Vendor: Symantec

Exam Code:250-428

Exam Name: Administration of Symantec Endpoint Protection 14

Version: Demo

QUESTION 1

Which technology can prevent an unknown executable from being downloaded through a browser session?

A. Browser Intrusion Prevention

B. Download Insight

C. Application Control

D. SONAR

Correct Answer: B

QUESTION 2

You have executed the vxdg -g diskgroup adddisk disk_name= command.

Which switch needs to be added to force VxVM to take the disk media name of the failed disk and assign it to the new replacement disk?

A. -force

B. -k
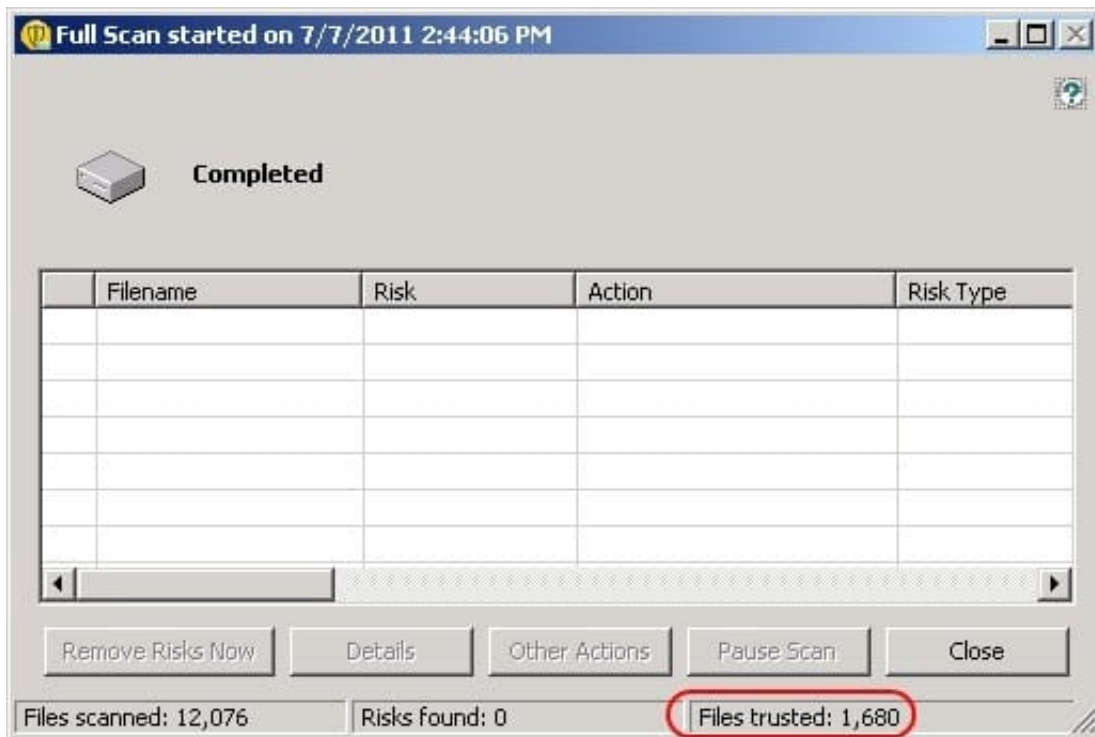
C. -f

D. -assign

Correct Answer: C

QUESTION 3

Which two Symantec Endpoint Protection components are used to distribute content updates? (Select two.)

A. Group Update Provider (GUP)

B. Shared Insight Cache Server

C. Symantec Protection Center

D. Symantec Endpoint Protection Manager

E. Symantec Insight Database

Correct Answer: AD

QUESTION 4

Refer to the exhibit.

Which settings can impact the Files trusted count?

A. SONAR settings in the Virus and Spyware Protection policy

B. System Lockdown Whitelist in the Application and Device Control policy

C. Insight settings in the Virus and Spyware Protection policy

D. File Cache settings in the Virus and Spyware Protection policy

Correct Answer: C

QUESTION 5

What does SONAR use to reduce false positives?

A. Virus and Spyware definitions

B. File Fingerprint list

C. Symantec Insight

D. Extended File Attributes (EFA) table

Correct Answer: C

References: https://support.symantec.com/en_US/article.HOWTO80929.html

QUESTION 6

Which two are policy types within the Symantec Endpoint Protection Manager? (Select two.)

A. Exceptions

B. Host Protection

C. Shared Insight

D. Intrusion Prevention

E. Process Control

Correct Answer: AD

References: https://support.symantec.com/en_US/article.TECH104434.html

---

QUESTION 7

A system running Symantec Endpoint Protection is assigned to a group with client user interface control settings set to mixed mode with Auto-Protect options set to Client. The user on the system is unable to turn off Auto-Protect. What is the likely cause of this problem?

A. Tamper protection is enabled.

B. System Lockdown is enabled.

C. Application and Device Control is configured.

D. The padlock on the enable Auto-Protect option is locked.

Correct Answer: D

QUESTION 8

Which Symantec Endpoint Protection component enables access to data through ad-hoc reports and charts with pivot tables?

A. Symantec Protection Center

B. Shared Insight Cache Server

C. Symantec Endpoint Protection Manager

D. IT Analytics

Correct Answer: D

QUESTION 9

Which two options are available when configuring DNS change detected for SONAR? (Select two.)

A. Block

B. Active Response

C. Quarantine

D. Log

E. Trace

Correct Answer: AD

QUESTION 10

An organization has a group of 500 SEP for Windows Clients running 12.1 RU5. The organization wants to migrate the clients to 14 RU1, but must minimize WAN bandwidth usage. What installation method should the organization use?

A. Push Deployment Wizard

B. Clients Install Package hosted on a local HTTP Server

C. Client Deployment Wizard

D. Auto Upgrade

Correct Answer: D

QUESTION 11

A company plans to install six Symantec Endpoint Protection Managers (SEPMs) spread evenly across two sites. The administrator needs to direct replication activity to SEPM3 server in Site 1 and SEPM4 in Site 2. Which two actions should the administrator take to direct replication activity to SEPM3 and SEPM4? (Select two.)

A. Install SEPM3 and SEPM4 after the other SEPMs

B. Install the SQL Server databases on SEPM3 and SEPM4

C. Ensure SEPM3 and SEPM4 are defined as the top priority server in the Site Settings

D. Ensure SEPM3 and SEPM4 are defined as remote servers in the replication partner configuration

E. Install IT Analytics on SEPM3 and SEPM4

Correct Answer: CD

QUESTION 12

What SEP feature is leveraged when configuring custom IPS?

A. Firewall

B. Virus and Spyware

C. Host Integrity

D. SONAR

Correct Answer: A

Reference: https://www.symantec.com/connect/forums/sep-custom-ips-signatures