

250-438 Dumps

Administration of Symantec Data Loss Prevention 15

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



NEW QUESTION 1

What detection server is used for Network Discover, Network Protect, and Cloud Storage?

- A. Network Protect Storage Discover
- B. Network Discover/Cloud Storage Discover
- C. Network Prevent/Cloud Detection Service
- D. Network Protect/Cloud Detection Service

Answer: B

Explanation:

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v16110606_v120691346/Modifying-the-Network-Discover-Cloud-Storage-Discover-Server-configuration?locale=EN_US

NEW QUESTION 2

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 3

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 4

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 5

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 6

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 7

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

Answer: AE

NEW QUESTION 8

What is required on the Enforce server to communicate with the Symantec DLP database?

- A. Port 8082 should be opened
- B. CryptoMasterKey.properties file
- C. Symbolic links to .dbf files
- D. SQL*Plus Client

Answer: D

Explanation:

Reference: <https://www.symantec.com/connect/articles/three-tier-installation-dlp-product>

NEW QUESTION 9

Which option is an accurate use case for Information Centric Encryption (ICE)?

- A. The ICE utility encrypts files matching DLP policy being copied from network share through use of encryption keys.
- B. The ICE utility encrypts files matching DLP policy being copied to removable storage through use of encryption keys.
- C. The ICE utility encrypts files matching DLP policy being copied to removable storage on an endpoint use of certificates.
- D. The ICE utility encrypts files matching DLP policy being copied from network share through use of certificates

Answer: B

Explanation:

Reference: https://help.symantec.com/cs/ICE1.0/ICE/v126756321_v120576779/Using-ICE-with-Symantec-Data-Loss-Preventionabout_dlp?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 10

Which action is available for use in both Smart Response and Automated Response rules?

- A. Log to a Syslog Server
- B. Limit incident data retention
- C. Modify SMTP message
- D. Block email message

Answer: D

NEW QUESTION 11

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

Answer: B

NEW QUESTION 12

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 17

Where in the Enforce management console can a DLP administrator change the "UI.NO_SCAN.int" setting to disable the "Inspecting data" pop-up?

- A. Advanced Server Settings from the Endpoint Server Configuration
- B. Advanced Monitoring from the Agent Configuration
- C. Advanced Agent Settings from the Agent Configuration
- D. Application Monitoring from the Agent Configuration

Answer: C

Explanation:

Reference: <https://www.symantec.com/connect/forums/dlp-pop-examining-content>

NEW QUESTION 19

What is the Symantec recommended order for stopping Symantec DLP services on a Windows Enforce server?

- A. Vontu Notifier, Vontu Incident Persister, Vontu Update, Vontu Manager, Vontu Monitor Controller
- B. Vontu Update, Vontu Notifier, Vontu Manager, Vontu Incident Persister, Vontu Monitor Controller
- C. Vontu Incident Persister, Vontu Update, Vontu Notifier, Vontu Monitor Controller, Vontu Manager.
- D. Vontu Monitor Controller, Vontu Incident Persister, Vontu Manager, Vontu Notifier, Vontu Update.

Answer: D

Explanation:

Reference: https://help.symantec.com/cs/dlp15.1/DLP/v23042736_v125428396/Stopping-an-Enforce-Server-on-Windows?locale=EN_US

NEW QUESTION 24

.....

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>