C2150-624 Q&As

IBM Security QRadar Risk Manager V7.2.6 Administration

Pass IBM C2150-624 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

What are three protocols that collect flow data from network devices, such as routers, and send this data to IBM 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

Correct Answer: A

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

QUESTION 2

An Administrator working with IBM Security QRadar SIEM V7.2.8 is constantly receiving the following

message:

"MPC: Unable to process offense. The maximum number of offenses has been reached."

What is the reason for this message?

A. The Multi Packet Capturer cannot handle more than 2500 attacks at the same time.

B. The Magistrate Processor Core has more than 2500 active Offenses or 100000 overall Offenses.

C. The Multi Packet Capturer cannot handle more than 500 offense reports at a certain point in time.

D. The Magistrate Processor Core has reached its maximum amount of network connections at a certain time.

Correct Answer: B

QUESTION 3

An IBM Security QRadar SIEM V7.2.8 deployment configured with High-Availability (HA) has both a

primary and secondary host. The administrator needs to test the operation of the primary high-availability

(HA) host automatic failover to the secondary HA host.

What must be configured to accomplish this test?

A. Configure the time interval of heartbeat timeout tests so the secondary HA host receives a response from the primary

![Pass2Lead](https://Pass2Lead.com)
HA host within 2 minutes.

B. Configure the time interval of heartbeat timeout tests so the secondary HA host does not receive a response from the primary HA host within 2 minutes.

C. Configure the time interval of heartbeat ping tests so the secondary HA host receives a response from the primary HA host within a preconfigured time period.

D. Configure the time interval of the heartbeat ping tests so the secondary HA host does not receive a response from the primary HA host within a preconfigured time period.

Correct Answer: C

QUESTION 4

An Administrator is creating custom rules and configuring log sources on an IBM Security QRadar SIEM

V7.2.8 console. This data needs to be retained so that it can be recovered in case of any system failure

with minimal effort.

Which option can the Administrator utilize from the Backup and Recovery Wizard to accomplish this task?

A. Data backups

B. Ariel database

C. Configuration and Data backups

D. Configuration and DB2 database

Correct Answer: A

QUESTION 5

An Administrator working with a IBM Security QRadar SIEM V7.2.8 deployment needs to build an Ariel

Query to find all events data received in the last 24 hours where the magnitude of the events is larger than

1 but smaller than 5.

What Query needs to be used?

A. SELECT * FROM events WHERE magnitude > 1 AND

B. SELECT * FROM events WHERE magnitude BETWEEN 1 AND 5 LAST 1 DAYS

C. SELECT * FROM eventstable WHERE magnitude BETWEEN 1 and 5 LAST 1 DAYS

D. SELECT * FROM eventstable WHERE magnitude BETWEEN 1 AND 5 LAST 1 DAYS

Correct Answer: A

C2150-624 PDF Dumps   C2150-624 VCE Dumps   C2150-624 Study Guide