Symantec

Exam 250-428

Administration of Symantec Endpoint Protection 14

Version: 7.0

[Total Questions: 120]

Question No : 1

An administrator needs to increase the access speed for client files that are stored on a file server.

Which configuration should the administrator review to address the read speed from the server?

A. Enable Network Cache in the client's Virus and Spyware Protection policy
B. Add the applicable server to a trusted host group
C. Create a Firewall allow rule for the server's IP address
D. Enable download randomization in the client group's communication settings

Answer: A

Question No : 2

An administrator is reviewing an Infected Clients Report and notices that a client repeatedly shows the same malware detection. Although the client remediates the files, the infection continues to display in the logs.

Which two functions should be enabled to automate enhanced remediation of a detected threat and its related side effects? (Select two.)

A. Risk Tracer
B. Terminate Processes Automatically
C. Early Launch Anti-Malware Driver
D. Stop Service Automatically
E. Stop and Reload AutoProtect

Answer: B,D

Question No : 3

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

Answer: A

Question No : 4

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

Answer: A

Question No : 5

An administrator is recovering from a Symantec Endpoint Manager (SEPM) site failure.

Which file should the administrator use during an install of SEPM to recover the lost environment according to Symantec Disaster Recovery Best Practice documentation?

A. original installation log
B. recovery_timestamp file
C. settings.properties file
D. Sylink.xml file from the SEPM

Answer: B

Question No : 6

The Security Status on the console home page is failing to alert a Symantec Endpoint Protection (SEP) administrator when virus definitions are out of date.

How should the SEP administrator enable the Security Status alert?

A. lower the Security Status thresholds
B. raise the Security Status thresholds
C. change the Notifications setting to "Show all notifications"
D. change the Action Summary display to "By number of computers"

Answer: A

Question No : 7

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.

Answer: C

Question No : 8

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

Answer: A

Question No : 9

A company plans to install six Symantec Endpoint Protection Managers (SEPMs) spread evenly across two sites. The administrator needs to direct replication activity to SEPM3 server in Site 1 and SEPM4 in Site 2.

Which two actions should the administrator take to direct replication activity to SEPM3 and SEPM4? (Select two.)

A. Install SEPM3 and SEPM4 after the other SEPMs
B. Install the SQL Server databases on SEPM3 and SEPM4
C. Ensure SEPM3 and SEPM4 are defined as the top priority server in the Site Settings
D. Ensure SEPM3 and SEPM4 are defined as remote servers in the replication partner configuration
E. Install IT Analytics on SEPM3 and SEPM4

Answer: C,D

Question No : 10

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 another server in the list randomly.
B. The client chooses a server based on the lowest server load.
C. The client chooses a server with the next highest IP address.
D. The client chooses the next server alphabetically by server name.

Answer: A

Question No : 11

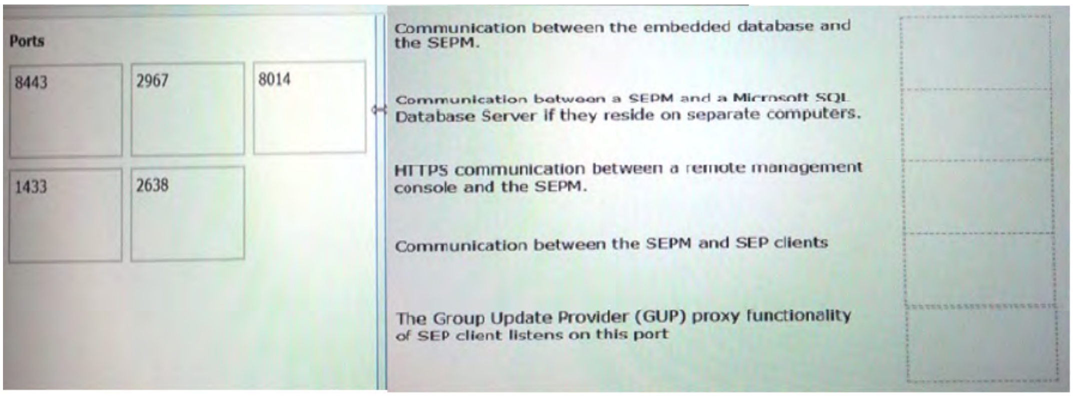
Which two criteria can an administrator use to determine hosts in a host group? (Select two.)

