MD-101$^{Q\&As}$

Managing Modern Desktops

Pass Microsoft MD-101 Exam with 100% Guarantee

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

https://www.geekcert.com/md-101.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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

You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.

From Microsoft Intune, you create a device configuration profile named Profile1.

You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.

Solution: You create an Azure Active Directory group that contains only the Windows 10 Enterprise devices. You assign Profile1 to the new group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You configure an applicability rule for Profile1. You assign Profile1 to Group1.

Note: Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile

assigned to devices running Windows Enterprise.

To do this task, create an applicability rule.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

QUESTION 2

You are currently making use of the Antimalware Assessment solution in Microsoft Azure Log Analytics. You have accessed the Protection Status dashboard and find that there is a device that is not reporting. Which of the following could be a reason for this occurring?

A. Windows Defender System Guard is incorrectly configured.

B. You need to install the Azure Diagnostic extension.

C. Windows Defender Application Guard is incorrectly configured.

D. The Microsoft Malicious Software Removal tool is installed.

Correct Answer: B

Azure Diagnostics extension is an agent in Azure Monitor that collects monitoring data from the guest operating system of Azure compute resources including virtual machines.

Note: As the Azure Diagnostic extension can only be used for Virtual Machines a better answer would be that the Microsoft Monitoring Agent (MMA) is missing.

Incorrect:

Not A: Windows Defender System Guard reorganizes the existing Windows 10 system integrity features under one roof and sets up the next set of investments in

Windows security. It\\'s designed to make these security guarantees:

Protect and maintain the integrity of the system as it starts up

Validate that system integrity has truly been maintained through local and remote attestation

Not C: For Microsoft Edge, Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the

Internet. As an enterprise administrator, you define what is among trusted web sites, cloud resources, and internal networks. Everything not on your list is considered untrusted. If an employee goes to an untrusted site through either Microsoft

Edge or Internet Explorer, Microsoft Edge opens the site in an isolated

Hyper-V-enabled container.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/diagnostics-extension-overview
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/tutorial-logs-dashboards

QUESTION 3

You have a Microsoft 365 tenant

You have devices enrolled in Microsoft intune.

You assign a conditional access policy nan-ted Policy1 to a group named Group1. Policy1 restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.

You need to identify which noncompliant devices attempt to access OneDrive for Business.

What should you do?

A. From the Microsoft Endpoint Manager admin center, review the Setting compliance report.

B. From the Microsoft Endpoint Manager admin center, review the Noncompliant devices reporter.

C. From the Microsoft Endpoint Manager admin center, review Device compliance report.

D. From the Azure Active Directory admin center, review the Conditional Access Insights and Reporting workbook.

Correct Answer: B

The Noncompliant devices report provides data typically used by Helpdesk or admin roles to identify problems and help remediate issues. The data found in this report is timely, calls out unexpected behavior, and is meant to be actionable.

Note: Compliance reports help you understand when devices fail to meet your compliance configurations and can help you identify compliance-related issues in your organization.

Open the compliance dashboard

Open the Intune Device compliance dashboard:

Sign in to the Microsoft Endpoint Manager admin center.

Select Devices > Overview > Compliance status tab.

When the dashboard opens, you get an overview with all the compliance reports. In these reports, you can see and check for:

Overall device compliance

Per-policy device compliance

Per-setting device compliance

Threat agent status

Device protection status

View compliance reports

In addition to using the charts on Compliance status, you can go to Reports > Device compliance.

Sign in to the Microsoft Endpoint Manager admin center. Select Devices > Monitor, and then from below Compliance select the report you want to view. Some of the available compliance reports include:

Device compliance

Noncompliant devices

Devices without compliance policy

Setting compliance

Policy compliance

Noncompliant policies (preview)

Windows health attestation report

Threat agent status

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor

QUESTION 4

Your on-premises network contains a database server and is accessible by using a VPN server.

You have a Microsoft 365 tenant.

You manage devices by using Microsoft Endpoint Manager.

You have an application named App1 that is deployed to every computer enrolled in Microsoft Intune. Each computer has a VPN profile assigned.

You need to ensure that App1 can access only the database server. App1 must be prevented from accessing other resources on the on-premises network.

What should you modify in the VPN profile?

A. Proxy

B. Network traffic rules

C. DNS Settings

D. Conditional Access

Correct Answer: B

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network

traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

A network security group contains zero, or as many rules as desired, within Azure subscription limits.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

QUESTION 5

You manage a Microsoft 365 environment that has co-management enabled.

All computers run Windows 10 and are deployed by using the Microsoft Deployment Toolkit (MDT).

You need to recommend a solution to deploy Microsoft Office 365 ProPlus to new computers. The latest version must always be installed. The solution must minimize administrative effort.

What is the best tool to use for the deployment? More than one answer choice may achieve the goal. Select the BEST answer.

A. Microsoft Intune

B. Microsoft Deployment Toolkit

C. Office Deployment Tool (ODT)

D. a Group Policy object (GPO)

E. Microsoft System Center Configuration Manager

Correct Answer: A

Intune --> Create device group --> Select o365 app --> deploy to group

ODT --> Download files -> create XML --> how to trigger install (manual install/MDT Task seq/powershell script/logon script etc)

SCCM --> create new package via ODT or via wizard --> select DPs to distribute -->deploy to collection

MDT --> requires ODT to have latest version, but is fastest with install as O365 is installed during TS, so at the end I would use this in production, but is not wat MS asks.

In the question it states the machines are in co-management, which indicates the presence of ConfigMgr and Intune otherwise machines cannot be co-managed. In configMgr there is a co-management workload you can move to Intune

specifically for Office 365 management. Office deployment and management from intune is by far the most simple way to deploy the Office apps (MS 365 Apps for business) .

https://docs.microsoft.com/en-us/mem/configmgr/comanage/workloads#office-click-to-run-apps

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365#select-microsoft-365-apps

MD-101 VCE Dumps MD-101 Study Guide MD-101 Braindumps