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.geekcert.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

Where are the logs for QFlow stored on IBM Security QRadar SIEM V7.2.8?

A. /var/log/qflow.debug

B. /opt/var/log/qflow.debug

C. /opt/log/qradar/qflow.debug

D. /opt/qradar/log/qflow.debug

Correct Answer: A

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

To help you troubleshoot errors or exceptions, review the following log files.

/var/log/qradar.log

/var/log/qradar.error

If you require more information, review the following log files:

/var/log/qradar-sql.log

/opt/tomcat6/logs/catalina.out

/var/log/qflow.debug

Review all logs by selecting Admin > System and License Mgmt> Actions > Collect Log Files.

QUESTION 2

An Administrator needs to create a new user role in the IBM Security QRadar SIEM V7.2.8 system. What steps need to be followed?

A. System Configuration tab -> Users and Roles -> Add New Role -> Add

B. Admin tab -> System Configuration -> User Management -> User Roles -> New

C. Admin tab -> System and Settings -> Users and Roles -> Role Management -> New

D. System Management tab -> System Configuration -> User Management -> User Roles -> New

Correct Answer: B

By default, your system provides a default administrative user role, which provides access to all areas of

QRadar SIEM. Users who are assigned an administrative user role cannot edit their own account.

This restriction applies to the default Admin user role. Another administrative user must make any account changes.

QUESTION 3

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to limit the networking team to see just the Network Flow functions.

What should the Administrator do?

A. Create a user with access to the Log Activity tab.

B. Create a user role with Network Activity -> View Flow Content.

C. Create a user role with Network Activity -> View Reference: Data.

D. Create a user role which grants access to all the functions in the Network Activity tab.

Correct Answer: B

QUESTION 4

What are three protocols that collect flow data from network devices, such as routers, and send this data to IBM Security QRadar SIEM V7.2.8?

A. NetFlow, J-Flow and sFlow

B. NetFlow, IPFIX and syslog

C. NetFlow, rsyslog and sFlow

D. NetFlow, Packeteer and syslog

Correct Answer: A

NetFlow, J-Flow, and sFlow are protocols that collect flow data from network devices, such as routers, and send this data to QRadar.

QUESTION 5

An Administrator has configured a customized log source extension to provide asset updates to IBM Security QRadar SIEM V7.2.8. Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name. In this situation what will QRadar report?

A. This will cause stale asset data.

B. This will cause asset growth deviations.

C. This will cause excessive authentication failure events.

D. This will cause excessive flow data to be processed by the Magistrate.

Correct Answer: B

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses and user names.