



NSE5_FSM-5.2^{Q&As}

Fortinet NSE 5 - FortiSIEM 5.2

Pass Fortinet NSE5_FSM-5.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse5_fsm-5-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which two FortiSIEM components work together to provide real-time event correlation?

- A. Collector and Windows agent
- B. Supervisor and worker
- C. Worker and collector
- D. Supervisor and collector

Correct Answer: D

QUESTION 2

To determine whether or not syslog is being received from a network device, which is the best command from the backend?

- A. tcpdump
- B. phDeviceTest
- C. netcat
- D. phSyslogRecorder

Correct Answer: A

QUESTION 3

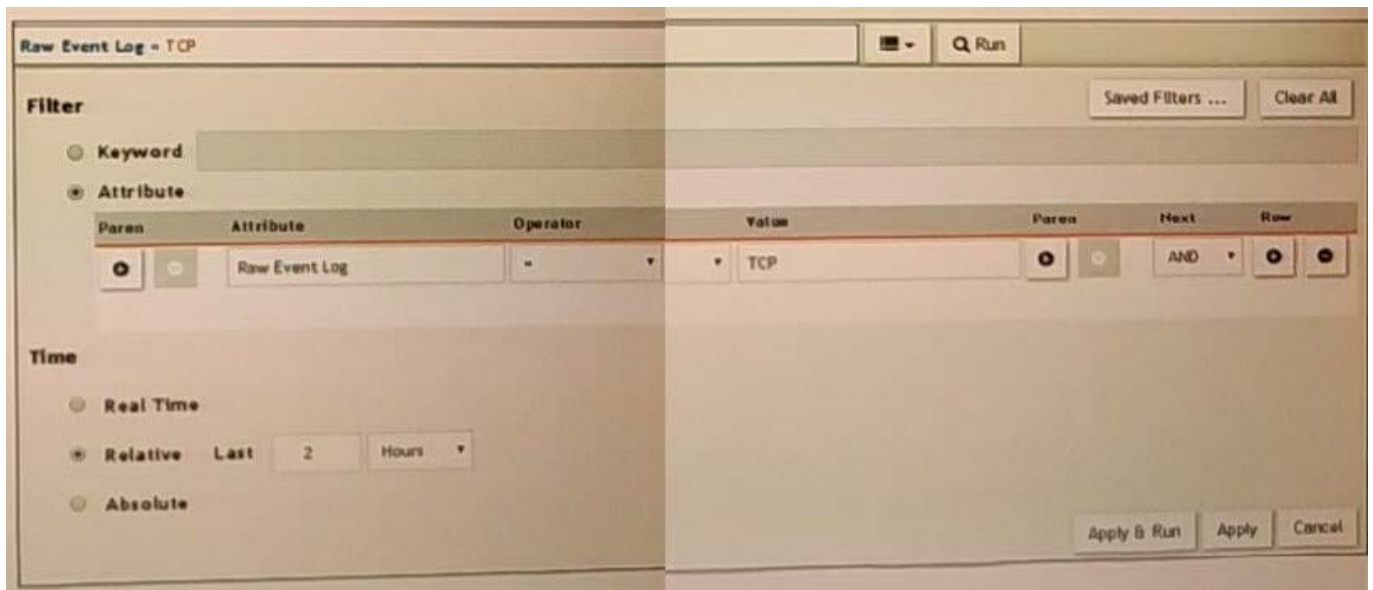
What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

- A. 16GB RAM
- B. 32GB RAM
- C. 64GB RAM
- D. 24GB RAM

Correct Answer: B

QUESTION 4

Refer to the exhibit.



A FortiSIEM is continuously receiving syslog events from a FortiGate firewall. The FortiSIEM administrator is trying to search the raw event logs for the last two hours that contain the keyword tcp. However, the administrator is getting no results from the search.

Based on the selected filters shown in the exhibit, why are there no search results?

- A. The keyword is case sensitive. Instead of typing TCP in the Value field, the administrator should type tcp.
- B. In the Time section, the administrator selected the Relative Last option, and in the drop-down lists, selected 2 and Hours as the time period. The time period should be 24 hours.
- C. The administrator selected = in the Operator column. That is the wrong operator.
- D. The administrator selected AND in the Next drop-down list. This is the wrong boolean operator.

Correct Answer: C

QUESTION 5

A FortiSIEM supervisor at headquarters is struggling to keep up with an increase of EPS (Events Per Second) being reported across the enterprise. What components should an administrator consider deploying to assist the supervisor with processing data?

- A. Supervisor
- B. Worker
- C. Collector
- D. Agent

Correct Answer: B



[Dumps](#)

[Dumps](#)

[Questions](#)