ST0-134 Q&As

Symantec EndPoint Protection 12.1 Technical Assessment

Pass Symantec ST0-134 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/st0-134.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec
Official Exam Center

QUESTION 1

Drive-by downloads are a common vector of infections. Some of these attacks use encryption to bypass traditional defense mechanisms. Which Symantec Endpoint Protection 12.1 protection technology blocks such obfuscated attacks?

A. SONAR

B. Bloodhound heuristic virus detection

C. Client Firewall

D. Browser Intrusion Prevention

Correct Answer: D

QUESTION 2

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

A. Favorite Reports Display list on the Monitors page

B. Scheduled Reports in the Reports section

C. Favorite Reports Display list on the Home page

D. Summary Dropdown in the Monitors section

Correct Answer: C

QUESTION 3

A large enterprise plans to deploy Symantec Endpoint Protection 12.1 (SEP) on 36,000 virtual endpoints distributed across 1,800 VMware ESX servers in a single datacenter. A system administrator needs to optimize endpoint scanning performance by enabling Shared Insight Cache (SIC) server functionality. Which two configuration changes should the administrator make to minimize the number of SIC servers that need to be deployed? (Select two.)

A. Perform regular scans of all virtual systems with the offline image scanner.

B. Enable scanning randomization across all SEP endpoints.

C. Enable virtual image exceptions across all SEP endpoints.

D. Disable Insight lookups for threat detection on each virtual SEP endpoint.

E. Enable download randomization across all SEP endpoints.

Correct Answer: BC

QUESTION 4

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

Correct Answer: A

QUESTION 5

Which Symantec Endpoint Protection 12.1 component improves performance because known good files are skipped?

A. LiveUpdate Administrator server

B. Group Update Provider

C. Shared Insight Cache server

D. Central Quarantine server

Correct Answer: C

QUESTION 6

A company is concerned that its clients may be out-of-date and it wants to ensure that all running applications are protected with Symantec\\'s latest definitions, even if they are unavailable on the Symantec Endpoint Protection 12.1 (SEP) client. How could the company configure SEP to achieve this goal?

A. Enable SONAR with High Risk detections set to Quarantine.

B. Enable Insight Lookup as part of a daily scheduled scan.

C. Enable Insight for Community and Symantec Trusted Files.

D. Enable and apply an Intrusion Prevention policy.

Correct Answer: B

QUESTION 7

Catastrophic hardware failure has occurred on a single Symantec Endpoint Protection Manager (SEPM) in an environment with two SEPMs. What is the quickest way an administrator can restore the environment to its original state?

A. build a new site and configure replication with the still functioning SEPM

B. install a new SEPM into the existing site

C. clone the still functioning SEPM and change the server.properties file

D. reinstall the entire SEPM environment

Correct Answer: B

QUESTION 8

An administrator is recovering from a Symantec Endpoint Manager (SEPM) site failure. Which file should the administrator use during an install of SEPM to recover the lost environment according to Symantec Disaster Recovery Best Practice documentation?

A. original installation log

B. recovery_timestamp file

C. settings.properties file

D. Sylink.xml file from the SEPM

Correct Answer: B

QUESTION 9

Which command line syntax invokes the Symantec Endpoint Protection Client Service to determine whether a more recent copy of the configuration file is available on the management server?

A. smc -getconfig

B. smc -getsylink

C. smc -update

D. smc updateconfig

Correct Answer: D

QUESTION 10

Which action does the Shared Insight Cache (SIC) server take when the whitelist reaches maximum capacity?

A. The SIC server allocates additional memory for the whitelist as needed.

B. The SIC server will start writing the cache to disk.

C. The SIC server will remove the least recently used items based on the prune size.

D. The SIC server will remove items with the fewest number of votes.

Correct Answer: C

QUESTION 11

An administrator is using the SylinkDrop tool to update a Symantec Endpoint Protection client install on a system. The client fails to migrate to the new Symantec Endpoint Protection Manager (SEPM), which is defined correctly in the Sylink.xml file that was exported from the SEPM.? Which settings must be provided with SylinkDrop to ensure the successful migration to a new Symantec Endpoint Protection environment with additional Group Level Security Settings?

