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.passapply.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

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

QUESTION 2

What is the minimum memory in gigabyte (GB) required for a QRadar All-in-One Virtual 3199 appliance?

A. 128

B. 32

C. 24

D. 16

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_ha_vrt_ap_reqs.html

QUESTION 3

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 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

An administrator has been tasked to create a saved search that shows a list of multiple login failures for a single user by username. The administrator has done the following:

1.

Selected Last Hour in the view option.

2.

In the Add filter window, selected the search parameter Custom Rule [Indexed].

3.

Selected Equals for Operator.

4.

Selected Authentication for Rule Group.

What is the next step the administrator needs to perform for the Rule option?

A. Select login failures followed by success to the same username

B. Select multiple login failures from the same source

C. Select multiple login failures to the same destination

D. Select multiple login failures for a single username

Correct Answer: C