Vendor: Microsoft

Exam Code:MD-102

Exam Name: Endpoint Administrator

Version: Demo

QUESTION 1

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.

You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.

What should you do?

A. Onboard the macOS devices to the Microsoft Purview compliance portal.

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

C. Install Defender for Endpoint on the macOS devices.

D. From the Microsoft Intune admin center, create a configuration profile.

Correct Answer: D

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac On macOS 11 (Big Sur) and above, Microsoft Defender for Endpoint requires additional configuration profiles. If you are an existing customer upgrading from earlier versions of macOS, make sure to deploy the additional configuration profiles listed on New configuration profiles for macOS Big Sur and newer versions of macOS.

QUESTION 2

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.

Which three types of data can you collect from the computers by using Log Analytics? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. failure events from the Security log

B. the list of processes and their execution times

C. the average processor utilization

D. error events from the System log

E. third-party application logs stored as text files

Correct Answer: CDE

E: The Custom Logs data source for the Log Analytics agent in Azure Monitor allows you to collect events from text files on both Windows and Linux computers. Many applications log information to text files instead of standard logging services, such as Windows Event log or Syslog. After the data is collected, you can either parse it into individual fields in your queries or extract it during collection to individual fields.

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.

C: Summary of data sources The following table lists the agent data sources that are currently available with the Log Analytics agent. Each agent data source links to an article that provides information for that data source. It also provides information on their method and frequency of collection.

*

Performance counters Performance counters in Windows and Linux provide insight into the performance of hardware components, operating systems, and applications. Azure Monitor can collect performance counters from Log Analytics agents at frequent intervals for near real time analysis. Azure Monitor can also aggregate performance data for longer-term analysis and reporting.

*

Etc.

Log queries with performance records The following table provides different examples of log queries that retrieve performance records. Example, CPU utilization across all computers Query: Perf | where ObjectName == "Processor" and CounterName == "% Processor Time" and InstanceName == "_Total" | summarize AVGCPU = avg(CounterValue) by Computer Average

B: The following table lists the objects and counters that you can specify in the configuration file. More counters are available for certain applications.

*

Processor, % Processor Time

*

Processor, % User Time

*

Etc.

Incorrect:

Not A: Not from the Security log.

Important

You can\\'t configure collection of security events from the workspace by using the Log Analytics agent. You must use Microsoft Defender for Cloud or Microsoft Sentinel to collect security events. The Azure Monitor agent can also be used to

collect security events.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-custom-logs
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-performance-counters

---

QUESTION 3

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps.

You need to ensure that App1 is installed before App2 on every device.

What should you configure?

A. the App1 deployment configurations

B. a dynamic device group

C. a detection rule

D. the App2 deployment configurations

Correct Answer: D

Detection rules in Win32 apps are telling Intune how to tell if the application has been installed or not. Configure a dependency in the win32 app deployment screen even has this wording: "Software dependencies are applications that must be installed before this application can be installed"

Configure App1 first so that it\\'ll be selectable in the dependencies section

---

QUESTION 4

Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 10. Users in the finance department use the computers.

You have a computer named Computer1 that runs Windows 10.

From Computer1, you plan to run a script that executes Windows PowerShell commands on the finance department computers.

You need to ensure that you can run the PowerShell commands on the finance department computers from Computer.

What should you do on the finance department computers?

A. From Windows PowerShell, run the Enable-MMAgent cmdlet.

B. From the local Group Policy, enable the Allow Remote Shell Access setting.

C. From Windows PowerShell, run the Enable-PSRemoting cmdlet.

D. From the local Group Policy, enable the Turn on Script Execution setting.

Correct Answer: D

about_Group_Policy_Settings

Short description Describes the Group Policy settings for PowerShell Long description

PowerShell includes Group Policy settings to help you define consistent configuration values for Windows computers in an enterprise environment. The policies are as follows:

*

Turn on Script Execution: Sets the PowerShell execution policy.

*

Etc. (does not include Allow Remote Shell Access).

Note: Turn on script execution

The Turn on Script Execution policy setting sets the execution policy for computers and users. The execution policy determines whether to permit scripts to run.

If you enable the policy setting, you can select from among the following policy settings.

