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.pass4itsure.com/250-428.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 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 2

A financial company enforces a security policy that prevents banking system workstations from connecting to the Internet. Which Symantec Endpoint Protection technology is ineffective on this company\\'s workstations?

A. Insight

B. Intrusion Prevention

C. Network Threat Protection

D. Browser Intrusion Prevention

Correct Answer: A

QUESTION 3

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

References: https://support.symantec.com/en_US/article.TECH134367.html

QUESTION 4

Where can an administrator obtain the Sylink.xml file?

A. C:\Program Files\Symantec\Symantec Endpoint Protection\ folder on the client

B. C:\Program Files\Symantec\Symantec Endpoint Protection\Manager\data\inbox\agent\ folder on the Symantec Endpoint Protection Manager

C. by selecting the client group and exporting the communication settings in the Symantec Endpoint Protection Manager Console

D. by selecting the location and exporting the communication settings in the Symantec Endpoint Protection Manager Console

Correct Answer: C

QUESTION 5

What options should an administrator uncheck in the database properties if you perform database maintenance in SQL Management Studio?

A. Uncheck "Truncate the database transaction logs" and "Rebuild Indexes" in the General tab of the Database Properties

B. Uncheck "Truncate the database transaction logs" and "Rebuild Indexes" in the General tab of the Administrator Properties

C. Uncheck "Truncate the database transaction logs" and "Rebuild Indexes" in the General tab of the Site Properties

D. Uncheck "Truncate the database transaction logs" and "Rebuild Indexes" in the General tab of the Server Properties

Correct Answer: A

Reference: https://support.symantec.com/us/en/article.howto81047.html

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

An organization needs to be notified when certain types of events happen in their SEP environment.

What notification type should the SEP Administrator create to see attacks and events that the firewall or Intrusion Protection System (IPS) detects?

A. Create a Client Security Notification that filters by Traffic Events

B. Create a Client Security Notification that filters by Compliance Events

C. Create a Client Security Notification that filters by Network and Host Mitigation Events

D. Create a Client Security Notification that filters by Packet Events

Correct Answer: C

QUESTION 8

What are two methods the SEP Administrator can use for gathering a fingerprint list? (Choose two.)

A. GatherSymantecInfo

B. DevViewer

C. Checksum

D. DeviceInf

E. Get File Fingerprint list command

Correct Answer: CE

Reference: https://www.symantec.com/connect/articles/how-collect-and-add-fingerprint-any-app-or-location-sep-manager-graphical

QUESTION 9

A large software company runs a small engineering department that is remotely located over a slow WAN connection.

Which option should the company use to install an exported Symantec Endpoint Protection (SEP) package to the remote site using the smallest amount of network bandwidth?

