Broadcom

250-428
Symantec Endpoint Protection 14 Technical Specialist

- **Up to Date products, reliable and verified.**
- **Questions and Answers in PDF Format.**

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

https://www.testsexpert.com/

- **Product Version**

Latest Version: 11.0

Question: 1

An administrator is re-adding an existing Replication Partner to the local Symantec Endpoint Protection Manager site.
Which two parameters are required to re-establish this replication partnership? (Select two.)

A. Remote site Encryption Password
B. Remote server IP Address and port
C. Remote SQL database account credentials
D. Remote server Administrator credentials
E. Remote site Domain ID

Answer: B,D

References: https://support.symantec.com/en_US/article.TECH104455.html

Question: 2

A company uses a remote administration tool that is detected and quarantined by Symantec Endpoint Protection (SEP).
Which step can an administrator perform to continue using the remote administration tool without detection by SEP?

A. Create a Tamper Protect exception for the tool
B. Create a SONAR exception for the tool
C. Create an Application to Monitor exception for the tool
D. Create a Known Risk exception for the tool

Answer: D

Question: 3

A Symantec Endpoint Protection (SEP) administrator performed a disaster recovery without a database backup.
In which file should the SEP administrator add “scm.agent.groupcreation=true” to enable the automatic creation of client groups?

A. conf.properties
B. httpd.conf
C. settings.conf

D. catalina.out

Answer: A

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

Question: 4

Why does Power Eraser need Internet access?

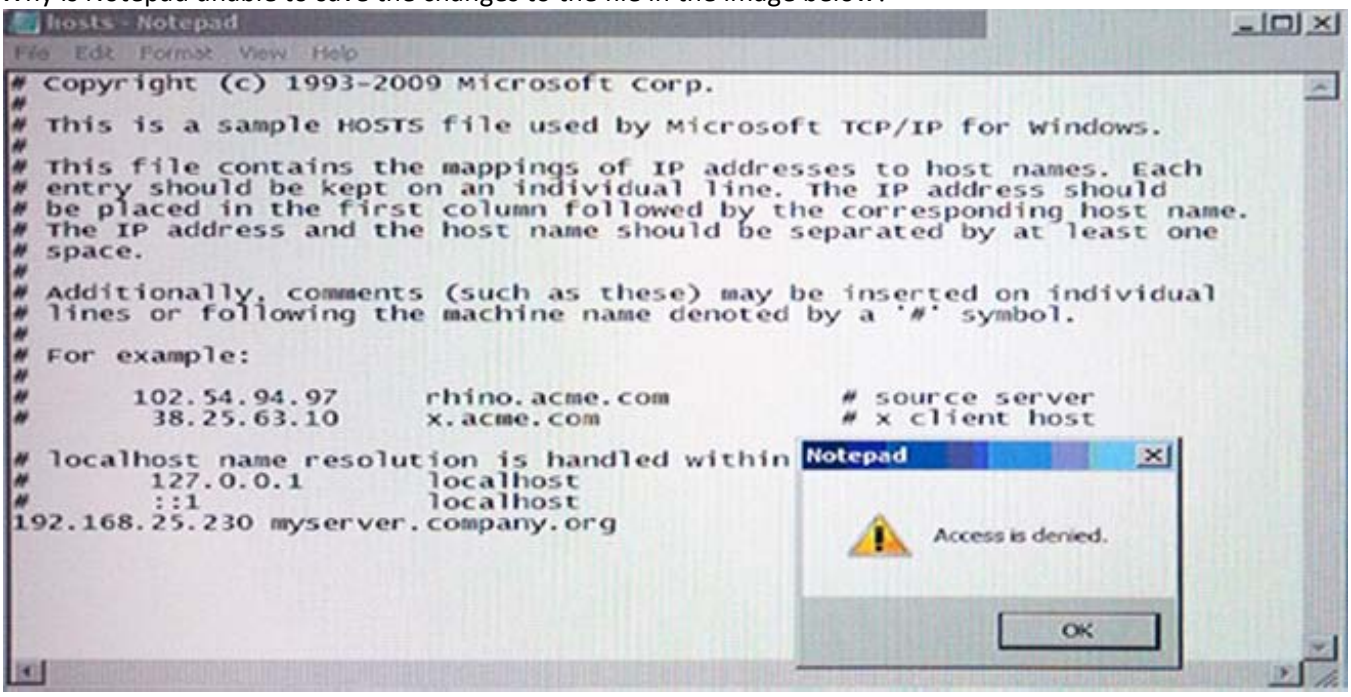
A. Validate root certificates on all portable executables (PXE) files
B. Leverage Symantec Insight
C. Ensure the Power Eraser tool is the latest release
D. Look up CVE vulnerabilities

Answer: B

References: https://support.symantec.com/en_US/article.TECH134803.html

Question: 5

Why is Notepad unable to save the changes to the file in the image below?



A. SONAR High Risk detection is set to Block
B. SONAR is set to block host file modifications.
C. Tamper Protection is preventing Notepad from modifying the host file.
D. System Lockdown is enabled.

Answer: B

Question: 6

Which package type should an administrator use to reduce a SEP environment's footprint when considering that new SEP 14 clients will be installed on point of sale terminals?

A. Default Standard Client
B. Default Embedded or VDI client
C. Default dark network client
D. Custom Standard client

Answer: B

References: https://support.symantec.com/en_US/article.HOWTO125381.html

Question: 7

An administrator plans to implement a multi-site Symantec Endpoint Protection (SEP) deployment. The administrator needs to determine whether replication is viable without having 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? (Type the port number.)

Answer: 8443

References: https://support.symantec.com/en_US/article.HOWTO81103.html

Question: 8

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. DevViewer.exe
C. TaskMgr.exe
D. DeviceTree.exe

Answer: B

Question: 9

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. Sylink.xml file from the SEPM
C. Settings.properties file
D. Recovery_timestamp file

Answer: D

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

Question: 10

DRAG DROP
An administrator is unknowingly trying to connect to a malicious website and download a known threat within a .rar file. All Symantec Endpoint Protection technologies are installed on the client's system.
Drag and drop the technologies to the right side of the screen in the sequence necessary to block or detect the malicious file.

Available Technologies	Appropriate
Download Insight	
Shared Insight Cache	
Device Control	
Firewall	
IPS	
Tamper Protection	

Answer:

Available Technologies	Appropriate
Download Insight	Firewall
Shared Insight Cache	IPS
Device Control	Download Insight
Firewall	
IPS	
Tamper Protection	

For More Information – **Visit link below:**

https://www.testsexpert.com/

16$ Discount Coupon: 9M2GK4NW

Features:

- Money Back Guarantee……..……...…. 

- 100% Course Coverage…… 

- 90 Days Free Updates…… 

- Instant Email Delivery after Order……