# ST0-237 Q&As

Symantec Data Loss Prevention 12 Technical Assessment

## Pass Symantec ST0-237 Exam with 100% Guarantee

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

**https://www.leads4pass.com/st0-237.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**

An administrator is checking System Overview and all of the detection servers are showing as \\'unknown\\'. The Vontu services are up and running on the detection servers. Thousands of .IDC files are building up in the Incidents directory on the detection servers. There is good network connectivity between the detection servers and the Enforce server when testing with the telnet command. How can the administrator bring the detection servers to a running state in the Enforce UI?

A. Delete all of the .BAD files in the incidents folder on the Enforce server

B. Restart the Vontu Monitor Service on all of the detection servers affected

C. Ensure the Vontu Monitor Controller service is running on the Enforce server

D. Ensure port 8300 is configured as open on the firewall

Correct Answer: C

**QUESTION 2**

An incident responder is viewing a discover incident snapshot and needs to determine which information to provide to the next level responder. Which information would be most useful in assisting the next level responder with data clean-up?

A. Incident Details: Message Body content

B. Custom Attributes: Most Active User from Data Insight

C. Incident Details: File Owner metadata

D. Access Information: File Permissions

Correct Answer: B

**QUESTION 3**

Which response rule action will be ignored when using an Exact Data Matching (EDM) policy?

A. Network Prevent: Remove HTTP/HTTPS Content

B. All: Send Email Notification

C. Network Protect: Copy File

D. Endpoint Prevent: Notify

Correct Answer: D

**QUESTION 4**

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.

Correct Answer: A

**QUESTION 5**

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.

Correct Answer: C

**QUESTION 6**

A divisional executive requests a report of all incidents generated by a particular region, summarized by department. What must be populated to generate this report?

A. remediation attributes

B. sender correlations

C. status groups

D. custom attributes

Correct Answer: C

**QUESTION 7**

An administrator needs to deploy a Symantec Data Loss Prevention solution that will monitor network traffic. Which traffic type is excluded from inspection when using the default configuration?

A. HTTP-get

B. NNTP

C. FTP-put

D. HTTP-post

Correct Answer: A

**QUESTION 8**

Which two components of Symantec Control Compliance Suite 9.0 must be deployed in an Active Directory domain? (Select two.)

A. application server

B. Data Processing Services

C. Production database

D. directory server

E. web portal server

Correct Answer: AD

**QUESTION 9**

The Symantec Control Compliance Suite 9.0 (CCS 9.0) stores large amounts of data in databases. The database administrator must perform tasks on the databases outside of CCS 9.0 to maintain the databases and to ensure that the databases are performing at an acceptable level.

Which three tasks should be routinely scheduled in SQL Server Management Studio? (Select three.)

A. Configure the databases

B. Back up the databases

C. Refresh the databases

D. Rebuild the indexes

E. Update the database statistics

Correct Answer: BDE

**QUESTION 10**

Where are assets stored?

A. Assets.XML

B. Production database

C. RMS database

D. ADAM

Correct Answer: D

**QUESTION 11**

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

Correct Answer: B

**QUESTION 12**

The chief information security officer (CISO) is responsible for overall risk reduction and develops high- level initiatives to respond to security risk trends. Which report will be useful to the CISO?

A. all high severity incidents that have occurred during the last week

B. all dismissed incidents violating a specific policy marked as false positive

C. all incidents from the previous month summarized by business units and policy

D. all new incidents that have been generated by a specific business unit during the last week

Correct Answer: B

**QUESTION 13**

A DLP administrator needs to modify a Network Discover scan that has started.

How should the administrator ignore files larger than 20 MB for the remaining shares?

A. Pause the scan, edit the scan target filters to ignore files greater than 20 MB, resume the scan

B. Modify the server settings for the Discover server running the scan, adjust the maxfilesize.level setting to greater than 20 MB, restart the Discover server

C. Stop the Vontu Monitor Controller Service, go to Manage > Discover Scanning > Discover Targets, set a new filter, restart the service

D. Create a new scan with updated file size filters and start the scan

Correct Answer: A

**QUESTION 14**

Which function does the Email Prevent server provide when integrating into an existing email environment?

A. inspects, stores, and blocks confidential emails as a Mail Transfer Agent (MTA)

B. integrates with a Mail Transfer Agent (MTA) to inspect SMTP email messages

C. maintains each inbound SMTP message transaction until the outbound is inspected

D. processes and inspects outbound SMTP messages until the email transaction has been closed

Correct Answer: B

**QUESTION 15**

Where does a Data Loss Prevention administrator recycle the FileReader process on a detection server?

A. System Overview page

B. Server Detail page

C. command prompt

D. Windows Services

Correct Answer: B

ST0-237 PDF Dumps ST0-237 Practice Test ST0-237 Exam Questions