# IBM

## C1000-055 Exam

**IBM QRadar SIEM V7.3.2 Deployment**

# Questions & Answers

(Demo Version - Limited Content)

Thank you for Downloading C1000-055 exam PDF Demo

Get Full File:

https://www.dumpshouse.com/c1000-055-dumps/

## Question: 1

What is anomaly detection rules used for?

A. Detecting volume changes that occur in regular patterns.
B. Detecting event traffic.
C. Detecting an activity that is greater or less than a specified range.
D. Detecting when unusual traffic patterns occur in the network.

**Answer: A**

## Question: 2

A deployment professional has been asked to ensure the system can be integrated with another system which contains lists of IP addresses and CIDR ranges in an automated manner, to allow rules to target specific communication endpoints.
Which part of QRadar is designed to hold and manage this data?

A. Domain Definition
B. Network Hierarchy
C. Asset Profiles
D. Building Blocks

**Answer: D**

## Question: 3

During an initial deployment, three retention buckets (longret, midret. testret) were configured withthe following characteristics, being (X) the number of the bucket:
longret (1): keep data in this bucket for 2 years. Delete when storage is needed.
midret (2): keep data in this bucket for 6 months. Delete when storage is needed.
testret (3): keep data in this bucket for 3 days. Delete immediately after expiration.
Default (0) retention bucket has a 3 months / delete immediately policy.
During testing last week, a significant amount of test data has been mistakenly categorized as 'longret'. This bucket does not contain any other important information. Everything else, including some important data, has been saved into the default bucket.
How can the deployment professional remove all data stored in the 'longret' bucket?

A. Manually delete old data from last week by issuing a rm * on /store/ariel/events/payloads/ and /store/ariel/events/records/ and select the directories containing events from the last week
B. Change the longret bucket period to 10 days and deploy the changes.
C. Change the system's time to 2 years in the future and wait until deletion has been made and thengo back to the real system's time.
D. Manually delete the files ending by -1 from /store/ariel/events/payloads/ and /store/ariel/events/records/

**Answer: B**

## Question: 4

A deployment professional is redesigning the existing deployment to add a event processor due to an increased event rate. The deployment professional observes the events per second (EPS) to be a collective 30,000 EPS from two event collectors (EC1 and EC2) and sometimes exceeds the EPS capacity. EC1 and EC2 are in same network segment.
Considering there are more licenses available than needed in the license pool, which processor should the deployment professional replace the event collector(s) with?

A. Replace EC1 with one QRadar Event Processor 1648
B. Replace EC1 and EC2 with one QRadar Event Processor 1605
C. Replace EC1 and EC2 with one QRadar Event Processor 1629
D. Replace EC1 with one QRadar Event Processor 1605

**Answer: C**

## Question: 5

IBM Security QRadar initiates a sequence of events when a primary high-availability (HA) host fails. During failover, the secondary HA host assumes the responsibilities of the primary HA host. The following actions are completed.
1.1. If configured, external shared storage devices are detected and the file systems are mounted.
2. 2. The secondary HA host connects to the console and downloads configuration files.
3. 3. A management interface network alias is created, for example, the network alias for ethO is ethO:0.
4. 4. The cluster virtual IP address is assigned to the network alias.
5. 5. All QRadar services are started.What is the order of the sequence?

A. 1,4,3,2,5
B. 1,3,4,5.2
C. 1.2,3,4,5
D. 1,4,5,3,2
A.

**Answer: C**

**Thank You for trying C1000-055 PDF Demo**

https://www.dumpshouse.com/c1000-055-dumps/

# Start Your C1000-055 Preparation

*[Limited Time Offer]* Use Coupon "SAVE20" for extra 20% discount on the purchase of PDF file. Test your C1000-055 preparation with actual exam questions