



# NSE5\_FSM-5.2<sup>Q&As</sup>

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.passapply.com/nse5\\_fsm-5-2.html](https://www.passapply.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

What is the best discovery scan option for a network environment where ping is disabled on all network devices?

- A. Smart scan
- B. Range scan
- C. CMDB scan
- D. L2 scan

Correct Answer: A

---

#### QUESTION 2

Which process converts Raw log data to structured data?

- A. Data enrichment
- B. Data classification
- C. Data parsing
- D. Data validation

Correct Answer: D

---

#### QUESTION 3

Which database is used for storing anomaly data, that is calculated for different parameters, such as traffic and device resource usage running averages, and standard deviation values?

- A. Profile DB
- B. Event DB
- C. CMDB
- D. SVN DB

Correct Answer: B

---

#### QUESTION 4

What operating system is FortiSIEM based on?

- A. Cent OS



B. Microsoft Windows

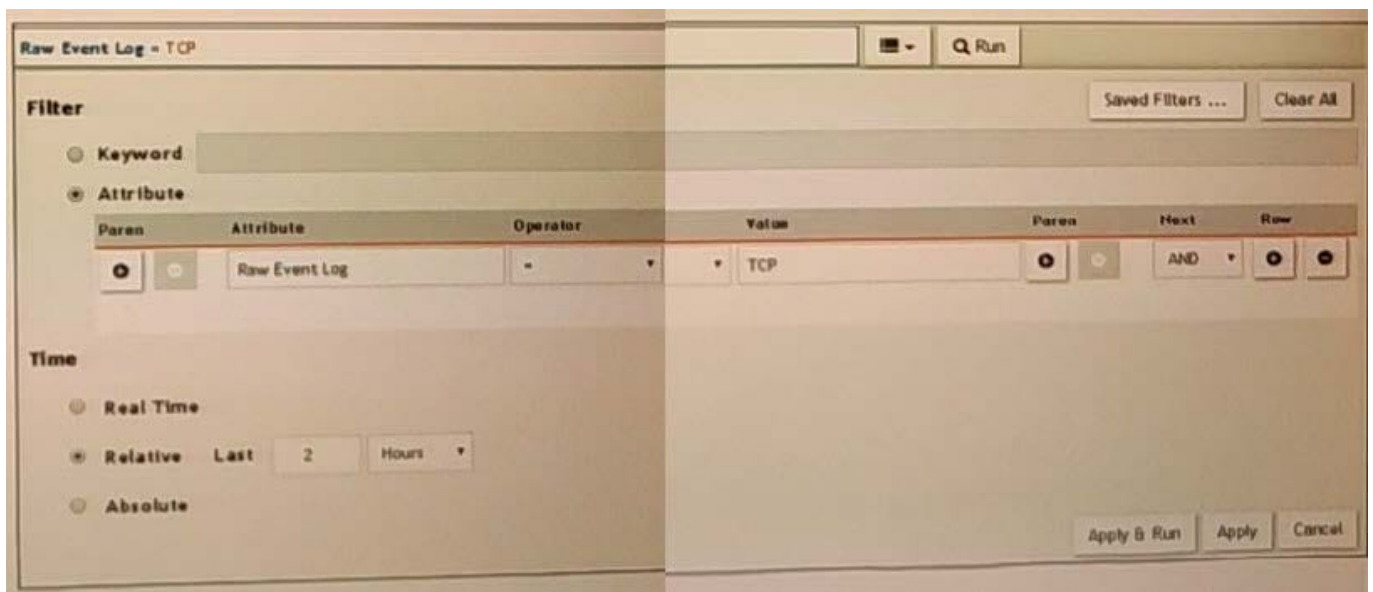
C. RedHat

D. Ubuntu

Correct Answer: A

### QUESTION 5

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

[NSE5 FSM-5.2 Practice Test](#)

[NSE5 FSM-5.2 Exam Questions](#)

[NSE5 FSM-5.2 Braindumps](#)