



# NSE5\_FSM-5.2<sup>Q&As</sup>

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.passapply.com/nse5\\_fsm-5-2.html](https://www.passapply.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

What is a prerequisite for a FortiSIEM supervisor with a worker deployment, using the proprietary flat file database?

- A. The CMDB database must be on NFS
- B. The event database must be on NFS
- C. The event database must be on a local disk
- D. The \archive mount must be on a local disk

Correct Answer: B

---

#### QUESTION 2

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 3

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

Correct Answer: C

---

#### 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

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

[NSE5 FSM-5.2 VCE Dumps](#)

[NSE5 FSM-5.2 Practice Test](#)

[NSE5 FSM-5.2 Study Guide](#)