

Fortinet

NSE5_FSM-5.2 Exam

Fortinet NSE 5 - FortiSIEM 5.2



Thank you for Downloading NSE5_FSM-5.2 exam PDF Demo

You can Buy Latest NSE5_FSM-5.2 Full Version Download

https://www.certkillers.net/Exam/NSE5_FSM-5.2

<https://www.certkillers.net>

Version: 4.0

Question: 1

Refer to the exhibit.

Display Fields		Saved Displays...		Clear All	
Attribute	Order	Display As	Row		Move
Event Receive Time			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reporting IP			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Event Type			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Raw Event Log			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
COUNT(Matched Events)			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply & Run Apply Cancel

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.

Answer: C

Question: 2

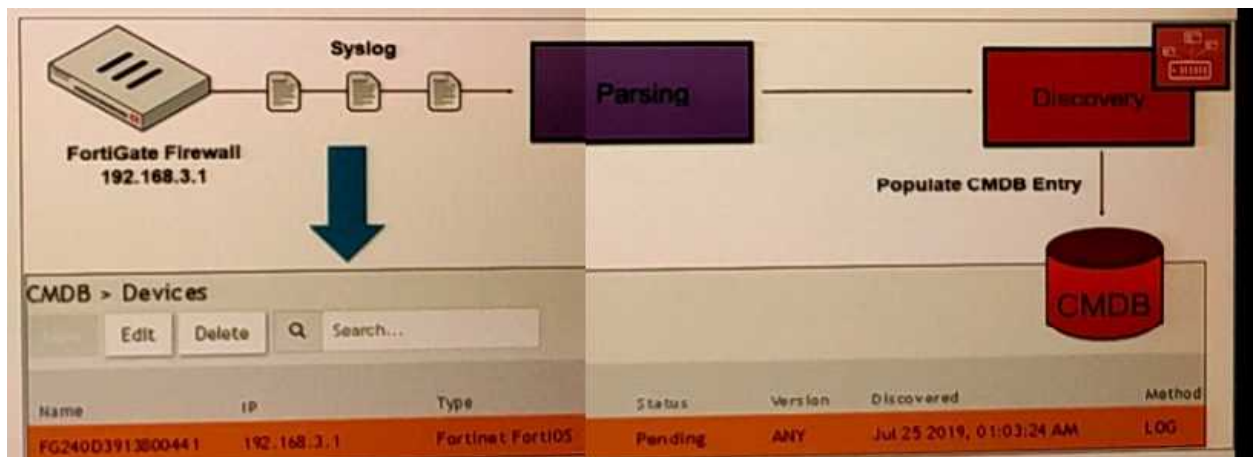
In the rules engine, which condition instructs FortiSIEM to summarize and count the matching evaluated data?

- A. Time Window
- B. Aggregation
- C. Group By
- D. Filters

Answer: C

Question: 3

Refer to the exhibit.



How was the FortiGate device discovered by FortiSIEM?

- A. Through GUI log discovery
- B. Through syslog discovery
- C. Using the pull events method
- D. Through auto log discovery

Answer: A

Question: 4

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 Reporting IP, Event Type, and user attributes in FortiSIEM, how many results will be displayed?

- A. Seven results will be displayed.
- B. Three results will be displayed.
- C. Unique attribute cannot be grouped.
- D. Five results will be displayed.

Answer: D

Question: 5

Which two FortiSIEM components work together to provide real-time event correlation?

- A. Collector and Windows agent
- B. Supervisor and worker
- C. Worker and collector
- D. Supervisor and collector

Answer:D

Thank You for trying NSE5_FSM-5.2 PDF Demo

To Buy Latest NSE5_FSM-5.2 Full Version Download visit link
below

https://www.certkillers.net/Exam/NSE5_FSM-5.2

**Start Your NSE5_FSM-5.2
Preparation**

[Limited Time Offer] Use Coupon “CKNET” for Further 10% discount
on your purchase. Test your NSE5_FSM-5.2 preparation with actual
exam questions.

<https://www.certkillers.net>