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

What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

A. 16GB RAM

B. 32GB RAM

C. 64GB RAM

D. 24GB RAM

Correct Answer: B

QUESTION 2

If an incident\\'s status is Cleared, what does this mean?

A. Two hours have passed since the incident occurred and the incident has not reoccurred.

B. A clear condition set on a rule was satisfied.

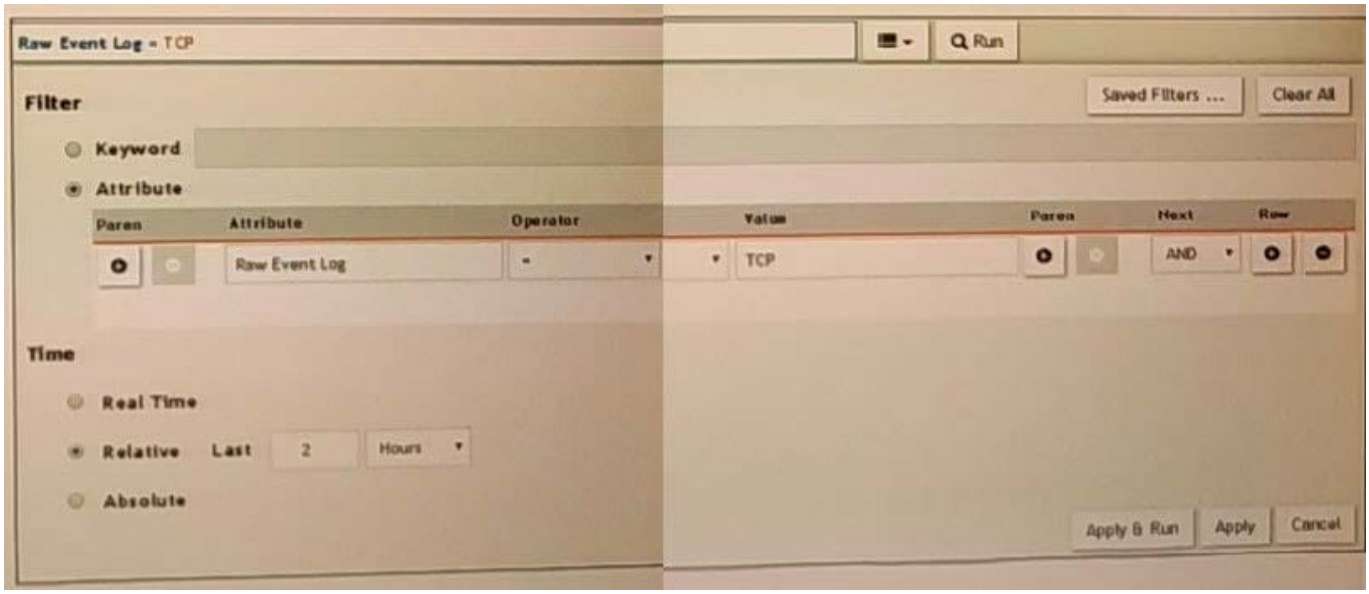
C. A security rule issue has been resolved.

D. The incident was cleared by an operator.

Correct Answer: A

QUESTION 3

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.

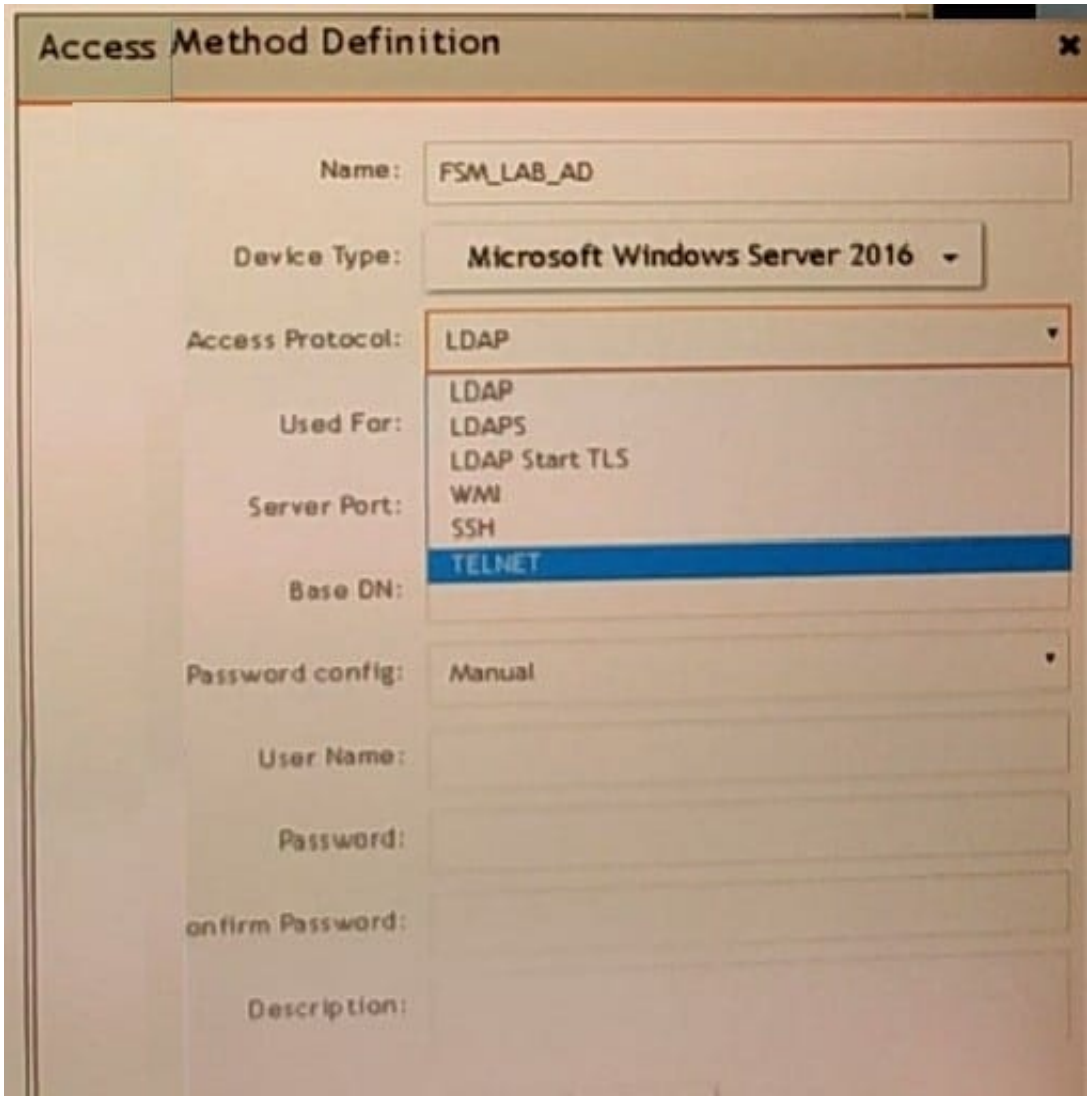
C. The administratorselected - inthe Operator column That a the wrong operator.

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

Correct Answer: C

QUESTION 4

Refer to the exhibit.



A FortiSIEM administrator wants to collect both SIEM event logs and performance and availability metrics (PAM) events from a Microsoft Windows server.

Which protocol should the administrator select in the AccessProtocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?

A. TELNET

B. WMI

C. LDAPS

D. LDAP start TLS

Correct Answer: A

QUESTION 5

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