A. -s "silent"

B. -t "Tamper Protect"

C. -r "reboot"

D. -p "password"

Correct Answer: D

QUESTION 12

Which two items should an administrator enter in the License Activation Wizard to activate a license? (Select two.)

A. password for the Symantec Licensing Site

B. purchase order number

C. serial number

D. Symantec License file

E. credit card number

Correct Answer: CD

QUESTION 13

A company needs to configure an Application and Device Control policy to block read/write access to all USB removable media on its Symantec Endpoint Protection (SEP) systems. Which tool should an administrator use to format the GUID and device IDs as required by SEP?

A. CheckSum.exe

B. DeviceTree.exe

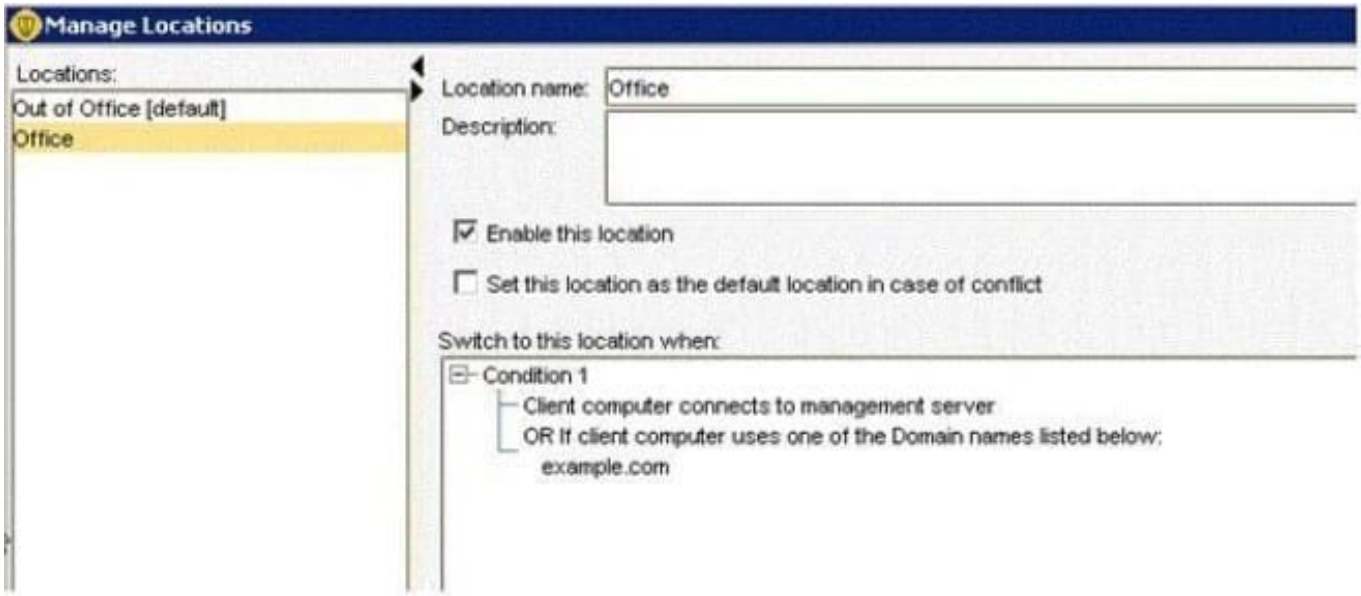
C. TaskMgr.exe

D. DevViewer.exe

Correct Answer: D

QUESTION 14

Refer to the exhibit.



In the use case displayed in the exhibit, why is the administrator unable to save the changes to this file?

A. Application Control is preventing Notepad from accessing the host file.

B. SONAR is set to block host file modifications.

C. Tamper Protection is enabled.

D. The Auto-Protect feature detected a malicious activity.

Correct Answer: B

QUESTION 15

A Symantec Endpoint Protection 12.1 (SEP) administrator deployed SEP clients, but the SEP clients are failing to register with the Symantec Endpoint Protection Manager (SEPM). Which solution would allow the clients to register with the SEPM?

A. Disable the firewall on the SEP client.

B. Allow port 8014 through the network firewall between the SEPM and the client.

C. Modify the network firewalls so that stateful packet inspection is performed.

D. Open the ephemeral TCP ports on the SEP client firewall.

Correct Answer: B

Latest ST0-134 Dumps ST0-134 Practice Test ST0-134 Study Guide