Symantec Endpoint Protection 12.1 Technical Assessment

1. Which Symantec Endpoint Protection Manager feature allows an administrator to view and modify commonly accessed reports?

A. Favorite Reports Display list on the Home page

B. Scheduled Reports in the Reports section

C. Summary Dropdown in the Monitors section

D. Favorite Reports Display list on the Monitors page

Answer(s): A

---

2. A company has 10,000 Symantec Endpoint Protection (SEP) clients deployed using two Symantec Endpoint Protection Managers (SEPMs). Which configuration is recommended to ensure that each SEPM is able to effectively handle the communications load with the SEP clients?

A. Server control mode

B. Push mode

C. Client control mode

D. Pull mode

Answer(s): D

---

3. In addition to adding exceptions directly into an Exceptions policy, what is another method of adding exceptions?

A. adding the exception from the Threat report

B. adding the application exception to a File Fingerprint list

C. adding the exception to a policy from the Application Control log

D. importing the exception into a policy from the Notifications window

Answer(s): C

---

4. An administrator is logged in to the Symantec Endpoint Protection Manager (SEPM) console for a system named SEPM01. The groups and policies that were previously in the SEPM01 console are unavailable and have been replaced with unfamiliar groups and policies. What was a possible reason for this change?

A. The administrator was modified from using Computer mode to User mode.

B. The administrator was changed from a limited administrator to a system administrator.

C. The administrator was using the Web console instead of the Java console.

D. The administrator was logged in to the incorrect domain for SEPM01.

Answer(s): D

---

5. Which Symantec Endpoint Protection 12.1 component uses Sybase SQL Anywhere?

A. Symantec Endpoint Protection Manager embedded database

B. Shared Insight Cache server

C. LiveUpdate Administrator server

D. Symantec Endpoint Protection Manager remote database

Answer(s): A

---

6. Acrobat Reader is being targeted by a threat using process injection. Which feature of SONAR is sandboxing Acroread32.exe so that the threat is prevented from dropping its payload?

A. Commercial Application Detection

B. System Change Events

C. Suspicious Behavior Detection

D. Signature Based Detection

Answer(s): C

---

7. A large software company runs a small engineering department that is remotely located over a slow WAN connection. Which option should the company use to install an exported Symantec Endpoint Protection (SEP) package to the remote site using the smallest amount of network bandwidth?

A. a SEP package using the Install Packages tab

B. a SEP package using a policy defined Multiple Group Update Provider (GUP) list

C. a SEP package using a policy defined Single Group Update Provider (GUP)

D. a SEP package using Basic content

Answer(s): D

---

8. An administrator needs to learn the applications running on a computer. Which step should the administrator take to configure functionality?

A. configure a local Symantec Endpoint Protection Manager administrator to have rights to view reports only

B. enable application tracking under communication settings at the site level

C. enable file fingerprinting on the Symantec Endpoint Protection client

D. configure pull mode for Application Learning

Answer(s): B

---

9. Which technology uses heuristics to scan outbound email?

A. Internet Email Auto-Protect

B. Lotus Notes Auto-Protect

C. Microsoft Outlook Auto-Protect

D. SONAR

Answer(s): A

---

10. A Symantec Endpoint Protection (SEP) client uses a management server list with three management servers in the priority 1 list. Which mechanism does the SEP client use to select an alternate management server if the currently selected management server is unavailable?

A. The client chooses another server in the list randomly.

B. The client chooses a server with the next highest IP address.

C. The client chooses a server based on the lowest server load.

D. The client chooses the next server alphabetically by server name.

Answer(s): A

---

11. A company creates free web access computers for use in public areas, such as airports. The software provided on the computers will be static and the systems must be secure. What should be used to restrict unauthorized applications from running on these computers?

A. client security settings and Tamper Protection

B. custom IPS signatures in an Intrusion Prevention policy

C. blocked devices in an Application and Device Control policy

D. file fingerprint list and System Lockdown

Answer(s): D

---

12. What is the default replication frequency when adding an additional site to a Symantec Endpoint Protection 12.1 deployment?

A. 1 hour

B. 8 hours

C. daily

D. Auto replicate

Answer(s): C

---

13. 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. Intrusion Prevention

B. Network Threat Protection

C. Browser Intrusion Prevention

D. Insight

Answer(s): D

---

14. A company is building a new Symantec Endpoint Protection Manager (SEPM) and building email notifications that will go to the security team. Which two notification conditions should the team implement into the SEPM? (Select two.)

A. Risk Outbreak

B. Group Update Provider Failure

C. Invalid Host Name

D. Unknown User

E. Authentication Failure

Answer(s): A,E

---

15. Employees of an accounting company often take their notebooks to customer sites. The administrator needs to apply a different firewall policy when the notebooks are disconnected from the accounting company's network. What must the administrator configure to use the two different policies?

A. Groups

B. Sites

C. Locations

D. Domains

Answer(s): D

---

16. Which protection technology can detect botnet command and control traffic generated on the Symantec Endpoint Protection client machine?

A. Intrusion Prevention

B. Risk Tracer

C. Insight

D. SONAR

Answer(s): A

---

17. A company is running the Symantec Endpoint Protection 12.1 firewall and wants to ensure that DNS traffic is allowed. Which feature should be enabled in the firewall policy?

A. Smart DNS

B. Reverse DNS Lookup

C. DNS exception

D. DNS Lookup

Answer(s): A

---

18. Multiple Windows virtual clients running on an ESX server need to be scanned daily by a scheduled scan. Which feature should an administrator use to improve scan performance on the clients?

A. Download Insight

B. Centralized Scan exceptions

C. Virtual Image exceptions

D. Tamper Protection

Answer(s): C

---

19. By default, the Client User Interface control is set to Server Control. Which two actions will the user who is logged in as a Windows administrator be able to perform? (Select two.)

A. Disable Tamper Protection.

B. Change Virus and Spyware Protection settings.

C. Change between Push and Pull mode.

D. Edit firewall rules below the blue line.

E. Edit the Intrusion Prevention policy.

Answer(s): A,B

---

20. An administrator wants to make sure users are warned when they decide to download potentially malicious files. Which option should the administrator configure?

A. the Notifications tab under Download Insight settings

B. the Notifications tab under the admin-defined scan settings

C. the Notifications tab under Auto-Protect settings

D. the Network Protection Security event notification in location-specific settings

Answer(s): A
