DUMPSBOSS.COM

Administration of Symantec Data Loss Prevention 15

Symantec 250-438

Version Demo

Total Demo Questions: 10

Total Premium Questions: 70

QUESTION NO: 1

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: A D

QUESTION NO: 2

A company needs to implement Data Owner Exception so that incidents when employees send or receive their own personal information.

What detection method should the company use?

A. Indexed Document Matching (IDM)

B. Vector Machine Learning (VML)

C. Exact data matching (EDM)

D. Described Content matching (DCM)

ANSWER: C

Explanation:

Reference: https://help.symantec.com/cs/dlp15.5/DLP/v40148006_v128674454/About-DataOwner-Exception?locale=EN_US

QUESTION NO: 3

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-withSymantec-Data-Loss-Preventionabout_dlp?locale=EN_US

QUESTION NO: 4

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: B E

Explanation:

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/

DOCUMENTATION/8000/DOC8244/en_US/Symantec_DLP_15.0_Cloud_Prevent_O365.pdf?
__gda__=1554430310_584ffada3918e15ced8b6483a2bfb6fb (14)

QUESTION NO: 5

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

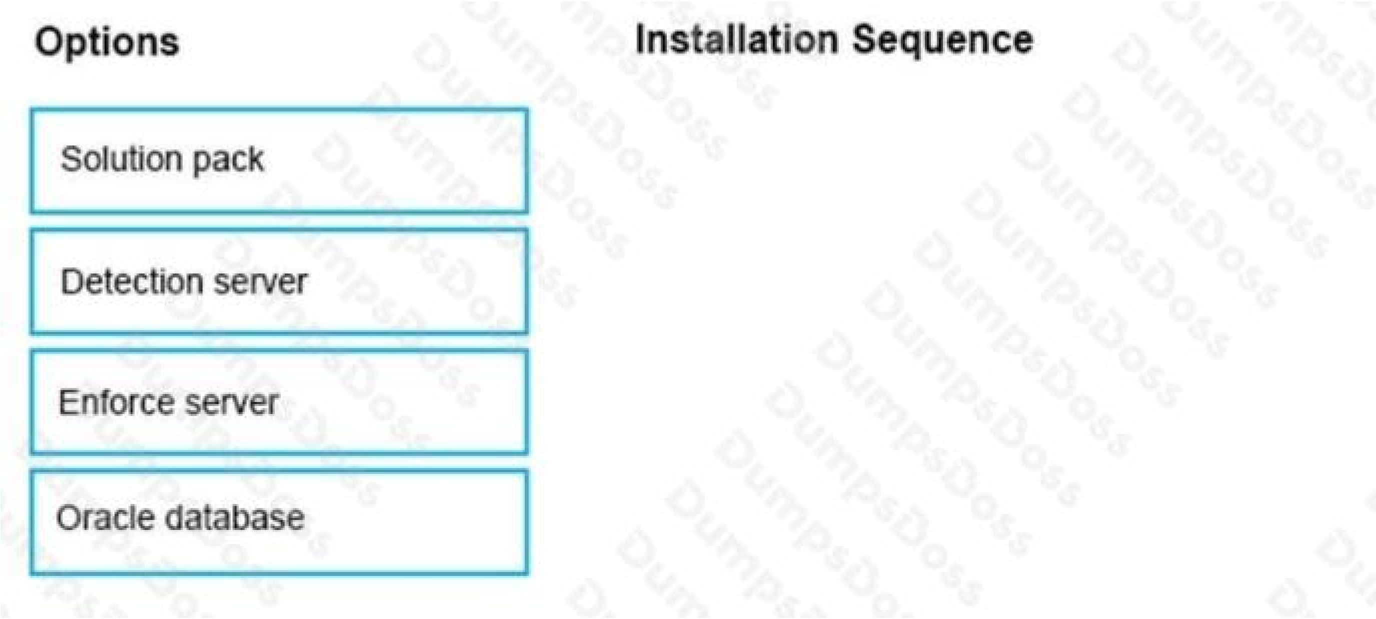
QUESTION NO: 6 - (DRAG DROP)

