C2150-624 $^{Q\&As}$

IBM Security QRadar Risk Manager V7.2.6 Administration

Pass IBM C2150-624 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official
Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

What is the procedure to upgrade an IBM Security QRadar SIEM V7.2.8 Distributed Deployment?

A. First the Console needs to be upgraded and then the rest of the managed hosts.

B. All systems in the environment need to be shutdown before all systems can be upgraded.

C. First the Collectors need to be upgraded before the rest of the environment can be upgraded.

D. Download the update to the QRadar update server which will automatically install the update to all hosts in the Distributed Deployment.

Correct Answer: A

QUESTION 2

An Administrators will add a secondary host to an IBM Security QRadar SIEM V7.2.8 Console in a High

Availability (HA) deployment scenario.

After checking the compatibility between primary and secondary HA pairs, what other prerequisite should

the Administrator check within Managed Interfaces?

A. The shared external storage.

B. The server certificate that is issued by the local CA.

C. The existence of an additional distributed file system.

D. The communication for Distributed Replicated Block Device.

Correct Answer: D

CP port 7789 must be open and allow communication between the primary and secondary for Distributed

Replicated Block Device (DRBD) traffic.

DRBD traffic is responsible for disk replication and is bidirectional between the primary and secondary

host.

QUESTION 3

What key point should be understood about how flow information in IBM Security QRadar SIEM V7.2.8 is used?

A. Flow information generates the response that is configured in the custom rule.

B. Flow information is sent to QRadarQFlow Collector which normalizes raw log source events.

C. Flow information is actively gathered from the QRadar Event Collector and provides views, reports and alerts to the administrator.

D. Flow information is used to detect threats and other suspicious activity that might be missed if only event information were tracked.

Correct Answer: D

QUESTION 4

When an IBM Security QRadar SIEM V7.2.8 distributed deployment requires scaling horizontally to achieve Event per Second (EPS) requirements, what QRadar Component needs to be added to meet the EPS demands?

A. Event Manager

B. Event Indexing

C. Event Collector

D. Event Processor

Correct Answer: D

QUESTION 5

Which appliance can run IBM Security QRadar SIEM V7.2.8 and includes a single QFlow Collector component?

A. QRadar 2100

B. QRadar 3105

C. QRadar 3124

D. QRadar 3128

Correct Answer: D