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.geekcert.com/c2150-606.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

During the initial phase of the Guardium deployment, the Guardium administrator wants to figure out an ideal time period to purge data from the appliance based on the data load.

Which predefined Guardium report(s) allows the administrator to determine the current database disk usage of the Guardium Appliance?

A. Disk Util report

B. Aggregation/Archive log

C. DB Server throughput report

D. Buff Usage Monitor and System Monitor reports

Correct Answer: D

QUESTION 2

In a centrally managed environment, while executing the report \\'Enterprise Buffer Usage Monitor\\', a Guardium administrator gets an empty report. Why is the report empty?

A. Sniffers are not running on the Collectors.

B. The report is not executed with a remote source on the Collector.

C. The report is not executed with a remote source on the Aggregator.

D. Correct custom table upload is not scheduled on the Central Manager.

Correct Answer: C

QUESTION 3

The Quick Search window does not show up on the GUI of a standalone Collector What technical feature should the Guardium administrator check first?

A. That the Collector has at least 24 GB.

B. That the Collector has at least 32 GB.

C. That the Collector has at least 64 GB.

D. Check the contract and verify whether that feature was purchased.

Correct Answer: A

QUESTION 4

A Guardium administrator installed an S-TAP but is not seeing any data in reports on the collector. The administrator discovered that an Inspection Engine is not configured for that S-TAP.

What is an Inspection Engine?

A. A piece of software residing on the Collectors.

B. Another software to be installed on the Database server.

C. The same thing as the policy and it runs on the S-TAP to inspect the traffic in real-time.

D. A set of parameters needed for the S-TAP to define how to monitor traffic for a particular database instance on a server.

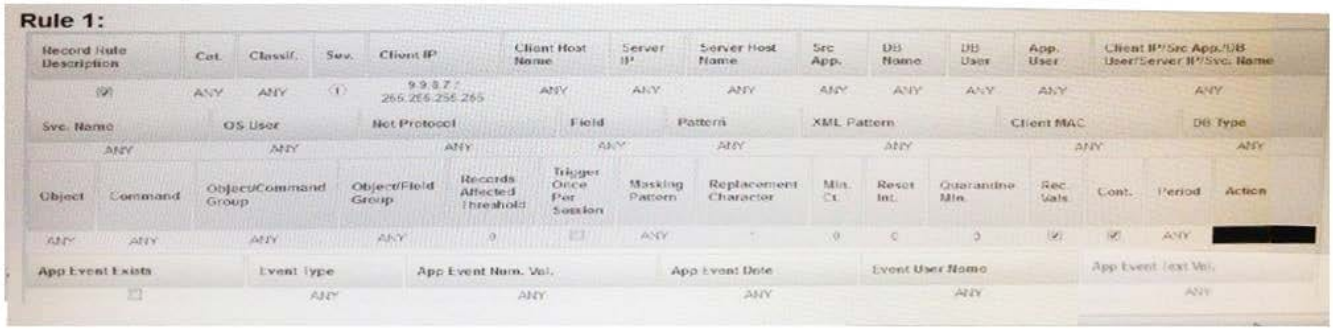
Correct Answer: C

QUESTION 5

The guard_tap.ini of a UNIX S-TAP is configured with the following parameters:

```
firewall_installed=1
firewall_fail_close=0
firewall_default_state=0
firewall_timeout=10
```

A Guardium administrator applies a policy to the Collector with two rules as below. The actions of the rules have been hidden.



The administrator must create a policy that will terminate the session on the delete statement in the below scenario:

A session is started to the monitored database from client IP 9.9.8.7. In the session the user plans to perform a select statement and then a delete statement.

What actions should the administrator configure?

A. Rule 1 - S-GATE Attach Rule2 - S-GATE Detach

B. Rule 1 - S-GATE Detach Rule 2 - S-GATE Terminate

C. Rule 1 - S-GATE Attach Rule 2 - S-GATE Terminate

D. Rule1 - S-TAP Terminate Rule 2 - S-GATE Terminate

Correct Answer: A