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.pass2lead.com/nse5_fsm-5-2.html

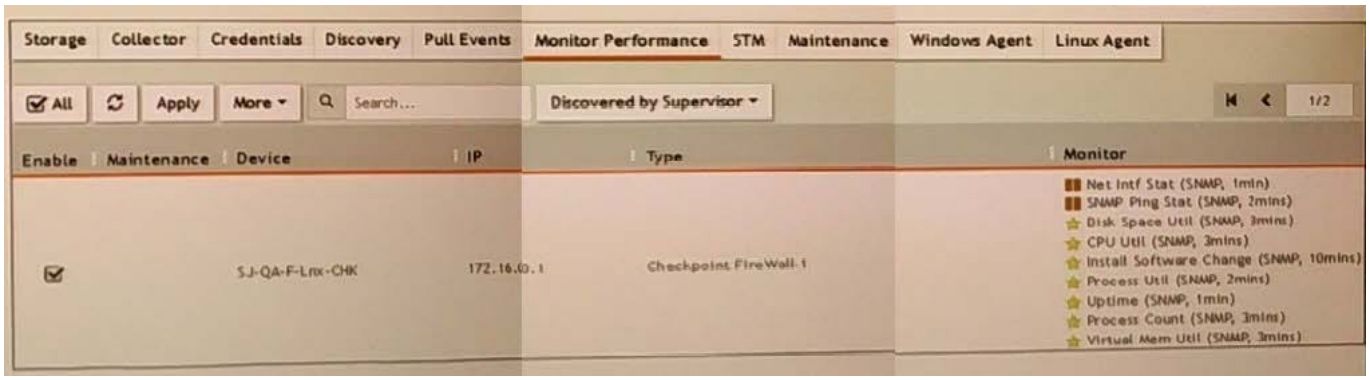
100% Passing Guarantee
100% Money Back Assurance

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

Refer to the exhibit.



What do the yellow stars listed in the Monitor column indicate?

A. A yellow star indicates that a metric was applied during discovery, and data has been collected successfully

B. A yellow star indicates that a metric was applied during discovery, but data collection has not started

C. A yellow star indicates that a metric was applied during discovery, but FortiSIEM is unable to collect data.

D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSEIM was unable to collect data.

Correct Answer: D

QUESTION 2

Which FortiSIEM components can do performance availability and performance monitoring?

A. Supervisor, worker, and collector

B. Supervisor and workers only

C. Supervisor only

D. Collectors only

Correct Answer: A

QUESTION 3

In the advanced analytical rules engine in FortiSIEM, multiple subpatterms can be referenced using which three operation?(Choose three.)

A. ELSE

B. NOT

C. FOLLOWED_BY

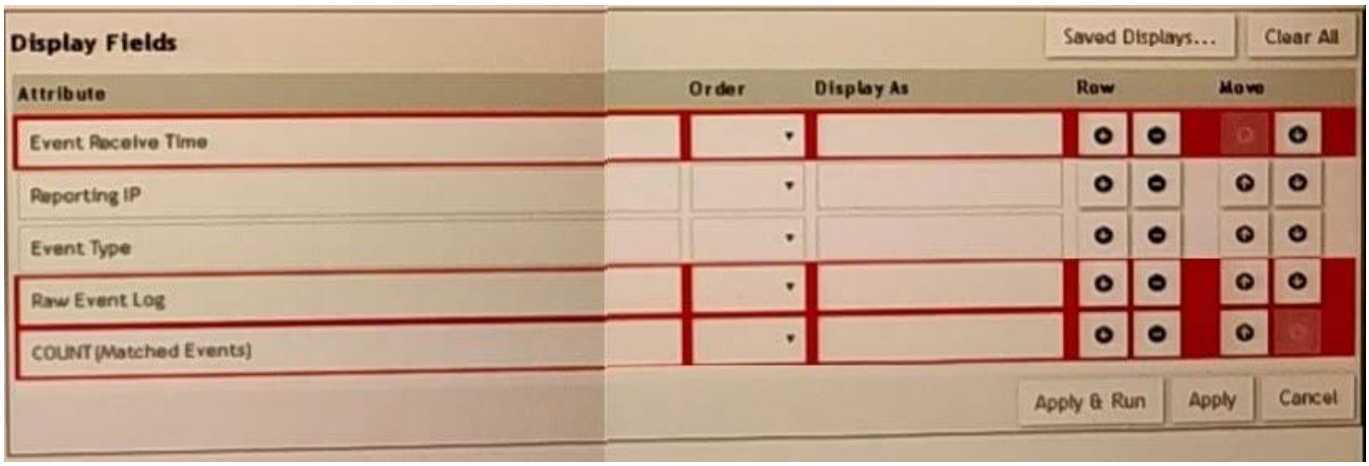
D. OR

E. AND

Correct Answer: ABE

QUESTION 4

Refer to the exhibit.



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 5

Which two export methods are available for FortiSIEM analytics results? (Choose two.)

A. CSV

B. PNG

C. HTML

D. PDF

Correct Answer: AD

QUESTION 6

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

Correct Answer: D

QUESTION 7

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

QUESTION 8

If a performance rule is triggered repeatedly due to high CPU use. what occurs m the incident table?

A. A new incident is created each time the rule is triggered, and the First Seen and Last Seen times are updated.

B. The incident status changes to Repeated and the First Seen and Last Seen times are updated.

C. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times are updated

D. The Incident Count value increases, and the First Seen and Last Seen tomes update

Correct Answer: A

QUESTION 9

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 10

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