

2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (51-60)

QUESTION 51

For which two does Symantec Security Information Manager automatically create values when you manually create a new incident?
(Select two.)

"Pass Any Exam. Any Time." - [www.actualtests.com](#) 26

Symantec ST0-085 Exam

- A. Event Creator
- B. Incident Creator
- C. Help desk ticket
- D. Rule Name
- E. Event ID number

Answer: BD

QUESTION 52

Which condition needs to be met for a rule to be triggered on the Symantec Security Information Manager Conditions tab?

- A. Incident Type
- B. Event Criteria
- C. Asset to be vulnerable
- D. Device Effectuated
- E. Applicable Licenses

Answer: B

QUESTION 53

What does a conclusion that is untrackable to an existing incident become?

- A. an occurring incident
- B. an occurring event
- C. a new incident
- D. a new event

Answer: A

QUESTION 54

Where is information about the health and performance of the Symantec Security Information Manager appliance found?

"Pass Any Exam. Any Time." - [www.actualtests.com](#) 27

Symantec ST0-085 Exam

- A. Statistics tab
- B. System tab
- C. Service tab
- D. Maintenance tab

Answer: A

QUESTION 55

Which tab on the Symantec Security Information Manager statistics page displays the appliance's memory and CPU utilization, the database statistics, and the status of any database jobs?

- A. Service Status
- B. Maintenance Schedule
- C. System Status
- D. Event Service

Answer: C

QUESTION 56

Which section can be found on the Status pane located on the Statistics page?

- A. Router Connectivity Status
- B. Agent Status
- C. Database Health Monitor
- D. Correlation Event Status
- E. Rule Congruency

Answer: C

QUESTION 57

Which type of database backup is performed during the Symantec Security Information Manager installation?

"Pass Any Exam. Any Time." - www.actualtests.com 28

Symantec ST0-085 Exam

- A. an incremental, offline backup
- B. a full, online backup
- C. a full, offline backup
- D. an incremental, online backup

Answer: C

QUESTION 58

When should a Symantec Security Information Manager database be restored?

- A. when false-positive data is confirmed to exist in the database
- B. when there is a database failure that cannot be fixed
- C. when the database has been compromised
- D. when the data has reached its lifetime expectancy

Answer: B

QUESTION 59

Which statement is true about re-installing the Symantec Security Information Manager appliance?

- A. Re-installing the software deletes all data that is stored on the appliance.
- B. During installation, the Repair Software option must be selected to retain data on the appliance.

- C. The database is off-storage, so re-installing software has no effect.
- D. Prior to installation, all database information must be saved to the DeepSight Global Data Repository.

Answer: A

QUESTION 60

Which RAID level is recommended in a DAS configuration?

"Pass Any Exam. Any Time." - www.actualtests.com 29

Symantec ST0-085 Exam

- A. RAID 1
- B. RAID 5
- C. RAID 7
- D. RAID 10

Answer: B

If you want to pass Symantec ST0-085 successfully, donot missing to read latest lead2pass Symantec ST0-085 dumps.
If you can master all lead2pass questions you will able to pass 100% guaranteed.

<http://www.lead2pass.com/ST0-085.html>