Symantec ST0-174

Symantec Data Loss Prevention 11.5 Technical Assessment

Version: 4.0

Topic 1, null

QUESTION NO: 1

Which two components are required for the Symantec Data Loss Prevention for Tablets solution in addition to the Tablet Prevent and Enforce servers? (Select two.)

A. DLP Agent
B. Virtual Private Network Gateway
C. Web Proxy
D. 2010 Exchange Server
E. Mobile Device Management

Answer: B,C
Explanation:

QUESTION NO: 2

Which profile contains information to enable the VPN on Demand functionality for the Data Loss Prevention for Tablets solution?

A. DLP Agent profile
B. SCEP profile
C. iOS profile
D. VPN client profile

Answer: C
Explanation:

QUESTION NO: 3

A scanner fails to return results upon completion of the scan process. Which file should be removed to eliminate previous scan issues?

A. scanner_typeScanner.cfg
B. Clean.exe
C. ScannerControllerLogging.properties
D. logs

Answer: A
Explanation:

QUESTION NO: 4

A Network Monitor server has been installed and the networking components configured accordingly. The server is receiving traffic, but fails to detect incidents. Running Wireshark indicates that the desired traffic is reaching the detection server. What is the most likely cause for this behavior?

A. The mirrored port is sending corrupted packets.
B. The wrong interface is selected in the configuration.
C. The configuration is set to process GET requests.
D. The communication to the database server is interrupted.

Answer: D
Explanation:

QUESTION NO: 5

An administrator has completed the example document training process, but is having difficulty deciding whether or not to accept a VML profile. Where can the administrator find information regarding the quality of each training set at a granular, per-fold level?

A. machinelearning_training_process.log file
B. machinelearning_native_filereader.log file
C. machinelearning_training.log file
D. machinelearning_native_manager.log file

Answer: C
Explanation:

QUESTION NO: 6

An approved Endpoint device has been configured and added as an exception to a policy that blocks the transfer of sensitive data. Data transfers to these approved Endpoint devices are still being blocked. What should the Data Loss Prevention administrator do to resolve this?

A. disable and enable the policy involved for the changes to take effect
B. edit the exception rule to ensure Match On is set to "Attachments"

C. verify that the proper device ID or class has been entered
D. assign the Endpoint device configuration to all the Endpoint servers

Answer: C
Explanation:

QUESTION NO: 7

Which product can replace a confidential document residing on a share with a marker file explaining why the document was removed?

A. Network Discover
B. Network Protect
C. Endpoint Prevent
D. Endpoint Discover

Answer: B
Explanation:

QUESTION NO: 8

What is one benefit of using FlexResponse for Network Discover?

A. Response rules trigger varying actions depending on which DLP Agent created the incident.
B. An email can be encrypted as it is being transmitted.
C. Displayed incident data can be redacted from the Data Loss Prevention interface automatically.
D. Customizable incident remediation actions can be manually executed.

Answer: D
Explanation:

QUESTION NO: 9

Which product must run on a physical server?

A. Endpoint Prevent
B. Network Monitor
C. Enforce

D. Network Prevent

Answer: B

Explanation:

QUESTION NO: 10

A user attempts to run Lookup Attributes manually on an incident. On the Incident List page under Incident Actions, the option for Lookup Attributes is missing. Which section in the Plugins.properties file is misconfigured?

A. Plugin Execution Chain is undefined.
B. Attribute Lookup parameters is set to "message".
C. Automatic plugin reload is set to false.
D. Automatic Lookup is set to false.

Answer: A

Explanation:

QUESTION NO: 11

What are two possible ways to provide incident match text information? (Select two.)

A. CSV export
B. Email notification
C. Reporting API
D. Syslog notification
E. XML export

Answer: C,E

Explanation:

QUESTION NO: 12

Which two should be used to collect log information from Enforce servers? (Select two.)

A. enable the VontuSNMP service and set the community strings accordingly
B. use the Log Collection and Configuration tool

C. navigate manually to the log directory of the Enforce server installation
D. .access the Enforce Log Viewer page athttps://<VONTU_SRV>/logs?view=true
E. use dbgmonitor from sysinternals to connect to the debug output of the service

Answer: B,C
Explanation:

QUESTION NO: 13

How can an administrator validate that once a policy is updated and saved it has been enabled on a specific detection server?

