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.leads4pass.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.

An administrator is trying to identify an issue using an expression bated on the Expression Builder settings shown in the exhibit however, the error message shown in the exhibit indicates that the expression is invalid.

Which is the correct expression?

A. Matched Events COUNT()

B. Matched Events(COUNT)

C. COUNT(Matched Events)

D. (COUNT) Matched Events

Correct Answer: C

QUESTION 2

What are the four possible incident status values?

A. Active, dosed, cleared, open

B. Active, cleared, cleared manually, system cleared

C. Active, closed, manual, resolved

D. Active, auto cleared, manual, false positive

Correct Answer: C

QUESTION 3

An administrator defines SMTP as a critical process on a Linux server. If the SMTP process is stopped, FortiSIEM would generate a critical event with which event type?

A. PH_DEV_MON_PROC_STOP

B. Postfix-Mail-Slop

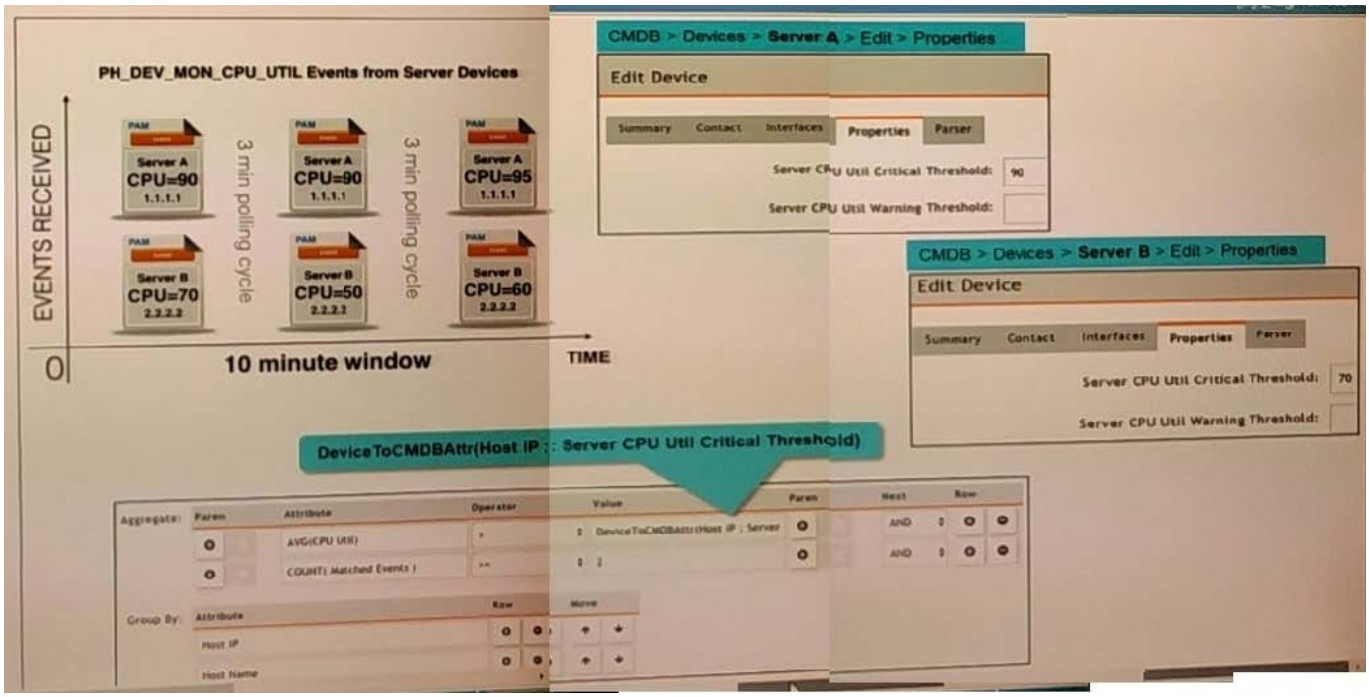
C. Generic_SMTP_Process_Exit

D. PH_DEV_MON_SMTP_STOP

Correct Answer: D

QUESTION 4

Refer to the exhibit.



Three events are collected over a 10-minutc time period from two servers Server A and Server B. Based on the settings being used for the rule subpattern. how many incidents will the servers generate?

A. Server A will not generate any incidents and Server B will not generate any incidents

B. Server A will generate one incident and Server B wifl generate one incident

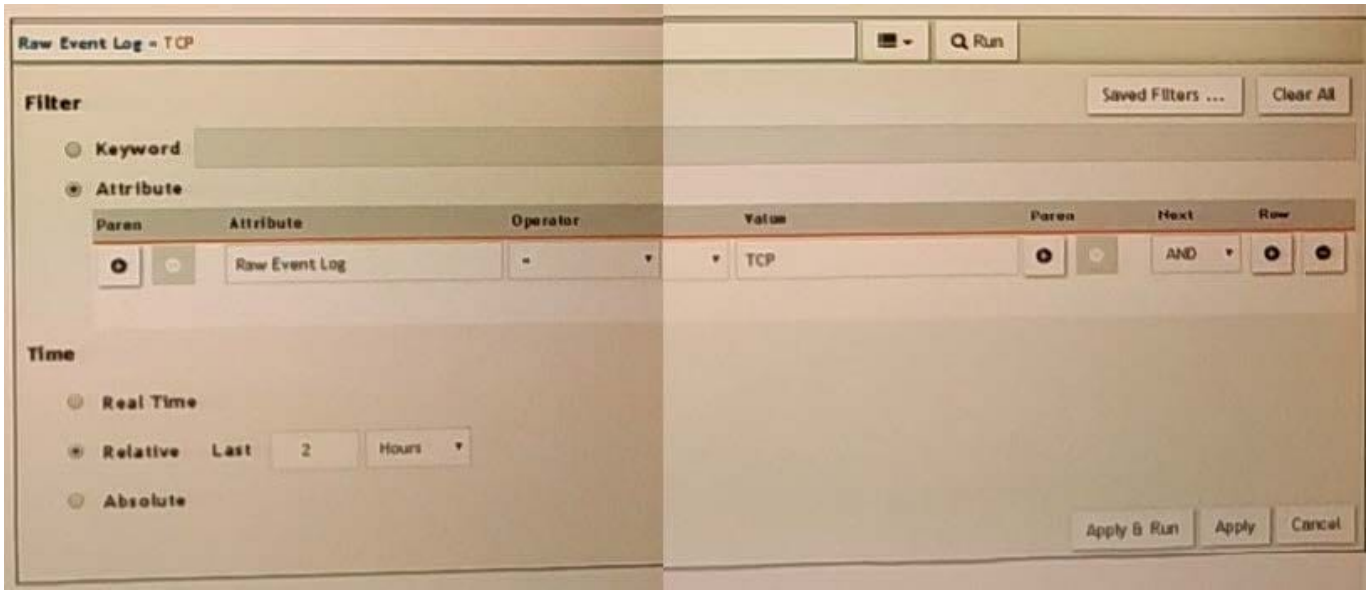
C. Server A will generate one incident and Server B will not generate any incidents

D. Server B will generate one incident and Server A will not generate any incidents

Correct Answer: A

QUESTION 5

Refer to the exhibit.



A FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSIfcM 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