Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

https://www.2passeasy.com/dumps/250-438/

NEW QUESTION 1
What are two reasons an administrator should utilize a manual configuration to determine the endpoint location? (Choose two.)

A. To specify Wi-Fi SSID names
B. To specify an IP address or range
C. To specify the endpoint server
D. To specify domain names
E. To specify network card status (ON/OFF)

Answer: BD

Explanation:
Reference: https://help.symantec.com/cs/dlp15.1/DLP/v18349332_v125428396/Setting-the-endpoint-location?locale=EN_US

NEW QUESTION 2
Which two locations can Symantec DLP scan and perform Information Centric Encryption (ICE) actions on? (Choose two.)

A. Exchange
B. Jiveon
C. File store
D. SharePoint
E. Confluence

Answer: CD

Explanation:
Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/information-centric-encryption-en.pdf

NEW QUESTION 3
Which channel does Endpoint Prevent protect using Device Control?

A. Bluetooth
B. USB storage
C. CD/DVD
D. Network card

Answer: B

Explanation:
Reference: https://support.symantec.com/en_US/article.HOWTO80865.html#v36651044

NEW QUESTION 4
A DLP administrator needs to stop the PacketCapture process on a detection server. Upon inspection of the Server Detail page, the administrator discovers that all processes are missing from the display. What are the processes missing from the Server Detail page display?

A. The Display Process Control setting on the Advanced Settings page is disabled.
B. The Advanced Process Control setting on the System Settings page is deselected.
C. The detection server Display Control Process option is disabled on the Server Detail page.
D. The detection server PacketCapture process is displayed on the Server Overview page.

Answer: B

Explanation:
Reference: https://support.symantec.com/content/unifiedweb/en_US/article.TECH220250.html

NEW QUESTION 5
What detection technology supports partial contents matching?

A. Indexed Document Matching (IDM)
B. Described Content Matching (DCM)
C. Exact Data Matching (EDM)
D. Optical Character Recognition (OCR)

Answer: A

Explanation:
Reference: https://help.symantec.com/cs/dlp15.1/DLP/v115965297_v125428396/Mac-agent-detection-technologies?locale=EN_US

NEW QUESTION 6
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)

Answer: D

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

NEW QUESTION 7
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

Answer: C

NEW QUESTION 8
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

Answer: C

NEW QUESTION 9
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

Answer: C

NEW QUESTION 10
Which detection server is available from Symantec as a hardware appliance?

A. Network Prevent for Email
B. Network Discover
C. Network Monitor
D. Network Prevent for Web

Answer: D

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122938258_v120691346/Setting-up-the-DLP-S500-Appliance?locale=EN_US

NEW QUESTION 10
Which Network Prevent action takes place when the Network Incident list shows the message is “Modified”?

A. Remove attachments from an email
B. Obfuscate text in the body of an email
C. Add one or more SMTP headers to an email
D. Modify content from the body of an email

Answer: C

NEW QUESTION 13
Why is it important for an administrator to utilize the grid scan feature?

A. To distribute the scan workload across multiple network discover servers
B. To distribute the scan workload across the cloud servers
C. To distribute the scan workload across multiple endpoint servers
D. To distribute the scan workload across multiple detection servers

Answer: D

Explanation:
If you plan to use the grid scanning feature to distribute the scanning workload across multiple detection servers, retain the default value (1)

NEW QUESTION 16
Which two Network Discover/Cloud Storage targets apply Information Centric Encryption as policy response rules?

A. Microsoft Exchange
B. Windows File System
C. SQL Databases
D. Microsoft SharePoint
E. Network File System (NFS)

Answer: AD

NEW QUESTION 18
What detection technology supports partial row matching?

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

Answer: D

Explanation:
Reference: https://www.slideshare.net/iftikhariqbal/technology-overview-symantec-data-loss-prevention-dlp

NEW QUESTION 19
A DLP administrator created a new agent configuration for an Endpoint server. However, the endpoint agents fail to receive the new configuration. What is one possible reason that the agent fails to receive the new configuration?

A. The new agent configuration was saved but not applied to any endpoint groups.
B. The new agent configuration was copied and modified from the default agent configuration.
C. The default agent configuration must be disabled before the new configuration can take effect.
D. The Endpoint server needs to be recycled so that the new agent configuration can take effect.

Answer: C

NEW QUESTION 21
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 250-438 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 250-438 Product From:

https://www.2passeasy.com/dumps/250-438/

Money Back Guarantee

250-438 Practice Exam Features:

* 250-438 Questions and Answers Updated Frequently

* 250-438 Practice Questions Verified by Expert Senior Certified Staff

* 250-438 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 250-438 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year