A. check the status of the policy on the policy list page
B. check to see whether the policy was loaded under System > Servers > Alerts
C. check the policy and validate the date and time it was last updated
D. check to see whether the policy was loaded under System > Servers > Events

Answer: D
Explanation:

QUESTION NO: 14

What is a possible solution when a Network Discover server is unable to scan a remote file server?

A. mount the IPC$ share on the file server
B. verify that the target file server is a Windows 2000 server
C. use the fully qualified name (FQDN) of the server
D. verify that the file server has .NET services running

Answer: C
Explanation:

QUESTION NO: 15

Which is the correct traffic flow for the Symantec Data Loss Prevention for Tablets solution?

A. iPad > VPN > Tablet Server > Exchange Server > final destination

B. iPad > VPN > Web proxy > Tablet Server > final destination
C. iPad > VPN > Web proxy > Tablet Server > Enforce Server > final destination
D. iPad > VPN > Tablet Server > Web proxy > final destination

Answer: B
Explanation:

QUESTION NO: 16

What is the function of the Remote Indexer?

A. to create Index Document Matching (IDM) profiles and Exact Data Matching (EDM) profiles on a remote server
B. to create Exact Data Matching (EDM) profiles on a remote server
C. to create policy templates on a remote server
D. to create Index Document Matching (IDM) profiles on a remote server

Answer: B
Explanation:

QUESTION NO: 17

What are two benefits of the Symantec Data Loss Prevention 11.5 security architecture? (Select two.)

A. Communication is initiated by the detection servers inside the firewall.
B. SSL communication is used for user access to the Enforce Platform.
C. Endpoint Agent to Endpoint Server communication uses the Triple Data Encryption Standard (Triple DES).
D. Confidential information captured by system components is stored using Advanced Encryption Standards (AES) symmetric keys.
E. All indexed data uploaded into the Enforce Platform is protected with a two-way hash.

Answer: B,D
Explanation:

QUESTION NO: 18

In which two ways can the default listener port for a detection server be modified? (Select two.)

A. through the Enforce user interface under System > Overview
B. by editing the Communication.properties file on a detection server
C. through the Enforce user interface under Manage > Policies
D. by editing the MonitorController.properties file on a detection server
E. by editing the jaas.config file on a detection server

Answer: A,B
Explanation:

QUESTION NO: 19

Which option describes the three-tier installation type for Symantec Data Loss Prevention?

A. Install the database, the Enforce Server, and a detection server all on the same computer.
B. Install the Oracle database and the Enforce Server on the same computer, then install detection servers on separate computers.
C. Install the Oracle Client (SQL*Plus and Database Utilities) on three detection servers.
D. Install the Oracle database, the Enforce Server, and a detection server on separate computers.

Answer: C
Explanation:

QUESTION NO: 20

Which detection server requires two physical network interface cards?

A. Network Protect
B. Network Discover
C. Endpoint Discover
D. Network Monitor

Answer: B
Explanation:

QUESTION NO: 21

Which tool is provided by default to edit a database on an endpoint?

A. vontu_sqlite3.exe
B. update_configuration.exe
C. logdump.exe
D. wdp.exe

Answer: A

Explanation:

QUESTION NO: 22

Which command line diagnostic utilities would give a user the operating system version of the detection servers?

A. Environment Check Utility
B. Log Collection Utility
C. NormalizationConfigCheck.exe
D. SC.exe

Answer: A

Explanation:

QUESTION NO: 23

Which delimiter is acceptable in Exact Data Matching (EDM) data sources?

A. space
B. semi-colon (;)
C. pipe (|)
D. slash (/)

Answer: C

Explanation:

QUESTION NO: 24

What must a policy manager do when working with Exact Data Matching (EDM) indexes?

A. re-index large data sources on a daily or weekly basis

B. index the original data source on the detection server
C. deploy the index only to specific detection servers
D. create a new data profile if data source schema changes

Answer: D
Explanation:

QUESTION NO: 25

What is a feature of keyword proximity matching?

A. It will match on whole keywords only.
B. It has a maximum distance between keywords of 99.
C. It only matches on message body.
D. It evaluates each keyword pair independently.

Answer: D
Explanation:

QUESTION NO: 26

What should a Data Loss Prevention administrator do when the license file expires?

A. enter a new license key to update the license file
B. reference a new license file on the System Settings page
C. overwrite the expired license key
D. enter a new license file on the Advanced Settings page

Answer: B
Explanation:

QUESTION NO: 27

A Data Loss Prevention 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. Why are the processes missing from the Server Detail page display?

A. The detection server Display Control Process option has been disabled on the Server Detail