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

QUESTION 1

An administrator modified a configuration setting in the Global System Notifications using the QRadar Console Admin tab.

What is the last step to apply changes?

A. Reload Web Server

B. Restart Services

C. Re-login to QRadar console

D. Deploy Changes

Correct Answer: D

QUESTION 2

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

QUESTION 3

An administrator needs to upgrade their QRadar environment. The administrator has downloaded the Patchupdate File from Fixcentral and transferred this Image to the Appliance.

Which commands does the administrator need to run to start the upgrade process?

A. 1. cd/medial/updates

2.

 systemctl stop Qradar

3.

 Qradar.sh upgrade all

4.

systemctl reboot

B. 1. mount –o loop –t squashfs XX_patchupdate.sfs /media/updates

2.

cd /media/updates

3.

/installer

C. 1. cd /media/updates

2. yum update XX_patchupdate.sfs

D. 1. patch XX_patchupdate.sfs

Correct Answer: B

QUESTION 4

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 5

An administrator needs to extract a property from an intrusion detection system (IDS) log. Using a regular expression,
the administrator wants to extract a specific part of the log showing the matching "policy ID" of the IDS.

Which type of property must the administrator create?

A. Custom event property

B. Custom flow property

C. Custom asset property

D. Normalized event property

Correct Answer: D