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.passapply.com/250-315.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 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 2

Which two considerations must an administrator make when enabling Application Learning in an environment? (Select two.)

A. Application Learning can generate increased false positives.

B. Application Learning should be deployed on a small group of systems in the enterprise.

C. Application Learning can generate significant CPU or memory use on a Symantec Endpoint Protection Manager.

D. Application Learning requires a file fingerprint list to be created in advance.

E. Application Learning is dependent on Insight.

Correct Answer: BC

QUESTION 3

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 4

Which tool should the administrator run before starting the Symantec Endpoint Protection Manager upgrade as a Symantec Best Practice?

A. collectLog.cmd

B. DBValidator.bat

C. LogExport.cmd

D. Upgrade.exe

Correct Answer: B

QUESTION 5

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

QUESTION 6

A company receives a high number of reports from users that files being downloaded from internal web servers are blocked. The Symantec Endpoint Protection administrator verifies that the Automatically trust any file downloaded from an intranet website option is enabled.

Which configuration can cause Insight to block the files being downloaded from the internal web servers?

A. Intrusion Prevention is disabled.

B. Local intranet zone is configured incorrectly on the Windows clients browser settings.

C. Local intranet zone is configured incorrectly on the Mac clients browser settings.

D. Virus and Spyware Definitions are out of date.

Correct Answer: B

QUESTION 7

Which action can an administrator take to improve the Symantec Endpoint Protection Manager (SEPM) dashboard performance and report accuracy?

A. decreasing the number of content revisions to keep

B. lowering the client installation log entries

C. rebuilding database indexes

D. limiting the number of backups to keep

Correct Answer: C

QUESTION 8

A Symantec Endpoint Protection (SEP) client uses a management server list with three management servers in the priority 1 list.

Which mechanism does the SEP client use to select an alternate management server if the currently selected management server is unavailable?

A. The client chooses another server in the list randomly.

B. The client chooses a server based on the lowest server load.

C. The client chooses a server with the next highest IP address.

D. The client chooses the next server alphabetically by server name.

Correct Answer: A

QUESTION 9

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 10

An administrator reports that the Home, Monitors, and Report pages are absent in the Symantec Endpoint Protection Management console when the administrator logs on.

Which action should the administrator perform to correct the problem?

A. configure proxy settings for each server in the site

B. configure External Logging to Enable Transmission of Logs to a Syslog Server

C. grant the Administrator Full Access to Root group of the organization

D. grant View Reports permission to the administrator

Correct Answer: D

QUESTION 11

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 12

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 13

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 14

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 15

An exception needs to be created for a file named "RunMe.exe" in a user\\'s Windows 7 "My Documents" folder. The user\\'s login name is Bob.

Which method should be used?

A. create a file exception for "RunMe.exe" with a Prefix Variable of [USERNAME]

B. create a file exception for "[Drive]:\Users\Bob\My Documents\RunMe.exe"

C. create a file exception for "*\RunMe.exe"

D. create a file exception for "RunMe.exe" with a Prefix Variable of %USERPROFILE%

Correct Answer: B