

2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (111-120)

QUESTION 111

You are installing the Symantec Security Information Manager Agent on a Windows platform.

- A. c:Symanteclog
- B. c:Program FilesSymanteclog
- C. c:Program FilesSymantecsesaagentlog
- D. c:Symantecagentlog

Answer: C

QUESTION 112

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. java -jar agentcmd.jar -status
- C. java -jar agentstatus.jar -a

Answer: B

QUESTION 113

You are in the process of installing and configuring a new Symantec Security Information Manager perform to allow the CheckPoint collector to receive log information from the CheckPoint firewall?

- A. create the OPSEC application
- B. configure CheckPoint ACL to communicate with the SSIM appliance
- C. configure the CheckPoint LEA server
- D. configure CheckPoint to forward syslog events to the SSIM appliance "Pass Any Exam. Any Time." - www.actualtests.com 47 Symantec ST0-085 Exam

Answer: AC

QUESTION 114

You manage the Symantec Security Information Manager(SSIM) solution for your company. You need to configure the Cisco PIX collector to process events from a Cisco PIX firewall.

What must you do 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 115

You manage the Symantec Security Information Manager (SSIM) solution for your company. Your company has recently installed a

Juniper NetScreen firewall.

Which two actions must be taken on the firewall to allow the SSIM appliance to process firewall events?

- A. enable the Event Sensor
- B. turn on the Include Traffic Log option
- C. enable syslog messaging
- D. define at least one event filtering rule

Answer: BC

"Pass Any Exam. Any Time." - www.actualtests.com 48

Symantec ST0-085 Exam

QUESTION 116

Which three statements about Symantec Security Information Manager domains are true?

- A. Domains allow logical grouping of appliances.
- B. Each domain must have its own model 9650 appliance.
- C. A domain can include many model 9630 appliances.
- D. A single master directory ties all domains together.

Answer: ABC

QUESTION 117

Domains are organized into hierarchically organized groups of computers called _____.

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

Answer: D

QUESTION 118

You are designing a new Symantec Security Information Manager (SSIM) solution for your company.

When designing the structure of your SSIM domain, computers are separated into logical groups called _____.

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

"Pass Any Exam. Any Time." - www.actualtests.com 49

Symantec ST0-085 Exam

- D. Domain Groups

Answer: B

QUESTION 119

Which two default administrative user accounts are created during the installation of Symantec Security Information Manager?

- A. Root Administrator
- B. Domain Administrator

- C. SES Administrator
- D. System Administrator
- E. Local Administrator

Answer: BC

QUESTION 120

Which two statements about Role Based Access Control are true?

- A. A user can be a member of many roles.
- B. Role membership defines what actions a user can perform.
- C. When a user is created, it is placed in the "Default" role.
- D. The Domain Administrator role has full authority over all domains in the system.

Answer: AB

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

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