IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **NSE5_FSM-5.2**

Title : Fortinet NSE 5 - FortiSIEM 5.2

Version : DEMO

1.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

2.What operating system is FortiSIEM based on?
A. Cent OS
B. Microsoft Windows
C. RedHat
D. Ubuntu
Answer: A

3.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

4.What protocol can be used to collect Windows event logs in an agentless method?
A. SSH
B. SNMP
C. WMI
D. SMTP
Answer: C

5.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