# Symantec

## Exam ST0-134

### Symantec EndPoint Protection 12.1 Technical Assessment

**Version: 8.0**

**[ Total Questions: 282 ]**

**Topic 1, Volume A**

**Question No : 1 - (Topic 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**

**Question No : 2 - (Topic 1)**

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: B,D**

**Question No : 3 - (Topic 1)**

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**

**Question No : 4 - (Topic 1)**

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**

**Question No : 5 - (Topic 1)**

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**

**Question No : 6 - (Topic 1)**

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**

**Question No : 7 - (Topic 1)**

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**

**Question No : 8 - (Topic 1)**

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**

**Question No : 9 - (Topic 1)**

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**

**Question No : 10 - (Topic 1)**

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**

**Question No : 11 - (Topic 1)**

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**

**Question No : 12 - (Topic 1)**

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: A,D**

**Question No : 13 - (Topic 1)**

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**

**Question No : 14 - (Topic 1)**

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**

**Question No : 15 - (Topic 1)**

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**

**Question No : 16 - (Topic 1)**

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**

**Question No : 17 - (Topic 1)**

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**

**Question No : 18 - (Topic 1)**

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**

**Question No : 19 - (Topic 1)**

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**

**Question No : 20 - (Topic 1)**

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: A,D**

**Question No : 21 - (Topic 1)**

What is a characteristic of a Symantec Endpoint Protection (SEP) domain?

**A.** Each domain has its own management server and database.
**B.** Every administrator from one domain can view data in other domains.
**C.** Data for each domain is stored in its own separate SEP database.
**D.** Domains share the same management server and database.

**Answer: D**

**Question No : 22 - (Topic 1)**

An organization employs laptop users who travel frequently. The organization needs to acquire log data from these Symantec Endpoint Protection clients periodically. This must

happen without the use of a VPN. Internet routable traffic should be allowed to and from which component?

**A.** Group Update Provider (GUP)
**B.** LiveUpdate Administrator Server (LUA)
**C.** Symantec Endpoint Protection Manager (SEPM)
**D.** IT Analytics Server (ITA)

**Answer: C**

**Question No : 23 - (Topic 1)**

An administrator is responsible for the Symantec Endpoint Protection architecture of a large, multi-national company with three regionalized data centers. The administrator needs to collect data fromclients; however, the collected data must stay in the the local regional data center. Communication between the regional data centers is allowed 20 hours a day. How should the administrator architect this organization?

**A.** set up 3 domains
**B.** set up 3 sites
**C.** set up 3 locations
**D.** set up 3 groups

**Answer: B**

**Question No : 24 - (Topic 1)**

A Symantec Endpoint Protection (SEP) Administrator is designing a new SEP architecture to ensure that clients continually maintain a current set of content updates. The criteria listed below must be considered.

1. Client systems are located in a single physical site where they are commonly offline for up to 2 weeks at a time

2. The Site consists of approximately 500 clients

3. Content Updates must be as current as possible

4. The embedded database must be used for the Symantec Endpoint Protection Manager

Which content update methodology minimizes the impact to the external Internet connection?

**A.** deploy an Internal LiveUpdate Administrator (LUA) and define the LiveUpdate Policy so the clients get their updates from the LUA
**B.** change the product defaults to define content revisions to 42 and configure the LiveUpdate Policy so the clients get their updates from the Symantec Endpoint Protection Manager
**C.** configure the Live Update Policy so the clients get their updates from a public Symantec LiveUpdate server
**D.** change the product defaults to define content revisions to 14 and configure the LiveUpdate Policy so the clients get their updates from a Group Update Provider (GUP)

**Answer: B**

**Question No : 25 - (Topic 1)**

An administrator is designing a new single site Symantec Endpoint Protection environment. Due to perimeter firewall bandwidth restrictions, the design needs to minimize the amount of traffic from content passing through the firewall. Which source must the administrator avoid using?

**A.** Symantec Endpoint Protection Manager
**B.** LiveUpdate Administrator (LUA)
**C.** Group Update Provider (GUP)
**D.** Shared Insight Cache (SIC)

**Answer: B**

**Question No : 26 - (Topic 1)**

A company plans to install six Symantec Endpoint Protection Managers (SEPMs) spread evenly across two sites. The administrator needs to direct replication activity to SEPM3 server in Site 1 and SEPM4 in Site 2. Which two actions should the administrator take to direct replication activity to SEPM3 and SEPM4? (Select two.)

**A.** install SEPM3 and SEPM4 after the other SEPMs
**B.** install the SQL Server databases on SEPM3 and SEPM4
**C.** ensure SEPM3 and SEPM4 are defined as the top priority server in the Site Settings