Symantec

Exam 250-315

Administration of Symantec Endpoint Protection 12.1

Version: 10.0

[Total Questions: 119]

Question No : 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

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

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 : 4

Users report abnormal behavior on systems where Symantec Endpoint Protection is installed.

Which tool can an administrator run on the problematic systems to identify the likely cause of the abnormal behavior?

A. smc.exe -stop
B. SymHelp.exe
C. PowerShell.exe
D. CleanWipe.exe

Answer: B

Question No : 5

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 : 6

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 : 7

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 : 8

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 : 9

Which option is unavailable in the Symantec Endpoint Protection console to 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 : 10

Which two Symantec Endpoint Protection components are used to distribute content updates? (Select two.)

A. Group Update Provider (GUP)
B. Shared Insight Cache Server
C. Symantec Protection Center
D. Symantec Endpoint Protection Manager
E. Symantec Insight Database

Answer: A,D

Question No : 11

What is a valid Symantec Endpoint Protection (SEP) single site design?

A. Multiple MySQL databases
B. One Microsoft SQL Server database
C. One Microsoft SQL Express database
D. Multiple embedded databases

Answer: A

Question No : 12

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 : 13

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 : 14

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 : 15

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 : 16

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 from clients; however, the collected data must stay in 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 : 17

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 : 18

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
D. Ensure SEPM3 and SEPM4 are defined as remote servers in the replication partner configuration
E. Install IT Analytics on SEPM3 and SEPM4

Answer: C,D

Question No : 19

A company needs to forward log data from Data Center A to Data Center B during off peak hours only.

How should the company architect its Symantec Endpoint Protection environment?

A. Set up two sites and schedule replication between them during off peak hours
B. Set up a single site and configure the clients to send their logs to the Manager during off peak hours
C. Set up a Group Update Provider (GUP) at Data Center A and configure it to send logs during off peak hours
D. Set up a LiveUpdate Server at Data Center A and configure it to send logs during off peak hours

Answer: D

Question No : 20

A Symantec Endpoint Protection administrator needs to comply with a service level agreement stipulating that all definitions must be internally quality assurance tested before

being deployed to customers.

Which step should the administrator take?

A. install a LiveUpdate Administrator Server
B. install a Shared Insight Cache Server
C. install a Group Update Provider (GUP) to the existing site
D. install a Symantec Protection Center

Answer: D

Question No : 21

In Symantec Endpoint Protection 12.1 Enterprise Edition, what happens when the license expires?

A. LiveUpdate stops.
B. Group Update Providers (GUP) stop.
C. Symantec Insight is disabled.
D. Content updates continue.

Answer: D

Question No : 22

An administrator receives a browser certificate warning when accessing the Symantec Endpoint Protection Manager (SEPM) Web console.

Where can the administrator obtain the certificate?

A. SEPM console Licenses section
B. Admin > Servers > Configure SecureID Authentication
C. SEPM console Admin Tasks
D. SEPM Web Access

Answer: D