



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



C1000-026 Dumps
C1000-026 Braindumps
C1000-026 Real Questions
C1000-026 Practice Test
C1000-026 Actual Questions



IBM

C1000-026

IBM Security QRadar SIEM V7.3.2 Fundamental Administration



Question: 53

An administrator is about to integrate logs from a custom firewall in a QRadar deployment using syslog. The SIEM has two domains, namely Domain A and Domain B. While reviewing the following sample logs, the administrator notices a "context" keyword:
May 14 11:05:01 192.168.1.23 20190514 11:05:00 context=contextA permit 192.168.1.24 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp; May 13 12:07:01 192.168.1.23 20190513 11:07:00 context=contextB permit 192.168.1.25 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp; Which options assign the "contextA" logs to DomainA and the "contextB" logs to domain B? (Choose two.)

- A. Create a single log source, create a "Context" custom event property, and assign the log to both domains using a custom rule.**
- B. Create two individual log sources by configuring a separated logging instance for each context on the firewall and assign each log source to the correct domain.**
- C. Create a single log source, create a "Context" custom event property, and assign the log to the correct domain using custom event property value.**
- D. Create two individual log sources using the context value as log source identifier and assign each log source to the correct domain.**
- E. Create a single log source, create a "Context" custom event property, and assign the log to the correct domain using a custom rule.**

Answer: BD

Question: 54

Which event routing rule is required to add QRadar Data Store (QDS) capability to a deployment?

- A. Log Only (exclude Analytics)**
- B. Delete data When storage space is required**
- C. Bypass Correlation**
- D. Delete data immediately after the retention period has expired**

Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_adm_data_store.html

Question: 55

An administrator is seeing the following system notification:
38750057 – A protocol source configuration may be stopping events from being collected.
What is a valid user action to this issue?

- A. Re-install the QRadar Console**
- B. Review the /var/log/qradar.log file for more information**
- C. Restart the QRadar Console**
- D. Review the /var/log/error.log file for more information**

Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/38750057.html

Question: 56

To comply with specific regulations, an administrator has been requested to increase asset retention to 365 days. In which QRadar section can the administrator find the asset retention settings?

- A. Admin Tab / Asset Retention**
- B. Assets Tab / Retention settings**
- C. Admin Tab / System settings**
- D. Assets Tab / Asset Retention**

Answer: C

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_adm_asset_tuning_ip_retention.html

Question: 57

A QRadar administrator added High Availability (HA) to the Event Processor and needs to verify the crossover link status between the primary and secondary hosts.

Which commands can be used to verify the crossover status? (Choose two.)

- A. `/opt/qradar/ha/bin/ha_getstate.sh`
- B. `/opt/qradar/ha/bin/getStatus crossover`
- C. `/opt/qradar/ha/bin/qradar_nettune.pl crossover status`
- D. `/opt/qradar/ha/bin/qradar_nettune.pl linkaggr <interface> status`
- E. `/opt/qradar/ha/bin/ha cstate`
- F. `cat /proc/drbd`

Answer: CF

Reference: <https://www.ibm.com/developerworks/community/forums/html/topic?id=5c01c198-016d-461b-a648-a87cdc445768>

Question: 58

An administrator needs to import data into QRadar for a specific use case.

The data that has been provided to the administrator is stored in records that map a key to a value.

Which type of data collection must the administrator create?

- A. Reference set
- B. Reference map of sets
- C. Reference map
- D. Reference map of maps

Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_conifig_rul_resp_reference_set.html

Question: 59

An administrator needs to know if a custom rule is being correlated correctly.

Which QRadar component is responsible for this process?

- A. QRadar Event Collector
- B. QRadar Console
- C. Magistrate
- D. QRadar Event Processor

Answer: D

Reference: <https://www.ibm.com/support/pages/qradar-global-correlation>

Question: 60

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`

Answer: D

Reference: <https://www.ibm.com/support/pages/getting-help-what-information-should-be-submitted-qradar-service-request>



SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>
Kill your exam at First Attempt....Guaranteed!