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

While looking at the S-TAP Status report on a Collector, a Guardium administrator notices that the status of the S-TAPs is changing every few minutes. The administrator suspects that the sniffer is restarting every few minutes and that is why the status change is happening.

How can the Guardium administrator confirm if the sniffer is restarting every few minutes?

A. Review the Audit Process Log for \\'Sniffer stopped\\' message.

B. Review the Aggregation/Archive Log for \\'Sniffer is restarting message.

C. Review the Scheduled Jobs Exceptions for \\'Sniffer process failed\\' message.

D. Review the Buff Usage Monitor for the column TID to see if it changed every few minutes.

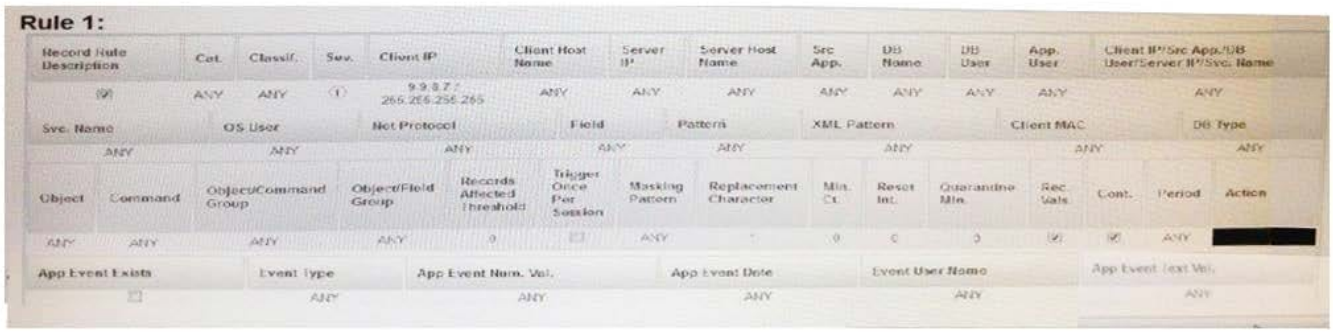
Correct Answer: D

QUESTION 2

The quard_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

QUESTION 3

A company is installing S-TAPS on new Database Clusters. The Guardium administrator was provided with the PVU load of each node. The clusters are in active/passive mode. The administrator is associating S-TAPs to Collectors using the PVU count.

How should the administrator treat the PVUs of passive nodes?

A. include the PVU load of passive nodes.

B. include half of the passive nodes PVU load.

C. include a third of the passive nodes PVU load.

D. Not include the PVU load of passive nodes.

Correct Answer: D

QUESTION 4

A Guardium policy has been configured with the following two rules:

AGuardium administrator is required to check for SQL statements from client IP 9.4.5.6 executed on object "TABLET. What domain(s) can the administrator create a report in to see the SQL?

A. Access

B. Policy Violations

C. Access and Access Policy

D. Access and Policy Violations

Correct Answer: A

QUESTION 5

A Guardium administrator needs to build new appliances with the latest version of Guardium. How should the administrator obtain the ISO image?

A. Contact IBM Support.

B. Download fromibm.com

C. Download from IBM Fix Central.

D. Download from IBM Passport Advantage.

Correct Answer: D