**Vendor:** IBM

**Exam Code:** C1000-026

**Exam Name:** IBM Security QRadar SIEM V7.3.2
Fundamental Administration

**Version:** DEMO

**QUESTION 1**
An administrator logs in to the Offenses tab and finds a large number of new Offenses that need action.

What column in the list of Offenses should the administrator use to prioritize them?

A. Magnitude
B. Offense Type
C. Source IPs
D. Last Event/Flow

**Answer:** A

**QUESTION 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 3**
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

**Answer:** A

**QUESTION 4**
What happens if QRadar receives events at a higher rate than the license allows?

A. The events will be put into queues
B. The source system will be asked to resend the events later
C. The events will not be parsed
D. The events will be dropped immediately

**Answer:** A

**QUESTION 5**
An administrator would like to add a new managed host which uses an existing Network Address Translation (NAT).

Which parameters have to be provided if "Host is NATed" is chosen while adding a managed host?

A. Select Network Attached Telemetric, Enter MAC address of the server or appliance to add
B. Select NATed network, Enter public IP of the server or appliance to add
C. Select NATed network, Enter MAC address of the server or appliance to add
D. Select Network Attached Telemetric, Enter public IP of the server or appliance to add

**Answer:** B

**QUESTION 6**
An administrator is tasked to reduce data volumes in the asset database and reduce stale data contributing to asset growth deviation.

How can the administrator tune the configuration of the Asset Profiler?

A. In the System Configuration section of the Admin, access the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save.
Next, deploy the changes into the environment for the updates to take effect.
B. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save.
Next, deploy the changes into the environment for the updates to take effect.
C. On the navigation menu, click Admin, click the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save.
On the navigation menu, click Admin and from the Advanced menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.
D. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save.
On the navigation menu, click Admin and from the Advanced menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.

**Answer:** B

**QUESTION 7**
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

**Answer:** A