Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

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

NEW QUESTION 1
Which two Infrastructure-as-a-Service providers are supported for hosting Cloud Prevent for Office 365? (Choose two.)

A. Any customer-hosted private cloud
B. Amazon Web Services
C. AT&T
D. Verizon
E. Rackspace

Answer: BE

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
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 5
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 6
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 7
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 8
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 9
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 10
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 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 13
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 14
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 15
A DLP administrator is testing Network Prevent for Web functionality. When the administrator posts a small test file to a cloud storage website, no new incidents are reported. What should the administrator do to allow incidents to be generated against this file?

A. Change the “Ignore requests Smaller Than” value to 1
B. Add the filename to the Inspect Content Type field
C. Change the “PacketCapture.DISCARD_HTTP_GET” value to “false”
D. Uncheck trial mode under the ICAP tab

Answer: A

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/id-SF0B0161467_v120691346/Configuring-Network-Prevent-for-Web-Server?locale=EN_US

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

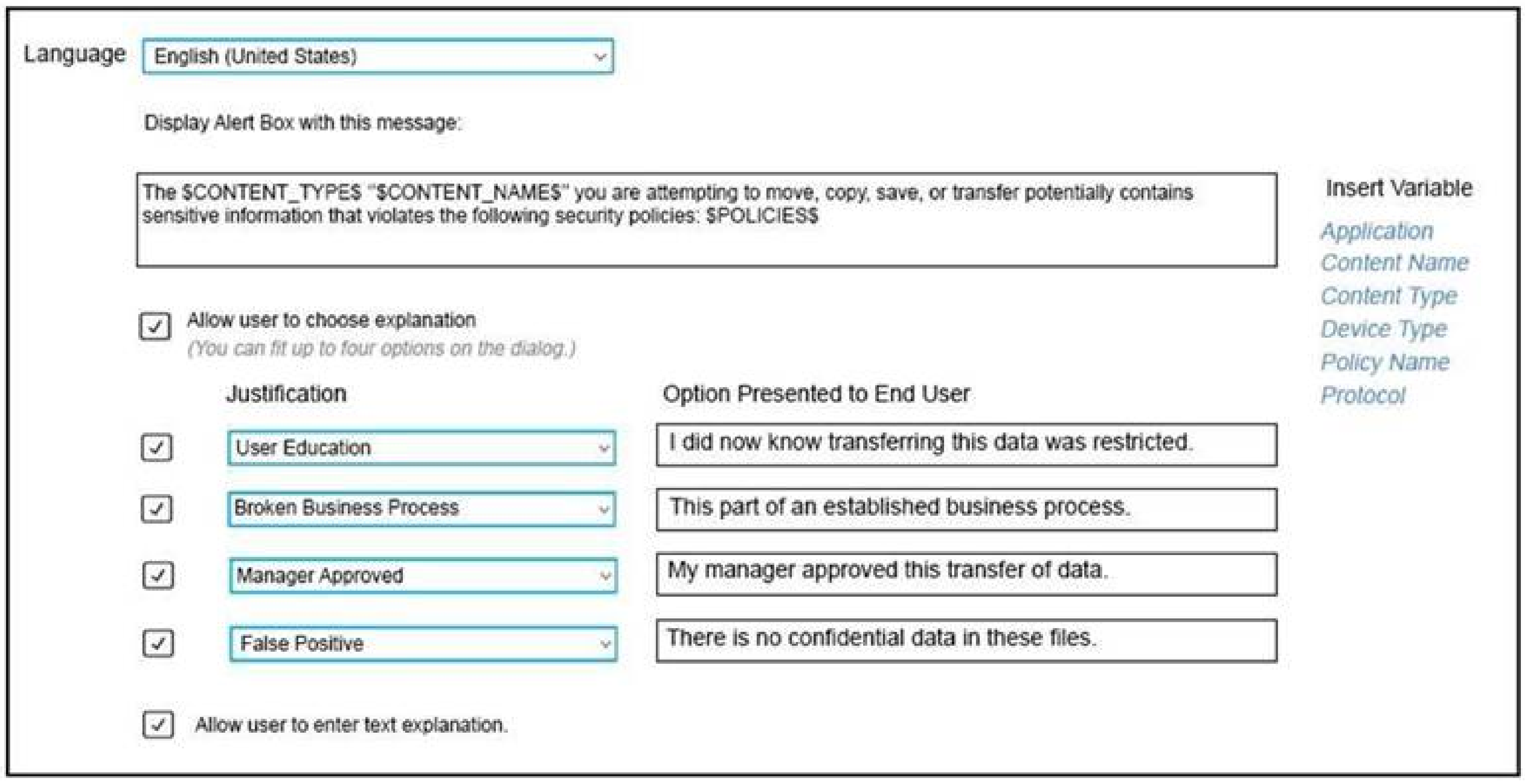
NEW QUESTION 17
Which detection server is available from Symantec as a hardware appliance?

A. Network Prevent for Email
B. Network Discover
C. Network Monitor
D. Network Prevent for Web

Answer: D

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122938258_v120691346/Setting-up-the-DLP-S500-Appliance?locale=EN_US

NEW QUESTION 20
Refer to the exhibit. Which type of Endpoint response rule is shown?



Language: English (United States)

Display Alert Box with this message:

The $CONTENT_TYPES "$CONTENT_NAME$" you are attempting to move, copy, save, or transfer potentially contains sensitive information that violates the following security policies: $POLICIES$

Insert Variable
Application
Content Name
Content Type
Device Type
Policy Name
Protocol

☑ Allow user to choose explanation
(You can fit up to four options on the dialog.)

	Justification	Option Presented to End User
☑	User Education	I did now know transferring this data was restricted.
☑	Broken Business Process	This part of an established business process.
☑	Manager Approved	My manager approved this transfer of data.
☑	False Positive	There is no confidential data in these files.

☑ Allow user to enter text explanation.

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 24
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 27
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 29
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 31
Which two detection technology options ONLY run on a detection server? (Choose two.)

A. Form Recognition
B. Indexed Document Matching (IDM)
C. Described Content Matching (DCM)
D. Exact Data Matching (EDM)
E. Vector Machine Learning (VML)

Answer: BD

Explanation:
Reference: https://support.symantec.com/en_US/article.INFO5070.html

NEW QUESTION 36
A DLP administrator needs to remove an agent its associated events from an Endpoint server.
Which Agent Task should the administrator perform to disable the agent’s visibility in the Enforce management console?

A. Delete action from the Agent Health dashboard
B. Delete action from the Agent List page
C. Disable action from Symantec Management Console
D. Change Endpoint Server action from the Agent Overview page

Answer: C

NEW QUESTION 38
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 40
Which two Network Discover/Cloud Storage targets apply Information Centric Encryption as policy response rules?

A. Microsoft Exchange
B. Windows File System
C. SQL Databases
D. Microsoft SharePoint
E. Network File System (NFS)

Answer: AD

NEW QUESTION 45
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 46
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 49
......