



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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A FortiSIEM supervisor at headquarters is struggling to keep up with an increase of EPS (Events Per Second) being reported across the enterprise. What components should an administrator consider deploying to assist the supervisor with processing data?

- A. Supervisor
- B. Worker
- C. Collector
- D. Agent

Correct Answer: B

QUESTION 2

Refer to the exhibit.

Attribute	Order	Display As	Row	Move
Event Receive Time			<input type="radio"/>	<input type="radio"/>
Reporting IP			<input type="radio"/>	<input type="radio"/>
Event Type			<input type="radio"/>	<input type="radio"/>
Raw Event Log			<input type="radio"/>	<input type="radio"/>
COUNT(Matched Events)			<input type="radio"/>	<input type="radio"/>

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 3



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

- A. SNMP
- B. WMI
- C. Syslog D. Telnet

Correct Answer: A

QUESTION 4

Which process converts Raw log data to structured data?

- A. Data enrichment
- B. Data classification
- C. Data parsing
- D. Data validation

Correct Answer: D

QUESTION 5

What are the four possible incident status values?

- A. Active, dosed, cleared, open
- B. Active, cleared, cleared manually, system cleared
- C. Active, closed, manual, resolved
- D. Active, auto cleared, manual, false positive

Correct Answer: C

[NSE5 FSM-5.2 PDF
Dumps](#)

[NSE5 FSM-5.2 VCE
Dumps](#)

[NSE5 FSM-5.2 Practice
Test](#)