Allow only signed scripts allows scripts to execute only if they\\'re signed by a trusted publisher. This policy setting is equivalent to the AllSigned execution policy.

Allow local scripts and remote signed scripts allows all local scripts to run. Scripts that originate from the Internet must be signed by a trusted publisher. This policy setting is equivalent to the RemoteSigned execution policy.

Allow all scripts allows all scripts to run. This policy setting is equivalent to the Unrestricted execution policy.

If you disable this policy setting, no scripts are allowed to run. This policy setting is equivalent to the Restricted execution policy.

If you don\\'t configure this policy setting, the execution policy that\\'s set for the computer or user by the Set-ExecutionPolicy cmdlet determines whether scripts are permitted to run. The default value is Restricted.

Reference:

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_group_policy_settings

---

QUESTION 5

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10.

On Computer1, you need to run the Invoke-Command cmdlet to execute several PowerShell commands on Computer2.

What should you do first?

A. On Computer2, run the Enable-PSRemoting cmdlet.

B. On Computer2, add Computer1 to the Remote Management Users group.

C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computer2.

D. On Computer1, run the New-PSSession cmdlet.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting

---

QUESTION 6

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:

1.

For the WinRM service, set Startup type to Automatic.

2.

Create a listener that accepts requests from any IP address.

3.

Enable a firewall exception for WS-Management communications. Which PowerShell cmdlet should you use?

A. Connect-WSMan

B. Enable-PSRemoting

C. Invoke-WSManAction

D. Enable-PSSessionConfiguration

Correct Answer: B

The Enable-PSRemoting cmdlet configures the computer to receive PowerShell remote commands that are sent by using the WS-Management technology. WS-Management based PowerShell remoting is currently supported only on Windows platform.

The Enable-PSRemoting cmdlet performs the following operations:

*

Runs the Set-WSManQuickConfig cmdlet, which performs the following tasks:

Starts the WinRM service.

Sets the startup type on the WinRM service to Automatic.

Creates a listener to accept requests on any IP address.

Enables a firewall exception for WS-Management communications.

Creates the simple and long name session endpoint configurations if needed.

Enables all session configurations.

Changes the security descriptor of all session configurations to allow remote access.

*

Restarts the WinRM service to make the preceding changes effective.

Reference:

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting

---

QUESTION 7

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to review the startup times and restart frequencies of the devices.

What should you use?

A. Azure Monitor

B. Intune Data Warehouse

C. Microsoft Defender for Endpoint

D. Endpoint analytics

Correct Answer: D

Restart frequency in endpoint analytics.

In endpoint analytics startup performance, we\\'ve provided insights into PC boot times, and how to improve the reboot times of poorly performing devices. Reboot frequency can be just as impactful to the user experience since a device that

reboots daily because of Stop errors will have a poor user experience even if the boot times are fast. We\\'ve recently added insights into restart frequencies within your organization to help you identify problematic devices.

Prerequisites

Devices are enrolled in endpoint analytics.

Enroll Configuration Manager devices

Enroll Intune devices

After enrollment, client devices require a restart to fully enable all analytics.

Etc.

Reference:

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

---

QUESTION 8

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You need to enable self-service password reset on the sign-in screen.

Which settings should you configure from the Microsoft Intune admin center?

A. Device configuration

B. Device enrollment

C. Conditional access

D. Device compliance

Correct Answer: A

To enable the self service password reset option with Intune.

Use the Azure portal to create a new configuration policy. Open Microsoft Intune, choose Device Configuration, Profiles and Create profile.

Reference:

https://www.inthecloud247.com/enable-self-service-password-reset-feature-on-the-windows-logon-screen/

QUESTION 9

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?

