# Exam Questions NSE5_FSM-5.2

Fortinet NSE 5 - FortiSIEM 5.2

https://www.2passeasy.com/dumps/NSE5_FSM-5.2/

**NEW QUESTION 1**
A FortiSIEM administrator wants to restrict a network administrator to running searches for only firewall devices. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

A. CMDB Report Conditions
B. Data Conditions
C. UI Access

**Answer:** B


**NEW QUESTION 2**
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

**Answer:** B


**NEW QUESTION 3**
Which protocol is almost always required for the FortiSIEM GUI discovery process?

A. SNMP
B. WMI
C. Syslog
D. Telnet

**Answer:** A


**NEW QUESTION 4**
What operating system is FortiSIEM based on?

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

**Answer:** A


**NEW QUESTION 5**
Which FortiSIEM components can do performance availability and performance monitoring?

A. Supervisor, worker, and collector
B. Supervisor and workers only
C. Supervisor only
D. Collectors only

**Answer:** A


**NEW QUESTION 6**
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

**Answer:** B


**NEW QUESTION 7**
Which process converts Raw log data to structured data?

A. Data enrichment
B. Data classification
C. Data parsing
D. Data validation

**Answer:** C


**NEW QUESTION 8**
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

**Answer:** ABE


**NEW QUESTION 9**
Refer to the exhibit.

A FortiSIEM administrator wants to collect both SIEM event logs and performance and availability metrics (PAM) events from a Microsoft Windows server
Which protocol should the administrator select in the Access Protocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?

A. TELNET
B. WMI
C. LDAPS
D. LDAP start TLS

**Answer:** A


**NEW QUESTION 10**
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

**Answer:** A


**NEW QUESTION 10**
Device discovery information is stored in which database?

A. CMDB
B. Profile DB
C. Event DB
D. SVN DB

**Answer:** A


**NEW QUESTION 15**
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 syslo
B. but slops performance collection
C. The collector continues performance collection of devices, but stops receiving syslog
D. The collector buffers events
E. The collector processes stop, and events are dropped

**Answer:** D

**NEW QUESTION 17**
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

**Answer:** C

**NEW QUESTION 18**
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.

**Answer:** B

**NEW QUESTION 22**
What is the best discovery scan option for a network environment where ping is disabled on all network devices?

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

**Answer:** A

**NEW QUESTION 27**
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

**NEW QUESTION 28**
Refer to the exhibit.

An administrator is trying to identify an issue using an expression bated on the Expression Builder settings shown in the exhibit however, the error message shown in the exhibit indicates that the expression is invalid.
Which is the correct expression?

A. Matched Events COUNT()
B. Matched Events(COUNT)
C. COUNT(Matched Events)
D. (COUNT) Matched Events

**Answer:** C

**NEW QUESTION 32**
Which FortiSIEM components are capable of performing device discovery?

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

**Answer:** D

**NEW QUESTION 33**
......

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FSM-5.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_FSM-5.2 Product From:

## https://www.2passeasy.com/dumps/NSE5_FSM-5.2/

# Money Back Guarantee

## NSE5_FSM-5.2 Practice Exam Features:

* NSE5_FSM-5.2 Questions and Answers Updated Frequently

* NSE5_FSM-5.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FSM-5.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FSM-5.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year