A. Subnet
B. Network Services
C. Application Protocol
D. DNS Domain
E. Network Adapters

Answer: A,D

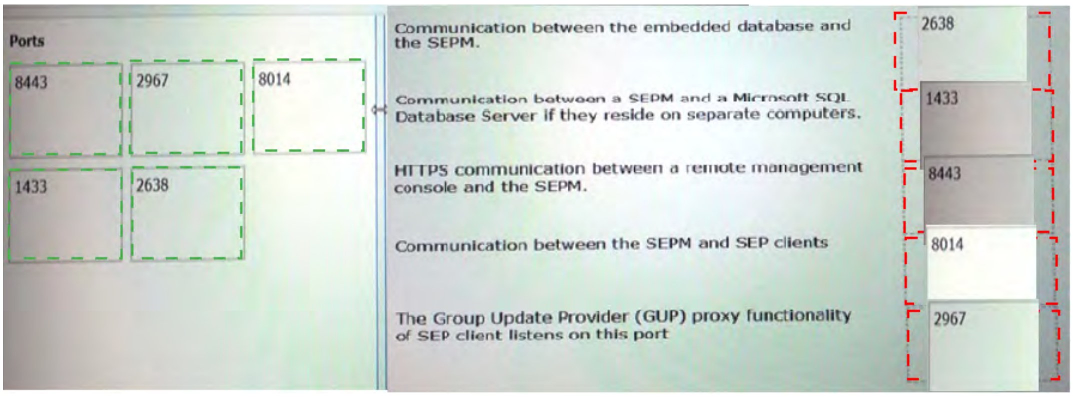
Question No : 12 DRAG DROP

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



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

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

Explanation:

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

Question No : 13

What is a valid Symantec Endpoint Protection (SEP) single site design?

A. Multiple MySQL databases
B. One Microsoft SQL Server database
C. One Microsoft SQL Express database
D. Multiple embedded databases

Answer: A

Question No : 14

Which protection engine should be enabled to drop malicious vulnerability scans against a client system?

A. SONAR
B. Intrusion Prevention
C. Tamper Protection
D. Application and Device Control

Answer: B

Question No : 15

A company needs to forward log data from Data Center A to Data Center B during off peak hours only.

How should the company architect its Symantec Endpoint Protection environment?

A. Set up two sites and schedule replication between them during off peak hours
B. Set up a single site and configure the clients to send their logs to the Manager during off peak hours
C. Set up a Group Update Provider (GUP) at Data Center A and configure it to send logs during off peak hours
D. Set up a LiveUpdate Server at Data Center A and configure it to send logs during off peak hours

Answer: D

Question No : 16

An administrator receives a browser certificate warning when accessing the Symantec Endpoint Protection Manager (SEPM) Web console.

Where can the administrator obtain the certificate?

A. SEPM console Licenses section
B. Admin > Servers > Configure SecureID Authentication
C. SEPM console Admin Tasks
D. SEPM Web Access

Answer: D

Question No : 17

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

Answer: B

Question No : 18

A company deploys Symantec Endpoint Protection (SEP) to 50 virtual machines running on a single ESXi host.

Which configuration change can the administrator make to minimize sudden IOPS impact on the ESXi server while each SEP endpoint communicates with the Symantec Endpoint Protection Manager?

A. increase Download Insight sensitivity level
B. reduce the heartbeat interval
C. increase download randomization window
D. reduce number of content revisions to keep

Answer: C

Question No : 19

What 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.

Answer: D

Question No : 20

An administrator configures the scan duration for a scheduled scan. The scan fails to complete in the specified time period.

When will the next scheduled scan occur on the computer?

A. when the computer reboots
B. when the user restarts the scan
C. at the next scheduled scan period
D. within the next hour

Answer: C

Question No : 21

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

Answer: C,D

Question No : 22

Which feature reduces the impact of Auto-Protect on a virtual client guest operating system?

A. Network Shared Insight Cache
B. Virtual Image Exception
C. Scan Randomization
D. Virtual Shared Insight Cache

Answer: B

Question No : 23

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