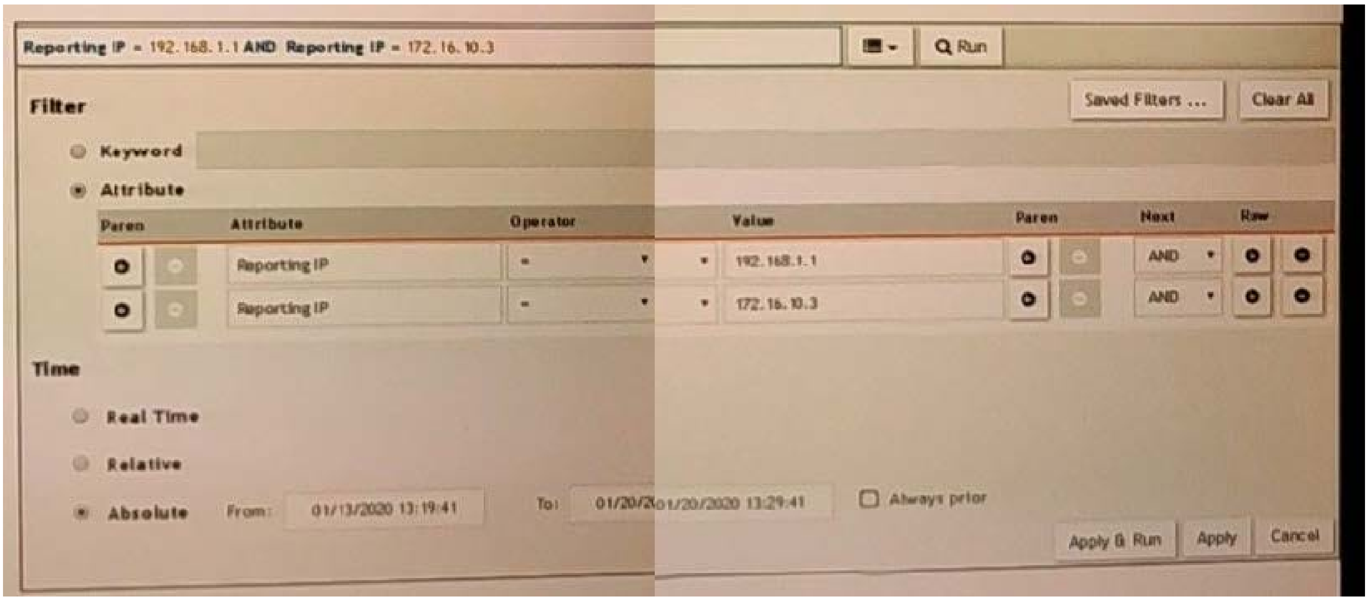
NSE5_FSM-5.2 Q&As

Fortinet NSE 5 - FortiSIEM 5.2

QUESTION 1

Refer to the exhibit.



Reporting IP = 192.168.1.1 AND Reporting IP = 172.16.10.3

Filter

○ Keyword

● Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
	Reporting IP	=	192.168.1.1		AND	
	Reporting IP	=	172.16.10.3		AND	

Time

○ Real Time

○ Relative

● Absolute From: 01/13/2020 13:19:41 To: 01/20/201/20/2020 13:29:41 □ Always prior

The FortiSIEM administrator is examining events for two devices to investigate an issue However, the administrator is not getting any results from their search.

Based on the selected fillers shown in the exhibit, why is the search returning no results?

A. Parenthesis are missing

B. The wrong boolean operator is selected in the Next column

C. The wrong option is selected in the Operator column

D. An invalid IP subnet is typed in the Value column

Correct Answer: D

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

If the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

A. Down status is assigned because of packet loss.

B. Up status is assigned because of received packets

C. Critical status is assigned because of reduction in number of packets received

D. Degraded status is assigned because of packet loss

Correct Answer: D

QUESTION 4

To determine whether or not syslog is being received from a network device, which is the best command from the backend?

A. tcpdump

B. phDeviceTest

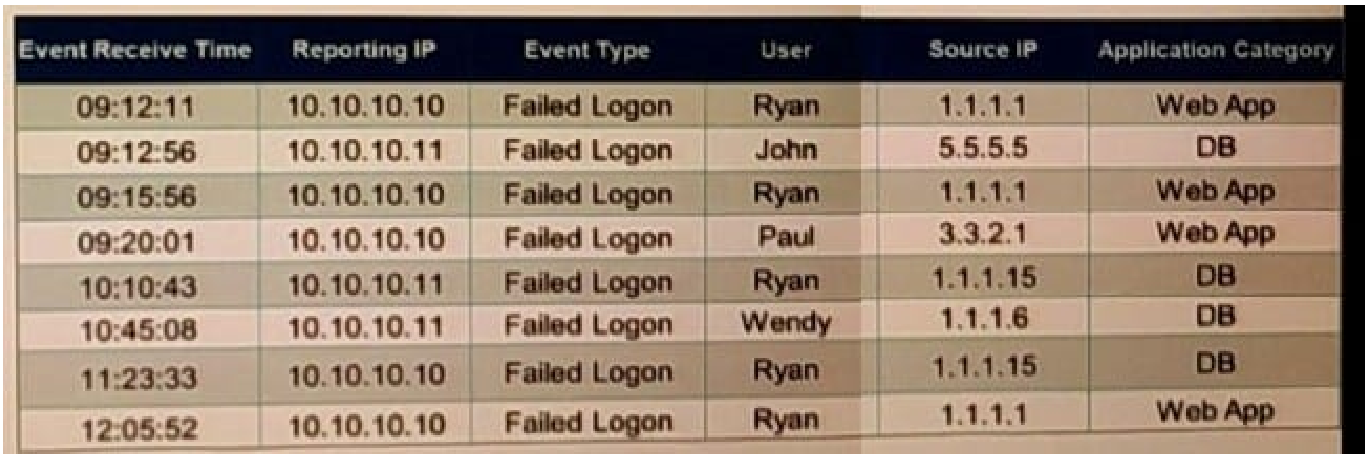
C. netcat

D. phSyslogRecorder

Correct Answer: A

QUESTION 5

Refer to the exhibit.



Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

If events are grouped by Event Receive Time, Reporting IP, and User attributes in FortiSIEM, how many results will be displayed?

A. Eight results will be displayed

B. Four results will be displayed

C. Two results will be displayed

D. Unique attributes cannot be grouped

Correct Answer: D