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 : **C2150-614**

Title : IBM Security QRadar SIEM V7.2.7 Deployment

Version : Demo

1.Which CLI command should be used to change the default password from PASSWORD to S3cure for the username USERID?
A. /opt/ibm/toolscenter/asu/asu set IMM. Password S3cure --ksu
B. /opt/ibm/toolscenter/asu/asu set IMM. Password.1 S3cure --ksu
C. /opt/ibm/toolscenter/asu/asu64 set IMM. Password S3cure -- ksu
D. /opt/ibm/toolscenter/asu/asu64 set IMM.Password.1 S3cure -- ksu
Answer: D
Explanation:
To reset the IMM password use the following command:
/opt/ibm/toolscenter/asu64 set IMM.Password.1 NewPassword --kcs
References: http://www-01.ibm.com/support/docview.wss?uid=swg21964070

2.A Deployment Professional is performing a new deployment, and the customer wants to monitor network traffic by sending raw data packets from a network device to IBM Security QRadar SEAM V7.2.7. Which method should be used?
A. AGP card
B. Napatech card
C. SFlow protocol
D. NetFlow protocol
Answer: B
Explanation:
You can monitor network traffic by sending raw data packets to a IBM QRadar QFlow Collector 1310 appliance. The QRadar QFlow Collector uses a dedicated Napatech monitoring card to copy incoming packets from one port on the card to a second port that connects to a IBM Security QRadar Packet Capture appliance.
References:
http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/t_qflow_forward_pcap.html

3.A Deployment Professional was asked to investigate the following error:
Custom Rule Engine has detected a total of 20487 dropped event(s).
20487 event(s) were dropped in the last 62 seconds. Queue is at 99 percent capacity
The Deployment Professional needs to run the command “/opt/qradar/bin/findExpensiveCustomRules.sh” to gather the necessary troubleshooting logs.
When should this command be run?
A. Right after a reboot
B. Run “service hostcontext restart” first
C. While the system is dropping events
D. Restart ECS, then run command
Answer: C
Explanation:
The script "findExpensiveCustomRules.sh" script is designed to query the QRadar data pipeline and report on the processing statistics from the Custom Rules Engine (CRE). The script monitors metrics and collecting statistics on how many events hit each rule, how long it takes to process a rule, total execution time and average execution time. When the script completes it turns off these performance metrics. The

find ExpensiveCustomRules script is a useful tool for creating on demand reports for rule performance, it is not a tool for tracking historical rule data in QRadar. The core functionality of this script is often run when users begin to see drops in events or events routed to storage between components in QRadar.
References:
http://www-01.ibm.com/support/docview.wss?uid=swg21985252&myns=swgother&mynp=OCSSBQAC&mync=R&cm_sp=swgother-_-OCSSBQAC-_-R

4.A current banking customer has just expanded by purchasing a small rural bank with a low bandwidth WAN connection.
The customer wants to expand its current QRadar SIEM 3105 all-in-one deployment to capture log events from the newly acquired branch and to forward them on a schedule, after hours during the trough of activity to the main branch. There is plenty of room for this additional EPS growth.
Which device will meet the requirements?
A. 1202 QFlow Collector
B. 1400 Data Node
C. 1501 Event Collector
D. 1605 Event Processor
Answer: D
Explanation:
The IBM Security QRadar Event Processor 1605 (MTM 4380-Q1E) appliance is a dedicated event processor that you can scale your QRadar deployment to manage higher EPS rates. The QRadar Event Processor 1605 appliance includes an on-board event collector, event processor, and internal storage for events.
With the Basic License the capacity is 2500 EPS, and with an upgrade license it is 20000 EPS.

5.What is the impact on network bandwidth when selecting 'Global' on a rule instead of 'Local' in a distributed environment?
A. All events are sent to the QRadar Console for processing and therefore, the QRadar Console uses more bandwidth.
B. All matching events are sent to the QRadar Console for processing and therefore, the QRadar Console uses more bandwidth.
C. All events are sent to each QRadar Event Processor for processing and therefore, all Events Processors use more bandwidth.
D. All matching events are sent to each QRadar Event Processor for processing and therefore, all Event Processor use more bandwidth.
Answer: B
Explanation:
If you select Local, all rules are processed on the Event Processor on which they were received and offenses are created only for the events that are processed locally.
If you select Global, all matching events are sent to the QRadar Console for processing and therefore, the QRadar Console uses more bandwidth and processing resources.
References:
http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/t_qradar_create_cust_rul.html