Vendor: McAfee

Exam Code:MA0-107

Exam Name: McAfee Certified Product Specialist - ENS

Version: Demo

QUESTION 1

A security professional is configuring ENS for a client and wants to ensure applications will be prevented from executing software locally from the browser or email client. Which of the following McAfee-defined rules should be implemented?

A. Creating new executable files in the Windows folder

B. Installing browser helper objects or shell extensions

C. Registering programs to autorun

D. Running files from common user folders by common programs

Correct Answer: B

QUESTION 2

The network operations team has configured the company\\'s VPN connector to deny connectivity if virus scan definitions are older than seven days. In order for a user to immediately meet the VPN connector\\'s policy, which of the following should the administrator enable?

A. Managed custom tasks

B. "Update now" button

C. Default client update task schedule

D. Proxy server

Correct Answer: A

QUESTION 3

For which of the following reasons does ENS 10 store two previous versions of AMCore content?

A. To allow for content rollback if it is needed

B. To allow for comparison of detections between content versions

C. To allow for backup when an Extra.DAT is deployed

D. To allow for choice of which content to scan a file against

Correct Answer: C

QUESTION 4

An administrator wants to add executables that are monitored with the Exploit Prevention engine. To which of the following policy sections should the executables be added?

A. Generic privilege escalation prevention

B. Exclusions

C. Signatures

D. Application protection rules

Correct Answer: A

QUESTION 5

While tuning the firewall policy, the ePO administrator notices unauthorized traffic is being initiated by a file transfer utility application. If this is a recently approved application, in which of the following locations should this be configured to allow FTP traffic only with this application?

A. Add a new rule within the Access Protection policy to block port 21 and exclude the executable for the software.

B. Put a new rule in the Exploit Prevention policy to include the executable for the software for additional protection.

C. Exclude the process associated with the software within the On Access Scan policy\\'s Low-Risk Processes section.

D. Create an allow rule within the Rules policy for inbound/outbound on port 21 and the executable for the software.

Correct Answer: A

QUESTION 6

Which of the following is the benefit of a TIE server with regard to the Adaptive Threat Protection module?

A. It communicates with McAfee GTI for file and certificate reputation for malicious code.

B. It is required, and the Adaptive Threat Protection will only work with the TIE server.

C. The Threat Protection cache flushes when the reputation rules change.

D. The stored file and certificate reputations are locally stored, making the remediation automatically quicker.

Correct Answer: A

QUESTION 7

When planning for a policy migration, in which of the following circumstances should automatic migration be used, rather than manual migration?

A. When fine-tuning assignments

B. When migrating smaller environments

C. When migrating settings to single-platform policies

D. When using multiple custom policies

Correct Answer: D

QUESTION 8

In which of the following locations are the installation log files stored by default on a Windows machine?

A. %TEMP%\McAfeeLogs

B. %PROGRAMDATA%\McAfee\Logs

C. %USERDATA%\McAfeeLogFiles

D. %PROGRAMFILES%\CommonFiles\McAfeeLogs

Correct Answer: C

QUESTION 9

If the ePO server\\'s access to the Internet is allowed, which of the following options would the administrator have to check in the McAfee ENS Migration Assistant extension?

A. Software Manager

B. Server Client Package Install

C. Master Repository

D. Workstation Client Package Install

Correct Answer: C

QUESTION 10

In Web Control, "Enable Web Category blocking of restricted content" is enforced. Which of the following describes the result if a user enters a restricted site?

A. The color is gray, and access is denied.

B. The pop-up color is red, and access is denied.

C. The color is orange, and access is denied.

D. The pop-up color is blue, and access denied.

Correct Answer: C

QUESTION 11

An administrator notices that on one endpoint, Threat Prevention is not currently on the latest version of AMContent. The administrator presses the "Update Now" button within the console, but a message shows the update was unsuccessful.

Which of the following logs should the administrator look at FIRST to troubleshoot the failure?

A. EndpointSecurityPlatform_Activity.log

B. ThreatPrevention_Activity.bg

C. AccessProtection_Activity.log

D. PackageManager_Activity.log

Correct Answer: D

QUESTION 12

Joe, an administrator, runs a policy-based, on-demand scan on a system and notices that after the scan, a threat event was created for what appears to be a false positive. Joe wants to submit the file for analysis to McAfee Labs; but every time he accesses the file, it is detected.

In which of the following default locations can Joe find the backups of the detected files?

A. %ProgramData%\McAfee\Common Framework\AgentEvents

B. C:\Quarantine

C. C:\Windows\Temp\Quarantine

D. %deflogfir%\Quarantine

Correct Answer: A