

MS-101.45q

Number: MS-101
Passing Score: 800
Time Limit: 120 min

MS-101



Website: <https://vceplus.com>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

Microsoft 365 Mobility and Security

Question Set 1

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.

<https://vceplus.com/>

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 site, you create an alert.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:



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 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

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

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.

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 configure the Apple MDM Push certificate.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get>

QUESTION 4

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.

<https://vceplus.com/>

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 an Apple Configurator enrollment profile.

Does this meet the goal?



<https://vceplus.com/>

A. Yes

B. No

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

QUESTION 5

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).

<https://vceplus.com/>

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 create a device configuration profile from the Intune admin center.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

QUESTION 6

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

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 7

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



Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 8

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

<https://vceplus.com/>

D. Flow

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 9

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

- A. the locations of the DLP policy
- B. the user overrides of the DLP policy rule
- C. the status of the DLP policy
- D. the conditions of the DLP policy rule



Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 10

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.

<https://vceplus.com/>

- 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.

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 11

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the **Exhibit** tab.)

You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.

What should you configure?

- A. an exception



Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

- Block people from sharing and restrict access to shared content

By default, users are blocked from sending email messages to people. You can choose who has access to shared SharePoint and OneDrive content. Block these people from accessing SharePoint and OneDrive content.

- Everyone. Only the content owner, the last modifier, and the site admin will continue to have access.

- Only people outside your organization. People inside your organization will continue to have access.

- Encrypt email messages (applies only to content in Exchange)

- B. an action
C. a condition
D. a group

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work>

QUESTION 12

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.

<https://vceplus.com/>

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.

Correct Answer: BCF

Section: [none]

Explanation

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

QUESTION 13

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.

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 14 HOTSPOT

You have a data loss prevention (DLP) policy.

You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM). The solution must minimize the number of false positives.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference: References: <https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>
<https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm>

QUESTION 15

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users.

From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. An administrator creates a new Microsoft SharePoint site collection.
- B. An administrator creates a new mail flow rule.
- C. A user shares a Microsoft SharePoint folder with an external user.
- D. A user delegates permissions to their mailbox.
- E. A user purges messages from their mailbox.

Correct Answer: ABC

Section: [none]

Explanation

Explanation/Reference:

<https://vceplus.com/>

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35390b-4518-800e-0c7ec95e946c>

QUESTION 16

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the **Exhibit** tab.)



SharePoint Content_Export ✕

↓ Restart report

↓ Download report

🗑 Delete

Status:

The export has completed. You can start downloading the results.

Items included from the search:

All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:

One PST file for each mailbox.



De-duplication for Exchange content:

Not enabled.

SharePoint document versions:

Included

Export files in a compressed (zipped) folder:

Yes

The export data was prepared within region:

Default region

Close

Feedback

What will be excluded from the export?

- A. a 60-MB DOCX file
- B. a 5-MB MP3 file
- C. a 10-MB XLSX file
- D. a 5-KB RTF file

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

QUESTION 17

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

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alerts-windows-defender-advanced-threat-protection> <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection>

QUESTION 18

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

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 19

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

 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.

Select and Place:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference:



QUESTION 20

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.

You need to analyze the traffic logs.

What should you do from Microsoft Cloud App Security?

- A. Click **Investigate**, and then click **Activity log**.
- B. Click **Control**, and then click **Policies**. Create a file policy.
- C. Click **Discover**, and then click **Create snapshot report**.
- D. Click **Investigate**, and then click **Files**.

Correct Answer: A

Section: [none]

Explanation

<https://vceplus.com/>

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/investigate-an-activity-in-office-365-cas>

QUESTION 21

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.



Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

QUESTION 22

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.

<https://vceplus.com/>

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 23

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint site.

What should you do?

- A. From the Security & Compliance admin center, create an alert policy.
- B. From the SharePoint site, create an alert.
- C. From the SharePoint admin center, modify the sharing settings.
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 24

Your company uses Microsoft Azure Advanced Threat Protection (ATP) and Windows Defender ATP.

You need to integrate Windows Defender ATP and Azure ATP.

What should you do?

- A. From Azure ATP, configure the notifications and reports.
- B. From Azure ATP, configure the data sources.
- C. From Windows Defender Security Center, configure the Machine management settings.
- D. From Windows Defender Security Center, configure the General settings.

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 25

You have Windows 10 Pro devices that are joined to an Active Directory domain.

You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business for SSO to Microsoft 365 services.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. computers that have biometric hardware features
- B. Microsoft Intune enrollment
- C. Microsoft Azure Active Directory (Azure AD)
- D. smartcards
- E. TPM-enabled devices



Correct Answer: BC

Section: [none]

Explanation

Explanation/Reference:

References: <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base>

QUESTION 26

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?

