

DUMPS ARENA

Fortinet NSE 5 - FortiSIEM 5.2

Fortinet NSE5 FSM-5.2

Version Demo

Total Demo Questions: 8

Total Premium Questions: 42

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

What operating system is FortiSIEM based on?

- A. Cent OS
- B. Microsoft Windows
- C. RedHat
- D. Ubuntu

ANSWER: A

QUESTION NO: 2

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 Event Receive Time, Reporting IP, and User attributes in FortiSIEM, how many results will be displayed?

- A. Eight results will be displayed
- B. Four results will be displayed
- C. Two results will be displayed
- D. Unique attributes cannot be grouped

ANSWER: D

QUESTION NO: 3

Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)

- A. UDP9999
- B. UDP 162
- C. TCP 514
- D. UDP 514
- E. TCP 1470

ANSWER: C D E

QUESTION NO: 4

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

- A. SSH
- B. SNMP
- C. WMI
- D. SMTP

ANSWER: C

QUESTION NO: 5

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

- A. CSV
- B. PNG
- C. HTML
- D. PDF

ANSWER: A D

QUESTION NO: 6

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

ANSWER: D

QUESTION NO: 7

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

ANSWER: A B E

QUESTION NO: 8

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

ANSWER: C