IBM

C2150-624

IBM Security QRadar SIEM V7.2.8 Fundamental Administration

QUESTION: 55

An Administrator working with an IBM Security QRadar SIEM V7.2.8 deployment needs to build an Ariel Queryto find all flow data send in the last 24 hours where the amount of bytes being sent and received are largerthan 64 bytes.
What Query needs to be used?

A. SELECT * FROM flows WHERE sourceBytes > 64 & destinationBytes > 64 LAST 1 DAY
B. SELECT * FROM flows WHERE sourceBytes > 64 AND destinationBytes > 64 LAST 1 DAYS
C. SELECT * FROM flowsdata WHERE sourceBytes > 64 AND destinationBytes > 64 LAST 1 DAY
D. SELECT * FROM flowsdata WHERE sourceBytes > 64 AND destinationBytes > 64 LAST 1 DAYS

Answer: B

Explanation:

Reference:
https://www.ibm.com/developerworks/community/forums/atom/download/AQLQueryCLIGuide_71.pdf?nodeId=95b7d2b5-f480-4c14-af22-6a350fb910d2

QUESTION: 56

An Administrator using IBM Security QRadar SIEM V7.2.8 needs to force an instant backup to run. Which option should be selected?

A. Backup Now
B. On Demand Backup
C. Launch On Demand Backup
D. Configure On Demand Backup

Answer: A

QUESTION: 57
Administrators on versions of IBM Security QRadar SIEM older than V7.2.4 must use a specific upgrade path to transition to newer software versions. These requirements are outlined in what technical document?

A. Fix Level Recommendation Tool
B. IBM latest firmware release notes
C. QRadar Software upgrade progress technical note
D. IBM System Security Interoperation Center (SSIC)

Answer: C

Explanation:
Most of the upgrades of IBM products are available in technical notes. IBM security Qradar SIEM upgrade process and information can be obtained through technical notes that IBM publishes on the web.

Reference:
http://www-01.ibm.com/support/docview.wss?uid=swg27038118

QUESTION: 58
What are three protocols that collect flow data from network devices, such as routers, and send this data toIBM Security QRadar SIEM V7.2.8?

A. NetFlow, J-Flow and sFlow
B. NetFlow, IPFIX and syslog
C. NetFlow, rsyslog and sFlow
D. NetFlow, Packeteer and syslog

Answer: A

Explanation:
NetFlow, J-Flow, and sFlow are protocols that collect flow data from network devices, such as routers, andsend this data to QRadar.

Reference:
https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.d oc/
c_tuning_guide_deploy_cfgflowsource.html

QUESTION: 59
Which appliance of the IBM Security QRadar SIEM V7.2.8 family is a specifically used to gather events fromlocal and remote log sources?

A. QRadar Event Console
B. QRadar QFlow Collector
C. QRadar Event Collector
D. QRadar Event Processor

Answer: C

Explanation:
Gathers events from local and remote log sources. Normalizes raw log source events. During this process, theMagistrate component examines the event from the log source and maps the event to a QRadar Identifier(QID). Then, the Event Collector bundles identical events to conserve system usage and sends theinformation to the Event Processor.

Reference:
https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/ shc_qradar_comps.html

QUESTION: 60
What are the four categories of notifications found in IBM Security QRadar SIEM V7.2.8 system notifications?

A. Errors, Critical, Minor and Information
B. Errors, Warning, Information, and Health
C. Warning, Information, System and Critical
D. Errors, Warning, Information, and Performance

Answer: B

Reference:
http://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.8/en/ b_qradar_system_notifications.pdf