250-311

Admin for Symantec Endpoint Protection 11.0 for windows

Version 11.4

250-311

QUESTION NO: 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 NO: 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 NO: 3

Which log type displays configured firewall connections?

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

Answer: C

QUESTION NO: 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 NO: 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 NO: 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 NO: 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 NO: 8

In which order are exceptions processed?

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

Answer: B

QUESTION NO: 9

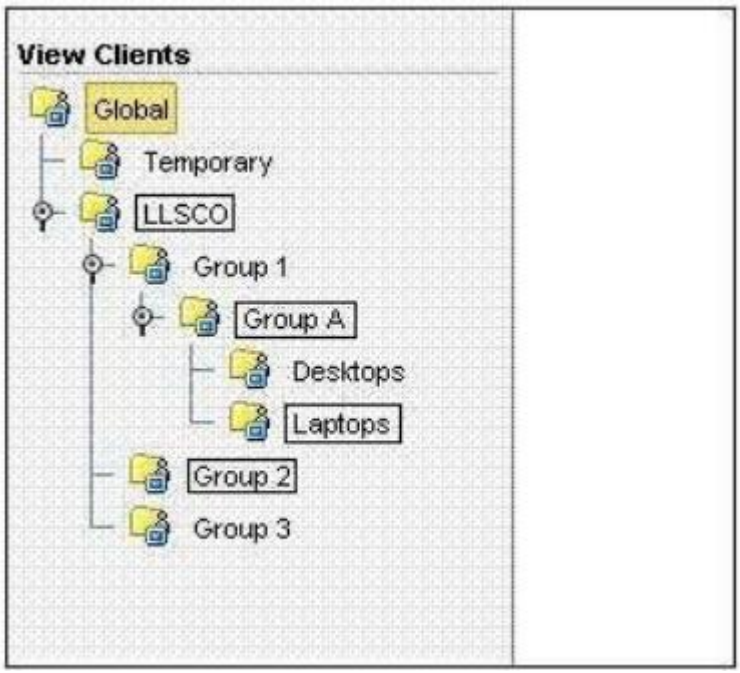
What is a possible use for a Custom IPS signature?

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 NO: 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 NO: 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 NO: 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 NO: 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 NO: 14

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

A. Home
B. Monitors
C. Reports
D. Admin

Answer: B

250-311

QUESTION NO: 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 NO: 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 NO: 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

QUESTION NO: 18

The administrator enabled the upload of a list of applications that clients ran, however, the list is empty. What is the cause of the problem?

A. The administrator lacks the necessary domain credentials to view applications on the clients.
B. The administrator disabled application learning at the site level.
C. The end users disabled learned applications.
D. he end users moved the applications to hidden folders.

Answer: B

QUESTION NO: 19

Using the Migration and Deployment Wizard, how can you identify computers for deployment?

A. by defining the appropriate management server list
B. by selecting the IP addresses from a domain server
C. by importing a text file of computer names
D. by importing a text file of computer IP addresses

Answer: D

QUESTION NO: 20

Lifeline Supply Company recently installed a proxy server and configured firewall rules to only allow HTTP traffic through the perimeter firewall. Since the change, Symantec Endpoint Protection is unable to receive updates.

Which step must be taken on the Symantec Endpoint Protection Manager to receive updates?

A. configure Proxy Settings at the site level
B. configure Proxy Settings at the server level
C. configure Proxy settings on the LiveUpdate Client on the manager
D. configure a Group Update Provider

Answer: B

QUESTION NO: 21

Where do you configure the LiveUpdate schedule for a client?

A. LiveUpdate Settings policy
B. LiveUpdate Content policy
C. Push or Pull heartbeat settings
D. Antivirus and Antispyware policy

Answer: A

QUESTION NO: 22

What is always replicated when replicating data between Symantec Endpoint Protection Managers?

A. policies, domains, install packages
B. content, install packages, logs
C. administrators, groups, policies
D. groups, logs, policies

Answer: C

QUESTION NO: 23

Which two types of firewall settings are found in Symantec Endpoint Protection? (Choose two.)

A. stealth
B. address transforms
C. protocol abnormality detection
D. smart traffic filters
E. VPN tunneling

Answer: A, D

QUESTION NO: 24

Which statement is true about Intrusion Prevention?

A. It must be managed from the policies applied only to the Global group.
B. It is a line of network defense after the firewall processes.
C. It is unavailable for use in an unmanaged client.
D. It provides secure tunneling for replication content.

Answer: B

QUESTION NO: 25

An administrator wants to create an Application Control rule that prevents notepad.exe from being executed from the command prompt, but allows the command prompt to remain running.

Which action must be used?

A. Continue Processing

B. Allow Access
C. Block Access
D. Terminate Process

Answer: C

QUESTION NO: 26

Where is Tamper Protection enabled or disabled?

A. Intrusion Prevention settings
B. Antivirus and Antispyware settings
C. General settings for that group
D. Application and Device Control settings

Answer: C

QUESTION NO: 27

Refer to the exhibit.

Based on the rules in the exhibit, what happens if the rule set is applied?

A. All computers can access the website www.symantec.com.
B. All computers can surf the Internet using Port 80.
C. All computers will have all communications blocked.
D. All computers will have all communications allowed.

Answer: C

QUESTION NO: 28

An administrator believes that client computers are running different software versions of Symantec Endpoint Protection.

Which report type shows which client computers are running different software versions?

A. Application and Device Control Report
B. System Report
C. Compliance Report
D. Computer Status Report

Answer: D

QUESTION NO: 29

You trigger on "Services" in a firewall rule.

Which layer of the OSI model does this trigger analyze?

A. physical
B. network
C. transport
D. presentation

Answer: C

QUESTION NO: 30

What happens when you mark the "Enable NetBIOS Protection" checkbox?

A. verifies remote computer identity using WINS server lookup
B. blocks NetBIOS requests on all NetBIOS potts
C. permits NetBIOS connections from local subnet only
D. dynamically adds an allow rule for NetBIOS

Answer: C

QUESTION NO: 31

Lifeline Supply Company employs 900 individuals at their location. Their data center is running Microsoft Exchange 2007 and an Oracle database. They are currently running different versions of Symantec Antivirus Corporate Edition managed through the Symantec System Center. They plan to migrate to Symantec Endpoint Protection and the IT director has to consider cost to benefit ratios given budgetary restrictions.

Which site design best fits this company's cost to benefit ratio requirements?

A. single site design with the embedded database and one Symantec Endpoint Protection Manager
B. single site design with clustered Microsoft SQL databases and multiple Symantec Endpoint Protection Managers
C. single site design with one Microsoft SQL database and multiple Symantec Endpoint Protection Managers D. single site design with the embedded database and multiple Symantec Endpoint Protection Managers

Answer: A

QUESTION NO: 32