Choose the information to protect

Name your policy

Choose locations

Policy settings

Review your settings

Review your settings

Template name: U.K. Personally Identifiable Information (PII) Data [Edit](#)

Policy name: U.K. Personally Identifiable Information (PII) Data [Edit](#)

Description: [Edit](#)

Applies to content in these locations: [Edit](#)
Exchange email
SharePoint sites
OneDrive accounts

Policy settings: [Edit](#)
If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.
If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created? [Edit](#)
Yes

[Back](#) [Create](#) [Cancel](#)

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

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [answer choice].

▼
allowed
blocked without warning
blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [answer choice].

▼
allowed
blocked without warning
blocked, but the user can override the policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 14

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 and Compliance admin 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 19

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 20

You have a Microsoft 365 subscription.
You need to view the IP address from which a user synced a Microsoft SharePoint library.
What should you do?

- A. From the SharePoint admin center, view the usage reports.
- B. From the Security & Compliance admin center, perform an audit log search.
- C. From the Microsoft 365 admin center, view the usage reports.
- D. From the Microsoft 365 admin center, view the properties of the user's user account.

Answer: B

Explanation:

References:

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

NEW QUESTION 22

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>

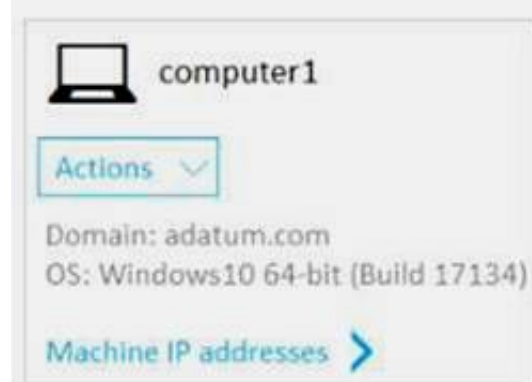
NEW QUESTION 27

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)	<i>Not applicable</i>

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 28

DRAG DROP

You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)

Workspace ?				Manage Azure ATP user roles ?
Create Workspace				
NAME	TYPE	INTEGRATION	GEOLOCATION	
testworkspace	Primary	Windows Defender ATP	Europe	

The sensors settings for the workspace are configured as shown in the Sensors exhibit. (Click the Sensors tab.)

Sensors ?					
① Configure Directory Services to install the first Sensor or Standalone Sensor.					
NAME	TYPE	DOMAIN CO...	VERSION	SERVICE STATUS	HEALTH
No Sensors registered					

You need to ensure that Azure ATP stores data in Asia.

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

Modify the integration setting for the workspace.

Delete the workspace.

Regenerate the access keys.

Create a new workspace.

Modify the Azure ATP user roles.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Delete the workspace.

Create a new workspace.

Regenerate the access keys.

NEW QUESTION 31

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 36

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 41

HOTSPOT

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain. You update the Windows 10 devices by using Windows Update for Business. What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Quality updates:	<div><div></div><div>14 days</div><div>30 days</div><div>60 days</div><div>120 days</div></div>
Feature updates:	<div><div></div><div>60 days</div><div>180 days</div><div>365 days</div><div>540 days</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wuwb>

NEW QUESTION 45

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/comanage/overview>

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

NEW QUESTION 49

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 50

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)

Locations

Control user access based on their physical location. [Learn more.](#)

