# 250-438$^{\text{Q\&As}}$

Administration of Symantec Data Loss Prevention 15

## Pass Symantec 250-438 Exam with 100% Guarantee

Following Questions and Answers are all new published by Symantec Official Exam Center

**QUESTION 1**

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

Correct Answer: D

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v45067125_v120691346/Adjusting-the-Similarity-Threshold?locale=EN_US

**QUESTION 2**

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

Correct Answer: C

**QUESTION 3**

Which two actions are available for a "Network Prevent: Remove HTTP/HTTPS content" response rule when the content is unable to be removed? (Choose two.)

A. Allow the content to be posted

B. Remove the content through FlexResponse

C. Block the content before posting

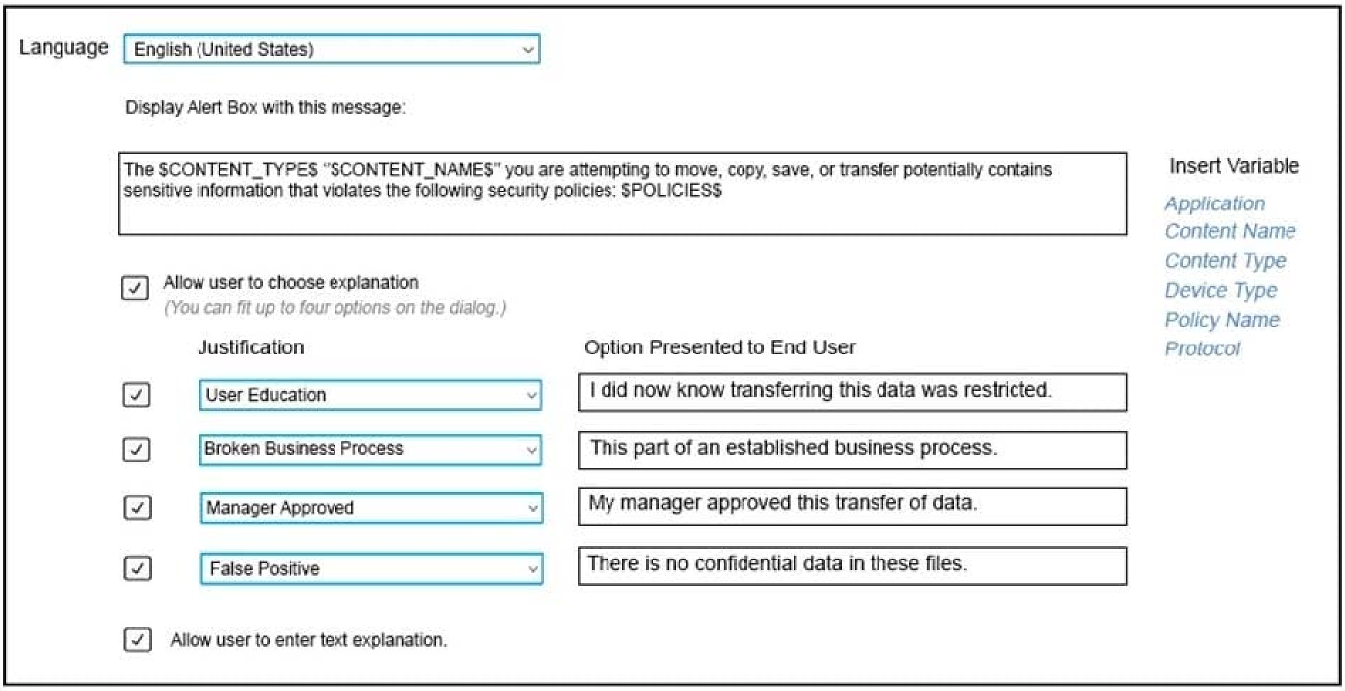
D. Encrypt the content before posting

E. Redirect the content to an alternative destination

Correct Answer: AE

**QUESTION 4**

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

☑ 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

Correct Answer: B

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

**QUESTION 5**

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

Correct Answer: B

**QUESTION 6**

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)

Correct Answer: D

Reference: https://help.symantec.com/cs/DLP15.0/DLP/v100774847_v120691346/Scheduling-remote-indexing?locale=EN_US

**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)

Correct Answer: A

Reference: https://help.symantec.com/cs/dlp15.1/DLP/v115965297_v125428396/Mac-agent-detection-technologies?locale=EN_US

**QUESTION 8**

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"

Correct Answer: D

**QUESTION 9**

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 ;

