Symantec

Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

NEW QUESTION 1
What is the correct configuration for “BoxMonitor.Channels” that will allow the server to start as a Network Monitor server?

A. Packet Capture, Span Port
B. Packet Capture, Network Tap
C. Packet Capture, Copy Rule
D. Packet capture, Network Monitor

Answer: C

Explanation:
Reference: https://support.symantec.com/en_US/article.TECH218980.html

NEW QUESTION 2
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 3
A DLP administrator has enabled and successfully tested custom attribute lookups for incident data based on the Active Directory LDAP plugin. The Chief Information Security Officer (CISO) has attempted to generate a User Risk Summary report, but the report is empty. The DLP administrator confirms the Cisco’s role has the “User Reporting” privilege enabled, but User Risk reporting is still not working.
What is the probable reason that the User Risk Summary report is blank?

A. Only DLP administrators are permitted to access and view data for high risk users.
B. The Enforce server has insufficient permissions for importing user attributes.
C. User attribute data must be configured separately from incident data attributes.
D. User attributes have been incorrectly mapped to Active Directory accounts.

Answer: D

NEW QUESTION 4
What are two reasons an administrator should utilize a manual configuration to determine the endpoint location? (Choose two.)

A. To specify Wi-Fi SSID names
B. To specify an IP address or range
C. To specify the endpoint server
D. To specify domain names
E. To specify network card status (ON/OFF)

Answer: BD

Explanation:
Reference: https://help.symantec.com/cs/dlp15.1/DLP/v18349332_v125428396/Setting-the-endpoint-location?locale=EN_US

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 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 8
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 9
An administrator is unable to log in to the Enforce management console as “sysadmin”. Symantec DLP is configured to use Active Directory authentication. The administrator is a member of two roles: “sysadmin” and “remediator.” How should the administrator log in to the Enforce console with the “sysadmin” role?

A. sysadmin\username
B. sysadmin\username@domain
C. domain\username
D. username\sysadmin

Answer: C

NEW QUESTION 10
Which tool must a DLP administrator run to certify the database prior to upgrading DLP?

A. Lob_Tablespace Reclamation Tool
B. Upgrade Readiness Tool
C. SymDiag
D. EnforceMigrationUtility

Answer: B

Explanation:
Reference: https://support.symantec.com/en_US/article.DOC10667.html

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 12
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 14
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 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 21
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 25
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 30
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 32
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 36
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 38
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 40
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 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 49
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 53
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 54
......