250-438 Q&As

Administration of Symantec Data Loss Prevention 15

Pass Symantec 250-438 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/250-438.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers

QUESTION 1

A DLP administrator is checking the System Overview in the Enforce management console, and all of the detection servers are showing as "unknown". The Vontu services are up and running on the detection servers. Thousands of .IDC files are building up in the Incidents directory on the detection servers. There is good network connectivity between the detection servers and the Enforce server when testing with the telnet command.

How should the administrator bring the detection servers to a running state in the Enforce management console?

A. Restart the Vontu Update Service on the Enforce server

B. Ensure the Vontu Monitor Controller service is running in the Enforce server

C. Delete all of the .BAD files in the Incidents folder on the Enforce server

D. Restart the Vontu Monitor Service on all the affected detection servers

Correct Answer: B

QUESTION 2

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

Correct Answer: C

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

QUESTION 3

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 4

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 5

Which two actions are available for a "Network Prevent: Remove HTTP/HTTPS content" response rule when the content is unable to be removed? (Choose two.)

A. Allow the content to be posted

B. Remove the content through FlexResponse

C. Block the content before posting

D. Encrypt the content before posting

E. Redirect the content to an alternative destination

Correct Answer: AE

[Latest 250-438 Dumps](#) [250-438 VCE Dumps](#) [250-438 Braindumps](#)