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.certbus.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

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 2

Which item is required to register a FortiSIEM appliance license?

A. Static storage

B. Static MAC address

C. Static IP address

D. Static Hardware ID

Correct Answer: D

QUESTION 3

What are the four categories of incidents?

A. Devices, users, high risk, and low risk

B. Performance, availability, security, and change

C. Performance, devices, high risk, and low risk

D. Security, change, high risk, and low risk

Correct Answer: B

QUESTION 4

If an incident\\'s status is Cleared, what does this mean?

A. Two hours have passed since the incident occurred and the incident has not reoccurred.

B. A clear condition set on a rule was satisfied.

C. A security rule issue has been resolved.

D. The incident was cleared by an operator.

Correct Answer: A

QUESTION 5

What protocol can be used to collect Windows event logs in an agentless method?

A. SSH

B. SNMP

C. WMI

D. SMTP

Correct Answer: C

QUESTION 6

Device discovery information is stored in which database?

A. CMDB

B. Profile DB

C. Event DB

D. SVN DB

Correct Answer: A

QUESTION 7

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

QUESTION 8

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 9

In FotiSIEM enterprise licensing mode, if the link between the collector and data center FortiSIEM cluster a down what happens?

A. The collector drops incoming events like syslog. but slops performance collection

B. The collector continues performance collection of devices, but stops receiving syslog

C. The collector buffers events

D. The collector processes stop, and events are dropped

Correct Answer: D

QUESTION 10

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

A. SNMP

B. WMI

C. Syslog D. Telnet

Correct Answer: A