Fortinet NSE5_FAZ-5.4 Exam

Volume: 25 Questions

Question No:1
In FortiAnalyzer's FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

A. Configure # set resolve-ip enable in the system FortiView settings

B. Resolve IPs on FortiGate

C. Configure local DNS servers on FortiAnalyzer

D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Answer: A

Question No:2
What is the purpose of the following CLI command?
#configure system global
set log-checksum md5
end

A. To add the MD5's hash value and authentication code

B. To encrypt log communications

C. To add a unique tag to each log to provide that it came from this FortiAnalyzer

D. To add a log file checksum

Answer: A

Question No:3
How does FortiAnalyzer retrieve specific log data from the database?

A. SQL FROM statement

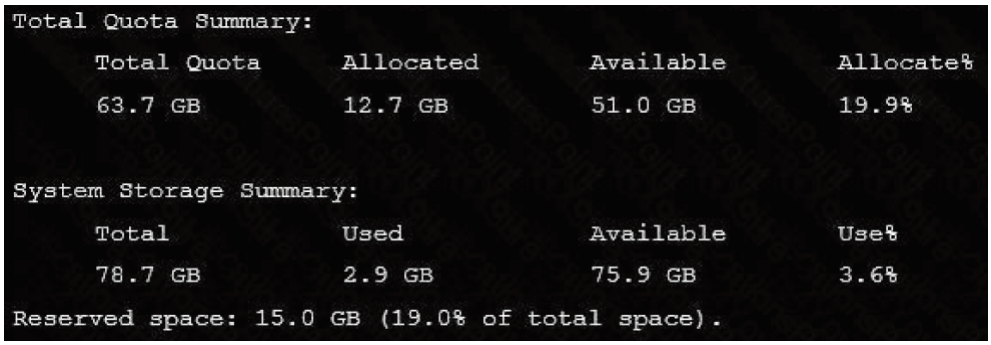
B. SQL GET statement

C. SQL SELECT statement

D. SQL EXTRACT statement

Answer: C

Question No:4
Refer to exhibit.



Why is the total quota less than the total system storage?

A. The oftpd process has not archived the logs yet

B. The logfiled process is just estimating the total quota

C. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files

D. 3.6% of the system storage is already being used

Answer: C

Question No:5
What FortiGate process caches logs when FortiAnalyzer is not reachable?

A. oftpd

B. miglogd

C. sqlplugind

D. logfiled