# 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.pass4itsure.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

**QUESTION 1**

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 2**

To determine SNMP discovery issues, which is the best command from the backend?

A. snmpwalk

B. phSNMPTest

C. snmptest

D. ssh

Correct Answer: A

**QUESTION 3**

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 4**

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

A. SNMP

B. WMI

C. Syslog D. Telnet

Correct Answer: A

### QUESTION 5

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 6

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 7

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 8

Which process convertsRaw log data to structured data?

A. Data enrichment

B. Data classification

C. Data parsing

D. Data validation

Correct Answer: D

**QUESTION 9**

If the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

A. Down status is assigned because of packet loss.

B. Up status is assigned because of received packets

C. Critical status is assigned because of reduction in number of packets received

D. Degraded status is assigned because of packet loss

Correct Answer: D

**QUESTION 10**

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

A. CSV

B. PNG

C. HTML

D. PDF

Correct Answer: AD

Latest NSE5_FSM-5.2 Dumps

NSE5_FSM-5.2 VCE Dumps

NSE5_FSM-5.2 Study Guide