2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (31-40)

QUESTION 31
Which two default administrative user accounts are created during the installation of Symantec Security Information Manager? (Select two.)

A.   Root Administrator
B.   Domain Administrator
C.   SES Administrator
D.   System Administrator E. Local Administrator

Answer: BC

QUESTION 32
When are the effective privileges of the SES Administrator role and Domain Administrator role equivalent?

A.   when there is only one domain in the system
B.   when the administrator is assigned the SES Administrator role
C.   when the system is newly installed and a domain has not yet been created
D.   when the Domain Administrator role is given permission to create users and roles

Answer: A

QUESTION 33
Which role is able to modify permissions within the Symantec Security Information Manager solution?

A.   DB2 Administrator
B.   Root Administrator
C.   System Administrator
D.   Domain Administrator

Answer: D

"Pass Any Exam. Any Time." - www.actualtests.com 15
Symantec ST0-085 Exam
QUESTION 34
How many days of data is stored in the archives before it is purged?

A.   10
B.   30
C.   60
D.   unlimited

Answer: D

QUESTION 35
When configuring the Event Archive settings of an Information Manager appliance, which two options can be configured? (Select two.)

A.   Auxiliary Storage Device
B.   Max Archive Quota
C.   Free disk space
D.   Purge Start Time
E.   Purge certain events

Answer: BC

QUESTION 36
Which is commonly used to view archived events?

A.   Information Manager Event Viewer
B.   Archive Management Console tab
C.   Event Viewer API
D.   Incident Management Console tab

Answer: A

"Pass Any Exam. Any Time." - www.actualtests.com 16
Symantec ST0-085 Exam
QUESTION 37
Which two user actions can be executed by the Information Manager Event Viewer by default? (Select two.)

A.   Finger
B.   ping
C.   touch
D.   nslookup
E.   whois

Answer: AB

QUESTION 38
Which two search templates are pre-defined by Information Manager? (Select two.)

A.   Host Activity
B.   Internal Activity
C.   IDS Activity
D.   Firewall Activity
E.   Port Activity

Answer: AE

QUESTION 39
When querying archived event data, how can you make a query available to other users of the system?

A.   Save it in Published Queries.
B.   Save it in Public Templates.
C.   Grant Read Query permission to the domain.
D.   Check the Shared option on the saved query.

"Pass Any Exam. Any Time." - www.actualtests.com 17
Symantec ST0-085 Exam

Answer: D

QUESTION 40
What is the common way in which new entries can be added to the Assets Table of a Symantec Security Information Manager solution?

A.   through the Lookup Tables pane of the Information Manager Console
B.   importing from HP OpenView through the OpenView Integration feature
C.   importing from a rule that is monitoring traffic on the network
D.   automatic population through a supported vulnerability scanner

Answer: D

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