Exam Code: 250-311

Exam Name: Admin for Symantec Endpoint Protection 11.0 for windows

Vendor: Symantec

Version: DEMO

Part: A

1: When Auto-Protect is enabled, protection is optional for which type of file access?
A.write
B.delete
C.backup
D.restore
Correct Answers: C

2: Which feature can be configured to increase or decrease performance of scheduled scans?
A.scan frequency
B.CPU throttling
C.heartbeat interval
D.tuning options
Correct Answers: D

3: In Symantec Endpoint Protection, which default action is taken when security risks such as spyware, adware, hacking tools, remote access programs, and trackware are detected?
A.log the detection event only
B.delete the infected file
C.clean the risk
D.quarantine the file locally
Correct Answers: D

4: Lifeline Supply Company deploys a freeware application, EasyWeatherView, that is funded by advertising. It is detected by Symantec Endpoint Protection as Adware.WeatherBorg because it includes banner advertisements in its client interface. The company accepts the risk and treats EasyWeatherView as an undetected application and bypasses the standard adware policy actions. How can this best be configured in Symantec Endpoint Protection?
A.edit the AntiVirus and AntiSpyware policy and set the Primary Action for security risks to Leave Alone
B.edit the Exclusion policy to exclude Adware.WeatherBorg from detection by marking the Exclude checkbox in the Threat list and clearing the
Log Option checkbox
C.edit the Application and Device Control policy and clear the EasyWeatherView checkbox in the Security Risk list for exclusions
D.edit the Exclusion policy to exclude Adware.WeatherBorg from detection by marking the Exclude checkbox in the Threat list and checking the
Deny Logging checkbox
Correct Answers: B

5: For which two items can users create exceptions? (Select two.) A.TruScan Proactive Threat Scan B.Client Firewall C.Intrusion Prevention D.Security Risks E.Application and Device Control
Correct Answers:

6: Which scan types can a user initiate?
A.idle, active, or full scan
B.custom, idle, or full scan
C.active, custom, or full scan
D.custom, quick, or full scan
Correct Answers: C

7: TruScan Proactive Threat Scans can respond to potentially malicious processes that they detect. Which two actions does the client take by default? (Select two.) A.logs the detection of processes that behave like trojan horses, worms, or keyloggers B.removes processes that behave like trojan horses, worms, or keyloggers C.quarantines processes that behave like trojan horses, worms, or keyloggers, and that require remediation D.terminates well-known commercial applications that exhibit suspicious behavior E.automatically creates an exception for well-known commercial applications so that future scans do not flag the process
Correct Answers:

8: Which two actions are available when TruScan Proactive Threat Scan detects a trojan or worm? (Select two.) A.delete B.ignore C.terminate D.quarantine E.clean
Correct Answers:

9: Centralized exceptions are exported as which file type?
A..dat
B..zip
C..exe
D..xml
Correct Answers: A

10: All email Auto-Protect is disabled, and an administrator receives an email from an associate with a .zip file attached. There are three files in the .zip file that are needed for the administrator's presentation the next day. What neither of them realize is that one of the files is infected with a virus. When will File System Auto-Protect detect this infected file?
A.when the email is opened
B.when the .zip file is opened
C.when the .zip file is saved to the administrator's desktop
D.when the email is closed
Correct Answers: B

11: Which content does an Intelligent Updater for Symantec Endpoint Protection client contain?
A.AntiVirus and AntiSpyware definitions only
B.AntiVirus and AntiSpyware definitions and Proactive Threat Scan definitions only
C.AntiVirus and AntiSpyware definitions, Proactive Threat Scan definitions, and IPS signatures only
D.AntiVirus and AntiSpyware definitions, Proactive Threat Scan definitions, IPS signatures, and

decomposer signatures
Correct Answers: A

12: Which log can have the most significant performance impact on Symantec Endpoint Protection Manager?
A.Traffic
B.Audit
C.Packet
D.System
Correct Answers: C

13: Which statement is true about the Database Backup and Restore utility?
A.It backs up and restores only an embedded database.
B.It allows an administrator to pause and resume backups.
C.It saves database backups to the local computer.
D.It backs up and restores the certificate keystore.
Correct Answers: C

14: LiveUpdate Content policies provide control over which two types of settings? (Select two.) A.how and where clients receive updates B.the specific update revisions the clients can download C.whether clients are able to download updates manually D.how often clients are able to receive updates E.which types of updates clients can download
Correct Answers:

15: How can an administrator manage multiple independent companies from one database while maintaining independent groups, computers, and policies?
A.set up limited administrators with appropriate rights
B.set up separate domains
C.set up additional sites using a single database
D.set up separate locations and turn off inheritance
Correct Answers: B

16: A company experiences a large number of Internet-based attacks. Which report can an administrator run to find the source of the highest number of attacks?
A.Computer Audit report
B.Host Compliance report
C.Computer Status report
D.Network Threat Protection report
Correct Answers: D

17: When can an administrator delete a location?
A.when the location is the default
B.when the group has inheritance turned off
C.when all client computers are disconnected

D.when the policy has been withdrawn
Correct Answers: B

18: By default, the client user interface control is set to Server Control. Which two will the user be able to perform? (Select two.) A.change AntiVirus and AntiSpyware settings B.edit firewall rules below the blue line C.change between Push and Pull mode D.disable Tamper Protection E.edit the Intrusion Prevention policy
Correct Answers:

19: An administrator needs to check when and by which account a policy was modified. Which log query should the administrator use?
A.Compliance
B.Audit
C.Access
D.System
Correct Answers: B

20: The server that contains the Symantec Endpoint Protection (SEP) MS SQL database has an unrecoverable hard drive failure. After rebuilding a new SQL server and ensuring that the SQL client on the Manager can connect, how is the database recovered?
A.select the database restore option in the Symantec Endpoint Protection Manager
B.launch Checksum, which will ask for the backup copy and restore the database
C.use the Backup and Restore utility included with SEP
D.restart the Manager and, when prompted, provide the path to the database
Correct Answers: C