Vendor: Symantec

Exam Code:250-438

Exam Name: Administration of Symantec Data Loss Prevention 15

Version: Demo

QUESTION 1

A DLP administrator has performed a test deployment of the DLP 15.0 Endpoint agent and now wants to uninstall the agent. However, the administrator no longer remembers the uninstall password. What should the administrator do to work around the password problem?

A. Apply a new global agent uninstall password in the Enforce management console.

B. Manually delete all the Endpoint agent files from the test computer and install a new agent package.

C. Replace the PGPsdk.dll file on the agent\\'s assigned Endpoint server with a copy from a different Endpoint server

D. Use the UninstallPwdGenerator to create an UninstallPasswordKey.

Correct Answer: D

QUESTION 2

A compliance officer needs to understand how the company is complying with its data security policies over time. Which report should be compliance officer generate to obtain the compliance information?

A. Policy report, filtered on date and summarized by policy

B. Policy Trend report, summarized by policy, then quarter

C. Policy report, filtered on quarter and summarized by policy

D. Policy Trend report, summarized by policy, then severity

Correct Answer: A

QUESTION 3

What is the correct order for data in motion when a customer has integrated their CloudSOC and DLP solutions?

A. User > CloudSOC Gatelet > DLP Cloud Detection Service > Application

B. User > Enforce > Application

C. User > Enforce > CloudSOC > Application

D. User > CloudSOC Gatelet > Enforce > Application

Correct Answer: C

QUESTION 4

What detection method utilizes Data Identifiers?

A. Indexed Document Matching (IDM)

B. Described Content Matching (DCM)

C. Directory Group Matching (DGM)

D. Exact Data Matching (EDM)

Correct Answer: D

Reference: https://www.symantec.com/connect/forums/edm-policy-exception

---

QUESTION 5

How do Cloud Detection Service and the Enforce server communicate with each other?

A. Enforce initiates communication with Cloud Detection Service, which is expecting connections on port 8100.

B. Cloud Detection Service initiates communication with Enforce, which is expecting connections on port 443.

C. Cloud Detection Service initiates communication with Enforce, which is expecting connections on port 1443.

D. Enforce initiates communication with Cloud Detection Service, which is expecting connections on port 443.

Correct Answer: D

QUESTION 6

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

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.TECH218980.html

---

QUESTION 7

Why would an administrator set the Similarity Threshold to zero when testing and tuning a Vector Machine Learning (VML) profile?

A. To capture the matches to the Positive set

B. To capture the matches to the Negative set

C. To see the false negatives only

D. To see the entire range of potential matches

Correct Answer: D

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v45067125_v120691346/Adjusting-the-Similarity-Threshold?locale=EN_US

QUESTION 8

Which two factors are common sources of data leakage where the main actor is well-meaning insider? (Choose two.)

A. An absence of a trained incident response team

B. A disgruntled employee for a job with a competitor

C. Merger and Acquisition activities

D. Lack of training and awareness

E. Broken business processes

Correct Answer: BD

QUESTION 9

A customer needs to integrate information from DLP incidents into external Governance, Risk and Compliance dashboards.

Which feature should a third party component integrate with to provide dynamic reporting, create custom incident remediation processes, or support business processes?

A. Export incidents using the CSV format

B. Incident Reporting and Update API

C. Incident Data Views

D. A Web incident extraction report

Correct Answer: B

QUESTION 10

Which server target uses the "Automated Incident Remediation Tracking" feature in Symantec DLP?

A. Exchange

B. File System

C. Lotus Notes

D. SharePoint

Correct Answer: B

Reference: https://help.symantec.com/cs/DLP15.0/DLP/v83981880_v120691346/Troubleshooting-automated-incident-remediation-tracking?locale=EN_US

QUESTION 11

A DLP administrator is attempting to add a new Network Discover detection server from the Enforce management console. However, the only available options are Network Monitor and Endpoint servers. What should the administrator do to make the Network Discover option available?

A. Restart the Symantec DLP Controller service

B. Apply a new software license file from the Enforce console

C. Install a new Network Discover detection server

D. Restart the Vontu Monitor Service

Correct Answer: C

QUESTION 12

When managing an Endpoint Discover scan, a DLP administrator notices some endpoint computers are NOT completing their scans. When does the DLP agent stop scanning?

A. When the agent sends a report within the "Scan Idle Timeout" period

B. When the endpoint computer is rebooted and the agent is started

C. When the agent is unable to send a status report within the "Scan Idle Timeout" period

D. When the agent sends a report immediately after the "Scan Idle Timeout" period

Correct Answer: C