

# Symantec

## Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15



#### NEW QUESTION 1

How should a DLP administrator change a policy so that it retains the original file when an endpoint incident has detected a “copy to USB device” operation?

- A. Add a “Limit Incident Data Retention” response rule with “Retain Original Message” option selected.
- B. Modify the agent config.db to include the file
- C. Modify the “Endpoint\_Retain\_Files.int” setting in the Endpoint server configuration
- D. Modify the agent configuration and select the option “Retain Original Files”

**Answer:** A

#### NEW QUESTION 2

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 3

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 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 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 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

A divisional executive requests a report of all incidents generated by a particular region, summarized by department. What does the DLP administrator need to configure to generate this report?

- A. Custom attributes
- B. Status attributes
- C. Sender attributes
- D. User attributes

**Answer:** A

#### NEW QUESTION 8

A DLP administrator needs to stop the PacketCapture process on a detection server. Upon inspection of the Server Detail page, the administrator discovers that all processes are missing from the display. What are the processes missing from the Server Detail page display?

- A. The Display Process Control setting on the Advanced Settings page is disabled.
- B. The Advanced Process Control setting on the System Settings page is deselected.
- C. The detection server Display Control Process option is disabled on the Server Detail page.
- D. The detection server PacketCapture process is displayed on the Server Overview page.

**Answer:** B

#### Explanation:

Reference: [https://support.symantec.com/content/unifiedweb/en\\_US/article.TECH220250.html](https://support.symantec.com/content/unifiedweb/en_US/article.TECH220250.html)

#### NEW QUESTION 9

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](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 10

What detection method utilizes Data Identifiers?

- A. Indexed Document Matching (IDM)
- B. Described Content Matching (DCM)
- C. Directory Group Matching (DGM)
- D. Exact Data Matching (EDM)

**Answer:** D

#### Explanation:

Reference: <https://www.symantec.com/connect/forums/edm-policy-exception>

#### NEW QUESTION 10

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](https://help.symantec.com/cs/dlp15.0/DLP/v123002905_v120691346/About-DLP-Appliances?locale=EN_US)

#### NEW QUESTION 14

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](https://help.symantec.com/cs/dlp15.0/DLP/v27161240_v120691346/White-listing-file-contents-to-exclude-from-partial-matching?locale=EN_US)

**NEW QUESTION 18**

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](https://support.symantec.com/en_US/article.DOC10667.html)

**NEW QUESTION 21**

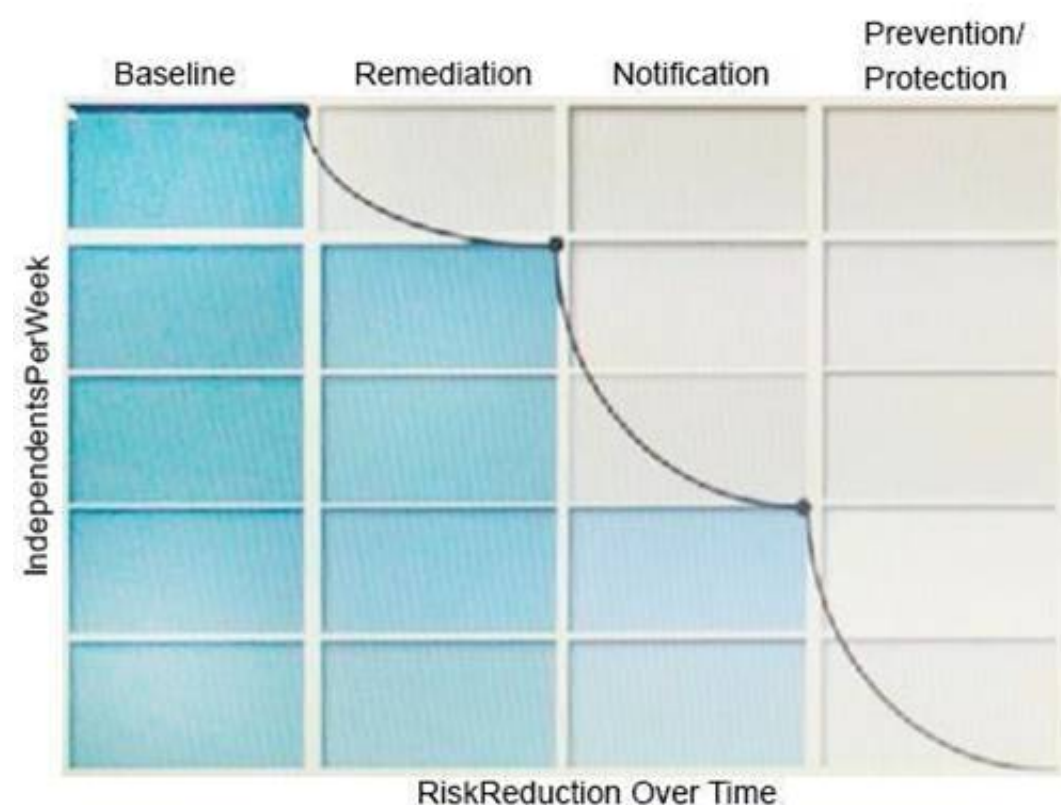
What is the correct order for data in motion when a customer has integrated their CloudSOC and DLP solutions?

