

100% Money Back
Guarantee

Vendor: IBM

Exam Code: C2150-400

Exam Name: IBM Security Qradar SIEM Implementation
v 7.2.1

Version: 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

Correct 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

Correct Answer: A

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

Correct Answer: C

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

Correct Answer: B

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.

Correct Answer: C

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

Correct Answer: AC

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

Correct Answer: D

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

Correct Answer: BE

QUESTION 9

What is a valid QVM scan status?

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

Correct Answer: A

QUESTION 10

Which NetFlow versions does QRadar SIEM 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

Correct Answer: D

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

Correct Answer: C

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

Correct Answer: B

QUESTION 13

What is the result when adding host definition building blocks to QRadar?

- A. Creates Offenses
- B. Reduces false positives
- C. Makes searches run faster
- D. Authorizes QRadar Services

Correct Answer: B

QUESTION 14

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

- A. QRadar 3124 Console
- B. QRadar 1624 Processor
- C. QRadar 1724 Processor
- D. QRadar 700 Risk Manager

Correct Answer: A

QUESTION 15

What will be restored when restoring event data or flow data for a particular period to a MH?

- A. Only data sent to the console for that time period is restored to the MH.
- B. Only event data or flow data for the MH being restored will be restored to that MH.
- C. Only data that was accumulated for reports and searches will be restored to the MH.
- D. All data for all MHs for a specific time period is restored to its respective hosts in the deployment.

Correct Answer: B

QUESTION 16

Where do you save the "Login Message File" on the system when setting up a banner message for the authentication page?

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

[Guarantee & Policy](#) | [Privacy & Policy](#) | [Terms & Conditions](#)

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2015, All Rights Reserved.