DUMPSARENA

# IBM Security QRadar SIEM V7.3.2 Fundamental Administration

## IBM C1000-026

**Version Demo**

**Total Demo Questions: 8**

**Total Premium Questions: 60**

**Buy Premium PDF**

https://dumpsarena.com

sales@dumpsarena.com

## QUESTION NO: 1

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

## ANSWER: D

**Explanation:**

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf (42)

## QUESTION NO: 2

An administrator receives an expensive custom rule notification.

Which tool can now be enabled via the Advanced ‘System Settings’ – Custom Rule Settings to help troubleshoot this?

**A.** Offense Analysis

**B.** Rule Analysis

**C.** Custom Rule Analysis

**D.** Performance Analysis

## ANSWER: C

## QUESTION NO: 3

An administrator needs to save the nightly QRadar backups on a network storage.

The administrator has established the connection to the network storage.

What should the administrator do next?

**A.** Change the Backup Repository Path to the network storage location using the Backup Recovery Configuration window.

**B.** Change the Backup Repository Path by adding a new Network Activity Rule.

**C.** Change the Backup Repository Path to the network storage location using the System Settings window.

**D.** Configure the new network storage using the Assets Manager

**ANSWER: A**

**Explanation:**

Reference: http://ftpmirror.your.org/pub/misc/ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_admin_guide.pdf (146)

## QUESTION NO: 4

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

**ANSWER: C**

**Explanation:**

Reference: https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+QRadar+Network+Insights&release=7.3.0&platform=Linux&function=all

## QUESTION NO: 5

A QRadar administrator added High Availability (HA) to the Event Processor and needs to verify the crossover link status between the primary and secondary hosts.

Which commands can be used to verify the crossover status? (Choose two.)

**A.** /opt/qradar/ha/bin/ha_getstate.sh

**B.** /opt/qradar/ha/bin/getStatus crossover

**C.** /opt/qradar/ha/bin/qradar_nettune.pl crossover status

**D.** /opt/qradar/ha/bin/qradar_nettune.pl linkaggr status

**E.** /opt/qradar/ha/bin/ha cstate

**F.** cat /proc/drbd

**ANSWER: C F**

**Explanation:**

Reference: https://www.ibm.com/developerworks/community/forums/html/topic?id=5c01c198-016d-461b-a648-a87cdc445768

## QUESTION NO: 6

What is a reason for restarting hostcontext service in QRadar?

**A.** A new user was created and it needs to be replicated

**B.** A new network hierarchy was uploaded

**C.** A new app was installed

**D.** The host is not responding to deploy requests

**ANSWER: D**

**Explanation:**

Reference: https://www.ibm.com/support/pages/qradar-restarting-hostcontext-q-switch

## QUESTION NO: 7

When an administrator attempts to edit a log source after upgrading QRadar, a Device Support Module (DSM), a protocol, or Vulnerability Information Services (VIS) components, the following error message appears.

An error has occurred. Refresh your browser (press F5) and attempt the action again. If the problem persists, please contact customer support for assistance.

What action should the administrator take to troubleshoot this issue? (Choose two.)

**A.** systemctl restart snmpd

**B.** systemctl restart iptables

**C.** systemctl restart ecs-ep

**D.** systemctl start tomcat

**E.** systemctl restart httpd

**F.** Clear browser cache

**ANSWER: D F**

**Explanation:**

Reference:
https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/t_QRadar_Troubleshooting_guide_PurgeFiles.html

## QUESTION NO: 8

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.** 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.)
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.

**ANSWER: B D**