Vendor: Fortinet

Exam Code: NSE5_FSM-5.2

Exam Name: NSE5_FSM-5.2 - Fortinet NSE 5 - FortiSIEM 5.2

Version: Demo

QUESTION 1
Which database is used for storing anomaly data, that is calculated for different parameters, such as traffic and device resource usage running averages, and standard deviation values?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which process converts Raw log data to structured data?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What is a prerequisite for FortiSIEM Linux agent installation?

A. The web server must be installed on the Linux server being monitored
B. The auditd service must be installed on the Linux server being monitored
C. The Linux agent manager server must be installed.
D. Both the web server and the audit service must be installed on the Linux server being monitored

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which two export methods are available for FortiSIEM analytics results? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

A. 16GBRAM
B. 32GBRAM
C. 64GBRAM
D. 24GB RAM

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which protocol is almost always required for the FortiSIEM GUI discovery process?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Thank You for Trying Our Product

EnsurePass Certification Exam Features:

♀ **More than 99,900 Satisfied Customers Worldwide.**

♀ **Average 99.9% Success Rate.**

♀ **Free Update to match latest and real exam scenarios**

♀ **Instant Download Access! No Setup required**

♀ **Questions & Answers are downloadable in PDF format and VCE test engine format.**

♀ **100% Guaranteed Success or 100% Money Back Guarantee**

♀ **Fast, helpful support 24x7.**

View list of all certification exams:

https://www.ensurepass.com

2023 Coupon Code 20% OFF : PASS20