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.pass4itsure.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A retention policy allows an IBM Security QRadar SIEM V7.2.8 Administrator to define how long the system is required to keep certain types of data and what to do when data reaches a certain age. If a 3month retention policy is defined for all events, then the system will not delete event data until it\\'s on disk timestamp is 3 months in the past. Which two choices are available in the `delete data in this bucket\\'? (Choose two.)

A. When the index is full

B. Upon reboot of the system

C. When storage space is required

D. When performance is heavily affected

E. Immediately after retention period has expired

Correct Answer: CE

From the list box, select a deletion policy. Options include: ?When storage space is required - Select this option if you want events or flows that match the Keep data placed in this bucket for parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads. When storage is required, only events or flows that match the Keep data placed in this bucket for parameter are deleted. Immediately after the retention period has expired ?Select this option if you want events to be deleted immediately on matching the Keep data placed in this bucket for parameter. The events or flows are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.

QUESTION 2

What are the four categories of notifications found in IBM Security QRadar SIEM V7.2.8 system notifications?

A. Errors, Critical, Minor and Information

B. Errors, Warning, Information, and Health

C. Warning, Information, System and Critical

D. Errors, Warning, Information, and Performance

Correct Answer: B

QUESTION 3

Which permission can be assigned to a user from User Roles in the IBM Security QRadar SIEM V7.2.8 Console?

A. Admin

B. DSM Updates

C. Flow Activity

D. Configuration Management

Correct Answer: A

Grants administrative access to the user interface. You can grant specific Admin permissions. Users with System Administrator permission can access all areas of the user interface. Users who have this access cannot edit other administrator accounts.

QUESTION 4

A backup failure occurs on an IBM Security QRadar SIEM V7.2.8 Console or on an Event Processor. Which system notification message can an Administrator configure for an email notification?

A. Backup: requires more disk space

B. Backup: unable to process backup request

C. Backup: last Backup exceeded space threshold

D. Backup: last Backup reached execution threshold

Correct Answer: A

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21691524

QUESTION 5

When it comes to licensing, what is the difference between Events and Flows and how they are licensed?

A. Flows are licensed based on overall count over a minute, where Events are licensed based on overall count per second.

B. Flows are licensed based on overall count per second, where Events are licensed based on overall count over a minute.

C. Flows and Events are both licensed by overall count per minute under an Upgraded License and per second on a Basic License.

D. Flows and Events are both licensed by overall count per second under an Upgraded License and per second on a Basic License.

Correct Answer: A

A significant difference between event and flow data is that an event, which typically is a log of a specific action such as a user login, or a VPN connection, occurs at a specific time and the event is logged at that time. A flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within the session. For example, a web request might download multiple files such as images, ads, video, and last for 5 to 10 seconds, or a user who watches a Netflix movie might be in a network session that lasts up to a few hours. The flow is a record of network activity between two hosts.

Latest C2150-624 Dumps C2150-624 Study Guide C2150-624 Braindumps