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

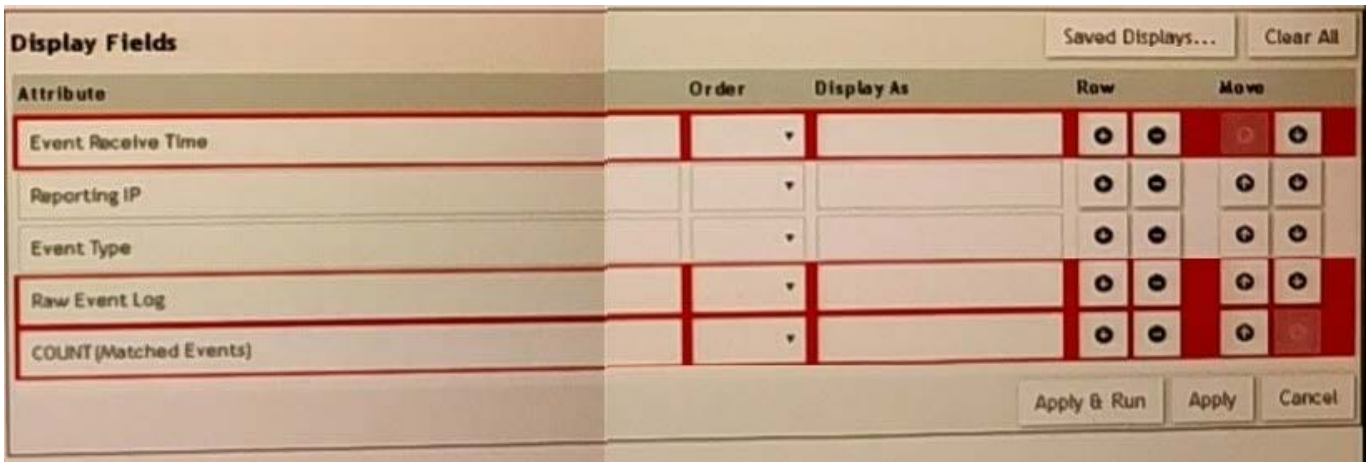
100% Passing Guarantee
100% Money Back Assurance

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.



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 2

Which protocol is almost always required for the FortiSIEM GUI discovery process?

A. SNMP

B. WMI

C. Syslog D. Telnet

Correct Answer: A

QUESTION 3

In the advanced analytical rules engine in FortiSIEM, multiple subpatterms can be referenced using which three operation?(Choose three.)

A. ELSE

B. NOT

C. FOLLOWED_BY

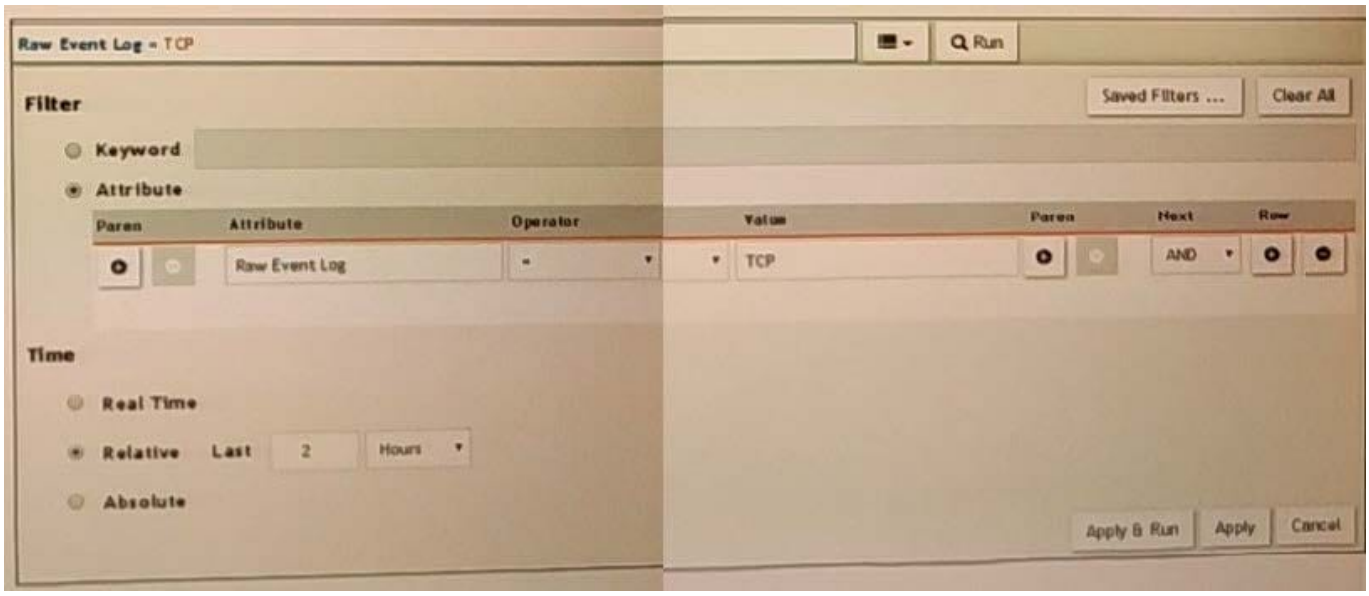
D. OR

E. AND

Correct Answer: ABE

QUESTION 4

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

QUESTION 5

Which process convertsRaw log data to structured data?

A. Data enrichment

B. Data classification

C. Data parsing

D. Data validation

Correct Answer: D

QUESTION 6

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 7

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 8

Which discovery scan type is prone to miss a device, if the device is quiet and the entry foe that device is not present in the ARP table of adjacent devices?

A. CMDB scan

B. L2 scan

C. Range scan

D. Smart scan

Correct Answer: D

QUESTION 9

Which FortiSIEM components are capable of performing device discovery?

A. FortiSIEM Windows agent

B. Worker

C. FortiSIEM Linux agent

D. Collector

Correct Answer: D

QUESTION 10

Which item is required to register a FortiSIEM appliance license?

A. Static storage

B. Static MAC address

C. Static IP address

D. Static Hardware ID

Correct Answer: D

NSE5_FSM-5.2 Practice Test NSE5_FSM-5.2 Exam Questions NSE5_FSM-5.2 Braindumps