250-428^{Q&As}

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.pass2lead.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

An administrator is designing a new single site Symantec Endpoint Protection environment. Due to perimeter firewall bandwidth restrictions, the design needs to minimize the amount of traffic from content passing through the firewall.

Which source must the administrator avoid using?

A. Symantec Endpoint Protection Manager

B. LiveUpdate Administrator (LUA)

C. Group Update Provider (GUP)

D. Shared Insight Cache (SIC)

Correct Answer: B

QUESTION 2

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 3

You have executed the vxdg -g diskgroup adddisk disk_name= command.

Which switch needs to be added to force VxVM to take the disk media name of the failed disk and assign it to the new replacement disk?

A. -force

B. -k

C. -f

D. -assign

![Pass2Lead](https://Pass2Lead.com)
Correct Answer: C

QUESTION 4

An organization has four locations setup in their Symantec Endpoint Protection Environment to match the physical sites they have ?NAM, LATAM, EMEA, and APAC. When users travel from site to site, they would like to control which SEPM a client connects to based on the client\\'s proximity to the nearest SEPM server. The location is triggered by IP range assigned by the DHCP of that site.

How can the organization utilize Locations to control which SEPM or set of SEPMs the clients connect to?

A. Assign the Management Server list to the Group with the appropriate SEPM order. (Each SEPM is on the same priority level)

B. Assign the Management Server list to the Location and Group with the appropriate SEPM order. (Each SEPM has its own priority level)

C. Assign the Management Server list to the Location with the appropriate SEPM order. (Each SEPM has its own priority level)

D. Assign the Management Server list to the Location under My Company. (Each SEPM is on the same priority level)

Correct Answer: D

QUESTION 5

What are two supported Symantec Endpoint Protection Manager authentication types? (Select two.)

A. Microsoft Active Directory

B. MS-CHAP

C. RSA SecurID

D. Biometrics

E. Network Access Control

Correct Answer: AC

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

![Pass2Lead logo](https://Pass2Lead.com)
Correct Answer: C

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

QUESTION 7

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 8

FILL BLANK

An administrator plans to implement a multi-site Symantec Endpoint Protection (SEP) deployment. The administrator needs to determine whether replication is viable without having 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? (Type the port number.)

Correct Answer: 8443

References: https://support.symantec.com/en_US/article.HOWTO81103.html

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.
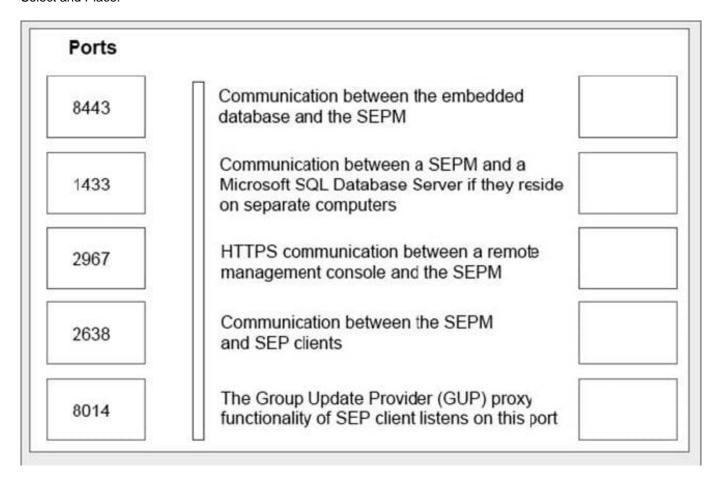
![Pass2Lead](https://Pass2Lead.com)
D. The location is currently assigned as the default location.
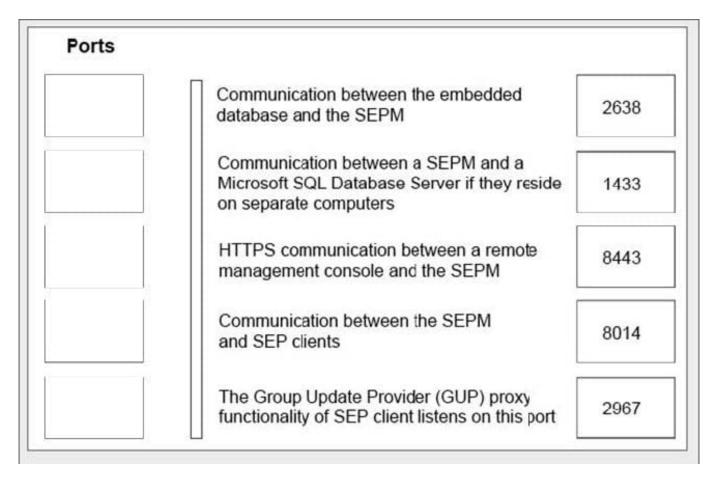
Correct Answer: D

QUESTION 10

Match the following list of ports used by Symantec Endpoint Protection (SEP) to the defining characteristics by clicking and dragging the port on the left to the corresponding description on the right.

Select and Place:

Ports

Ports	Description	
8443	Communication between the embedded database and the SEPM	
1433	Communication between a SEPM and a Microsoft SQL Database Server if they reside on separate computers	
2967	HTTPS communication between a remote management console and the SEPM	
2638	Communication between the SEPM and SEP clients	
8014	The Group Update Provider (GUP) proxy functionality of SEP client listens on this port	

Correct Answer:

Ports

	Communication between the embedded database and the SEPM	2638
	Communication between a SEPM and a Microsoft SQL Database Server if they reside on separate computers	1433
	HTTPS communication between a remote management console and the SEPM	8443
	Communication between the SEPM and SEP clients	8014
	The Group Update Provider (GUP) proxy functionality of SEP client listens on this port	2967

References: https://support.symantec.com/en_US/article.HOWTO81103.html

QUESTION 11

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 12

An administrator is unknowingly trying to connect to a malicious website and download a known threat within a .rar file.

All Symantec Endpoint Protection technologies are installed on the client\\\'s system. Drag and drop the technologies to the right side of the screen in the sequence necessary to block or detect the malicious file.

Select and Place:

Available Technolcgies

Download Insight

Shared Insight Cache

Device Control

Firewall

IPS

Tamper Protection

Appropriate

Correct Answer:

Available Technolcgies

Shared Insight Cache

Device Control

Tamper Protection

Appropriate

Firewall

IPS

Download Insight

![Pass2Lead logo](https://Pass2Lead.com)
QUESTION 13

Winch Symantec Endpoint Protection technology blocks a downloaded program from installing browser plugins?

A. Intrusion Prevention

B. SONAR

C. Tamper Protection

D. Application and Device Control

Correct Answer: D

QUESTION 14

A Symantec Endpoint Protection (SEP) client uses a management server list with three management servers in the priority 1 list.

Which mechanism does the SEP client use to select an alternate management server if the currently selected management server is unavailable?

A. The client chooses the next server alphabetically by server name.

B. The client chooses another server alphabetically in the list randomly.

C. The client chooses a server with the next highest IP address.

D. The client chooses a server based on the lowest server load.

Correct Answer: B

QUESTION 15

Which action can an administrator take to improve the Symantec Endpoint Protection Manager (SEPM) dashboard performance and report accuracy?

A. Decreasing the number of content revisions to keep

B. Lowering the client installation log entries

C. Rebuilding database indexes

D. Limiting the number of backups to keep

Correct Answer: C

250-428 VCE Dumps   250-428 Practice Test   250-428 Exam Questions