MD-102 Q&As

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You are creating a device configuration profile in Microsoft Intune. You need to configure specific OMA-URI settings in the profile. Which profile type template should you use?

A. Device restrictions (Windows 10 Team)

B. Identity protection

C. Custom

D. Device restrictions

Correct Answer: C

Windows client custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. These settings are typically used by mobile device manufacturers to control features on the device.

Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10

QUESTION 2

You have a Microsoft 365 tenant that contains the devices shown in the following table.

Name	Member of
Device1	Group1
Device2	Group1
Device3	Group1

The devices are managed by using Microsoft Intune.

You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the device security settings match the settings specified in the policy.

You discover that devices that are not members of Group1 are shown as Compliant.

You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not compliant.

What should you do from the Microsoft Intune admin center?

A. From Device compliance, configure the Compliance policy settings.

B. From Endpoint security, configure the Conditional access settings.

C. From Tenant administration, modify the Diagnostic settings.

D. From Policy1, modify the actions for noncompliance.

Correct Answer: A

There are two parts to compliance policies in Intune:

Compliance policy settings - Tenant-wide settings that are like a built-in compliance policy that every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that haven\\'t received any device compliance policies are compliant or noncompliant.

Device compliance policy - Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION 3

You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune.

You need to review the startup processes and how often each device restarts.

What should you use?

A. Endpoint analytics

B. Device Management

C. Azure Monitor

D. Intune Data Warehouse

Correct Answer: A

https://learn.microsoft.com/en-us/mem/analytics/restart-frequency

QUESTION 4

You have computers that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from the Windows event logs.

The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

A. 1 only

B. 2 and 3 only

C. 1 and 3 only

D. 1, 2, and 4 only

E. 1, 2, 3, and 4

Correct Answer: D

Collect Windows event log data sources with Log Analytics agent

Windows event logs are one of the most common data sources for Log Analytics agents on Windows virtual machines because many applications write to the Windows event log. You can collect events from standard logs, such as System

and Application, and any custom logs created by applications you need to monitor.

Incorrect:

Not 3: Not Security events.

Reference:

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events

QUESTION 5

You have a computer named Computer1 that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.

What should you do on Computer1?

A. Turn on Reputation-based protection

B. Enable Network Level Authentication (NLA)

C. Turn on Network Discovery

D. Configure the Remote Desktop Configuration service

Correct Answer: B

What is Network Level Authentication?

Network level authentication is used for authenticating Remote Desktop services, such as Windows RDP, and Remote Desktop Connection (RDP Client). You might also hear it called front authentication.

What is Network Level Authentication (NLA) used for?

Before you can start a remote desktop session, the user will need to authenticate themselves - ie, prove that they are who they say they are. Using network level authentication means that a false connection can\\'t be made, which would use

up CPU and cause a strain on the resources of the network. This offers a level of security against some cyberattacks such as Denial of Service attacks, where multiple requests are made all at once towards a network, overwhelming its ability

to cope. To combat this, you can turn on network level authentication to authenticate the user\\'s credentials before starting a remote access session. If the user\\'s credentials aren\\'t authenticated, then the connection is simply denied.

Reference:

https://www.atera.com/blog/what-is-network-level-authenticatio