IBM 000-M75

IBM InfoSphere Guardium Technical Mastery Test v1
Version: 4.0

QUESTION NO: 1

Which of the following logging actions will not log the full SQL and parameter values?

A. Log Full Details.
B. Log Full Details with Values.
C. Audit Only.
D. Log Full Details per Session.

Answer: C
Explanation:

QUESTION NO: 2

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
Explanation:

QUESTION NO: 3

When the S-TAP is in open mode, what would you need to configure to enforce a termination without any data leaking?

A. Using a rule with an S-GATE Attach action to terminate the activity.
B. Using a rule with an S-GATE Terminate action to terminate the activity.
C. Using an S-GATE Attach action to put the session in closed mode when the session is initiated, and using a rule with an S-GATE Terminate action to terminate the activity.
D. Using an S-GATE Terminate action to put the session in closed mode when the session is initiated, and using a rule with an S-TAP Terminate action to terminate the activity.

Answer: C

Explanation:

QUESTION NO: 4

How would a DBA or developer notify Guardium using the Application User API that an application user has taken or given up control of a data server connection?

A. By importing the GuardUtils library and issuing calls through it from the application.
B. By creating a wrapper solution that sends HTTP requests to Guardium's service- oriented API whenever an event like this happens.
C. By registering the application's connection pool with Guardium.
D. By using the GuardAppUser call in the form of a SQL SELECT statement to indicate that a new application user has taken control of the connection.

Answer: D

Explanation:

QUESTION NO: 5

An audit administrator wants to track database changes performed by database administrators and reconcile these changes with an existing change tracking database. Which Guardium features can be used to implement this scenario?

A. External Data Connector and Entitlement Reports.
B. Application Events API and External Data Correlation.
C. Application Events API and Entitlement Reports.
D. Sensitive Object Discovery and User Application Translation.

Answer: B

Explanation:

QUESTION NO: 6

What are the different types of rules available to be used with Guardium policies?

A. Access, Data Throughput and Privileged Transactions.
B. Extrusion, Exception and Analysis.