C1000-026$^{\text{Q\&As}}$

IBM Security QRadar SIEM V7.3.2 Fundamental Administration

Pass IBM C1000-026 Exam with 100% Guarantee

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

https://www.pass4itsure.com/c1000-026.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An administrator needs to collect logs from the Command Line Interface (CLI). Which command should the administrator use?

A. /opt/bin/qradar/support/get_logs.sh

B. /opt/support/get_logs.sh

C. /opt/support/qradar/get_logs.sh

D. /opt/qradar/support/get_logs.sh

Correct Answer: D

Reference: https://www.ibm.com/support/pages/getting-help-what-information-should-be-submitted-qradarservice-request

QUESTION 2

An administrator modified a configuration setting in the Global System Notifications using the QRadar Console Admin tab.

What is the last step to apply changes?

A. Reload Web Server

B. Restart Services

C. Re-login to QRadar console

D. Deploy Changes

Correct Answer: D

QUESTION 3

What happens if QRadar receives events at a higher rate than the license allows?

A. The events will be put into queues

B. The source system will be asked to resend the events later

C. The events will not be parsed

D. The events will be dropped immediately

Correct Answer: A

Reference: https://www.ibm.com/support/pages/qradar-event-and-flow-burst-handling-buffer

QUESTION 4

An administrator needs to extract a property from an intrusion detection system (IDS) log. Using a regular expression, the administrator wants to extract a specific part of the log showing the matching "policy ID" of the IDS.

Which type of property must the administrator create?

A. Custom event property

B. Custom flow property

C. Custom asset property

D. Normalized event property

Correct Answer: D

QUESTION 5

A company has two different domains in their IBM QRadar system: Domain_A and Domain_B. An administrator has been tasked to create a rule to look only at events that are tagged with Domain_A and ignore rules that are tagged with the other domains.

What domain text should the administrator use to create this rule?

A. is from domain: Domain_A

B. from domain: Domain_A

C. domain is: Domain_A

D. domain is one of: Domain_A

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/
c_domain_specific_rules_offenses.html