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

Administration of Symantec Data Loss Prevention 15

Pass Symantec 250-438 Exam with 100% Guarantee

QUESTION 1

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

Correct Answer: CD

Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/information-centric-encryption-en.pdf

QUESTION 2

Which channel does Endpoint Prevent protect using Device Control?

A. Bluetooth

B. USB storage

C. CD/DVD

D. Network card

Correct Answer: B

Reference: https://support.symantec.com/en_US/article.HOWTO80865.html#v36651044

QUESTION 3

Which two DLP products support the new Optical Character Recognition (OCR) engine in Symantec DLP 15.0? (Choose two.)

A. Endpoint Prevent

B. Cloud Service for Email

C. Network Prevent for Email

D. Network Discover

E. Cloud Detection Service

Correct Answer: BC

QUESTION 4

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

Correct Answer: D

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

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

Correct Answer: B

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

QUESTION 7

Under the "System Overview" in the Enforce management console, the status of a Network Monitor detection server is shown as "Running Selected." The Network Monitor server\\'s event logs indicate that the packet capture and filereader processes are crashing.

What is a possible cause for the Network Monitor server being in this state?

A. There is insufficient disk space on the Network Monitor server.

B. The Network Monitor server\\'s certificate is corrupt or missing.

C. The Network Monitor server\\'s license file has expired.

D. The Enforce and Network Monitor servers are running different versions of DLP.

Correct Answer: D

QUESTION 8

Where in the Enforce management console can a DLP administrator change the "UI.NO_SCAN.int" setting to disable the "Inspecting data" pop-up?

A. Advanced Server Settings from the Endpoint Server Configuration

B. Advanced Monitoring from the Agent Configuration

C. Advanced Agent Settings from the Agent Configuration

D. Application Monitoring from the Agent Configuration

Correct Answer: C

Reference: https://www.symantec.com/connect/forums/dlp-pop-examining-content

QUESTION 9

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 10

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. ATandT

D. Verizon

E. Rackspace

Correct Answer: BE

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 11

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)

Correct Answer: D

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

QUESTION 12

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

Correct Answer: C

QUESTION 13

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

Correct Answer: C

QUESTION 14

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 15

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)

Correct Answer: BE