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

IBM Security QRadar SIEM V7.3.2 Fundamental Administration

Pass IBM C1000-026 Exam with 100% Guarantee

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

An administrator enters the QRadar web console into a web browser but does not get a response. Which process is responsible for the QRadar GUI?

A. tomcat

B. consoled

C. magistrated

D. guid

Correct Answer: A

Reference: https://www.ibm.com/support/pages/qradar-core-services-and-impact-when-restarted

QUESTION 2

A QRadar upgrade is planned and a maintenance window is scheduled. The administrator must stage the FIXPACK from IBM Fix Central.

Which QRadar FIXPACK file type must the administrator download?

A. RPM

B. IMG

C. SFS

D. XFS

Correct Answer: C

Reference: https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Securityandproduct=ibm/Other+software/IBM+QRadar+Network+Insightsandrelease=7.3.0andplatform=Linuxandfunction=all

QUESTION 3

An administrator needs to add, delete and modify user accounts.

When deleting a user, what dependency checks are carried out?

A. Custom Rules, Historical Correlation Profiles, Security Profiles

B. Custom Rules, Report and Search Criteria, Security Roles

C. Custom Rules, Security Profiles, Report and Search Criteria

D. Custom Rules, Report and Search Criteria, Historical Correlation Profiles

Correct Answer: D

QUESTION 4

An administrator is about to integrate logs from a custom firewall in a QRadar deployment using syslog. The SIEM has two domains, namely Domain A and Domain B. While reviewing the following sample logs, the administrator notices a "context" keyword:

```
May 14 11:05:01 192.168.1.23 20190514 11:05:00 context=contextA permit 192.168.1.24 source: 10.10.1.15;
source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp;

May 13 12:07:01 192.168.1.23 20190513 11:07:00 context=contextB permit 192.168.1.25 source: 10.10.1.15;
source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp;
```

Which options assign the "contextA" logs to DomainA and the "contextB" logs to domain B? (Choose two.)

A. Create a single log source, create a "Context" custom event property, and assign the log to both domains using a custom rule.

B. Create two individual log sources by configuring a separated logging instance for each context on the firewall and assign each log source to the correct domain.

C. Create a single log source, create a "Context" custom event property, and assign the log to the correct domain using custom event property value.

D. Create two individual log sources using the context value as log source identifier and assign each log source to the correct domain.

E. Create a single log source, create a "Context" custom event property, and assign the log to the correct domain using a custom rule.

Correct Answer: BD

QUESTION 5

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