Symantec

250-438 Exam

Administration of Symantec Data Loss Prevention 15 Exam

Questions & Answers
Demo

Version: 8.0

Question: 1

How should a DLP administrator change a policy so that it retains the original file when an endpoint incident has detected a “cope to USB device” operation?

A. Add a “Limit Incident Data Retention” response rule with “retain Original Message” option selected.
B. Modify the agent config.db to include the file
C. Modify the “Endpoint_Retain_Files.int” setting in the Endpoint server configuration
D. Modify the agent configuration and select the option “retain Original Files”

Answer: A

Question: 2

What is the correct configuration for “BoxMonitor.Channels” that will allow the server to start as a Network Monitor server?

A. Packet Capture, Span Port
B. Packet Capture, Network Tap
C. Packet Capture, Copy Rule
D. Packet capture, Network Monitor

Answer: C

Question: 3

Under the “System Overview” in the Enforce management console, the status of a Network Monitor detection server is shown as “Running Selected.” The Network Monitor server’s event logs indicate that the packet capture and filereader processes are crashing.
What is a possible cause for the Network Monitor server being in this state?

A. There is insufficient disk space on the Network Monitor server.
B. The Network Monitor server’s certificate is corrupt or missing.
C. The Network Monitor server’s license file has expired.
D. The Enforce and Network Monitor servers are running different versions of DLP.

Answer: D

Question: 4

Which two Infrastructure-as-a-Service providers are supported for hosting Cloud Prevent for Office 365? (Choose two.)

A. Any customer-hosted private cloud
B. Amazon Web Services
C. AT&T
D. Verizon
E. Rackspace

Answer: B,E

Question: 5

A DLP administrator has enabled and successfully tested custom attribute lookups for incident data based on the Active Directory LDAP plugin. The Chief Information Security Officer (CISO) has attempted to generate a User Risk Summary report, but the report is empty. The DLP administrator confirms the Cisco's role has the "User Reporting" privilege enabled, but User Risk reporting is still not working.
What is the probable reason that the User Risk Summary report is blank?

A. Only DLP administrators are permitted to access and view data for high risk users.
B. The Enforce server has insufficient permissions for importing user attributes.
C. User attribute data must be configured separately from incident data attributed.
D. User attributes have been incorrectly mapped to Active Directory accounts.

Answer: D

Question: 6

How should a DLP administrator exclude a custom endpoint application named "custom_app.exe" from being monitoring by Application File Access Control?

A. Add "custom_app.exe" to the "Application Whitelist" on all Endpoint servers.
B. Add "custom_app.exe" Application Monitoring Configuration and de-select all its channel options.
C. Add "custom_app_.exe" as a filename exception to the Endpoint Prevent policy.
D. Add "custom_app.exe" to the "Program Exclusion List" in the agent configuration settings.

Answer: A

Question: 7

A software company wants to protect its source code, including new source code created between scheduled indexing runs.

Which detection method should the company use to meet this requirement?

A. Exact Data Matching (EDM)
B. Described Content Matching (DCM)
C. Vector Machine Learning (VML)
D. Indexed Document Matching (IDM)

Answer: D