Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

NSE5_FSM-6.3 Dumps
NSE5_FSM-6.3 Braindumps
NSE5_FSM-6.3 Real Questions
NSE5_FSM-6.3 Practice Test
NSE5_FSM-6.3 Actual Questions

Fortinet

NSE5_FSM-6.3

NSE 5 - FortiSIEM 6.3

Question: 119

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

Question: 120

What operating system is FortiSIEM based on?

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

Answer: A

Question: 121

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

Question: 122

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: 123

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: 124

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

Answer: B

Question: 125

Which FortiSIEM components are capable of performing device discovery?

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

Answer: D

Question: 126

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

Answer: D

Question: 127

In FotiSlEM enterprise licensing mode, if the link between the collector and data center FortiSlEM cluster a down what happens?

A. The collector drops incoming events like syslog. but slops performance collection
B. The collector continues performance collection of devices, but stops receiving syslog
C. The collector buffers events
D. The collector processes stop, and events are dropped

Answer: C

Question: 128

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

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*