



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.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

In the advanced analytical rules engine in FortiSIEM, multiple subpatterns 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

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 3

Which FortiSIEM components are capable of performing device discovery?

- A. FortiSIEM Windows agent
- B. Worker
- C. FortiSIEM Linux agent
- D. Collector

Correct Answer: D

QUESTION 4

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 5

Which discovery scan type is prone to miss a device, if the device is quiet and the entry for that device is not present in the ARP table of adjacent devices?

- A. CMDB scan
- B. L2 scan
- C. Range scan
- D. Smart scan

Correct Answer: D

QUESTION 6

Refer to the exhibit.

Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

If events are grouped by Reporting IP, Event Type, and user attributes in FortiSIEM, how many results will be displayed?

- A. Seven results will be displayed.
- B. Three results will be displayed.



- C. Unique attribute cannot be grouped.
- D. Five results will be displayed.

Correct Answer: D

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

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

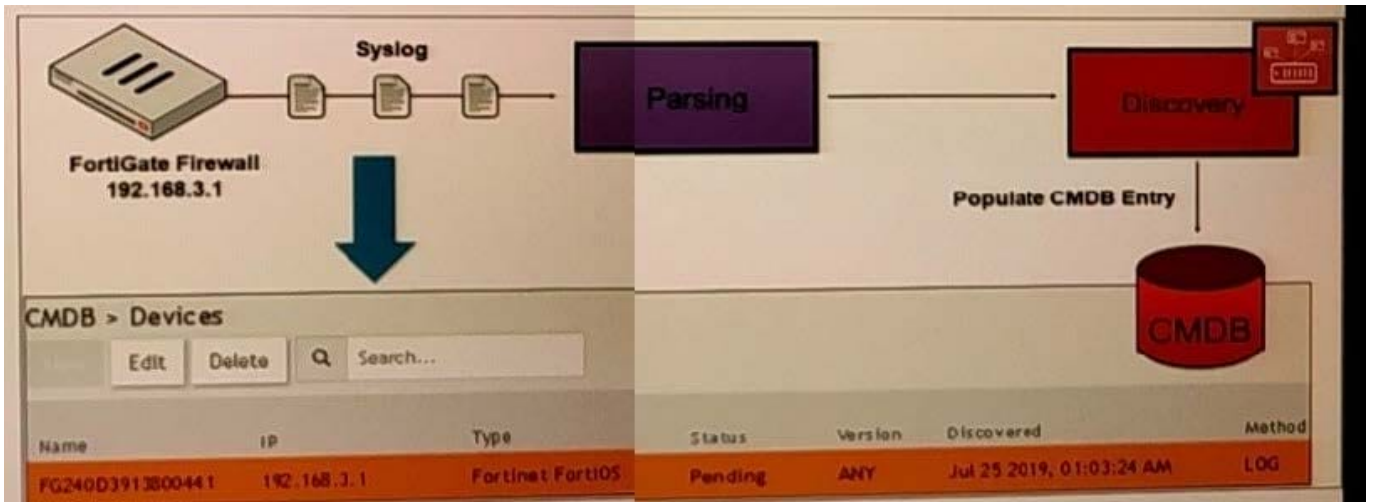
- A. The collector drops incoming events like syslog, but stops performance collection
- B. The collector continues performance collection of devices, but stops receiving syslog
- C. The collector buffers events
- D. The collector processes stop, and events are dropped

Correct Answer: D



QUESTION 10

Refer to the exhibit.



How was the FortiGate device discovered by FortiSIEM?

- A. Through GUI log discovery
- B. Through syslog discovery
- C. Using the pull events method
- D. Through auto log discovery

Correct Answer: A

[Latest NSE5_FSM-5.2 Dumps](#)

[NSE5_FSM-5.2 Practice Test](#)

[NSE5_FSM-5.2 Braindumps](#)