250-438 Q&As

Administration of Symantec Data Loss Prevention 15

Pass Symantec 250-438 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/250-438.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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)

Correct Answer: BD

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

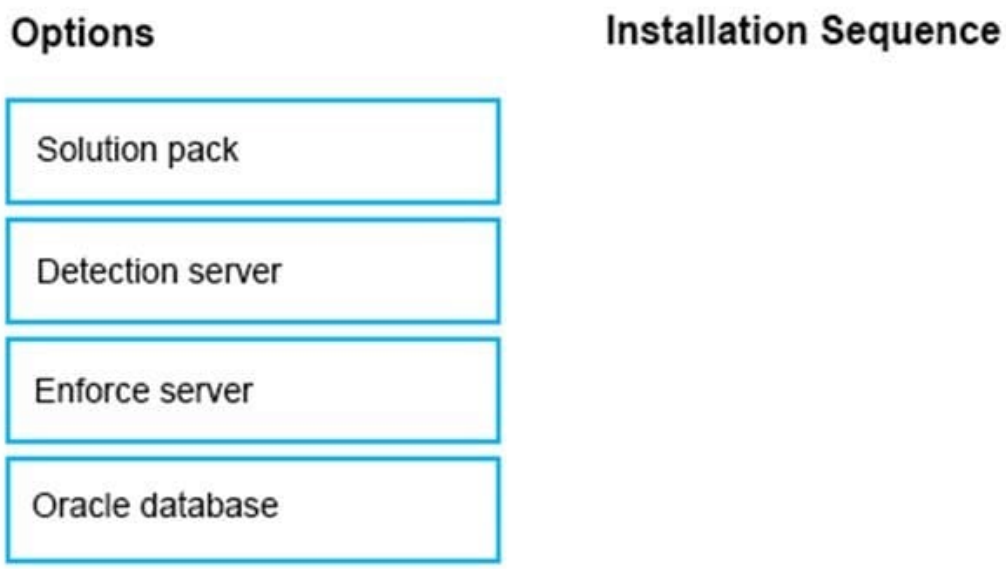
QUESTION 2

DRAG DROP

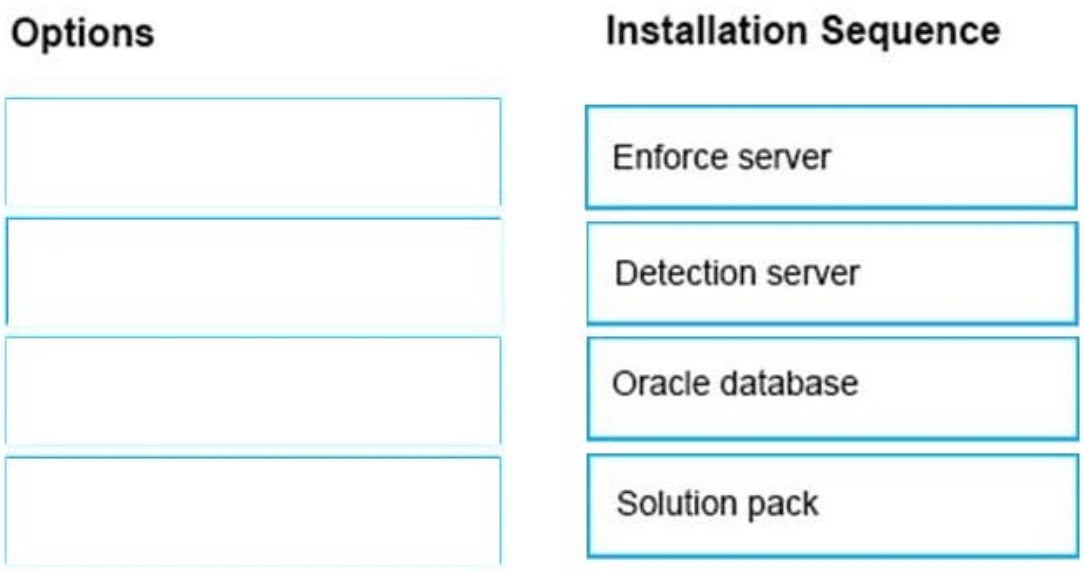
What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide?