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

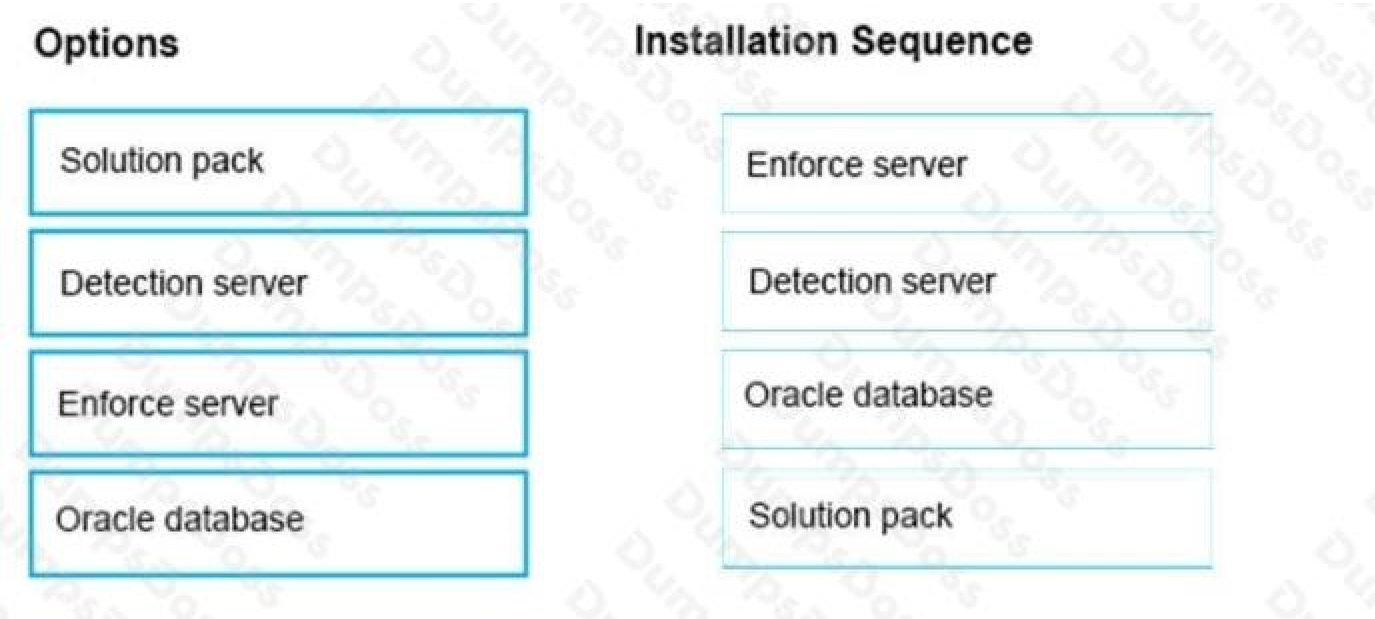
Detection server

Enforce server

Oracle database

Installation Sequence

ANSWER:



Options	Installation Sequence
Solution pack	Enforce server
Detection server	Detection server
Enforce server	Oracle database
Oracle database	Solution pack

Explanation:

QUESTION NO: 7

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: B D

Explanation:

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

QUESTION NO: 8

What detection technology supports partial contents matching?

A. Indexed Document Matching (IDM)

B. Described Content Matching (DCM)

C. Exact Data Matching (DCM)

D. Optical Character Recognition (OCR)

ANSWER: A

Explanation:

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

QUESTION NO: 9

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 attributed.

D. User attributes have been incorrectly mapped to Active Directory accounts.

ANSWER: D

QUESTION NO: 10

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: B D

Explanation:

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