

C2150-606^{Q&As}

IBM Security Guardium V10.0 Administration

Pass IBM C2150-606 Exam with 100% Guarantee

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

<https://www.leads4pass.com/c2150-606.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

A Guardium administrator must configure real time policy alerts to be sent to a remote SIEM for every SQL statement run on a sensitive object. There is no requirement for the data to be viewed or reported on in the Guardium appliance.

Which policy action would achieve that task and store the least amount of data in the Guardium internal database?

- A. Log Only
- B. Alert Only
- C. Alert Daily
- D. Alert Per Match

Correct Answer: C

QUESTION 2

A company wants to deploy S-TAPs for 2 groups of database servers located in 2 different data centers. The current set of Collectors are fully utilized. The Aggregators and Central Manager can handle more load.

What should a Guardium administrator recommend?

- A. Deploy 2 new Collectors, 1 in each data center.
- B. Connect S-TAPs directly to Aggregators to avoid network latency.
- C. Connect S-TAPs directly to the Central Manager to avoid network latency.
- D. Deploy 2 new Collectors in the third data center located in between the 2 data centers.

Correct Answer: A

QUESTION 3

A Guardium administrator handles a large environment and has been asked to restore old data for auditors to review. This old data needs to be restored so that it does not impact the current data being collected or any merge settings. In order to keep the reports separate (old data vs current data), the administrator sets up an Investigation Center.

Which is a key requirement for users of the Investigation Center?

- A. The user must be in one of the groups INV_1, INV_2, or INV_3 (case-sensitive).
- B. The users must login as one of the predefined user accounts INV_1, INV_2, or INV_3 (case-sensitive).
- C. A separate user must be used with a role of either INV_1, INV_2, or INV_3 (case-sensitive).
- D. To correctly configure an investigation user, the user's Last Name must be set to the name of one of the three investigation databases, INV_1, INV_2, or INV_3 (case-sensitive).

Correct Answer: D

QUESTION 4

An administrator manages a Guardium environment including 4 Collectors exporting data to an Aggregator. The Collectors export their data daily at 2, 3, 4 and 5 am Eastern Standard Time (EST) respectively. The Collectors receive traffic every day. The logs on all the Collectors confirm data is exported daily without errors, and all the exported files always have data. A Session report is run on the Aggregator at noon EST for data from the last day.

Which of the following will ensure there is data in the report?

- A. Schedule Data Purge on the Aggregator to run every day after 5 am EST.
- B. Schedule Data Import on the Aggregator to run at any time of the day.
- C. Schedule Data Import in the Aggregator to run every day before 2 am EST.
- D. Schedule Data Import on the Aggregator to run every day at 6 am EST or later.

Correct Answer: C

QUESTION 5

A Guardium administrator has rebuilt an appliance, and wants now to restore a backup image of the entire database, audit data, and all definitions from Data backup. Which CLI command should the administrator use to accomplish this?

- A. restore config
- B. restore system
- C. restore pre-patch-backup
- D. restore certificate sniffer backup

Correct Answer: B

[Latest C2150-606 Dumps](#)

[C2150-606 Study Guide](#)

[C2150-606 Exam Questions](#)