



250-311

Administration of Symantec Endpoint Protection 11.0 for Windows

Document version: 1 .04 .11

Important Note About 250-311 PDF

techeXams' **250-311 PDF** is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Copyright

techeXams holds the copyright of this material. techeXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Question: 1

Which installation type options are available when defining Client Install Settings?

- A. Interactive, Silent, and Unattended
- B. Interactive, Restart, and Silent
- C. Restart, Silent, and Unmanaged
- D. Enable, Log, and Silent

Answer: A

Question: 2

In which Client Management Log can you identify when the client last connected to the Symantec Endpoint Protection Manager?

- A. Control
- B. Security
- C. System
- D. Compliance

Answer: C

Question: 3

Which log type displays configured firewall connections?

- A. Compliance
- B. System
- C. Traffic
- D. Audit

Answer: C

Question: 4

What are the three configurable actions in TruScan Proactive Threat Scan? (Choose three.)

- A. log suspect process only
- B. set a public SNMP trap
- C. quarantine suspect process
- D. terminate the suspect process
- E. generate dump of system state
- F. suspend the suspect process

Answer: A, C, D

Question: 5

Which firewall technique helps prevent OS fingerprinting?

- A. randomize TTL value
- B. close the IDENT port
- C. use varying ranges of ephemeral ports
- D. set QOS values to 0

Answer: A

Question: 6

Which two engines does Symantec Intrusion Prevention contain that identify attack signatures? (Choose two.)

- A. protocol anomaly based engine
- B. stream based engine
- C. packet based engine
- D. inference based engine
- E. reputation based engine

Answer: B, C

Question: 7

Which statement is true about the Database Backup and Restore utility?

- A. It only backs up an embedded database.
- B. It allows you to define the backup location.
- C. It saves database backups to the local computer.
- D. It is run from the Symantec Endpoint Protection Manager console.

Answer: C

Question: 8

In which order are exceptions processed?

- A. antispymware then antivirus
- B. administrator then user
- C. Intrusion Prevention then firewall
- D. Computer mode then User mode

Answer: B

Question: 9

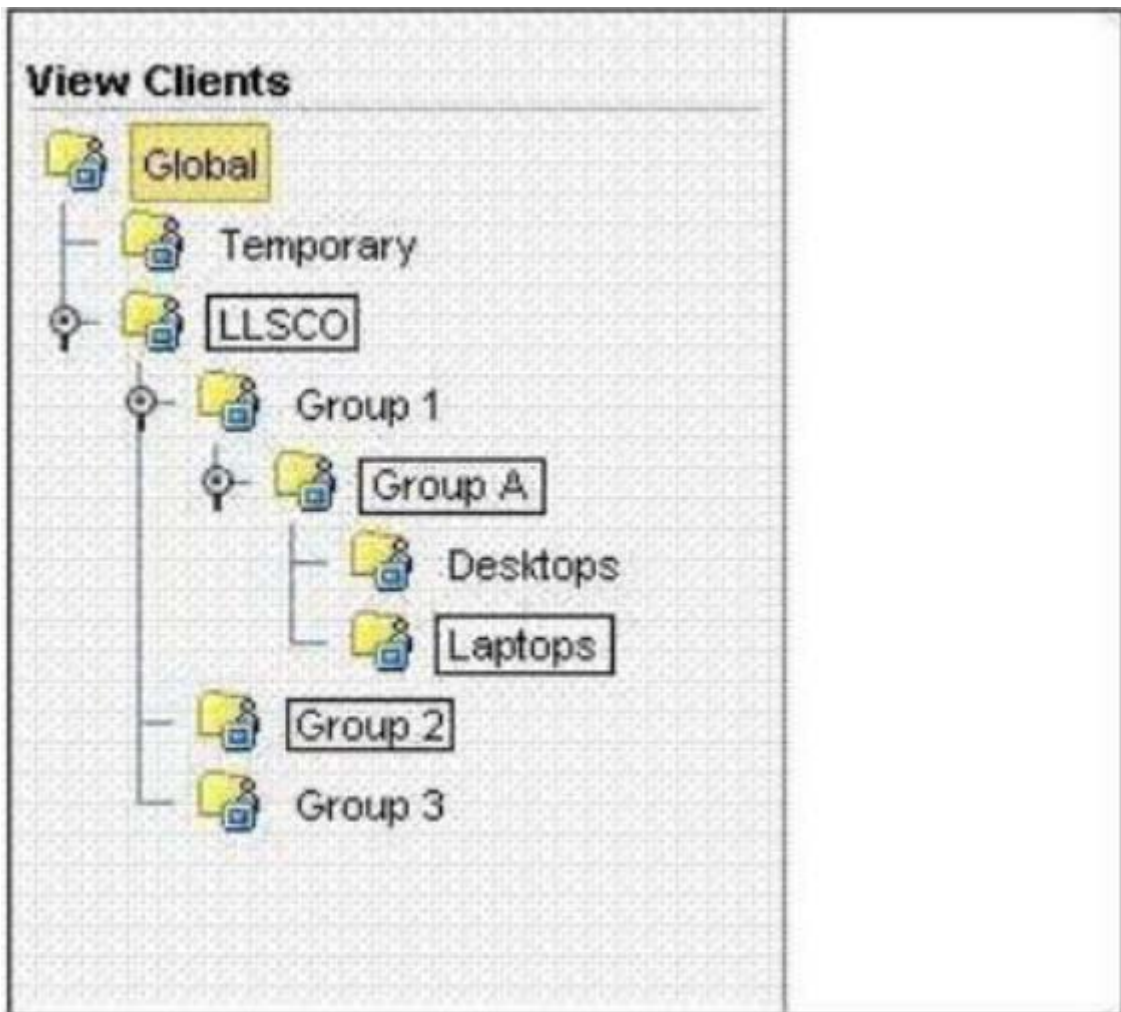
What is a possible use for a Custom IPS signature?

