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:

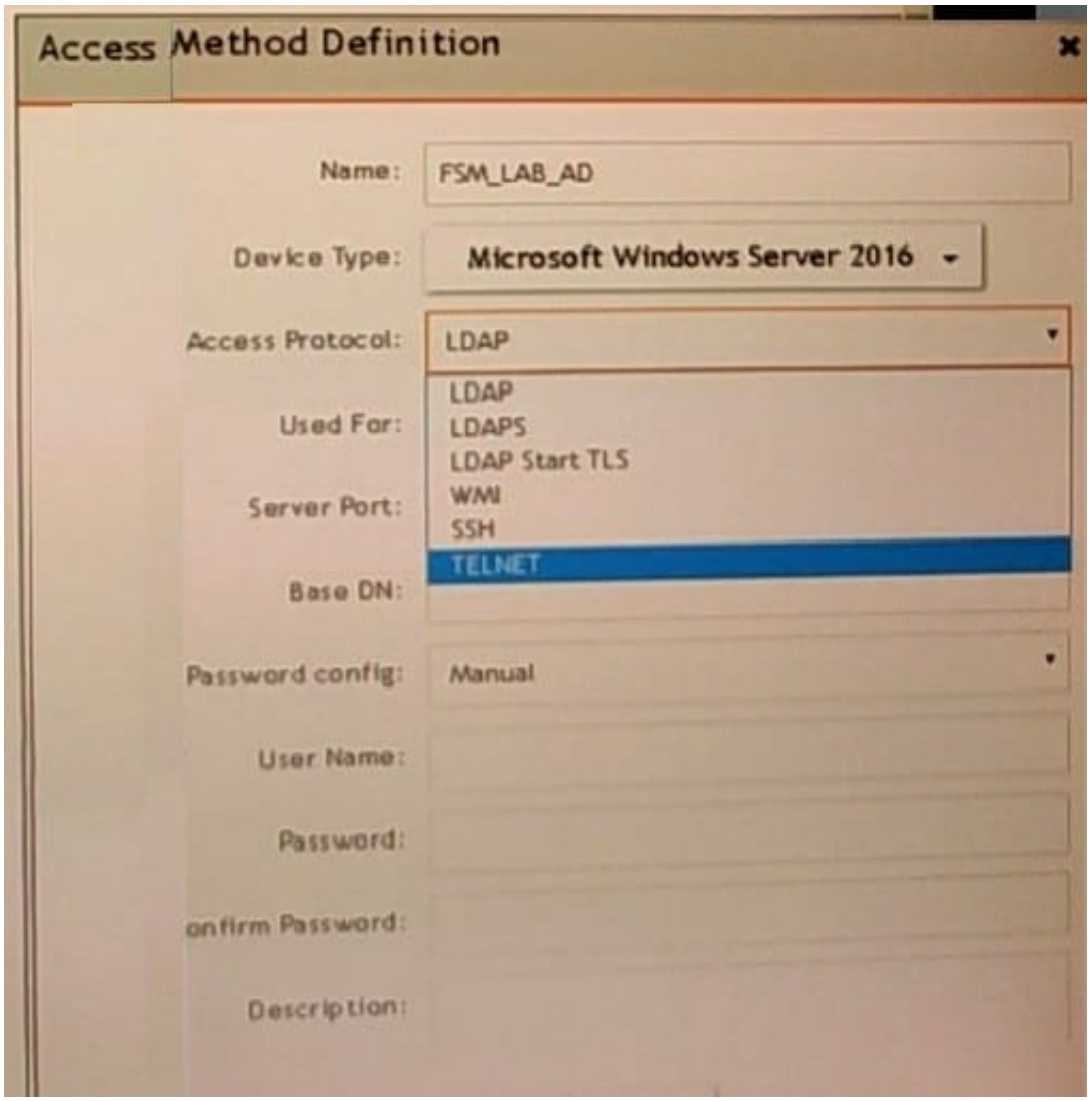
https://www.geekcert.com/nse5_fsm-5-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

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 2

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

A. UDP9999

B. UDP 162

C. TCP 514

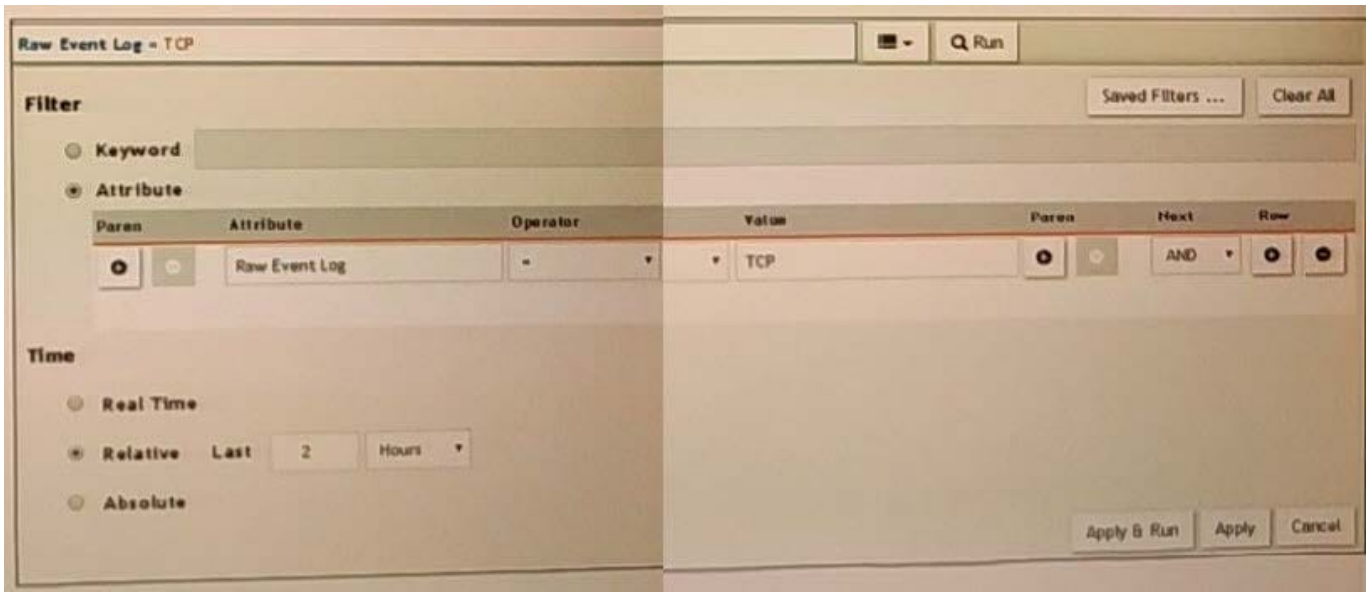
D. UDP 514

E. TCP 1470

Correct Answer: BDE

QUESTION 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

An administrator wants to search for events received from Linux and Windows agents.

Which attribute should the administrator use in search filters, to view events received from agents only.

A. External Event Receive Protocol

B. Event Received Proto Agents

C. External Event Receive Raw Logs

D. External Event Receive Agents

Correct Answer: C

QUESTION 5

Which command displays the Linux agent status?

A. Service fsm-linux-agent status

B. Service Ao-linux-agent status

C. Service fortisiem-linux-agent status

D. Service linux-agent status

Correct Answer: C