A. a SEP package using Basic content

B. a SEP package using a policy defined Single Group Update Provider (GUP)

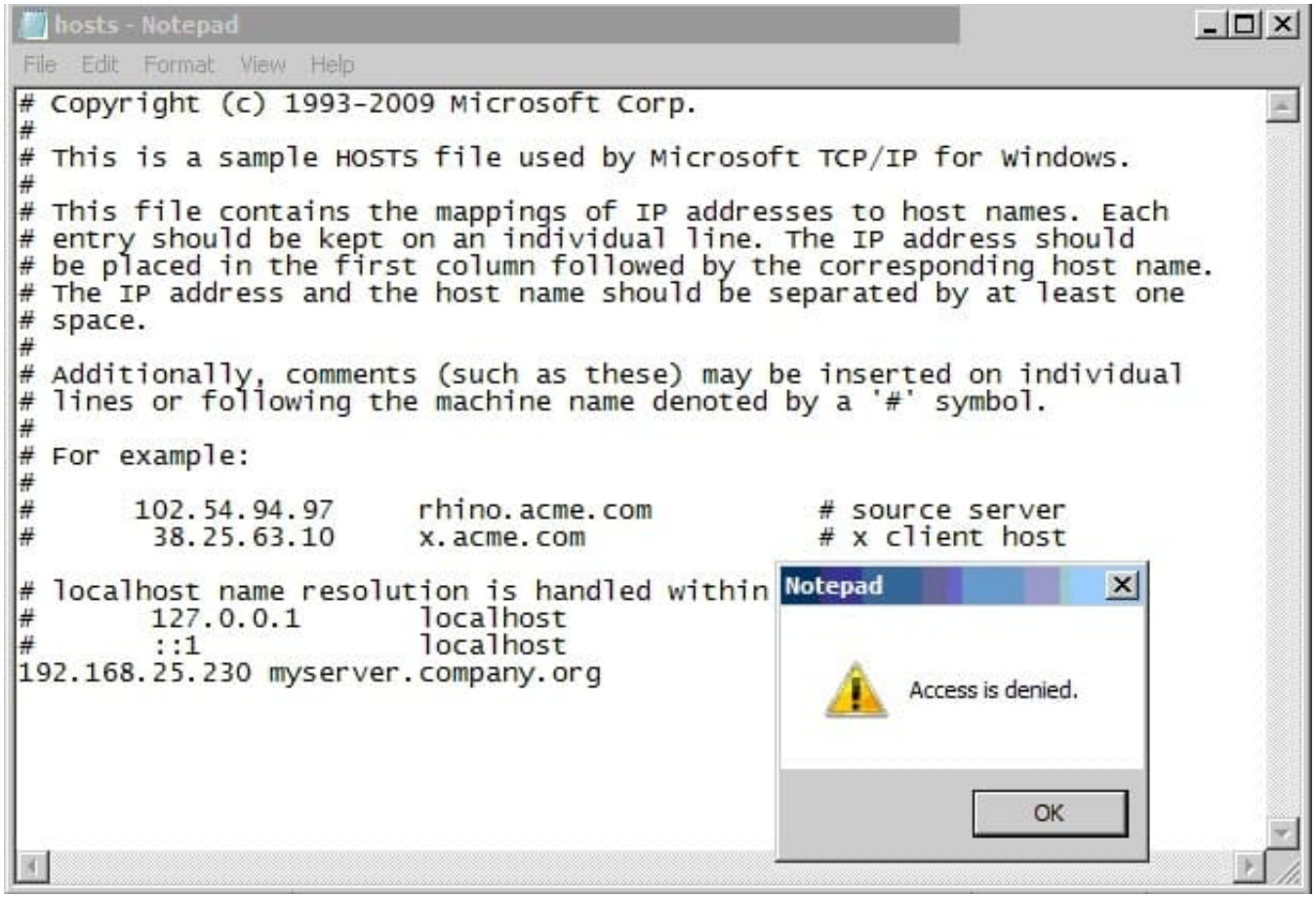
C. a SEP package using a policy defined Multiple Group Update Provider (GUP) list

D. a SEP package using the Install Packages tab

Correct Answer: A

QUESTION 10

Refer to the exhibit.



In the use case displayed in the exhibit.

Why is Notepad unable to save the changes to the file in the image below?

A. Tamper Protection is preventing Notepad from modifying the host file.

B. SONAR is set to block host file modifications.

C. System Lockdown is enabled.

D. SONAR High Risk detection is set to Block.

Correct Answer: B

QUESTION 11

Which content distribution method can distribute content to all client types and provides validation scheduling?

A. Group Update Provider

B. Internal LiveUpdate

C. Intelligent Updater

D. Management Server

Correct Answer: B

Reference: https://www.it-klinika.rs/dogadjaj/tajni-agenti/Symantec-Endpoint-Protection-14-Overview.pdf

QUESTION 12

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 13

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 14

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 15

Which option is a characteristic of a Symantec Endpoint Protection (SEP) domain?

A. Each domain has its own management server and database.

B. Every administrator from one domain can view data in other domains.

C. Data for each domain is stored in its own separate SEP database.

D. Domains share the same management server and database.

Correct Answer: D

References: https://support.symantec.com/en_US/article.HOWTO80764.html