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 service is responsible for importing assets via a CSV file?

A. Application Server Service

B. Data Processing Service

C. Directory Support Service

D. Management Services Service

Correct Answer: B

QUESTION 2

If Endpoint Prevent and Endpoint Discover are competing for resources on an endpoint computer, how does the system resolve the conflict?

A. Endpoint Discover queues files until resources are available.

B. Endpoint Discover pauses any scans if resources are needed.

C. Endpoint Prevent pauses detection until any scans complete.

D. Endpoint Prevent queues files until resources are available.

Correct Answer: B

QUESTION 3

A software company needs to protect its source code including new source code between indexing times.

Which detection method should the company use to meet this requirement?

A. Exact Data Matching (EDM)

B. Described Content Matching (DCM)

C. Indexed Document Matching (IDM)

D. Vector Machine Learning (VML)

Correct Answer: D

QUESTION 4

Which command is used to save queries/commands written to the database when one of the following DMLs is used: Update, Insert, or Delete?

A. commit

B. finalize

C. :wq

D. exit

Correct Answer: A

QUESTION 5

A business unit is generating a large number of high severity incidents on a Network Prevent credit card policy.

What are two likely causes? (Select two.)

A. The business unit\\'s employees are storing credit card data insecurely on a local file share.

B. A business process within the business unit violates corporate security policies.

C. The business unit\\'s employees are copying credit card data to removable drives.

D. The business unit\\'s employees may be unaware of correct credit card handling procedures.

E. The policy is unable to detect corporate security policies with respect to credit cards.

Correct Answer: BD

QUESTION 6

How should an administrator determine which Database version is running?

A. Run the command select database version from database;

B. Right click on database folder and select version

C. Run the command select * from v$version;

D. Look in add/remove programs for the database program

Correct Answer: C

QUESTION 7

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 at https:///logs?view=true

E. Use dbgmonitor from sysinternals to connect to the debug output of the service

Correct Answer: BC

QUESTION 8

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

Correct Answer: D

QUESTION 9

The DLP services on an Endpoint Server keep stopping. The only events displayed in the Enforce UI are that the server processes have stopped. What is the first step the administrator should take to keep the services on the Endpoint server running?

A. Perform a complete uninstall and reinstall of the Product

B. Install malware detection software on the server

C. Remove the Endpoint server from the UI and add it again

D. Exclude the DLP directories from any scheduled or real-time virus scanning

Correct Answer: D

QUESTION 10

What can cause an increase in the DLP Agent footprint?

A. Smart Response rules

B. additional Agent Components

C. additional policies

D. API lookups

Correct Answer: C

QUESTION 11

A DLP administrator is writing one policy to block sensitive data from being copied to removable media. The administrator is applying two response rules to the policy: \\'Endpoint Prevent: Notify\\' and \\'Endpoint Prevent: Block\\'.

Why are some copies blocked while others are only notified?

A. There are different conditions for the different response actions

B. The monitor and ignore filters are defined incorrectly

C. The DLP administrator needs to fine tune the throttling options

D. The Directory Group Matching (DGM) profile has users in different groups

Correct Answer: A

QUESTION 12

What are two reasons why a company should implement data loss prevention? (Select two.)

A. To prevent the threat of malware

B. To demonstrate regulatory compliance

C. To protect the CISO from liability due to a security breach

D. To prevent employee malicious activity

E. To protect brand and reputation

Correct Answer: BE

QUESTION 13

What are two functions of the Enterprise Configuration Service? (Select two.)

A. It maintains a list of master and slave query engines.

B. It maintains rules for query engine data collection.

C. It maintains a list of RMS configured users.

D. It maintains a list of registered UNIX targets.

E. It maintains Scope files.

Correct Answer: AB

QUESTION 14

Which feature should an incident responder use to begin to determine where an attachment has created other violations?

A. Report Filters

B. Incident History

C. Incident Details

D. Policy Matches

Correct Answer: A

QUESTION 15

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