Free Questions for MD-102 by braindumpscollection

Shared by Rosales on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You have a Windows 10 device named Device! that is joined to Active Directory and enrolled in Microsoft Intune.

Device1 is managed by using Group Policy and Intune.

You need to ensure that the Intune settings override the Group Policy settings.

What should you configure?

Options:

A- a device configuration profile

B- a device compliance policy

C- an MDM Security Baseline profile

D- a Group Policy Object (GPO)

Answer:

A

Explanation:

A device configuration profile is a collection of settings that can be applied to devices enrolled in Microsoft Intune. You can use device configuration profiles to manage Windows 10 devices that are joined to Active Directory and enrolled in Intune. To ensure that the Intune settings override the Group Policy settings, you need to enable the policy CSP setting called MDMWinsOverGP in the device configuration profile. This setting will give precedence to the MDM policy over any conflicting Group Policy settings.Reference:[Use policy CSP settings to create custom device configuration profiles]

Question 2

Question Type: MultipleChoice

You have a computer named Computed that has Windows 10 installed.

You create a Windows PowerShell script named config.psl.

You need to ensure that config.psl runs after feature updates are installed on Computer5.

Which file should you modify on Computer5?

Options:

A- LiteTouch.wsf

B- SetupConfig.ini

C- Unattendb*

D- Unattend.xml

Answer:

B

Explanation:

SetupConfig.ini is a file that can be used to customize the behavior of Windows Setup during feature updates. You can use this file to specify commands or scripts that run before or after the installation process. To run a PowerShell script after a feature update, you can use the PostOOBE parameter in SetupConfig.ini and specify the path to the script file.Reference:[SetupConfig.ini reference]

Question 3

Question Type: MultipleChoice

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers.

You need to prevent users from disabling Microsoft Defender Antivirus,

What should you do?

Options:

A- From the Microsoft Intune admin center, create a security baseline.

B- From the Microsoft 365 Defender portal, enable tamper protection.

C- From the Microsoft Intune admin center, create an account protection policy.

D- From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.

Answer:

B

Explanation:

Tamper protection is a feature of Microsoft Defender Antivirus that prevents users or malicious software from disabling or modifying the antivirus settings. Tamper protection can be enabled from the Microsoft 365 Defender portal for devices that are Azure AD joined and enrolled in Microsoft Intune. This will prevent users from turning off Microsoft Defender Antivirus or changing its configuration through Windows Security, PowerShell, Registry, or Group Policy.Reference:[Enable tamper protection]

Question 4

Question Type: MultipleChoice

You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

Options:

A- 30 days

B- 60 days

C- 90 days

D- 365 days

Answer:

B

Explanation:

The Device compliance trends report shows the number of devices that are compliant, noncompliant, and not evaluated over time. The report displays trend data for the last 60 days by default, but you can change the time range to view data for the last 7, 14, or 30 days as well. The report does not show data for more than 60 days.Reference:[Device compliance trends report]

Question 5

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.

You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Options:

A- Enroll the devices in Microsoft Intune by using the Intune Company Portal.

B- Create a compliance policy.

C- Enroll the devices in Microsoft Intune by using Apple Business Manager.

D- Create an iOS app provisioning profile.

E- Create a device configuration profile.

Answer:

C, E

Explanation:

To deploy a specific iOS update to the unmanaged iPad devices, you need to perform the following actions:

Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices.You can also use Apple Business Manager to create device groups and assign roles and permissions12.

Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices.You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices34.

The other options are not correct for this scenario because:

Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune.However, this method requires user interaction and consent, and does not enroll the devices as supervised devices5.

Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings.However, a compliance policy does not deploy or manage software updates on the devices6.

Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune.However, an iOS app provisioning profile does not affect the software updates on the devices7.

Question 6

Question Type: **MultipleChoice**

You have an Azure subscription.

You have an on-premises Windows 11 device named Device 1.

You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription.

To what should you associate DCR1 ?

Options:

A- Azure Network Watcher

B- Device1

C- a Log Analytics workspace

D- a Monitored Object

Answer:

B

Explanation:

To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it.A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1.To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2.You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.

The other options are not correct for this scenario because:

Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources.It is not related to data collection rules or Azure Monitor4.

A Log Analytics workspace is a destination where you can send the data collected by a data collection rule.It is not an entity that you can associate a DCR with5.

A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules.

Question 7

Question Type: MultipleChoice

You have an Azure AD tenant named contoso.com.

You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.

What should you configure?

Options:

A- Windows Autopilot

B- provisioning packages for Windows

C- Security defaults in Azure AD

D- Device settings in Azure AD

Answer:

D

Explanation:

To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users.By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected1.

The other options are not relevant for this scenario because:

Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune.It does not control the local administrator role of the users who join the devices2.

Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process.They do not affect the Azure AD join process or the local administrator role of the users3.

Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks.They do not include any settings related to device management or local administrator role4.

Question 8

Question Type: MultipleChoice

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

* Ensure that you can manage the personal devices by using Microsoft Intune.

* Ensure that users can access company data seamlessly from their personal devices.

* Ensure that users can only sign in to their personal devices by using their personal account

What should you use to add the devices to Azure AD?

Options:

A- Azure AD registered

B- hybrid Azure AD join

C- AD joined

Answer:

A

Explanation:

To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization's resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account.Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.

The other options are not suitable for this scenario because:

Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD.Users can sign in to these devices by using their organizational account that exists in both directories2.

AD joined is for devices that are joined only to on-premises Active Directory.These devices are not managed by Microsoft Intune and do not have access to cloud resources3.