250-315 Q&As

Administration of Symantec Endpoint Protection 12.1

Pass Symantec 250-315 Exam with 100% Guarantee

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

https://www.pass4itsure.com/250-315.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

An administrator changes the Virus and Spyware Protection policy for a specific group that disables Auto-Protect. The administrator assigns the policy and the client systems applies the corresponding policy serial number. Upon visual inspection of a physical client system, the policy serial number is correct. However, Auto-Protect is still enabled on the client system.

Which action should the administrator take to ensure that the desired setting is in place on the client?

A. Restart the client system

B. Run a command on the computer to Update Content

C. Enable the padlock next to the setting in the policy

D. Withdraw the Virus and Spyware Protection policy

Correct Answer: C

QUESTION 3

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 an Application to Monitor exception for the tool

C. create a Known Risk exception for the tool

D. create a SONAR exception for the tool

Correct Answer: C

QUESTION 4

When can an administrator add a new replication partner?

A. immediately following the first LiveUpdate session of the new site

B. during a Symantec Endpoint Protection Manager upgrade

C. during the initial install of the new site

D. immediately following a successful Active Directory sync

Correct Answer: C

QUESTION 5

Which ports on the company firewall must an administrator open to avoid problems when connecting to Symantec Public LiveUpdate servers?

A. 25, 80, and 2967

B. 2967, 8014, and 8443

C. 21, 443, and 2967

D. 21, 80, and 443

Correct Answer: D

QUESTION 6

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 7

Catastrophic hardware failure has occurred on a single Symantec Endpoint Protection Manager (SEPM) in an environment with two SEPMs.

What is the quickest way an administrator can restore the environment to its original state?

A. build a new site and configure replication with the still functioning SEPM

B. install a new SEPM into the existing site

C. clone the still functioning SEPM and change the server.properties file

D. reinstall the entire SEPM environment

Correct Answer: B

QUESTION 8

Which two instances could cause Symantec Endpoint Protection to be unable to remediate a file? (Select two.)

A. Another scan is in progress.

B. The detected file is in use.

C. There are insufficient file permissions.

D. The file is marked for deletion by Windows on reboot.

E. The file has good reputation.

Correct Answer: BC

QUESTION 9

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 10

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. DeviceTree.exe

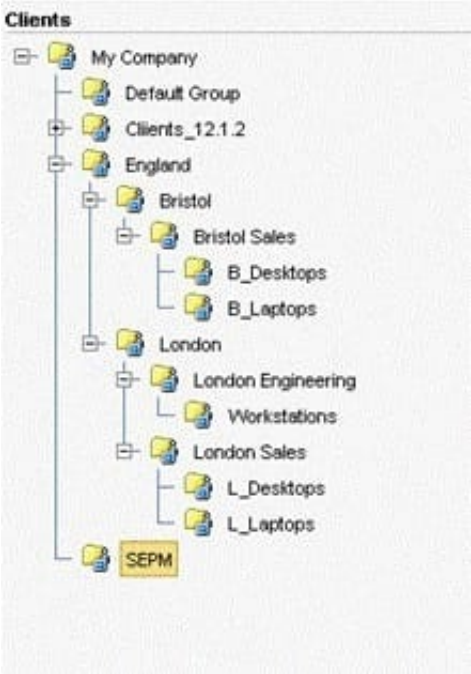
C. TaskMgr.exe

D. DevViewer.exe

Correct Answer: D

QUESTION 11

Refer to the exhibit.



A manufacturing company runs three shifts at their Bristol Sales office. These employees currently share desktops in the B_Desktops group. The administrators need to apply different policies/configurations for each shift.

Which step should the administrator take in order to implement shift policies after switching the clients to user mode?

A. create three shift policies for the Bristol group

B. create a group for each shift of users in the Bristol group

C. turn on inheritance for all groups in England

D. turn on Active Directory integration

E. modify the B_Desktops policy

Correct Answer: B

QUESTION 12

An administrator selects the Backup files before attempting to repair the Remediations option in the Auto-Protect policies.

Which two actions occur when a virus is detected? (Select two.)

A. replace the file with a place holder

B. check the reputation

C. store in Quarantine folder

D. send the file to Symantec Insight

E. encrypt the file

Correct Answer: CE

QUESTION 13

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 14

An administrator is designing a new single site Symantec Endpoint Protection environment. Due to perimeter firewall bandwidth restrictions, the design needs to minimize the amount of traffic from content passing through the firewall.

Which source must the administrator avoid using?

A. Symantec Endpoint Protection Manager

B. LiveUpdate Administrator (LUA)

C. Group Update Provider (GUP)

D. Shared Insight Cache (SIC)

Correct Answer: B

QUESTION 15

A company has an application that requires network traffic in both directions to multiple systems at a specific external domain. A firewall rule was created to allow traffic to and from the external domain, but the rule is blocking incoming traffic.

What should an administrator enable in the firewall policy to allow this traffic?

A. TCP resequencing

B. Smart DHCP

C. Reverse DNS Lookup

D. Smart WINS

Correct Answer: C