- A. to send a TCP reset
- B. to detect connected USB devices
- C. to identify Internet Relay Chat (IRC)
- D. to identify presence of a file on a local hard drive

Answer: C

Question: 10

Inheritance is turned on for groups LLSCO, Group A, Laptops, and Group 2 (outlined). Without turning inheritance off, which top level group must be modified to affect users in the Laptop group?



- A. Desktops
- B. Laptops
- C. Group 1
- D. Group A

Answer: C

Question: 11

When a security-related condition is met, which notification action can be performed?

- A. send an SNMP trap

- B. alert with a GUI popup on the admin console
- C. run a batch file or another executable file
- D. send an alert to a client

Answer: C

Question: 12

When a Group Update Provider (GUP) goes offline, what provides definition updates to the GUP's clients?

- A. Symantec LiveUpdate Servers
- B. Internal LiveUpdate Server
- C. Symantec Endpoint Protection Manager
- D. A different Group Update Provider

Answer: C

Question: 13

Which criteria can be used to define a process when creating an Application Control rule? (Choose three.)

- A. wildcards
- B. drive type
- C. username
- D. regular expressions
- E. port used by process

Answer: A, B, D

Question: 14

On which Symantec Endpoint Protection Manager console page are notifications configured?

- A. Home

- B. Monitors
- C. Reports
- D. Admin

Answer: B

Question: 15

What can you select when defining a new administrator account?

- A. a minimum and maximum password length
- B. a logon attempt threshold
- C. a specific management server
- D. a domain

Answer: B

Question: 16

Which three communication options can client communication to an internal LiveUpdate server use? (Choose three.)

- A. HTTP
- B. SSH
- C. UNC
- D. FTP
- E. TFTP

Answer: A, C, D

Question: 17

A user of the Lifeline Supply Company added a daily 10:00 am scheduled scan to their Symantec Endpoint Protection Client. After reviewing the logs, the user confirms that the scan failed to start at 10:00 am. What are two possible reasons that the scan failed to start? (Choose two.)

- A. The user was logged off of the computer.

- B. Delay scheduled scans when running on battery was enabled.
- C. Scan Progress options were set to not show progress.
- D. Auto-Protect was disabled.
- E. Auto-Protect was unlocked.

Answer: A, B

Get Full Version of Exam 250-311 PDF Q&A

techeXams presents authentic, genuine and valid study material, which promise 100% success in very first attempt. To take optimal results for 250-311 exam, you need to buy full version of 250-311 question and answer. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. So come join us and quench your thirst for knowledge.

Get complete 250-311 questions and answers by visiting URL

["http://www.techexams.ws/exams/250-311.do"](http://www.techexams.ws/exams/250-311.do)