# 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**

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 2**

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

**QUESTION 3**

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 query using the QRadar Scratchpad

B. Combine GROUP BY and ORDER BY clauses in a single query

C. Use the IBM DataStudio to create the query

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 4**

What is a reason for restarting hostcontext service in QRadar?

A. A new user was created and it needs to be replicated

B. A new network hierarchy was uploaded

C. A new app was installed

D. The host is not responding to deploy requests

Correct Answer: D

Reference: https://www.ibm.com/support/pages/qradar-restarting-hostcontext-q-switch

**QUESTION 5**

Due to regulatory constraints, an administrator must increase the minimum password length and complexity.

In which QRadar section can the administrator change this setting?

A. Admin / System settings

B. Admin / Password policy

C. Admin / Security profiles

D. Admin / Authentication

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SSHLHV_5.4.0/com.ibm.alps.doc/tasks/alps_configuring_admin_settings.htm