250-428 Q&As

Administration of Symantec Endpoint Protection 14

Pass Symantec 250-428 Exam with 100% Guarantee

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

https://www.geekcert.com/250-428.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

An organization is considering multiple sites for their Symantec Endpoint Protection environment.

What are two reasons that the organization should consider? (Choose two.)

A. Legal constraints

B. Control your hardware and administration costs

C. Content distribution

D. Tolerable downtime

E. Control when your WAN links are used

Correct Answer: BE

QUESTION 2

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

Correct Answer: A

QUESTION 3

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

Correct Answer: A

QUESTION 4

How should an administrator set up an alert to be notified when manual remediation is needed on an endpoint?

A. Add a System event notification and specify "Left Alone" for the action taken. Choose to log the notification and send an e-mail to the system administrators

B. Add a Single Risk Event notification and specify "Left Alone" for the action taken. Choose to log the notification and send an e-mail to the system administrators

C. Add a New risk detected notification and specify "Left Alone" for the action taken. Choose to log the notification and send an e-mail to the system administrators

D. Add a Client security alert notification and specify "Left Alone" for the action taken. Choose to log the notification and send an e-mail to the system administrators

Correct Answer: A

Reference: https://support.symantec.com/us/en/article.tech182388.html

QUESTION 5

A Symantec Endpoint Protection (SEP) administrator creates a firewall policy to block FTP traffic and assigns the policy to all of the SEP clients. The network monitoring team informs the administrator that a client system is making an FTP connection to a server. While investigating the problem from the SEP client GUI, the administrator notices that there are zero entries pertaining to FTP traffic in the SEP Traffic log or Packet log. While viewing the Network Activity dialog, there is zero inbound/outbound traffic for the FTP process.

What is the most likely reason?

A. The block rule is below the blue line.

B. The server has an IPS exception for that traffic.

C. Peer-to-peer authentication is allowing the traffic.

D. The server is in the IPS policy excluded hosts list.

Correct Answer: D