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.leads4pass.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

QUESTION 1

An administrator would like to extend the functionality of QRadar using an external application.

Which file format is supported to successfully upload an application from the QRadar Console?

A. .zip

B. .tgz

C. .sh

D. .exe

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.appfw.doc/
b_qradar_appframework_devguide.pdf

QUESTION 2

A custom rule is generating events reporting that a specific user is failing to login too many times in the last 5 minutes. The administrator opens the event details to investigate the anomaly associated with the events but finds that no Anomaly details pane is shown.

What is the reason?

The events were generated by:

A. a Behavioral Detection Rule

B. an Anomaly Detection Rule

C. a Threshold Detection Rule

D. a standard Custom Rule

Correct Answer: B

Reference: http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 3

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 4

An administrator needs data backup.

What information is contained in the data backup?

A. Audit log information, Event data, Flow data, Report data, Indexes, Log sources

B. Audit log information, Event data, Indexes, Index management information, Flow data, Report data

C. Audit log information, Event data, Flow data, Report data, Indexes

D. Audit log information, Event data, Indexes, Index management information, Flow data, Report data, Groups

Correct Answer: C

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

QUESTION 5

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

[C1000-026 PDF Dumps](#)   [C1000-026 Practice Test](#)   [C1000-026 Study Guide](#)