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.leads4pass.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

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 2

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 3

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

A. Insight

B. SONAR

C. Risk Tracer

D. Intrusion Prevention

Correct Answer: D

QUESTION 4

Which Symantec Endpoint Protection defense mechanism provides protection against threats that propagate from

system to system through the use of autorun.inf files?

A. Application and Device Control

B. SONAR

C. TruScan

D. Host Integrity

Correct Answer: A

QUESTION 5

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 6

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 7

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 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

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

QUESTION 10

Which two criteria can an administrator use to determine hosts in a host group? (Select two.)

A. Subnet

B. Network Services

C. Application Protocol

D. DNS Domain

E. Network Adapters

Correct Answer: AD

QUESTION 11

Why does Power Eraser need Internet access?

A. to leverage Symantec Insight

B. to validate root certificates on all portable executables (PXE) files

C. to ensure the Power Eraser tool is the latest release

D. to look up CVE vulnerabilities

Correct Answer: A

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

In Symantec Endpoint Protection 12.1 Enterprise Edition, what happens when the license expires?

A. LiveUpdate stops.

B. Group Update Providers (GUP) stop.

C. Symantec Insight is disabled.

D. Content updates continue.

Correct Answer: D

QUESTION 14

A Symantec Endpoint Protection (SEP) administrator creates a firewall policy to block FTP traffic and assigns the policy to all of the SEP clients. The network monitoring team informs the administrator that a client system is making an FTP connection to a server. While investigating the problem from the SEP client GUI, the administrator notices that there are zero entries pertaining to FTP traffic in the SEP Traffic log or Packet log. While viewing the Network Activity dialog, there is zero inbound/outbound traffic for the FTP process.

What is the most likely reason?

A. The block rule is below the blue line.

B. The server has an IPS exception for that traffic.

C. Peer-to-peer authentication is allowing the traffic.

D. The server is in the IPS policy excluded hosts list.

Correct Answer: D

QUESTION 15

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