MA0-107 Q&As

McAfee Certified Product Specialist - ENS

Pass McAfee MA0-107 Exam with 100% Guarantee

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

https://www.leads4pass.com/ma0-107.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

If a TIE server is unavailable and the system is connected to the Internet, which of the following components can the Adaptive Threat Protection leverage for reputation decisions?

A. Event Security Manager

B. Global Threat Intelligence

C. Data Exchange Layer

D. Advanced Threat Defense

Correct Answer: B

QUESTION 2

Which of the following groups of legacy products can be migrated to ENS 10.5?

A. VirusScan Enterprise, Host Intrusion Prevention, and SiteAdvisor Enterprise

B. Host Intrusion Prevention, SiteAdvisor Enterprise, and Data Loss Prevention

C. VirusScan Enterprise, Host Intrusion Prevention, and Data Loss Prevention

D. Host Intrusion Prevention, SiteAdvisor Enterprise, and Application Control

Correct Answer: C

QUESTION 3

An IT department is looking for a way to optimize performance with on-access scanning. To maximize security and minimize the impact on the system, on-access scanning should be configured to scan files at which of the following frequencies?

A. Disable on-access scanning.

B. Let McAfee decide.

C. Only scan files on write.

D. Only scan files on read.

Correct Answer: C

QUESTION 4

A hospital in another county just received a new variant of ransom ware that infected 70% of its systems. After learning the characteristics of this ransom ware, the security team wants to implement a protection policy to stop certain files

from being modified and new registry keys from being created that are relevant to the ransom ware. Which of the following policies meets this requirement?

A. Exploit prevention policy

B. Block and allow list policy

C. Access protection policy

D. Firewall rules policy

Correct Answer: C

QUESTION 5

An ePO administrator decides to define a trusted network in the firewall policy. This will result in:

A. an inbound directional allow rule for that remote network.

B. an outbound directional allow rule for that remote network.

C. a bidirectional allow rule for that remote network.

D. a bidirectional deny rule for that remote network.

Correct Answer: A

QUESTION 6

The security team has requested that adaptive threat protection be integrated with a TIE server. Which of the following is required?

A. Data Exchange Layer

B. Advanced Threat Defense

C. Event Security Manager

D. Active Response

Correct Answer: A

QUESTION 7

An ePO administrator is experiencing issues installing an ENS module on a client machine and decides to investigate by analyzing the install log. In which of the following locations will the administrator find the install log, assuming it is in its default location on the endpoint?

A. %programdata%\mcafee\datreputation\logs

B. **\program files\mcafee\

C. %temp%\mcafeelogs

D. %programdata%\mcafee\Agent\logs

Correct Answer: D

QUESTION 8

An administrator suspects that Self Protection is preventing local installation of a patch. Which of the following log levels should the administrator review?

A. Event logging

B. Debug logging

C. Activity logging

D. High severity logging

Correct Answer: D

QUESTION 9

Which of the following items are sent to the cloud when Real Protect scanning is enabled on endpoints that are connected to the Internet?

A. System information

B. Running process

C. Behavioral information

D. File reputation

Correct Answer: B

QUESTION 10

Organizational security policy requires a host-based firewall on endpoints. Some endpoints have applications where documentation depicting network traffic flows is not readily available. Which of the following ENS 10.5 firewall features should be used to develop rules for their firewall policy?

A. Location-aware Groups

B. Trusted Networks

C. Trusted Executables

D. Adaptive Mode

Correct Answer: B

QUESTION 11

An administrator wants to exclude folder ABC on various drives. In which of the following ways should the administrator list the exclusion in the policy?

A. ??\ABC

B. **\ABC

C. ***\ABC

D. ???\ABC

Correct Answer: C

QUESTION 12

The security team wants to schedule an on-demand scan to run at noon every day for all workstations. However, the team would like to ensure system performance is not impacted because users may be working. Which of the following is a system utilization setting that meets this criteria?

A. Below normal

B. Low

C. Scan only when the system is idle

D. Normal

Correct Answer: D

QUESTION 13

A user goes to four different websites, each with a different rating. One of the four sites is blocked and unable to be accessed. Using default configuration to determine the rating, which of the following ratings does this site have?

A. Gray

B. Red

C. Yellow

D. Green

Correct Answer: A

QUESTION 14

When configuring the Adaptive Threat Protection Options policy, which of the following is a rule assignment group that

needs to be selected to accommodate an environment consisting of high-change systems with frequent installations and updates of trusted software?

A. Adaptive

B. Productivity

C. Balanced

D. Security

Correct Answer: D

QUESTION 15

The ePO administrators have already tuned and configured dynamic application containment rules within the policy. In which of the following ways will dynamic application containment protect against malware once enforcement is enabled?

A. The scan engine will learn the behavior of the application and send up to GT1 for analysis, and then receive an action to block all actions from the application\\'s process.

B. If an application\\'s reputation is below the threshold while triggering a block rule and is not an excluded application, malicious behavior of the application will be contained.

C. The ENS client will receive the reputation as "highly suspicious" from either the McAfee GTI or TIE server, and then immediately uninstall the application on the system.

D. The adaptive threat protection scanner will send the file automatically to a preconfigured "Sandbox" folder and analyze the application for malicious features before use.

Correct Answer: B