250-428$^{Q\&As}$

Administration of Symantec Endpoint Protection 14

Pass Symantec 250-428 Exam with 100% Guarantee

QUESTION 1

A Symantec Endpoint Protection Manager (SEPM) administrator notices performance issues with the SEPM server. The Client tab becomes unresponsive in the SEPM console and .DAT files accumulate in the "agentinfo" folder. Which tool should the administrator use to gather log files to submit to Symantec Technical Support?

A. collectLog.cmd

B. LogExport.exe

C. ExportLog.vbs

D. smc.exe

Correct Answer: A

References: https://support.symantec.com/en_US/article.TECH105955.html

QUESTION 2

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 3

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

A. Insight

B. Advanced Machine Learning

C. Application Control

D. Intrusion Prevention

Correct Answer: A

QUESTION 4

An organization created the following locations for their endpoint:

Internet (for remote user with no VPN)

VPN (remote users connected to the corporate network)

LAN Ethernet

LAN Wifi

The corporate network and VPN users have internet traffic filtered through a Content Analysis Appliance and a Next-Gen Firewall.

Which location is the most exposed to malicious downloads and needs a higher security posture in the Virus and Spyware protection policy?

A. Internet

B. LAN Wifi

C. LAN Ethernet

D. VPN

Correct Answer: A

QUESTION 5

Which protection technology can detect botnet command and control traffic generated on the Symantec Endpoint Protection client machine?

A. Intrusion Prevention

B. Insight

C. Risk Tracer

D. SONAR

Correct Answer: A

QUESTION 6

What should an administrator utilize to identify devices on a Mac?

A. Use DevViewer when the Device is connected

B. Use GatherSymantecInfo when the Device is connected

C. Use DeviceInfo when the Device is connected

D. Use Device Manager when the Device is connected

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.HOWTO80865.html

QUESTION 7

After several failed logon attempts, the Symantec Endpoint Protection Manager (SFPM) has locked the default admin account. An administrator needs to make system changes as soon as possible to address an outbreak, but the admin account is the only account.

Which action should the administrator lake to correct the problem with minimal impact to the existing environment?

A. Wait 15 minutes and attempt to log on again

B. Restore the SEPM from a backup

C. Run the Management Server and Configuration Wizard to reconfigure the server

D. Reinstall the SEPM

Correct Answer: A

Explanation: https://support.symantec.com/en_US/article.HOWTO80757.html

QUESTION 8

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

Correct Answer: B

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

QUESTION 9

A managed service provider (MSP) is managing Symantec Endpoint Protection for a number of independent companies. Each company has administrators who will log in from time to time to add new clients. Administrators must be prevented from seeing the existence of other companies in the console.

What should an administrator create for each independent company?

A. Domain

B. Location

C. Group

D. Site

Correct Answer: A

QUESTION 10

What is a function of Symantec Insight?

A. Provides reputation ratings for structured data

B. Enhances the capability of Group Update Providers (GUP)

C. Increases the efficiency and effectiveness of LiveUpdate

D. Provides reputation ratings for binary executables.

Correct Answer: D

QUESTION 11

A Symantec Endpoint Protection administrator needs to prevent users from modifying files in a specific program folder that is on all client machines. What does the administrator need to configure?

A. a file and folder exception in the Exception policy

B. an application rule set in the Application and Device Control policy

C. a file fingerprint list and System Lockdown

D. the Tamper Protection settings for the client folder

Correct Answer: B

QUESTION 12

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 13

What is the file scan workflow order when Shared Insight Cache and reputation are enabled?

A. Symantec Insight > Shared Insight Cache server > local client Insight cache

B. Local client Insight cache > Shared Insight Cache server > Symantec Insight

C. Shared Insight Cache server > local client Insight cache > Symantec Insight

D. Local client Insight cache > Symantec Insight > Shared Insight Cache server

Correct Answer: B

QUESTION 14

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. settings.conf

B. conf.properties

C. catalina.out

D. httpd.conf

Correct Answer: B

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

QUESTION 15

Which two criteria should an administrator use when defining Location Awareness for the Symantec Endpoint Protection (SEP) client? (Select two.)

A. NIC description

B. SEP domain

C. geographic location

D. WINS server

E. Network Speed

Correct Answer: AD

References: https://support.symantec.com/en_US/article.TECH97369.html