250-428^{Q&As}

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.passapply.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

A large-scale virus attack is occurring and a notification condition is configured to send an email whenever viruses infect five computers on the network. A Symantec Endpoint Protection administrator has set a one hour damper period for that notification condition.

How many notifications does the administrator receive after 30 computers are infected in two hours?

A. 1

B. 2

C. 6

D. 15

Correct Answer: B

QUESTION 2

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)

Correct Answer: C

QUESTION 3

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

References: https://support.symantec.com/en_US/article.TECH160736.html

QUESTION 4

What are two supported Symantec Endpoint Protection Manager authentication types? (Select two.)

A. Microsoft Active Directory

B. MS-CHAP

C. RSA SecurID

D. Biometrics

E. Network Access Control

Correct Answer: AC

QUESTION 5

An administrator plans to implement a multi-site Symantec Endpoint Protection (SEP) deployment. The administrator needs to determine whether replication is viable without needing to make network firewall changes or change defaults in SEP.

Which port should the administrator verify is open on the path of communication between the two proposed sites?

A. 1433

B. 2967

C. 8014

D. 8443

Correct Answer: D