IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **C2150-400**

Title : IBM Security Qradar SIEM Implementation v 7.2.1

Version : DEMO

1.The following message is displayed in the System Notification Widget on the Dashboard:

Jan 15Jan 15 14:34:32 172.16.77.109 [ecs] [[type=com.eventgnosis.system.ThreadedEventProcessor] [parent[parent=crssiem.crosig.group:ecs0/EP/Processor2]] com.q1labs.semsources.cre.CRE: [WARN] [NOT:0[NOT:0080004101][172.16.77.109/- -] [-/- -]Custom Rule Engine has sent a total of 9125354 event(s) to storito storage. 22350 event(s) were sent in the last 60 seconds. Queue is at 99 percent capacity.

Which script should be run to help determine the cause of the dropped events?

A. /opt/qradar/support/dumpGvData.sh

B. /opt/qradar/support/dumpDSMInfo.sh

C. /opt/qradar/support/cleanAssetModel.sh

D. /opt/qradar/support/findExpensiveCustomRules.sh

Answer: D

2.What is used to collect netflow and jflow traffic in a QRadar Distributed Deployment?

A. QRadar 3105 Console

B. QRadar 1705 Processor

C. QRadar 1605 Processor

D. QRadar 700 Risk Manager

Answer: A

Explanation:http://www.arrowecs.ae/FMS/16966.appliance_datasheet.pdf(page 3)

3.What should the format of a CSV file be while importing assets on the QRadar console?

A. ip,portweight,description

B. ip,name,weightmagnitude

C. ip.name.weight.description

D. ip.name.severity.description

Answer: C

Explanation:http://www-03.ibm.com/certify/tests/objC2150-195.shtml(search for name, weight, description)

4.Which option needs to be specified in the syslinux configuration file to reinstall an IBM QRadar appliance via serial port from an USB flash-drive?

A. USB to serial

B. Default serial

C. Serial to USB

D. serial redirect

Answer: B

Explanation:ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.0/QLM/EN/USB_Installation.pdf(page 5)

5.With a Data Deletion Policy of "When storage is required", data will remain in storage until which scenario is reached?

A. If used disk space reaches 88% for records and 85% for payloads.

B. If used disk space reaches 85% for records and 88% for payloads.

C. If used disk space reaches 85% for records and 83% for payloads.

D. If used disk space reaches 83% for records and 85% for payloads.

Answer: C

Explanation:http://www.juniper.net/techpubs/software/management/strm/2013_2/strm-adminguide.pdf(page 85, see the table, 5throw, second column, first bulleted point)