McAfee

Exam MA0-103

McAfee Certified Product Specialist - DLPE

Verson: Demo

[Total Questions: 10]

Question No : 1

Which of the following is a potential indicator of an issue with the DLP Endpoint client?

A. Multiple FCAGTE processes are present in the Task Manager
B. Multiple FCAG processes are present in the Task Manager
C. FCAGSD process is present in the Task Manager
D. FCAGTE is running as a user instead of the System account in the Task Manager

Answer: B

Question No : 2

Which of the following is an indication of potential data loss?

A. Removable Storage Device rule triggers a lot of incidents for one user
B. Removable Storage File Access rule triggers a lot of incidents for one user
C. Discovery rule triggers a lot of incidents for one user
D. Removable Storage Protection rule triggers a lot of incidents for one user

Answer: D

Question No : 3

What result types are supported in a McAfee DLPe query?

A. Properties and Events
B. Roles and permissions
C. User data
D. Protection status

Answer: A

Question No : 4

Which of the following is NOT a DLPe incident task?

A. Mail notification task
B. Purge task
C. Set reviewer task
D. Purge client task

Answer: D

Question No : 5

Which of the following is NOT a proactive approach to preventing performance issues?

A. Adding exclusions for security and indexing software
B. Removing unnecessary applications and application definitions from the policy
C. Disabling unused modules in Agent Configuration
D. Running a File System Discovery Scan

Answer: D

Question No : 6

There is a known virus spreading using removable media. What action should be taken to mitigate this risk?

A. Monitor all removable media devices
B. Enable McAfee endpoint encryption controls
C. Block all removable media devices
D. Make plug and play devices read only

Answer: C

Question No : 7

What does DLP Endpoint client use to send operational events and incidents to ePO?

A. DLPe Windows Communication Foundation (WCF) service
B. McAfee Agent
C. ePO Event Parser
D. DLP Endpoint Event Parser

Answer: B

Question No : 8

By default, McAfee DLP will copy evidence to its configured share using which of the following accounts?

A. ePO Service Account
B. MCAFEE AGENT ACCOUNT
C. NETWORK SERVICE
D. Pre-defined service account

Answer: C

Question No : 9

Following production deployment the DLP Endpoint Administrator begins to receive an increasing number of calls related to credit card number content detection false positives. Which of the following can the administrator do to reduce false positives?

A. Turn on verbose logging
B. Increase dictionary weights
C. Increase text pattern thresholds
D. Use regular expression validators

Answer: D

Question No : 10

What must be deployed to all target computers before an endpoint policy can be

distributed?

A. A Policy Analyzer
B. A DLP global policy
C. The McAfee DLPe extension
D. A supported version of McAfee Agent

Answer: D