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.passapply.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

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

Correct Answer: A

QUESTION 2

A company needs to disable USB devices on computers that are generating a number of recurring DLP incidents. It decides to implement Endpoint Lockdown using Endpoint Prevent, which integrates with Symantec Endpoint Protection Manager and Symantec Management Platform. After incidents are still detected from several agents, the company determines that a component is missing.

Which component needs to be added to disable the USB devices once incidents are detected?

A. Control Compliance Suite

B. Workflow Solution

C. pcAnywhere

D. Risk Automation Suite

Correct Answer: B

QUESTION 3

A Data Loss Prevention administrator notices that several errors occurred during a Network Discover scan.

Which report can the administrator use to determine exactly which errors occurred and when?

A. Discover Incident report sorted by target name and scan

B. Full Activity report for that particular scan

C. Server Event report from Server Overview

D. Full Statistics report for that particular scan

Correct Answer: B

QUESTION 4

With respect to the entitlements workflow, what is the first step that is performed?

A. Assign a data owner

B. Mark control point

C. Import entitlements

D. Gather business data

Correct Answer: B

QUESTION 5

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