Symantec

Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

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
How should a DLP administrator exclude a custom endpoint application named “custom_app.exe” from being monitoring by Application File Access Control?

A. Add “custom_app.exe” to the “Application Whitelist” on all Endpoint servers.
B. Add “custom_app.exe” Application Monitoring Configuration and de-select all its channel options.
C. Add “custom_app_.exe” as a filename exception to the Endpoint Prevent policy.
D. Add “custom_app.exe” to the “Program Exclusion List” in the agent configuration settings.

Answer: A

Explanation:
Reference: https://docs.mcafee.com/bundle/data-loss-prevention-11.0.400-product-guide-epolicy-orchestrator/page/GUID-0F81A895-0A46-4FF8-A869-0365D6620185.html

NEW QUESTION 3
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 4
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 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
A DLP administrator has added several approved endpoint devices as exceptions to an Endpoint Prevent policy that blocks the transfer of sensitive data. However, data transfers to these devices are still being blocked. What is the first action an administrator should take to enable data transfers to the approved endpoint devices?

A. Disable and re-enable the Endpoint Prevent policy to activate the changes
B. Double-check that the correct device ID or class has been entered for each device
C. Verify Application File Access Control (AFAC) is configured to monitor the specific application
D. Edit the exception rule to ensure that the “Match On” option is set to “Attachments”

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 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 9
Which two DLP products support the new Optical Character Recognition (OCR) engine in Symantec DLP 15.0? (Choose two.)

A. Endpoint Prevent
B. Cloud Service for Email
C. Network Prevent for Email
D. Network Discover
E. Cloud Detection Service

Answer: BC

NEW QUESTION 10
Which two factors are common sources of data leakage where the main actor is well-meaning insider? (Choose two.)

A. An absence of a trained incident response team
B. A disgruntled employee for a job with a competitor
C. Merger and Acquisition activities
D. Lack of training and awareness
E. Broken business processes

Answer: BD

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 11
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)

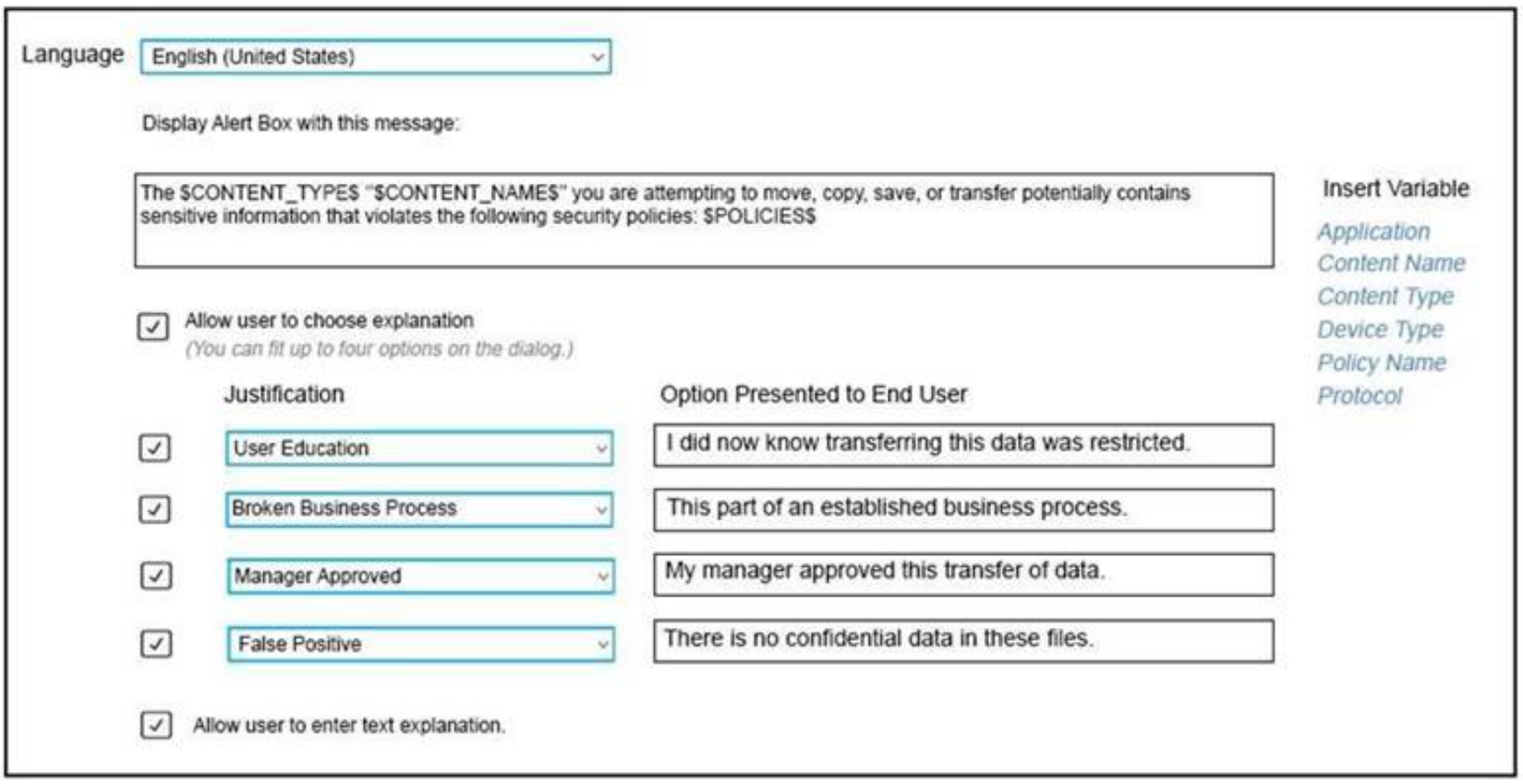
Answer: D

NEW QUESTION 13
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 14
Refer to the exhibit. Which type of Endpoint response rule is shown?



A. Endpoint Prevent: User Notification
B. Endpoint Prevent: Block
C. Endpoint Prevent: Notify
D. Endpoint Prevent: User Cancel

Answer: B

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v27595430_v120691346/Configuring-the-Endpoint-Prevent:-Block-action?locale=EN_US

NEW QUESTION 15
Which Network Prevent action takes place when the Network Incident list shows the message is “Modified”?

A. Remove attachments from an email
B. Obfuscate text in the body of an email
C. Add one or more SMTP headers to an email
D. Modify content from the body of an email

Answer: C

NEW QUESTION 17
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 21
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 22
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 24
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 29
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 34
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 37
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 41
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 42
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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