A. 30 days

B. 60 days

C. 90 days

D. 365 days

Correct Answer: B

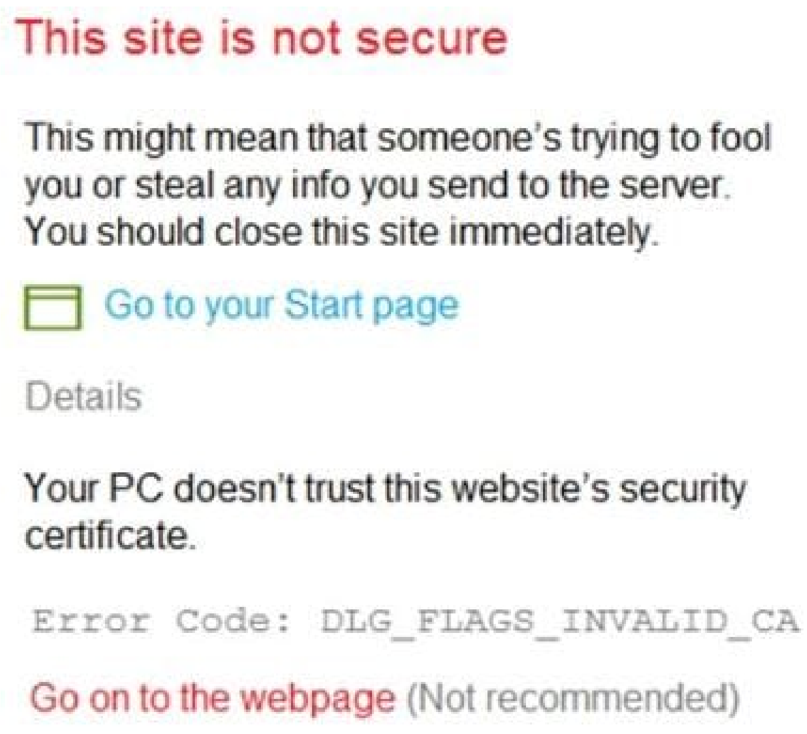
https://learn.microsoft.com/en-us/mem/intune/fundamentals/reports#device-compliance-trends-report-historical

---

QUESTION 10

You use Windows Admin Center to remotely administer computers that run Windows 10.

When connecting to Windows Admin Center, you receive the message shown in the following exhibit.



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

Go on to the webpage (Not recommended)

You need to prevent the message from appearing when you connect to Windows Admin Center. To which certificate store should you import the certificate?

A. Client Authentication Issuers

B. Personal

C. Trusted Root Certification Authorities

Correct Answer: C

"Error Code: DLG_FLAGS_INVALID_CA" while login to Admin Console after enabling HTTPS in PowerCenter.

Solution

To resolve this issue, add the CA-signed certificates to the "Trusted Root Certification Authorities" in the browser. After adding the certificates, restart the browser.

Reference:

https://knowledge.informatica.com/s/article/578585

QUESTION 11

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.

You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.

Which extension should you select for the app package file?

A. .intunemac

B. .ipa

C. .apk

D. .appx

Correct Answer: B

Add an iOS/iPadOS line-of-business app to Microsoft Intune

Step 1 - App information

Select the app package file

In the Add app pane, click Select app package file.

In the App package file pane, select the browse button. Then, select an iOS/iPadOS installation file with the extension .ipa. The app details will be displayed.

When you\\'re finished, select OK on the App package file pane to add the app.

Etc.

Reference:

https://learn.microsoft.com/en-us/mem/intune/apps/lob-apps-ios

---

QUESTION 12

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to deploy and manage Windows devices.

You have 100 devices from users that left your company.

You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

A. Deploy a new configuration profile to the devices.

B. Perform a Windows Autopilot reset on the devices.

C. Perform an in-place upgrade on the devices.

D. Perform a clean installation of Windows 11 on the devices.

Correct Answer: B

Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

Removes personal files, apps, and settings.

Reapplies a device\\'s original settings.

Sets the region, language, and keyboard to the original values.

Maintains the device\\'s identity connection to Azure AD.

Maintains the device\\'s management connection to Intune.

The Windows Autopilot Reset process automatically keeps information from the existing device:

Wi-Fi connection details.

Provisioning packages previously applied to the device.

A provisioning package present on a USB drive when the reset process is started.

Azure Active Directory device membership and MDM enrollment information.

SCEP certificates.

Windows Autopilot Reset blocks the user from accessing the desktop until this information is restored, including reapplying any provisioning packages. For devices enrolled in an MDM service, Windows Autopilot Reset also blocks until an

MDM sync is completed. When Autopilot reset is used on a device, the device\\'s primary user is removed. The next user who signs in after the reset will be set as the primary user.

Reference:

https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset