Vendor: IBM

Exam Code: P2090-075

Exam Name: IBM InfoSphere Guardium Technical Mastery Test v1

Version: Demo

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

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

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

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

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

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

Answer: D

Question No : 7

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 No : 8

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 No : 9

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 No : 10

Which of the following is TRUE about Guardium's entitlement reports?

A. Guardium includes a set of built-in entitlement report definitions for all supported databases.
B. Guardium does not offer standard built-in entitlement reports and the user must create these reports based on their database specifications.
C. Guardium includes Oracle entitlement reports as a standard feature, however reports for all other database engines (ie. IBM DB2) must be manually created.
D. Guardium's entitlement reporting requires a monthly subscription service.

Answer: A

Question No : 11

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 Inspection Engine
D. The Live Report Builder

Answer: C

Question No : 12

Which of the following items cannot be identified using database auto-discovery?

A. IP address of servers with a database instance.
B. Port(s) on which a database is communicating on each server.
C. List of databases for each database instance.
D. Type of database running on each server.

Answer: C

Question No : 13

Which of the following actions is NOT a known benefit of using correlation alerts?

A. Monitoring database usage and pinpointing suspicious activity.
B. Real time database traffic analysis and security policy inspection.
C. Automatically alerting users when established behavioral baselines are exceeded.
D. Saving time in alerting and analyzing versus manually doing so.

Answer: B