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

QUESTION 1

Which event QID test is used to send an email as a rule response when disk usage reaches a threshold?

A. (38750076) Disk Sentry Reached Warn threshold

B. (38750076) Disk Sentry Disk Usage Exceeded Warning threshold levels

C. (38750076) Disk Usage Exceeded Warn threshold

D. (38750076) Disk Sentry Disk Usage Exceeded Warn threshold

Correct Answer: B

Reference: https://www.ibm.com/support/pages/qradar-configuring-qradar-remote-alerts-about-disk-usage

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

An administrator needs to save a search to use it in the dashboards.

To do so, which search feature does the administrator need to select in the "Include in my Dashboard" checkbox?

A. Filter events of the last 7 days

B. Filter events of the last month

C. Filter events of the last 5 minutes

D. Group by some property

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf (42)

QUESTION 4

An administrator is tasked to reduce data volumes in the asset database and reduce stale data contributing to asset growth deviation.

How can the administrator tune the configuration of the Asset Profiler?

A. In the System Configuration section of the Admin, access the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save. Next, deploy the changes into the environment for the updates to take effect.

B. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save. Next, deploy the changes into the environment for the updates to take effect.

C. On the navigation menu, click Admin, click the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save. On the navigation menu, click Admin and from the Advanced menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.

D. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save. On the navigation menu, click Admin and from the Advanced menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.

Correct Answer: B

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 5

When troubleshooting issues with QRadar applications, which application Docker container log file can be used to get more information about the apps?

A. /var/log/qradar.error

B. /var/log/qradar.log

C. /var/log/app.log

D. /store/log/app.log

Correct Answer: D

Reference: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/24f91a23-846b483c-ba22-d78b95eed91e/page/d504c946-a9b0-4277-8e4f-bc554ac30e4e/versions