- 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 24**

Refer to the exhibit.



What activity should occur during the baseline phase, according to the risk reduction model?

- A. Define and build the incident response team
- B. Monitor incidents and tune the policy to reduce false positives
- C. Establish business metrics and begin sending reports to business unit stakeholders
- D. Test policies to ensure that blocking actions minimize business process disruptions

**Answer: C**

**NEW QUESTION 25**

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](https://help.symantec.com/cs/ICE1.0/ICE/v126756321_v120576779/Using-ICE-with-Symantec-Data-Loss-Preventionabout_dlp?locale=EN_US)

**NEW QUESTION 30**

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

**NEW QUESTION 33**

DRAG DROP

The Symantec Data Loss risk reduction approach has six stages.

Drag and drop the six correct risk reduction stages in the proper order of Occurrence column.

Select and Place:

| Risk Reduction Stages | Order of Occurrence |
|-----------------------|---------------------|
| Notification          |                     |
| Planning              |                     |
| Migration             |                     |
| Prevention            |                     |
| Deployment            |                     |
| Remediation           |                     |
| Baseline              |                     |
| Development           |                     |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference: <https://www.slideshare.net/iftikhariqbal/symantec-data-loss-prevention-technical-proposal-general>

**NEW QUESTION 37**

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 40**

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 43**

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 48

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 53

A DLP administrator is checking the System Overview in the Enforce management console, and all of the detection servers are showing as “unknown”. The Vontu services are up and running on the detection servers. Thousands of .IDC files are building up in the Incidents directory on the detection servers. There is good network connectivity between the detection servers and the Enforce server when testing with the telnet command. How should the administrator bring the detection servers to a running state in the Enforce management console?

- A. Restart the Vontu Update Service on the Enforce server
- B. Ensure the Vontu Monitor Controller service is running in the Enforce server
- C. Delete all of the .BAD files in the Incidents folder on the Enforce server
- D. Restart the Vontu Monitor Service on all the affected detection servers

**Answer:** B

#### NEW QUESTION 56

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 60

A DLP administrator is preparing to install Symantec DLP and has been asked to use an Oracle database provided by the Database Administration team. Which SQL \*Plus command should the administrator utilize to determine if the database is using a supported version of Oracle?

- A. select database version from <database name>;
- B. select \* from db\$version;
- C. select \* from v\$version;
- D. select db\$ver from <database name>;

**Answer:** C

#### Explanation:

Reference: <https://www.symantec.com/connect/forums/new-install-oracle-returns-error>

#### NEW QUESTION 64

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 66

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 71**

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

#### **NEW QUESTION 73**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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 First Try
- \* 250-438 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 250-438 Practice Test Here](#)**