C1000-026$^{\text{Q\&As}}$

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.pass4itsure.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

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

What happens if QRadar receives events at a higher rate than the license allows?

A. The events will be put into queues

B. The source system will be asked to resend the events later

C. The events will not be parsed

D. The events will be dropped immediately

Correct Answer: A

Reference: https://www.ibm.com/support/pages/qradar-event-and-flow-burst-handling-buffer

QUESTION 3

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 4

An administrator has been asked to configure a new QRadar console high availability (HA) deployment. Both the primary and secondary consoles have been installed with the QRadar software.

What should the administrator do to complete the HA configuration?

A. Add the secondary console to the deployment, and then create the HA host.

B. Reinstall the QRadar software on the secondary console using an "HA Recovery Setup".

C. Select "Secondary Host" on the wizard when adding the secondary host to the deployment.

D. Create the HA host to add the secondary console to the deployment.

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/ b_qradar_ha_guide.pdf

QUESTION 5

An administrator has to change the system hardware clock of the QRadar server. The administrator has already restarted the main services (hostservices, tomcat, hostcontext) and needs to synchronize the QRadar Console time with the QRadar managed hosts.

Which command can the administrator use to accomplish this?

A. /opt/qradar/support/all_servers.sh systemctl restart systemd-timedated.service

B. /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh

C. /sbin/hwclock –systohc /opt/qradar/bin/time_sync.sh

D. /opt/qradar/support/all_servers.sh service ntpd restart

Correct Answer: B

Reference: https://www.ibm.com/support/pages/qradar-configuring-ntp-settings-qradar-appliance