# 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.pass2lead.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
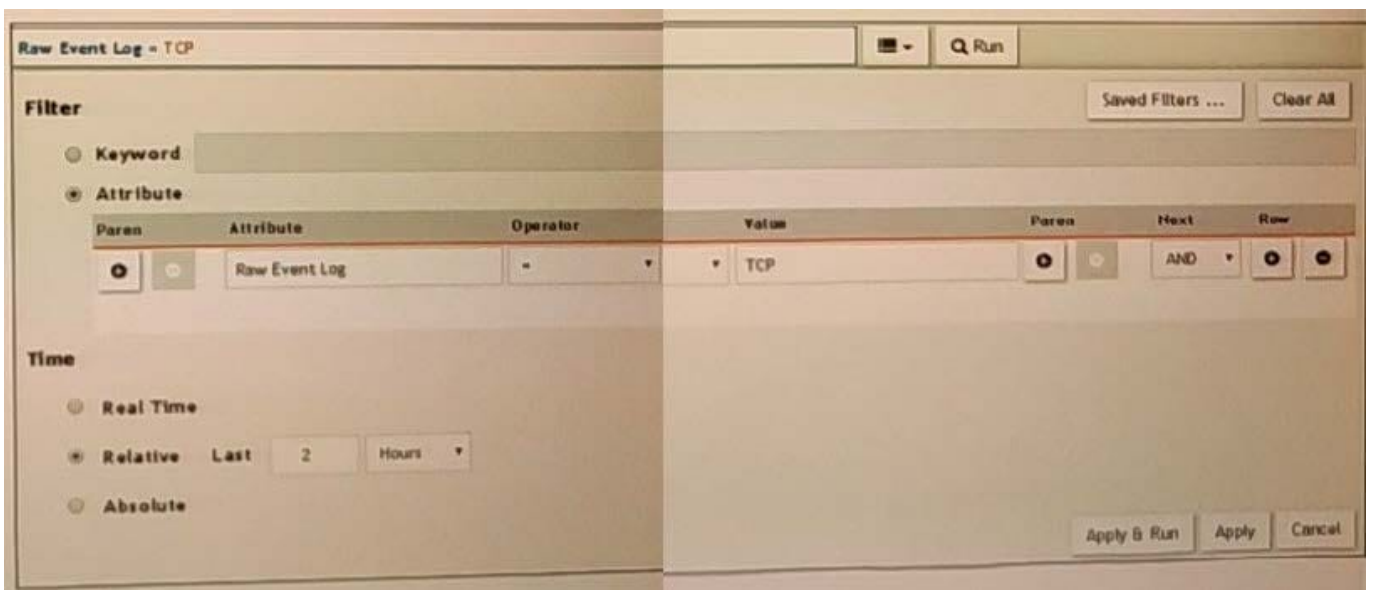
⚙ **800,000+** Satisfied Customers

**QUESTION 1**

In the rules engine, which condition instructs FortiSIEM to summarize and count the matching evaluated data?

A. Time Window

B. Aggregation

C. Group By

D. Filters

Correct Answer: C

**QUESTION 2**

Refer to the exhibit.



A FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSlfcM 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 lime period The time period should be 24 hours.

C. The administratorselected - inthe Operator column That a the wrong operator.

D. The administrator selected AND in the Nextdrop-down list. Thisis the wrong boolean operator.

Correct Answer: C

---

**QUESTION 3**

Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)

A. UDP9999

B. UDP 162

C. TCP 514

D. UDP 514

E. TCP 1470

Correct Answer: BDE

---

**QUESTION 4**

Which process convertsRaw log data to structured data?

A. Data enrichment

B. Data classification

C. Data parsing

D. Data validation

Correct Answer: D

---

**QUESTION 5**

Which FortiSIEM components are capable of performing device discovery?

A. FortiSIEM Windows agent

B. Worker

C. FortiSIEM Linux agent

D. Collector

Correct Answer: D

---

Latest NSE5_FSM-5.2 Dumps     NSE5_FSM-5.2 Practice Test     NSE5_FSM-5.2 Exam Questions