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.certbus.com/250-428.html

100% Passing Guarantee
100% Money Back Assurance

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

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

A Symantec Endpoint Protection administrator must block traffic from an attacking computer for a specific time period. Where should the administrator adjust the time to block the attacking computer?

A. in the firewall policy, under Protection and Stealth

B. in the firewall policy, under Built in Rules

C. in the group policy, under External Communication Settings

D. in the group policy, under Communication Settings

Correct Answer: A

QUESTION 3

Solusell recently deployed SEP 14 in their environment and created the following groups for their computers: Desktops Laptops Servers

What type of group structure does Solusell use?

A. Role

B. Combination

C. Folder

D. Geography

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.tech134409.html

QUESTION 4

Which Symantec Endpoint Protection defense mechanism provides protection against threats that propagate from system to system through the use of autotun.inf files?

A. Host Integrity

B. SONAR

C. Application and Device Control

D. Emulator

Correct Answer: C

QUESTION 5

In the virus and Spyware Protection policy, an administrator sets the First action to Clean risk and sets If first action fails to Delete risk. Which two factors should the administrator consider? (Select two.)

A. The deleted file may still be in the Recycle Bin.

B. IT Analytics may keep a copy of the file for investigation.

C. False positives may delete legitimate files.

D. Insight may back up the file before sending it to Symantec.

E. A copy of the threat may still be in the quarantine.

Correct Answer: CE

QUESTION 6

Which action should an administrator take to prevent users from using Windows Security Center?

A. Set Disable antivirus alert within Windows Security Center to Disable

B. Set Disable Windows Security Center to Always

C. Set Disable Windows Security Center to Disable

D. Set Disable antivirus alert within Windows Security Center to Never

Correct Answer: B

QUESTION 7

A Symantec Endpoint Protection administrator needs to comply with a service level agreement stipulating that all

definitions must be internally quality assurance tested before being deployed to customers.

Which step should the administrator take?

A. install a LiveUpdate Administrator Server

B. install a Shared Insight Cache Server

C. install a Group Update Provider (GUP) to the existing site

D. install a Symantec Protection Center

Correct Answer: D

QUESTION 8

An administrator needs to identify infected computers that require a restart to finish remediation of a threat. What steps in the SEPM should an administrator perform to identify and restart the systems?

A. View the Computer Status log to determine if any computers require a restart. Run a command from the SONAR log to restart computers.

B. View the Computer Status log to determine if any computers require a restart. Run a command from the Attack log to restart computers.

C. View the SONAR log to determine if any computers require a restart. Run a command from the Computer Status log to restart computers.

D. View the Computer Status log to determine if any computers require a restart. Run a command from the Risk log to restart computers.

Correct Answer: D

Reference: https://support.symantec.com/us/en/article.HOWTO80936.html

QUESTION 9

An administrator is unable to delete a location.

What is the likely cause?

A. The location currently contains clients.

B. Criteria is defined within the location.

C. The administrator has client control enabled.

D. The location is currently assigned as the default location.

Correct Answer: D

QUESTION 10

Which step is unnecessary when an administrator creates an application rule set?

A. define a provider

B. select a process to apply

C. select a process to exclude

D. define rule order

Correct Answer: A

QUESTION 11

An organization has a small group of Incident Responders (IR) using pentest tools and network monitoring (AngryIP scanner, Nmap). They need to allow all inbound and outbound traffic for their tools. What policy changes does the SEP Administrator need to configure in the SEPM?

A. Create a Firewall rule that allows all hosts in the Firewall policy and enable Host Integrity

B. Create a Firewall rule that allows all hosts in the Firewall policy and add the computers as a Trusted Web Domain in the Exceptions policy

C. Create a Firewall rule that allows all hosts in the Firewall policy and enable System Lockdown

D. Create a Firewall rule for each application in the firewall policy and add the IR computers to the Excluded Hosts in the IPS policy

Correct Answer: B

QUESTION 12

A Symantec Endpoint Protection (SEP) administrator is remotely deploying SEP clients, but the clients are failing to install on Windows XP.

What are two possible reasons for preventing installation? (Select two.)

A. Windows firewall is enabled.

B. Internet Connection firewall is disabled.

C. Administrative file shares are enabled.

D. Simple file sharing is enabled.

E. Clients are configured for DHCP.

Correct Answer: AD

QUESTION 13

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 14

An administrator uses ClientSideClonePrepTool to clone systems and virtual machine deployment.

What will the tool do when it is run on each system?

A. Run Microsoft SysPrep and removes all AntiVirus/AntiSpyware definitions

B. Disable Tamper Protect and deploys a Sylink.xml

C. Add a new Extended File Attribute value to all existing files

D. Remove unique Hardware IDs and GUIDs from the system

Correct Answer: D

QUESTION 15

An administrator is using the SylinkDrop tool to update a Symantec Endpoint Protection client install on a system. The client fails to migrate to the new Symantec Endpoint Protection Manager (SEPM), which is defined correctly in the Sylink.xml file that was exported from the SEPM.

Which settings must be provided with SylinkDrop to ensure the successful migration to a new Symantec Endpoint Protection environment with additional Group Level Security Settings?

A. -s "silent"

B. -t "Tamper Protect"

C. -r "reboot"

D. -p "password"

Correct Answer: D