IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **ST0-134**

Title : Symantec EndPoint Protection 12.1 Tcehnical Assessment

Version : DEMO

1.A financial company enforces a security policy that prevents banking system workstations from connecting to the Internet.
Which Symantec Endpoint Protection technology is ineffective on this company's workstations?
A.Insight
B.Intrusion Prevention
C.Network Threat Protection
D.Browser Intrusion Prevention
Answer:A

2.In addition to performance improvements, which two benefits does Insight provide? (Select two.)
A.reputation scoring for documents
B.zero-day threat detection
C.protection against malicious java scripts
D.false positive mitigation
E.blocking of malicious websites
Answer:BD

3.Which Symantec Endpoint Protection defense mechanism provides protection against threats that propagate from system to system through the use of autorun.inf files?
A.Application and Device Control
B.SONAR
C.TruScan
D.Host Integrity
Answer:A

4.Which protection technology can detect botnet command and control traffic generated on the Symantec Endpoint Protection client machine?
A.Insight
B.SONAR
C.Risk Tracer
D.Intrusion Prevention
Answer:D

5.Which technology can prevent an unknown executable from being downloaded through a browser session?
A.Browser Intrusion Prevention
B.Download Insight
C.Application Control
D.SONAR
Answer:B

6.Which Symantec Endpoint Protection technology blocks a downloaded program from installing browser plugins?
A.Intrusion Prevention

B.SONAR
C.Application and Device Control
D.Tamper Protection
Answer:C

7.Which protection engine should be enabled to drop malicious vulnerability scans against a client system?
A.SONAR
B.Intrusion Prevention
C.Tamper Protection
D.Application and Device Control
Answer:B

8.What is the file scan workflow order when Shared Insight Cache and reputation are enabled?
A.Symantec Insight > Shared Insight Cache server > local client Insight cache
B.local client Insight cache > Shared Insight Cache server > Symantec Insight
C.Shared Insight Cache server > local client Insight cache > Symantec Insight
D.local client Insight cache > Symantec Insight > Shared Insight Cache server
Answer:B

9.What is a function of Symantec Insight?
A.provides reputation ratings for structured data
B.enhances the capability of Group Update Providers (GUP)
C.increases the efficiency and effectiveness of LiveUpdate
D.provides reputation ratings for binary executables
Answer:D

10.Which Symantec Endpoint Protection component enables access to data through ad-hoc reports and charts with pivot tables?
A.Symantec Protection Center
B.Shared Insight Cache Server
C.Symantec Endpoint Protection Manager
D.IT Analytics
Answer:D

11.Which Symantec Endpoint Protection Management (SEPM) database option is the default for deployments of fewer than 1,000 clients?
A.Embedded: Using the Sybase SQL Anywhere database that comes with the product
B.On SEPM: Installing Microsoft SQL on the same server as the SEPM
C.External to SEPM: Using a preexisting Microsoft SQL server in the environment
D.Embedded: Using the Microsoft SQL database that comes with the product
Answer:A

12.Which two items are stored in the Symantec Endpoint Protection database? (Select two.)

A.Device Hardware IDs
B.User Defined Scans
C.Symantec Endpoint Protection Client for Linux
D.Symantec Endpoint Protection Client for Macintosh
E.Active Directory Synced Logon Credentials
Answer:AD

13.Which task should an administrator perform to troubleshoot operation of the Symantec Endpoint Protection embedded database?
A.verify that dbsrv11.exe is listening on port 2638
B.check whether the MSSQLSERVER service is running
C.verify the sqlserver.exe service is running on port 1433
D.check the database transaction logs in X:\Program Files\Microsoft SQL server
Answer:A

14.What is a function of the Symantec Endpoint Protection client?
A.uploads logs to the Shared Insight Cache
B.sends and receives application reputation ratings from LiveUpdate
C.downloads virus content updates from Symantec Insight
D.provides a Lotus Notes email scanner
Answer:D

15.Which option is unavailable in the Symantec Endpoint Protection console Run a command on the group menu item?
A.Disable SONAR
B.Scan
C.Disable Network Threat Protection
D.Update content and scan
Answer:A

16.Which object in the Symantec Endpoint Protection Manager console describes the most granular level to which a policy can be assigned?
A.Group
B.Computer
C.User
D.Client
Answer:A

17.Where can an administrator obtain the Sylink.xml file?
A.C:\Program Files\Symantec\Symantec Endpoint Protection\ folder on the client
B.C:\Program Files\Symantec\Symantec Endpoint Protection\Manager\data\inbox\agent\ folder on the Symantec Endpoint Protection Manager
C.by selecting the client group and exporting the communication settings in the Symantec Endpoint Protection Manager Console

D.by selecting the location and exporting the communication settings in the Symantec Endpoint Protection Manager Console
Answer:C

18.An administrator edited a firewall policy from the Clients > Policies tab.? Later, the administrator is unable to find the modified policy under the Policies > Firewall policies list.
What is the likely cause?
A.The administrator has set the policy to shared.
B.The administrator has set the policy to non-shared.
C.The administrator failed to save the policy.
D.The policy failed to deploy.
Answer:B

19.An administrator is unable to delete a location.
What is the likely cause?
A.The location currently contains clients.
B.Criteria is defined within the location.
C.The administrator has client control enabled.
D.The location is currently assigned as the default location.
Answer:D

20.Which two are policy types within the Symantec Endpoint Protection Manager? (Select two.)
A.Exceptions
B.Host Protection
C.Shared Insight
D.Intrusion Prevention
E.Process Control
Answer:AD