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.pass2lead.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 incident responder can see basic incident data, but is unable to view specific details of the incident. What could be wrong with the configuration in the incident responder\\'s role?

A. View option is selected and all display attributes are deselected.

B. Incident Access tab conditions are specified.

C. Available Smart Response rules are deselected.

D. Server administration rights are deselected.

Correct Answer: A

QUESTION 2

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 3

What is the minimum number of plexes required for true mirroring to provide redundancy of data?

A. One

B. Two

C. Three

D. Four

Correct Answer: B

QUESTION 4

You execute the qio_convertdbfiles command to convert the database files to use Quick I/O. The command results with an error that the database files are not on a VxFS file system. You need to convert the database files to use Quick I/O.

What should you do?

A. Run the qio_getdbfiles command to get the database files on the VxFS file system.

B. Remove the files from the mkgio.dat file.

C. Predefine the DB2 environment variable $DB2DATABASE.

D. Set the database type to DB2.

Correct Answer: B

QUESTION 5

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 6

To run a bv-Control query targeting Microsoft SQL Server 2005, which Microsoft component is required on the information server?

A. SQL Agent

B. Reporting Services

C. Integration Services

D. Distributed Management Objects

Correct Answer: D

QUESTION 7

Which user store is essential for using the user risk summary feature?

A. Tomcat

B. Active Directory

C. MySQL

D. Samba

Correct Answer: B

QUESTION 8

A company has created an Exact Data Matching profile and referenced it in a policy to protect customer credit card information. New customers are added daily, but the profile is updated weekly.

Until the profile can be updated, which rule should be added to protect new credit card numbers?

A. A compound rule that also matches on a data identifier

B. A detection rule that matches on sender/user

C. A separate detection rule that uses a data identifier

D. A detection rule that matches on regular expressions

Correct Answer: C

QUESTION 9

An administrator pulls the Services and Operation logs off of a DLP Agent by using the Pull Logs action. What happens to the log files after the administrator performs the Pull Logs action?

A. they are stored directly on the Enforce server

B. they are transferred directly to the Enforce Server and deleted from the DLP Agent

C. they are created on the DLP Agent then pulled down to the Enforce server

D. they are temporarily stored on the DLP Agent\\'s Endpoint server

Correct Answer: D

QUESTION 10

An incident responder can see basic incident data, but is unable to view any specific details of the incident.

What is the configuration for this role?

A. The View option is selected and all display attributes are deselected.

B. Server administration rights have been deselected.

C. Custom attributes have been selected and set to View Only.

D. Incident Access tab conditions are specified.

Correct Answer: A

QUESTION 11

An administrator is applying a newly created agent configuration to an Endpoint server. Upon inspection, the new configuration is unassigned in the Endpoint Server Details. What is a possible cause for the new configuration failing to be assigned?

A. the system default settings were saved to the new agent configuration

B. the server that the new agent configuration was applied to needs to be recycled

C. the new agent configuration was saved without applying it to the Endpoint server

D. the new agent configuration was copied and modified from the default agent configuration

Correct Answer: C

QUESTION 12

Which four functional roles can be registered to the Data Processing Service? (Select four.)

A. Load Balancer

B. Data Provider

C. Collector

D. Evaluator

E. Reporter

F. Manager

Correct Answer: ACDE

QUESTION 13

What is required to assign permissions to the asset system?

A. user/group

B. role

C. role and user/group

D. group

Correct Answer: C

QUESTION 14

A network architect needs to install Symantec Data Loss Prevention detection servers in a hosted environment.

Which action should the network architect take to ensure secured communication between the detection server and the Enforce server?

A. use the sslkeytool utility to create multiple unique certificates for each detection server

B. generate a certificate directly on each detection server

C. use the built-in Symantec Data Loss Prevention certificate for the hosted server

D. generate identical certificates for on-premise servers and identical certificates for hosted servers

Correct Answer: A

QUESTION 15

What is the maximum number of port lets that can be used in a dashboard?

A. 4

B. 6

C. 8

D. 10

Correct Answer: B