2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (21-30)

QUESTION 21
Which console utility should be used to view the number of dropped packets on the network interface when troubleshooting performance problems on the Symantec Security Information Manager system?

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

Answer: A

QUESTION 22
"Pass Any Exam. Any Time." - www.actualtests.com 11
Symantec ST0-085 Exam
Which is an off-box collector of Symantec Security Information Manager?

A. Snort
B. Checkpoint Firewall
C. Cisco PIX
D. Windows

Answer: D

QUESTION 23
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 24
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

QUESTION 25
"Pass Any Exam. Any Time." - www.actualtests.com 12
Symantec ST0-085 Exam

When installing the Symantec Security Information Manager Agent and Collector on a Windows platform, which command shows that the agent is installed and running?

A. sesa_status
B. agentmgmt.bat
C. java -jar agentstatus.jar -a

Answer: B

QUESTION 26
When managing the Symantec Security Information Manager (SSIM) solution for a company, the Cisco PIX collector needs to be configured to process events from a Cisco PIX firewall.
What must be done on the PIX firewall to accomplish this?

A. Configure it to send syslog messages to the SSIM appliance.
B. Open port 514 on the firewall for access from the SSIM appliance.
C. Configure SSL communication from the firewall to the SSIM appliance.
D. Enable the Log Export API.

Answer: A

QUESTION 27
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: C

"Pass Any Exam. Any Time." - www.actualtests.com 13
Symantec ST0-085 Exam
QUESTION 28
Which statement about Symantec Security Information Manager domains is true?

A. Domains are based on Active Directory domains.
B. A domain can be a group of separate correlation systems.
C. A domain can be a group of a single correlation system and multiple collection systems.
D. A single master directory ties all domains together.

Answer: C

QUESTION 29
How are computers logically grouped in Symantec Security Information Manager (SSIM)?

A. Global Groups
B. Organizational Roles
C. Domain Local Groups
D. Organizational Units

Answer: D

QUESTION 30
When designing a new Symantec Security Information Manager (SSIM) solution for a company, what structure should be created in a SSIM domain to place systems under?

A. Domain Roles
B. Organizational Units
C. Operational Groups
D. Domain Groups

Answer: B
"Pass Any Exam. Any Time." - www.actualtests.com 14
Symantec ST0-085 Exam

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

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