

IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

Exam: **000-M75**

Title : IBM InfoSphere Guardium
Technical Mastery Test

Version : DEMO

1. Which of the following components collects and parses the live database traffic used to trigger a real-time alert when a security policy rule is broken?

- A. The Real Time Communications Framework
- B. The Change Audit System
- C. The Policy Engine
- D. The Live Report Builder

Answer: C

2. What is Guardium's primary storage mechanism for logs and audit information?

- A. Data can only be stored in flat files on the collector (one file per S-TAP).
- B. Data storage can only be managed individually by each S-TAP, with audit data stored locally on the data server in flat files.
- C. Data is stored on the collector in a normalized relational database.
- D. Data is stored locally on each server with an S-TAP but is managed centrally through the collector.

Answer: C

3. In a Guardium environment where data servers can talk to the collector, what is the relationship between the S-TAP and the collector appliance?

- A. There exists no relationship since the S-TAP and the collector are incompatible Guardium entities.
- B. The S-TAP reports database activity to the collector for policy management and auditing.
- C. A collector can only interact with one S-TAP for policy management and auditing.
- D. The collector sends the S-TAP information about its policies so it knows what traffic to intercept.

Answer: B

4. Which of the following best describes the role of the aggregator in a Guardium environment?

- A. The aggregator is a Guardium appliance that collects and consolidates information from multiple collectors to a single Aggregation Server, allowing for reporting across the enterprise.
- B. The aggregator is the Guardium appliance that communicates with mainframes.
- C. The aggregator is a Guardium appliance that allows a collector and a Central Policy Manager to communicate and is required in multi-collector environments.

D. The aggregator is another name for the Central Policy Manager.

Answer: A

5. How is authentication and encryption implemented between collectors, aggregators and the Central Policy Manager in a multi-tier Guardium environment?

A. Using an encrypted file containing the system password that must be copied to the Central Policy Manager and collectors.

B. A System Shared Secret is specified through the GUI for each collector and the Central Policy Manager.

C. The Central Policy Manager scans the network for Guardium collectors and performs a security handshake with each appliance.

D. The communication between collectors and the Central Policy Manager is based on unsecured network packets.

Answer: B