IBM

P2150-739

IBM InfoSphere Guardium Technical Mastery Test v2

QUESTION: 36
What is the effect of enabling the Log Policy Violation option when creating a new correlation alert?

A. The Guardium administrator is automatically notified whenever this alerts occurs.
B. A policy violation is logged when this alert is triggered, so it may be viewed alongside real-time alerts in the Policy Violations domain.
C. This is not an option available in the alert definition tab of the user interface.
D. All following occurrences of this specific alert are ignored.

Answer: B

QUESTION: 37
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

QUESTION: 38
What is a Guardium vulnerability assessment (VA)?

A. A test that employs state-of-the-art algorithms to determine the potential risks of your network.
B. A series of predefined and custom tests that allow customers to automatically identify and address database vulnerabilities.
C. An optional service from Guardium where a security specialist visits a customer's site before a proof-of-concept engagement to determine the customer's specific requirements.
D. A piece of software distributed as a multi-platform plug-in that allows a supported database management system to constantly monitor potential threats and report on these periodically.

Answer: B

QUESTION: 39
Which of the following problems is the Application User Translation feature designed to help with?

A. The use of non-English parameter values in SQL statements issued by some applications.
B. The fact that there is no easy way for the application server to communicate with both Guardium and the data server concurrently.
C. The inability to relate a database action to a specific application user when a pool of database connections is used by an application.
D. Translating an application's requests made to a data server so these are compatible with all the database management systems that Guardium supports.

Answer: C

QUESTION: 40
Which of the following statements is true about queries and reports in Guardium?

A. A query can only be used to create one report.
B. A query can be used to create many reports.
C. A report can be based on the combination of multiple queries.
D. A query can only be used to create either a tabular or a chart style report, but not both.

Answer: B

QUESTION: 41
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

QUESTION: 42
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

QUESTION: 43
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.
C. Data Morphing, SOX-compliant, Extrusion and Data Throughput.
D. Access, Extrusion and Exception.

Answer: D