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.leads4pass.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 action does the Shared Insight Cache (SIC) server take when the whitelist reaches maximum capacity?

A. The SIC server allocates additional memory for the whitelist as needed.

B. The SIC server will start writing the cache to disk.

C. The SIC server will remove the least recently used items based on the prune size.

D. The SIC server will remove items with the fewest number of votes.

Correct Answer: C

QUESTION 2

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 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

How could an administrator decrease the timeout period before logging back onto the management console?

A. On the General tab of the Server Properties, click the Console Timeout drop-down list and select one of the available options for length of time

B. On the General tab of the Domain Properties, click the Console Timeout drop-down list and select one of the available options for length of time

C. On the General tab of the Site Properties, click the Console Timeout drop-down list and select one of the available options for length of time

D. On the General tab of the Administrator Properties, click the Console Timeout drop-down list and select one of the available options for length of time

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.HOWTO80882.html

QUESTION 5

An organization needs to add a collection of DNS host names to permit in the firewall policy.

How should the SEP Administrator add these DNS host names as a single rule in the firewall policy?

A. Create a Host Group and add the DNS domain. Then create a firewall rule with the new Host Group as the Source/Destination

B. Create a Host Group and add the DNS host names. Then create a firewall rule with the new Host Group as the Source/Destination

C. Create a Host Group and add the DNS host names. Then create a firewall rule with the new Host Group as the Local/Remote

D. Create a Host Group and add the DNS domain. Then create a firewall rule with the new Host Group as the Local/Remote

Correct Answer: A

QUESTION 6

Where could a SEP Administrator specify a notice to display before logging onto the Symantec Endpoint Protection Manager?

A. Add banner title and banner text under the Logon Banner tab of the Site Properties

B. Add banner title and banner text under the Logon Banner tab of the Administrator Properties

C. Add banner title and banner text under the Logon Banner tab of the Server Properties

D. Add banner title and banner text under the Logon Banner tab of the Domain Properties

Correct Answer: B

QUESTION 7

An organization is considering multiple sites for their Symantec Endpoint Protection environment.

What are two reasons that the organization should consider? (Choose two.)

A. Legal constraints

B. Control your hardware and administration costs

C. Content distribution

D. Tolerable downtime

E. Control when your WAN links are used

Correct Answer: BE

QUESTION 8

A Symantec Endpoint Protection administrator must block traffic from an attacking computer for a specific time period. Where should the administrator adjust the time to block the attacking computer?

A. in the firewall policy, under Protection and Stealth

B. in the firewall policy, under Built in Rules

C. in the group policy, under External Communication Settings

D. in the group policy, under Communication Settings

Correct Answer: A

QUESTION 9

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 10

An organization has several Symantec Endpoint Protection Management (SEPM) Servers without access to the Internet. The SEPM can only run LiveUpdate within a specified "maintenance window" outside of business hours. What content distribution method should the organization utilize?

A. Group Update Provider

B. External LiveUpdate

C. JDB file

D. Internal LiveUpdate

Correct Answer: A

Reference: https://support.symantec.com/us/en/article.howto80888.html

QUESTION 11

Which task should an administrator perform to troubleshoot operation of the Symantec Endpoint Protection embedded database?

A. verify that dbsrv11.exe is listening on port 2638

B. check whether the MSSQLSERVER service is running

C. verify the sqlserver.exe service is running on port 1433

D. check the database transaction logs in X:\Program Files\Microsoft SQL server

Correct Answer: A

References: https://support.symantec.com/en_US/article.TECH160964.html

QUESTION 12

Which command attempts to find the name of the drive in the private region and to match it to a disk media record that is missing a disk access record?

A. vxdisk

B. vxdctl

C. vxreattach

D. vxrecover

Correct Answer: C

QUESTION 13

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 14

Which Symantec Endpoint Protection defense mechanism provides protection against threats that propagate from system to system through the use of autotun.inf files?

A. Host Integrity

B. SONAR

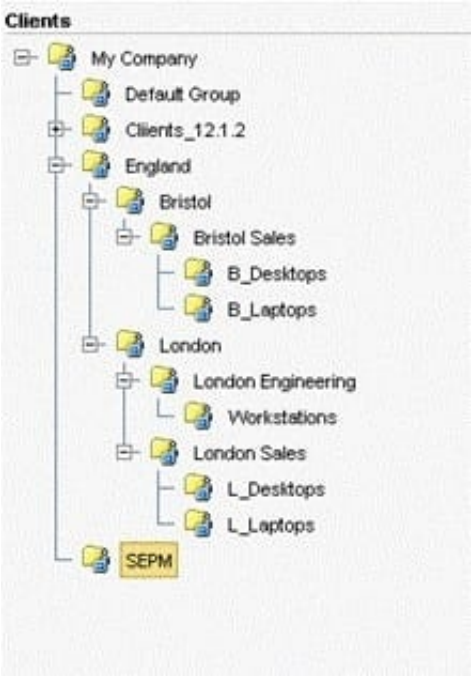
C. Application and Device Control

D. Emulator

Correct Answer: C

QUESTION 15

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