

250-438 Dumps

Administration of Symantec Data Loss Prevention 15

<https://www.certleader.com/250-438-dumps.html>



NEW QUESTION 1

How should a DLP administrator change a policy so that it retains the original file when an endpoint incident has detected a “copy 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

NEW 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

Explanation:

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

NEW QUESTION 3

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: BE

NEW QUESTION 4

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 attributes.
- D. User attributes have been incorrectly mapped to Active Directory accounts.

Answer: D

NEW QUESTION 5

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

Explanation:

Reference: https://help.symantec.com/cs/DLP15.0/DLP/v100774847_v120691346/Scheduling-remote-indexing?locale=EN_US

NEW QUESTION 6

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 7

Which detection method depends on “training sets”?

- A. Form Recognition
- B. Vector Machine Learning (VML)
- C. Index Document Matching (IDM)
- D. Exact Data Matching (EDM)

Answer: B

Explanation:

Reference: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-dlp_machine_learning.WP_en-us.pdf

NEW QUESTION 8

Which action should a DLP administrator take to secure communications between an on-premises Enforce server and detection servers hosted in the Cloud?

- A. Use the built-in Symantec DLP certificate for the Enforce Server, and use the “sslkeytool” utility to create certificates for the detection servers.
- B. Use the built-in Symantec DLP certificate for both the Enforce server and the hosted detection servers.
- C. Set up a Virtual Private Network (VPN) for the Enforce server and the hosted detection servers.
- D. Use the “sslkeytool” utility to create certificates for the Enforce server and the hosted detection servers.

Answer: A

Explanation:

Reference: <https://www.symantec.com/connect/articles/sslkeytool-utility-and-server-certificates>

NEW QUESTION 9

A divisional executive requests a report of all incidents generated by a particular region, summarized by department. What does the DLP administrator need to configure to generate this report?

- A. Custom attributes
- B. Status attributes
- C. Sender attributes
- D. User attributes

Answer: A

NEW QUESTION 10

What is Application Detection Configuration?

- A. The Cloud Detection Service (CDS) process that tells Enforce a policy has been violated
- B. The Data Loss Prevention (DLP) policy which has been pushed into Cloud Detection Service (CDC) for files in transit to or residing in Cloud apps
- C. The terminology describing the Data Loss Prevention (DLP) process within the CloudSOC administration portal
- D. The setting configured within the user interface (UI) that determines whether CloudSOC should send a file to Cloud Detection Service (CDS) for analysis.

Answer: A

Explanation:

Reference: https://help.symantec.com/cs/DLP15.0/DLP/v119805091_v120691346/About-Application-Detection%7CSymantec%EF%BF%BD-Data-Loss-Prevention-15.0?locale=EN_US

NEW QUESTION 10

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 12

A DLP administrator is testing Network Prevent for Web functionality. When the administrator posts a small test file to a cloud storage website, no new incidents are reported. What should the administrator do to allow incidents to be generated against this file?

- A. Change the “Ignore requests Smaller Than” value to 1
- B. Add the filename to the Inspect Content Type field
- C. Change the “PacketCapture.DISCARD_HTTP_GET” value to “false”
- D. Uncheck trial mode under the ICAP tab

Answer: A

Explanation:

Reference: https://help.symantec.com/cs/dlp15.0/DLP/id-SF0B0161467_v120691346/Configuring-Network-Prevent-for-Web-Server?locale=EN_US

NEW QUESTION 14

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

Answer: A

NEW QUESTION 16

An organization wants to restrict employees to copy files only a specific set of USB thumb drives owned by the organization. Which detection method should the organization use to meet this requirement?

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

Answer: D

NEW QUESTION 17

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

Answer: D

Explanation:

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

NEW QUESTION 22

Which two detection technology options ONLY run on a detection server? (Choose two.)

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

Answer: BD

Explanation:

Reference: https://support.symantec.com/en_US/article.INFO5070.html

NEW QUESTION 26

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 28

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 31

A DLP administrator is preparing to install Symantec DLP and has been asked to use an Oracle database provided by the Database Administration team. Which SQL *Plus command should the administrator utilize to determine if the database is using a supported version of Oracle?

- A. select database version from <database name>;

- B. select * from db\$version;
- C. select * from v\$version;
- D. select db\$ver from <database name>;

Answer: C

Explanation:

Reference: <https://www.symantec.com/connect/forums/new-install-oracle-returns-error>

NEW QUESTION 35

Which service encrypts the message when using a Modify SMTP Message response rule?

- A. Network Monitor server
- B. SMTP Prevent
- C. Enforce server
- D. Encryption Gateway

Answer: D

Explanation:

Reference: <https://www.symantec.com/connect/articles/network-prevent>

NEW QUESTION 38

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 250-438 Exam with Our Prep Materials Via below:

<https://www.certleader.com/250-438-dumps.html>