DUMPSBOSS.

IBM Security QRadar SIEM V7.4.3 Deployment

IBM C1000-140

Version Demo

Total Demo Questions: 8

Total Premium Questions: 62

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A QRadar deployment professional was asked to plan a system migration from an on-premises, appliance-based environment to an AWS environment. As part of this transition, the Ariel data must be moved to the new logical appliances and must be searchable by using the existing mechanisms (for example, to filter by log source).

Which approach can the deployment professional use to migrate the configuration after the VM is built (and before the Ariel data is restored)?

A. Use the Content Management Tool (CMT) to transfer the security configuration

B. Use the QRadar configuration backup and restore process to transfer all configurations

C. Export the security content with CMT and import using the REST-API

D. Use rsync to transfer the contents of the /store partition to the new system

ANSWER: C

QUESTION NO: 2

Which two statements are prerequisites for an to upgrade of QRadar? (Choose two.)

A. Verify that scan runs and reports are complete.

B. Verify that all changes are deployed on the appliances.

C. Ensure an admin account is logged on the UI.

D. Clean up all the Offenses before any version upgrade.

E. Ensure that the ISO file is copied to all the appliances.

ANSWER: A C

QUESTION NO: 3

While a search runs on the Network Activity tab, the direction of a set of flows is seen as R2R. The source IP of this set of flows is an internal email server.

What does this situation suggest about the QRadar configuration?

A. QRadar might be having performance issues.

B. The email server is offline or down.

C. The email server is not included in the network hierarchy.

D. The flow pipeline is choked because of high incoming flows.

ANSWER: C

QUESTION NO: 4

Which two of these authentication types are valid for RADIUS authentication? (Choose two.)

A. MSCHAP

B. ASCII

C. TCP

D. PAP

E. XML

ANSWER: A D

QUESTION NO: 5

Which two passwords does a deployment professional configure when installing QRadar? (Choose two.)

A. admin

B. sudo

C. root

D. qruser

E. analyst

ANSWER: B C

QUESTION NO: 6

What approach does QRadar take when it imposes EPS license (not hardware) limits on events that temporarily spike above that limit?

A. Excessive events in a spike cause a System Notification that advises the customer to increase their EPS license allocation.

B. QRadar EPS license allocation is implemented with a hard cutoff to ensure resources are not saturated.

C. During the spike, excess events are written to a queue, and they are processed after the EPS rate drops.

D. QRadar EPS licensing is measured as an average over a 24-hour period, which allows spikes to be handled gracefully.

ANSWER: D

QUESTION NO: 7

Consider this scenario and instruction.

Vulnerability assessment products launch attacks that can result in offense creation. To avoid this behavior and define vulnerability assessment products or any server that you want to ignore as a source, edit the “and when the source IP is one of the following” test to include the IP addresses of the following scanners.

VA Scanners

Authorized Scanners

What type of editable building block is described?

A. BB:HostDefinition: Authorized ScannersSource IP

B. BB:HostDefinition: VA Scanner Source IP

C. BB:NetworkDefinition: Server Networks

D. BB:HostDefinition: Proxy Servers

ANSWER: C

QUESTION NO: 8

On an App Host, to reload an SSL certificate, which service needs to be restarted?

A. tomcat

B. docker

C. httpd

D. ecs-ec-ingress

ANSWER: C