

Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

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



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

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 3

Which product is able to replace a confidential document residing on a file share with a marker file explaining why the document was removed?

- A. Network Discover
- B. Cloud Service for Email
- C. Endpoint Prevent
- D. Network Protect

Answer: D

Explanation:

Reference: https://help.symantec.com/cs/dlp15.1/DLP/v15600645_v125428396/Configuring-Network-Protect-for-file-shares?locale=EN_US

NEW QUESTION 4

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 5

Which two detection technology options run on the DLP agent? (Choose two.)

- A. Optical Character Recognition (OCR)
- B. Described Content Matching (DCM)
- C. Directory Group Matching (DGM)
- D. Form Recognition
- E. Indexed Document Matching (IDM)

Answer: BE

NEW QUESTION 6

What is the default fallback option for the Endpoint Prevent Encrypt response rule?

- A. Block
- B. User Cancel
- C. Encrypt
- D. Notify

Answer: D

NEW QUESTION 7

Which two components can perform a file system scan of a workstation? (Choose two.)

- A. Endpoint Server
- B. DLP Agent
- C. Network Prevent for Web Server
- D. Discover Server
- E. Enforce Server

Answer: BD

NEW QUESTION 8

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 9

Which two detection servers are available as virtual appliances? (Choose two.)

- A. Network Monitor
- B. Network Prevent for Web
- C. Network Discover
- D. Network Prevent for Email
- E. Optical Character Recognition (OCR)

Answer: BD

Explanation:

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v123002905_v120691346/About-DLP-Appliances?locale=EN_US

NEW 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

Answer: B

Explanation:

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

NEW QUESTION 10

An administrator is unable to log in to the Enforce management console as “sysadmin”. Symantec DLP is configured to use Active Directory authentication. The administrator is a member of two roles: “sysadmin” and “remediator.” How should the administrator log in to the Enforce console with the “sysadmin” role?

- A. sysadmin\username
- B. sysadmin\username@domain
- C. domain\username
- D. username\sysadmin

Answer: C

NEW QUESTION 12

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 16

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 18

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 20

Which two technologies should an organization utilize for integration with the Network Prevent products? (choose two.)

- A. Network Tap
- B. Network Firewall
- C. Proxy Server
- D. Mail Transfer Agent
- E. Encryption Appliance

Answer: CD

Explanation:

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

NEW QUESTION 21

What should an incident responder select in the Enforce management console to remediate multiple incidents simultaneously?

- A. Smart Response on the Incident page
- B. Automated Response on the Incident Snapshot page
- C. Smart Response on an Incident List report
- D. Automated Response on an Incident List report

Answer: B

NEW QUESTION 24

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 25

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 27

Where should an administrator set the debug levels for an Endpoint Agent?

- A. Setting the log level within the Agent List
- B. Advanced configuration within the Agent settings
- C. Setting the log level within the Agent Overview
- D. Advanced server settings within the Endpoint server

Answer: C

Explanation:

Reference: https://support.symantec.com/en_US/article.TECH248581.html

NEW QUESTION 31

Which two automated response rules will be active in policies that include Exact Data Matching (EDM) detection rule? (Choose two.)

- A. Endpoint Discover: Quarantine File
- B. All: Send Email Notification
- C. Endpoint Prevent: User Cancel
- D. Endpoint Prevent: Block
- E. Network Protect: Quarantine File

Answer: AD

NEW QUESTION 35

.....

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