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

![Pass2Lead](https://Pass2Lead.com)
QUESTION 1

An administrator wants to have all QRadar apps running on a new App Host that was configured to have dedicated CPU, storage and memory resources for the Apps. Several issues were presented during the installation of the App Host.

To troubleshoot, what should the administrator check?

A. If the completion of the /opt/qradar/check_app_host.sh script was successful

B. If port 5000 is opened on the console

C. If an IP table entry was already created to allow traffic from the App Host IP

D. If IP tables are disabled on the console

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_adm_apphost.html

QUESTION 2

A company has several appliances and the administrator needs to copy a file to all appliances to run some tests to verify the integrity of the processes. The /opt/qradar/support/all_servers.sh script can be used to issue commands to all QRadar appliances within the deployment.

What option must be used with the script to copy the file to all appliances in the deployment?

A. /opt/qradar/support/all_servers.sh -p

B. /opt/qradar/support/all_servers.sh -k

C. /opt/qradar/support/all_servers.sh -C

D. /opt/qradar/support/all_servers.sh -g

Correct Answer: A

Reference: https://www-01.ibm.com/support/docview.wss?uid=swg21998517

QUESTION 3

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 4

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

QUESTION 5

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)

Latest C1000-026 Dumps   C1000-026 Practice Test   C1000-026 Study Guide