



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.pass4itsure.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

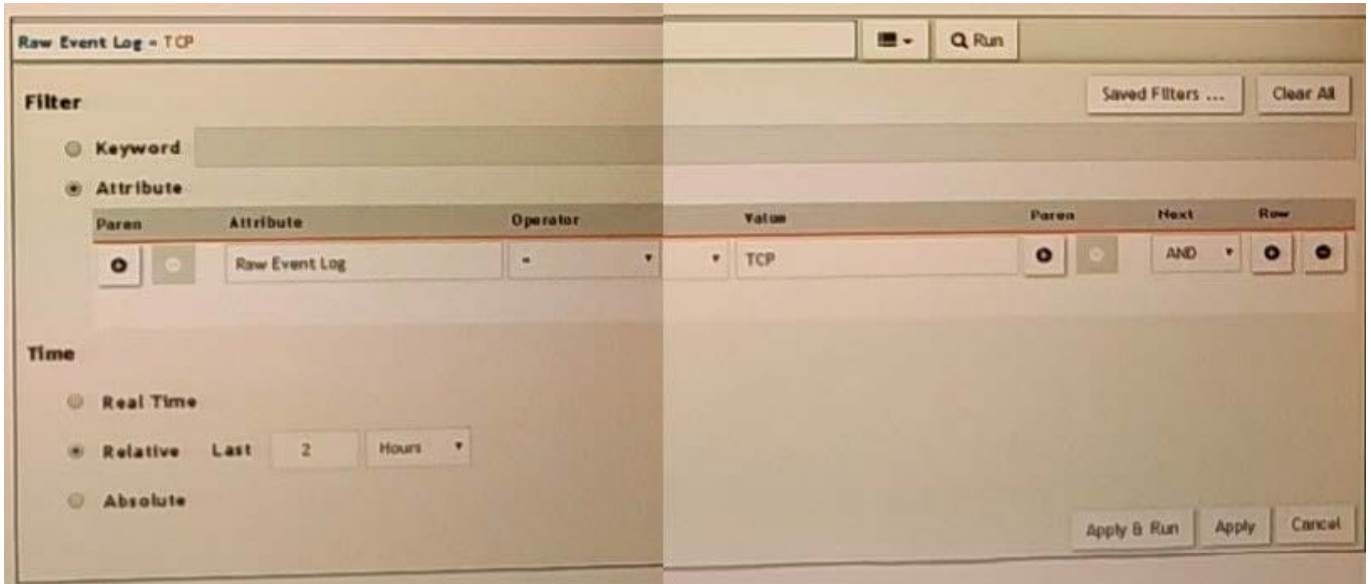
-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

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 2

Refer to the exhibit.



Attribute	Order	Display As	Row	Move
Event Receive Time				
Reporting IP				
Event Type				
Raw Event Log				
COUNT(Matched Events)				

A FortiSIEM administrator wants to group some attributes for a report, but is not able to do so successfully. As shown in the exhibit, why are some of the fields highlighted in red?

- A. The Event Receive Time attribute is not available for logs.
- B. The attribute COUNT(Matched event) is an invalid expression.
- C. Unique attributes cannot be grouped.
- D. No RAW Event Log attribute is available for devices.

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

In FortiSIEM enterprise licensing mode, if the link between the collector and data center FortiSIEM cluster is down, what happens?

- A. The collector drops incoming events like syslog, but stops performance collection
- B. The collector continues performance collection of devices, but stops receiving syslog



- C. The collector buffers events
- D. The collector processes stop, and events are dropped

Correct Answer: D

QUESTION 5

A FortiSIEM administrator wants to restrict a network administrator to running searches for only firewall devices. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

- A. CMDB Report Conditions
- B. Data Conditions
- C. UI Access

Correct Answer: B

[Latest NSE5 FSM-5.2 Dumps](#)

[NSE5 FSM-5.2 Practice Test](#)

[NSE5 FSM-5.2 Exam Questions](#)