

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 item is required to register a FortiSIEM appliance license?

- A. Static storage
- B. Static MAC address
- C. Static IP address
- D. Static Hardware ID

Answer: D

NEW QUESTION 4

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: CDE

NEW QUESTION 5

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

Answer: B

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 subpatterns 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 13

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
- B. but stops 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 14

An administrator wants to search for events received from Linux and Windows agents.
Which attribute should the administrator use in search filters, to view events received from agents only.

- A. External Event Receive Protocol
- B. Event Received Proto Agents
- C. External Event Receive Raw Logs
- D. External Event Receive Agents

Answer: A

NEW QUESTION 15

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 20

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

NEW QUESTION 23

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

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

Answer: C

NEW QUESTION 25

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 29

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

Answer: D

NEW QUESTION 34

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 38

Refer to the exhibit.

What do the yellow stars listed in the Monitor column indicate?

- A. A yellow star indicates that a metric was applied during discovery, and data has been collected successfully
- B. A yellow star indicates that a metric was applied during discovery, but data collection has not started
- C. A yellow star indicates that a metric was applied during discovery, but FortiSIEM is unable to collect data.
- D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSEIM was unable to collect data.

Answer: B

NEW QUESTION 42

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 46

.....

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