<https://vceplus.com/>

- 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

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 27

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

Correct Answer: B

Section: [none]

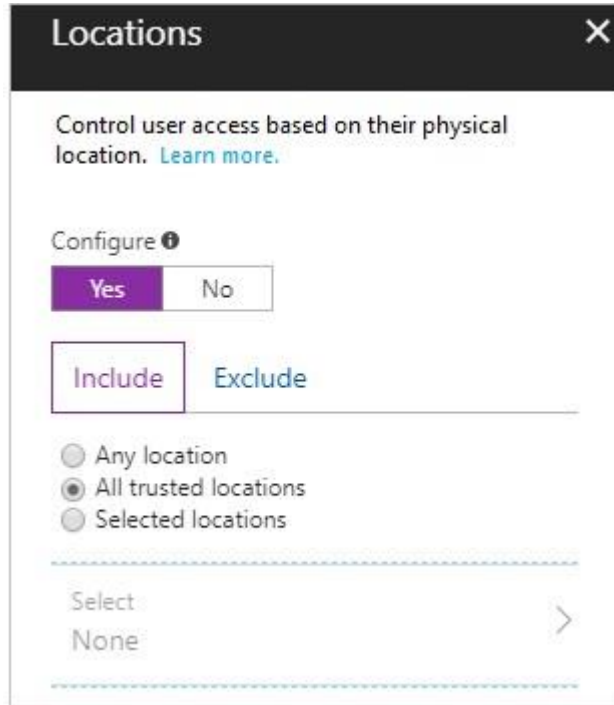
Explanation

Explanation/Reference:

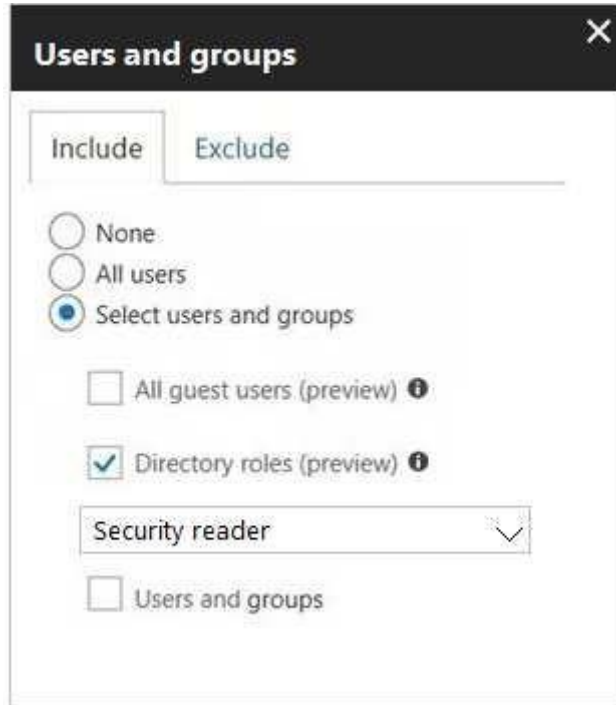
References: <https://docs.microsoft.com/en-us/intune/mdm-authority-set>

QUESTION 28

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



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 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.

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

<https://vceplus.com/>

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

QUESTION 29

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

Correct Answer: BD

Section: [none]

Explanation

Explanation/Reference:

References: <https://insider.windows.com/en-us/for-business-organization-admin/>

QUESTION 30

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

Correct Answer: C

<https://vceplus.com/>

Section: [none]
Explanation

Explanation/Reference:

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

QUESTION 31

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 a Configuration Manager device collection.

Does this meet the goal?



<https://vceplus.com/>

- A. Yes
- B. No

Correct Answer: B

<https://vceplus.com/>

Section: [none]

Explanation

Explanation/Reference:

QUESTION 32

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



Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 33

Your network contains an on-premises Active Directory domain.

Your company has a security policy that prevents additional software from being installed on domain controllers.

You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP).

What should you do? More than one answer choice may achieve the goal. Select the **BEST** answer.

- A. Deploy an Azure ATP sensor, and then configure port mirroring.
- B. Deploy an Azure ATP sensor, and then configure detections.

<https://vceplus.com/>

- C. Deploy an Azure ATP standalone sensor, and then configure detections.
- D. Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 34

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.

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

References:

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

QUESTION 35

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.

<https://vceplus.com/>

You need to be alerted by email if impossible travel is detected for a user of App1. 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.

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 36

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

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

References:

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

QUESTION 37

<https://vceplus.com/>

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

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 38

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

Correct Answer: A

Section: [none]

Explanation

<https://vceplus.com/>

Explanation/Reference:

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

QUESTION 39

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. eDiscovery 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

Correct Answer: A

Section: [none]

Explanation

**Explanation/Reference:**

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

QUESTION 40

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

- A. incident reports
- B. actions
- C. exceptions

<https://vceplus.com/>

D. user overrides

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

References:

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



Testlet 2

Case Study

Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment

Current Infrastructure

ADatum 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.adatum.com.

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

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

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

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

Technical Requirements

<https://vceplus.com/>

ADatum 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 shown 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 U.S. PII data to other New York office uses. 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.

QUESTION 1

Which report should the New York office auditors view?

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



Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 2

You need to meet the technical requirement for large-volume document retrieval.

What should you create?

- A. an activity policy from Microsoft Cloud App Security
- B. a data loss prevention (DLP) policy from the Security & Compliance admin center
- C. a file policy from Microsoft Cloud App Security

<https://vceplus.com/>

D. an alert policy from the Security & Compliance admin center

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 3

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

- A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- B. Microsoft Azure Active Directory (Azure AD) Identity Protection
- C. Microsoft Azure Active Directory (Azure AD) conditional access policies
- D. Microsoft Azure Active Directory (Azure AD) authentication methods

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 4

You need to meet the technical requirement for the EU PII data.

What should you create?

- A. a data loss prevention (DLP) policy from the Security & Compliance admin center
- B. a data loss prevention (DLP) policy from the Exchange admin center
- C. a retention policy from the Exchange admin center
- D. a retention policy from the Security & Compliance admin center

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 5

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

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

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



<https://vceplus.com/>

<https://vceplus.com/>