

C1000-026^{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.pass2lead.com/c1000-026.html

100% Passing Guarantee 100% Money Back Assurance

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

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers





https://www.pass2lead.com/c1000-026.html

2024 Latest pass2lead C1000-026 PDF and VCE dumps Download

QUESTION 1

An administrator needs to develop advanced filters to retrieve information from the QRadar System pertaining to the top abnormal events of the most bandwidth-intensive IP addresses.

How can the administrator do this?

- A. Build an AQL guery using the QRadar Scratchpad
- B. Combine GROUP BY and ORDER BY clauses in a single query
- C. Use the IBM DataStudio to create the guery
- D. Build an AQL query using the QRadar GUI using Assets > Search Filter

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/ b_qradar_aql.pdf (21)

QUESTION 2

What should an administrator do to successfully upgrade an IBM Security QRadar system from an older version?

- A. Verify the upgrade path, and review the software, hardware and high availability requirements.
- B. Verify the upgrade path and update the QRadar apps.
- C. Review the release notes and review the architecture.
- D. Review the software, hardware and high availability requirements, and consider to update the firmware on IBM Security QRadar appliances.

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/ b_qradar_upgrade.pdf (9)

QUESTION 3

An administrator needs to import a list of HR staff logins into a reference set.

Which file type can be used with the import function in the reference set editor window?

- A. xml
- B. csv
- C. xls
- D. json



https://www.pass2lead.com/c1000-026.html

2024 Latest pass2lead C1000-026 PDF and VCE dumps Download

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c gradar adm refdata_ui.html

QUESTION 4

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

Correct 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 5

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

C1000-026 Practice Test C1000-026 Exam Questions C1000-026 Braindumps