Place the options in the correct installation sequence.

Select and Place:



Correct Answer:



QUESTION 3

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

Correct Answer: B

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

QUESTION 4

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 5

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

Correct Answer: A

QUESTION 6

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 7

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 8

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.

Correct Answer: C

QUESTION 9

What is the default fallback option for the Endpoint Prevent Encrypt response rule?

A. Block

B. User Cancel

C. Encrypt

D. Notify

Correct Answer: D

QUESTION 10

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

QUESTION 11

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.

Correct Answer: B

Reference: https://support.symantec.com/content/unifiedweb/en_US/article.TECH220250.html

QUESTION 12

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)

Correct Answer: D

QUESTION 13

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

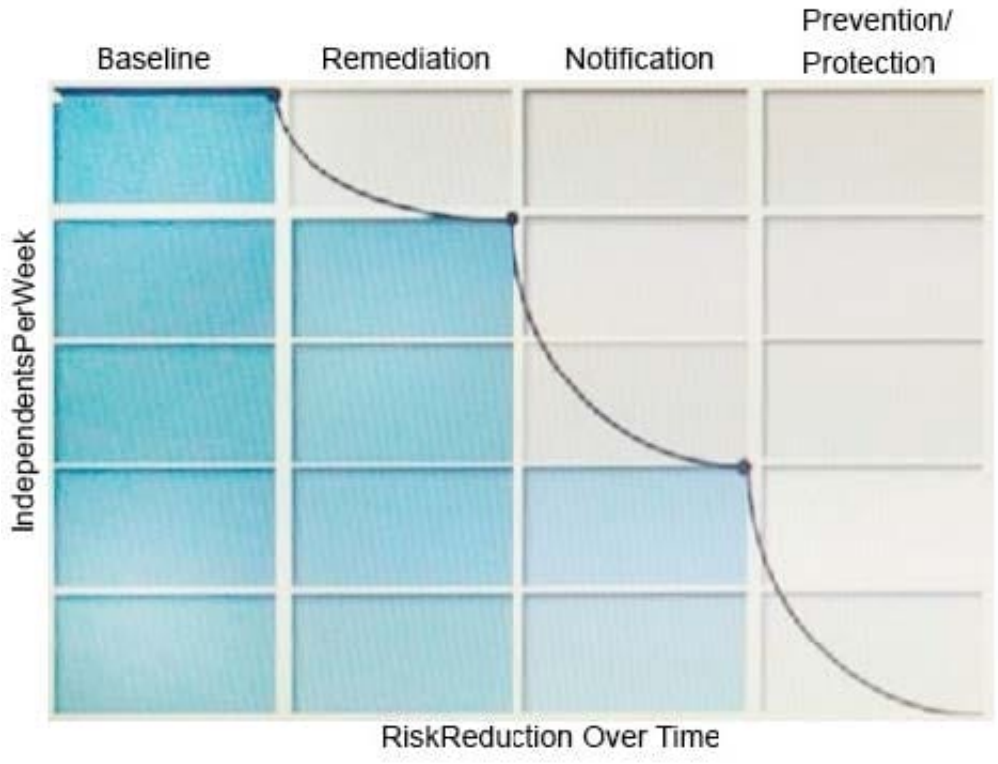
C. Verify Application File Access Control (AFAC) is configured to monitor the specific application

D. Edit the exception rule to ensure that the "Match On" option is set to "Attachments"

Correct Answer: D

QUESTION 14

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

Correct Answer: C

QUESTION 15

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

Correct Answer: CD

Reference: https://www.symantec.com/connect/articles/network-prevent

250-438 PDF Dumps 250-438 Practice Test 250-438 Braindumps