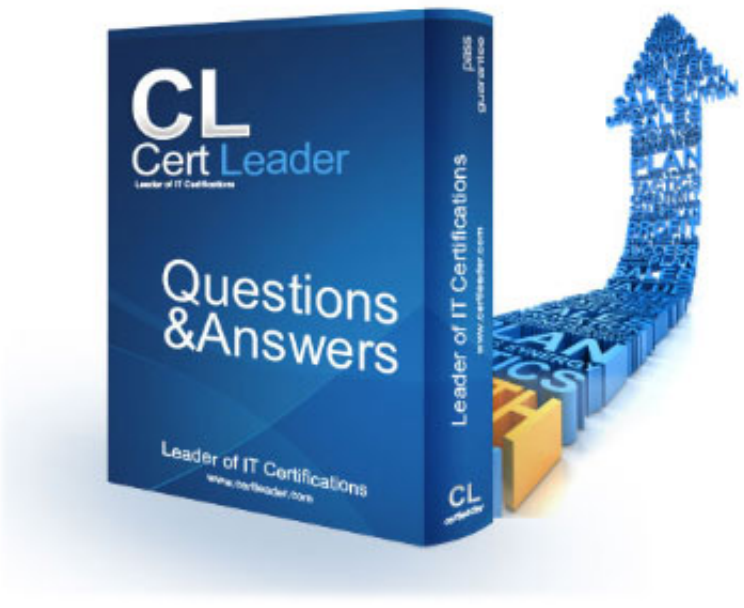
250-438 Dumps

Administration of Symantec Data Loss Prevention 15

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



NEW QUESTION 1
Under the “System Overview” in the Enforce management console, the status of a Network Monitor detection server is shown as “Running Selected.” The Network Monitor server’s event logs indicate that the packet capture and filereader processes are crashing.
What is a possible cause for the Network Monitor server being in this state?

A. There is insufficient disk space on the Network Monitor server.
B. The Network Monitor server’s certificate is corrupt or missing.
C. The Network Monitor server’s license file has expired.
D. The Enforce and Network Monitor servers are running different versions of DLP.

Answer: D

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 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 4
Which option correctly describes the two-tier installation type for Symantec DLP?

A. Install the Oracle database on the host, and install the Enforce server and a detection server on a second host.
B. Install the Oracle database on a local physical host, and install the Enforce server and detection servers on virtual hosts in the Cloud.
C. Install the Oracle database and a detection server in the same host, and install the Enforce server on a second host.
D. Install the Oracle database and Enforce server on the same host, and install detection servers on separate hosts.

Answer: D

Explanation:
Reference: https://www.symantec.com/connect/forums/deployment-enforce-and-detection-servers

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

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 8
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 9
A company needs to secure the content of all Mergers and Acquisitions Agreements However, the standard text included in all company literature needs to be excluded. How should the company ensure that this standard text is excluded from detection?

A. Create a Whitelisted.txt file after creating the Vector Machine Learning (VML) profile.
B. Create a Whitelisted.txt file after creating the Exact Data Matching (EDM) profile
C. Create a Whitelisted.txt file before creating the Indexed Document Matching (IDM) profile
D. Create a Whitelisted.txt file before creating the Exact Data Matching (EDM) profile

Answer: C

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v27161240_v120691346/White-listing-file-contents-to-exclude-from-partial-matching?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
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 13
Which statement accurately describes where Optical Character Recognition (OCR) components must be installed?

A. The OCR engine must be installed on detection server other than the Enforce server.
B. The OCR server software must be installed on one or more dedicated (non-detection) Linux servers.
C. The OCR engine must be directly on the Enforce server.
D. The OCR server software must be installed on one or more dedicated (non-detection) Windows servers.

Answer: C

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122760174_v120691346/Setting-up-OCR-Servers?locale=EN_US

NEW QUESTION 17
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 19
What detection server type requires a minimum of two physical network interface cards?

A. Network Prevent for Web
B. Network Prevent for Email
C. Network Monitor
D. Cloud Detection Service (CDS)

Answer: A

NEW QUESTION 21
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 25
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.

Answer: D

NEW QUESTION 26
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 29
.....

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