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.passapply.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

Given the following RegEx: (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b) What data does this expression extract?

A. URL

B. User Name

C. IP address

D. Email Address

Correct Answer: C

QUESTION 2

What is the difference between Flows and Event data collected by IBM Security QRadar SIEM V7.2.8?

A. Events are streamed each minute to the Event Processor. Flows are streamed immediately to the Flow Processor.

B. Flow data is collected from different log sources. Event data is collected from internal or external network sources.

C. An Event occurs at a specific time and is logged at that time. A Flow is a record of network activity that can last for seconds, minutes, hours, or days.

D. An Event can span time lasting seconds, minutes, hours depending on the duration of a network session. A Flow happens at a single point in time and then is complete.

Correct Answer: C

QUESTION 3

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 4

An Administrator working with IBM Security QRadar SIEM V7.2.8 has to add a new host name to a reference set with the name "Allowed Hosts" from the command line interface.

Which command would accomplish this task?

A. ./ReferenceSetUtil.sh add Allowed\ Hosts computer.domain.com

B. ./UtilReferenceSet.sh add "Allowed Hosts" "computer.domain.com"

C. ./UtilReferenceSet.sh update Allowed\ Hosts "computer.domain.com"

D. ./ReferenceSetUtil.sh update "Allowed Hosts" "computer.domain.com"

Correct Answer: A

QUESTION 5

An Administrator working with IBM Security QRadar SIEM V7.2.8 has updated the date/time on the QRadar console system and wants to update these date/time settings to all his hosts in the distributed environment.

What command should be run?

A. /opt/qradar/bin/datesync_all_servers.sh

B. /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh

C. /opt/qradar/support/fullDeployment.sh /opt/qradar/bin/time_sync.sh

D. /opt/qradar/support/all_servers.sh /opt/qradar/bin/check_date_change.sh

Correct Answer: B

To run time synchronization on all hosts and see if any fail to synchronize with the Console, from the root directory (/) type the following command: ./opt/qradar/support/all_servers.sh "/opt/qradar/bin/time_sync.sh"