2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (101-110)

QUESTION 101
When troubleshooting the installation of Symantec Security Information Manager (SSIM), the "status" console command displays the status of which critical SSIM service?

A. Information Manager
B. DB2 database
C. Tomcat servlet engine
D. Apache web server

Answer: B

QUESTION 102
When troubleshooting the installation of Symantec Security Information Manager, which console command would you use to determine the "status" of the HTTP server?
"Pass Any Exam. Any Time." - www.actualtests.com 43
Symantec ST0-085 Exam

A. sesa_chk http
B. eventservice
C. status
D. java -jar SesaInfo.jar

Answer: C

QUESTION 103
You are troubleshooting your Symantec Security Information Manager (SSIM) system. You issue
information does the "status" command display?

A. process ID
B. maximum uptime
C. process uptime
D. number of connections

Answer: ABC

QUESTION 104
You are troubleshooting your Symantec Security Information Manager (SSIM) system. You issue
information does the "status" command display?

A. # of times started
B. current status
C. exit code
D. CPU utilization

Answer: ABC

QUESTION 105
You manage the Symantec Security Information Manager system for your company. A newly
"Pass Any Exam. Any Time." - www.actualtests.com 44
Symantec ST0-085 Exam
installed server is performing very slowly on the network. You suspect a problem with the Ethernet duplex status on the server?

A. ifconfig
B. ethtool
C. netstat
D. traceroute

Answer: B

QUESTION 106
You are troubleshooting performance problems on your Symantec Security Information Manager
Which console utility should you use to view the number of dropped packets on the network interface?

A. ifconfig
B. mii-tool
C. ps
D. top

Answer: A

QUESTION 107
Which is an off-box collector of Symantec Security Information Manager?

A. Snort
B. Checkpoint Firewall
C. Cisco PIX
D. Symantec AntiVirus

Answer: D
"Pass Any Exam. Any Time." - www.actualtests.com 45
Symantec ST0-085 Exam

QUESTION 108
Which component of a Symantec Event Collector reads event data from a specific security product?

A. Sensor
B. Translator
C. Filter
D. Data Parser

Answer: A

QUESTION 109
Which component of a Symantec Event Collector processes raw events into security events using a set of event mapping rules?

A. Data Parser
B. Sensor
C. Filter
D. Translator

Answer: D

QUESTION 110
Which step should be taken to prepare for an installation of a Symantec Security Information Manager Agent on a new system?

A. verify that JRE 1.4.2 or higher is installed
B. ping the appliance IP address and name
C. remove old versions of the agent
D. run "setup -i" to run the pre-installation check

Answer: B
"Pass Any Exam. Any Time." - www.actualtests.com 46
Symantec ST0-085 Exam

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

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