考試編碼:C2150-400

考試名稱: IBM Security Qradar SIEM Implementation v 7.2.1

版本: Demo

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

Jan 15 14:34:32 172.16.77.109 [ecs] [[type=com.eventgnosis.system.ThreadedEventProcessor] [parent=crssiem.crosig.group:ecs0/EP/Processor2]] com.q1labs.semsources.cre.CRE: [WARN] [NOT:0080004101][172.16.77.109/- -] [-/- -]Custom Rule Engine has sent a total of 9125354 event(s) directly to 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

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

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

QUESTION: 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
Reference:ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.0/QL M/EN/USB_Installation.pdf(page 5)

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

QUESTION: 6

Which two actions can be selected from the license drop-down in the system and license management screen when working with a new license? (Choose two.)

A. Apply license
B. Upload license
C. Allocate license to system
D. Allocate system to license
E. Register system to license

Answer: A,C

QUESTION: 7

How frequently does the Automated Update Process run if Configuration files are updated on Primary and then Deploy Changes is not performed, and the updates are made on the Secondary host through an Automated Update Process?

A. Every 10 minutes
B. Every 15 minutes
C. Every 30 minutes
D. Every 60 minutes

Answer: D
Reference:http://www.juniper.net/techpubs/software/management/strm/2010_0_R1/Admin_ STRM.pdf(page 68, see the second note)

QUESTION: 8

What two are valid actions that a user can perform when monitoring offenses? (Choose two.)

A. Import offenses
B. Backup offenses
C. Restore offenses
D. Send email notifications
E. Hide or close an offense from any offense list

Answer: B,E

QUESTION: 9

What is a valid QVM scan status?

A. Active
B. Paused
C. Scanning
D. Complete

Answer: A

QUESTION: 10

Which NetFlow versions doesQRadarSIEM support?

A. 1,2,3, and 4
B. 1,4,7, and 9
C. 1,3,5,and 9
D. 1,5,7,and 9

Answer: D
Reference:http://www-01.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_qradar_ adm_netflow.html(second para, first sentence)

QUESTION: 11

How do you view Raw Events on the Log Activity tab?

A. Select "Raw Events" from the View list box
B. Select "Raw Events" from the Actions list box
C. Select "Raw Events" from the Display list box
D. Select "Raw Events" from the Quick Searches list box

Answer: C
Reference:ftp://ftp.software.ibm.com/software/security/products/qradar/documents/71MR1/ LogMgr/LM-71MR1-Usersguide.pdf(page 33)

QUESTION: 12

There is a requirement at the customer site to double the default QFlow Maximum Content Capture size.

What would be the resulting packet size?

A. 64 bytes
B. 128 bytes
C. 256 bytes
D. 1024 bytes

Answer: B