B. select * from db$version;

C. select * from v$version;

D. select db$ver from ;

Correct Answer: C

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

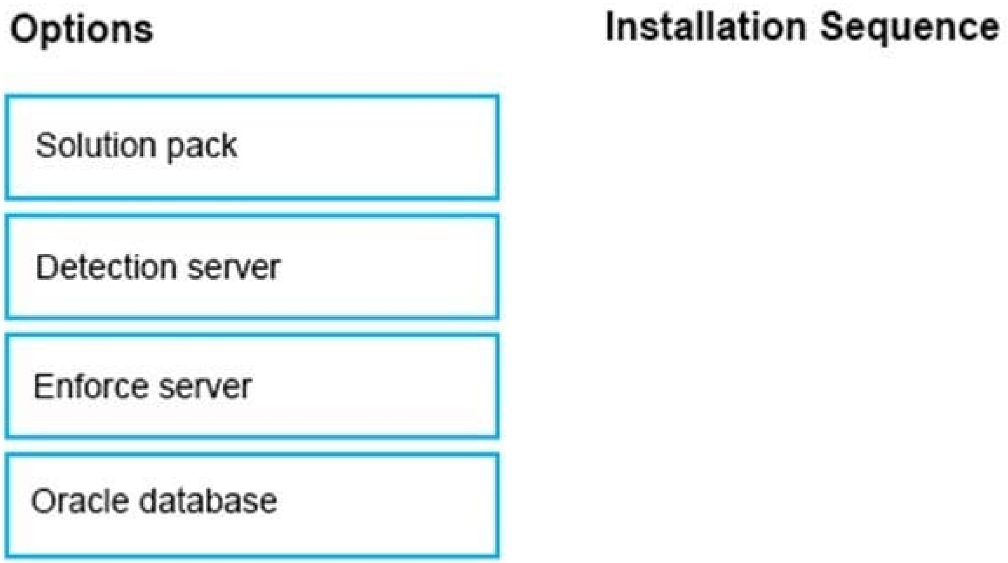
**QUESTION 10**

DRAG DROP

What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide?

Place the options in the correct installation sequence.

Select and Place:



Options

Solution pack

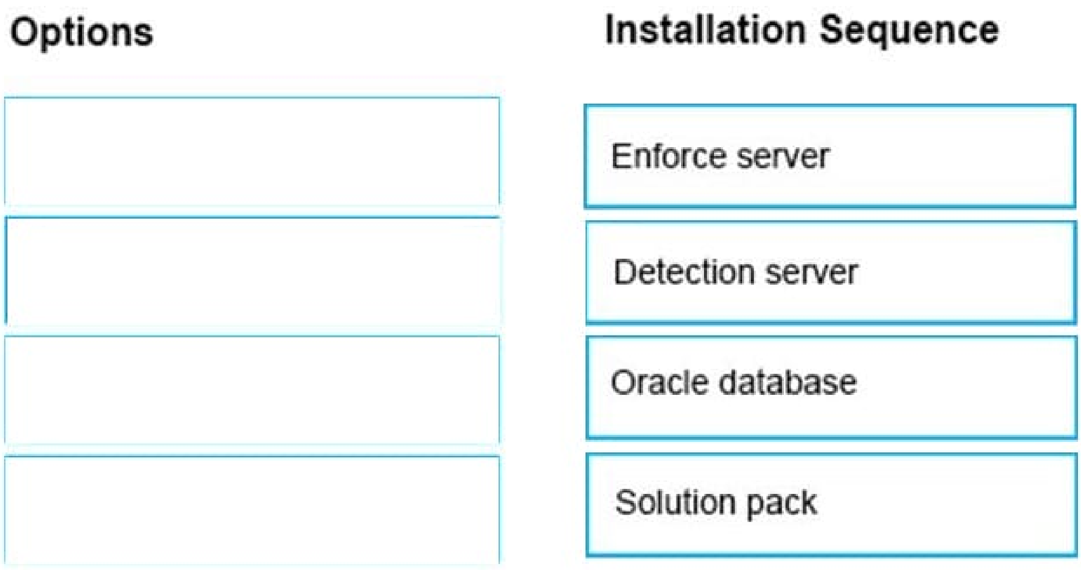
Detection server

Enforce server

Oracle database

Installation Sequence

Correct Answer:



Options

Installation Sequence

Enforce server

Detection server

Oracle database

Solution pack

**QUESTION 11**

Which two components can perform a file system scan of a workstation? (Choose two.)

A. Endpoint Server

B. DLP Agent

C. Network Prevent for Web Server

D. Discover Server

E. Enforce Server

Correct Answer: BD

**QUESTION 12**

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

Correct Answer: D

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122938258_v120691346/Setting-up-the-DLP-

S500-Appliance?locale=EN_US

**QUESTION 13**

A DLP administrator determines that the \SymantecDLP\Protect\Incidents folder on the Enforce server contains. BAD files dated today, while other. IDC files are flowing in and out of the \Incidents directory. Only .IDC files larger than 1MB are

turning to .BAD files.

What could be causing only incident data smaller than 1MB to persist while incidents larger than 1MB change to .BAD files?

A. A corrupted policy was deployed.

B. The Enforce server\\'s hard drive is out of space.

C. A detection server has excessive filereader restarts.

D. Tablespace is almost full.

Correct Answer: D

**QUESTION 14**

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

Correct Answer: B

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v16110606_v120691346/Modifying-the-Network-Discover-Cloud-Storage-Discover-Server-configuration?locale=EN_US

**QUESTION 15**

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)

Correct Answer: A