Fortinet

NSE5_FSM-6.3
Fortinet NSE 5 - FortiSIEM 6.3

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ **Up to Date products, reliable and verified.**
✓ **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

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

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

Answer: AC

Question: 2

Which statement correctly describes how FortiSIEM uses thresholds for different metrics?
Response:

A. FortiSIEM uses global and per device thresholds for all performance metrics.
B. FortiSIEM uses global thresholds for all security metrics.
C. FortiSIEM uses fixed hardcoded thresholds for all performance metrics.
D. FortiSIEM uses per device thresholds for all security metrics.

Answer: A

Question: 3

Which is the best command to use to determine whether or not syslog is being received from a network device?
Response:

A. phDeviceTest
B. tcpdump
C. netcat
D. phSyslogRecorder

Answer: B

Question: 4

What is a prerequisite for a FortiSIEM supervisor with a worker deployment, using the proprietary flat file database?
Response:

A. The archive mount must be on a local disk.
B. The event database must be on NFS.
C. The CMDB database must be on NFS.
D. The event database must be on a local disk.

Answer: B

Question: 5

Which is the best command to use to troubleshoot SNMP discovery issues?
Response:

A. snmpwalk
B. phSNMPTest
C. ssh
D. snmptest

Answer: A

Question: 6

Which two FortiSIEM components are capable of performing discovery?
(Choose two.)
Response:

A. FortiSIEM Windows Agent
B. Collector
C. Worker
D. Supervisor

Answer: BD

Question: 7

What operating system is FortiSIEM based on?
Response:

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

Answer: D

Question: 8

What protocol can you use to collect Windows event logs in an agentless method?
Response:

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

Answer: C

Question: 9

What is the best discovery scan option for a network environment where ping is disabled on all network devices?
Response:

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

Answer: B

Thank You for Trying Our Product

For More Information – **Visit link below:**

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**