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 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 2

Which two Symantec Endpoint Protection components are used to distribute content updates? (Select two.)

A. Group Update Provider (GUP)

B. Shared Insight Cache Server

C. Symantec Protection Center

D. Symantec Endpoint Protection Manager

E. Symantec Insight Database

Correct Answer: AD

QUESTION 3

A company has a small number of systems in their Symantec Endpoint Protection Manager (SEPM) group with federal mandates that AntiVirus definitions undergo a two week testing period. After being loaded on the client, the tested virus definitions must remain unchanged on the client systems until the next set of virus definitions have completed testing. All other clients must remain operational on the most recent definition sets. An internal LiveUpdate Server has been considered as too expensive to be a solution for this company.

What should be modified on the SEPM to meet this mandate?

A. The LiveUpdate Settings policy for this group should be modified to use an Explicit Group Update Provider.

B. The LiveUpdate Content policy for this group should be modified to use a specific definition revision.

C. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 1.

D. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 14.

Correct Answer: B

QUESTION 4

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 5

An administrator is responsible for the Symantec Endpoint Protection architecture of a large, multi-national company with three regionalized data centers. The administrator needs to collect data from clients; however, the collected data must stay in the local regional data center. Communication between the regional data centers is allowed 20 hours a day.

How should the administrator architect this organization?

A. set up 3 domains

B. set up 3 sites

C. set up 3 locations

D. set up 3 groups

Correct Answer: A

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

QUESTION 6

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 7

An administrator plans to implement a multi-site Symantec Endpoint Protection (SEP) deployment. The administrator needs to determine whether replication is viable without needing to make network firewall changes or change defaults in SEP.

Which port should the administrator verify is open on the path of communication between the two proposed sites?

A. 1433

B. 2967

C. 8014

D. 8443

Correct Answer: D

QUESTION 8

Which two items should an administrator enter in the License Activation Wizard to activate a license? (Select two.)

A. password for the Symantec Licensing Site

B. purchase order number

C. serial number

D. Symantec License file

E. credit card number

Correct Answer: CD

QUESTION 9

An administrator is unable to delete a location.

What is the likely cause?

A. The location currently contains clients.

B. Criteria is defined within the location.

C. The administrator has client control enabled.

D. The location is currently assigned as the default location.

Correct Answer: D

QUESTION 10

An organization has several remote locations with minimum bandwidth and would like to use a content distribution method that does NOT involve configuring an internal LiveUpdate server. What content distribution method should be utilized?

A. Intelligent Updater

B. Management Server

C. External LiveUpdate

D. Group Update Provider

Correct Answer: A

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

QUESTION 11

Which action does SONAR take before convicting a process?

A. quarantines the process

B. blocks suspicious behavior

C. reboots the system

D. checks the reputation of the process

Correct Answer: D

QUESTION 12

An administrator uses the search criteria displayed in the image below. Which results ore returned from the query?

A. Only VMware Servers in the Default Group

B. All Windows 2012 Servers in the Default Group

C. Only Windows 2012 Servers that are Virtualized in the Default Group

D. All Windows 2012 Servers and all Virtualized Servers in the Default Group

Correct Answer: D

QUESTION 13

An organization created a rule in the Application and Device Control policy to block peer-to-peer applications. What two other protection technologies can block and log such unauthorized application? (Choose two.)

A. Memory Exploit Mitigation

B. Virus and Spyware Protection

C. Custom IPS Signatures

D. Host Integrity

E. Firewall

Correct Answer: CE

Reference: https://support.symantec.com/us/en/article.tech122597.html

QUESTION 14

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

References: https://support.symantec.com/en_US/article.TECH134803.html

QUESTION 15

What type of exceptions can an administrator create from the Symantec Endpoint Protection Manager for a Mac client?

A. Security Risk Exceptions - File

B. Security Risk Exceptions for both File or Folder

C. Security Risk Exceptions - Folder

D. Security Risk Exceptions - Extension

Correct Answer: D