Configure

Yes

No

Include

Exclude

☐ Any location

☒ All trusted locations

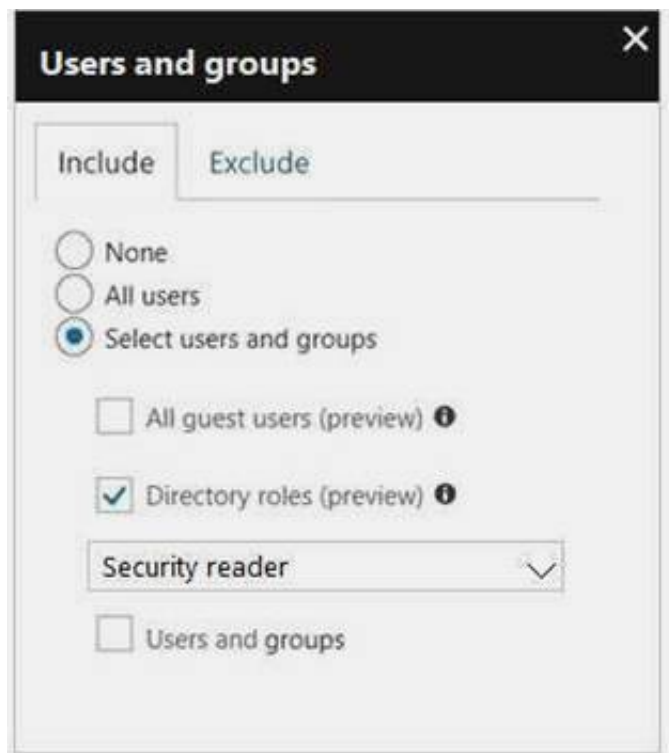
☐ Selected locations

Select

None

>

The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office. You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege. What should you do?

- A. From the conditional access policy, configure the device state.
- B. From the Azure Active Directory admin center, create a custom control.
- C. From the Intune admin center, create a device compliance policy.
- D. From the Azure Active Directory admin center, create a named location.

Answer: D

Explanation:

References:

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

NEW QUESTION 51

You have computers that run Windows 10 Enterprise and are joined to the domain.

You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.

You need to prevent Windows from being updated for the next 30 days.

Which two Group Policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Select when Quality Updates are received
- B. Select when Preview Builds and Feature Updates are received
- C. Turn off auto-restart for updates during active hours
- D. Manage preview builds
- E. Automatic updates detection frequency

Answer: BD

NEW QUESTION 53

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

You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A. Cloud application administrator
- B. Application administrator
- C. Global administrator
- D. Service administrator

Answer: C

Explanation:

References:

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

NEW QUESTION 56

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	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.

Statements	Yes	No
User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 60

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 61

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-ComplianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search>

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

NEW QUESTION 62

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2

The domain contains the devices shown in the following table.

Name	Compliance status
Device1	Compliant
Device2	Noncompliant

The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.

Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	None	All device states	Device marked as compliant	Block access
Policy2	Group1	Group2	None	None	Block Access
Policy3	Group1	None	All device states	None	Grant access

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 access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 65

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 67

HOTSPOT

Your company has a Microsoft 365 subscription.


You need to configure Microsoft 365 to meet the following requirements:

- Malware found in email attachments must be quarantined for 20 days.
- The email address of senders to your company must be verified.

Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.


NOTE: Each correct selection is worth one point.

Answer Area




ATP anti-phishing

Protect users from phishing attacks like impersonation and spoofing, and use safety tips to warn users about potentially harmful messages.



ATP safe attachments

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.



ATP Safe Links

Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 69

HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Seattle:	<div><div>▼</div><div>6 months</div><div>18 months</div><div>24 months</div><div>30 months</div><div>5 years</div></div>
New York:	<div><div>▼</div><div>6 months</div><div>18 months</div><div>24 months</div><div>30 months</div><div>5 years</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://www.windowscentral.com/whats-difference-HYPERLINK> "https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10"between-quality-updates-and-feature-updates-windows-10

NEW QUESTION 74

You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

- A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- C. From the Intune admin center, add User1 as a device enrollment manager.
- D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrHYPERLINK> "https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager"ollment-manager

NEW QUESTION 78

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 79

HOTSPOT

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Minimum number of data sources:	<div><div>▼</div><div>1</div><div>3</div><div>6</div></div>
Minimum number of log collectors:	<div><div>▼</div><div>1</div><div>3</div><div>6</div></div>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker>

NEW QUESTION 81

.....

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>