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.pass4itsure.com/st0-134.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

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 2

A company is building a new Symantec Endpoint Protection Manager and is setting the remediation actions for threats in the Virus and Spyware Protection policy. For security risks, the first action is set to Repair and the second action is Quarantine. In this environment, Symantec Endpoint Protection 12.1 (SEP) has been deployed to a small group of clients for testing. Which condition would cause Auto-Protect to stop sending notifications and stop logging the event after three detections?

A. A client continuously downloads the same security risk.

B. File System Auto Protect is malfunctioning on the SEP Client.

C. SEP services on the client are stopped.

D. SEP is unable to read virus definitions.

Correct Answer: A

QUESTION 3

A company is experiencing a malware outbreak. The company deploys Symantec Endpoint Protection 12.1, with only Virus and Spyware Protection, Application and Device Control, and Intrusion Prevention technologies. Why would Intrusion Prevention be unable to block all communications from an attacking host?

A. Intrusion Prevention needs the firewall component to block all traffic from the attacking host.

B. Intrusion Prevention blocks the attack only if the administrator wrote a signature for it.

C. Intrusion Prevention definitions are out-of-date.

D. Intrusion Prevention is set to log only.

Correct Answer: A

QUESTION 4

A company is currently testing Symantec Endpoint Protection 12.1 on 100 clients. The company has decided to deploy SEP to an additional 20,000 clients. They are concerned about the number of clients supported on a single Symantec Endpoint Protection Manager (SEPM). What should the company do to ensure that the SEPM can support the clients?

A. Configure the clients for Pull mode.

B. Decrease the heartbeat interval.

C. Switch to HTTPS for client communications.

D. Switch to IIS as the web server.

Correct Answer: A

QUESTION 5

Which two criteria can an administrator use to determine hosts in a host group? (Select two.)

A. Subnet

B. Network Services

C. Application Protocol

D. DNS Domain

E. Network Adapters

Correct Answer: AD