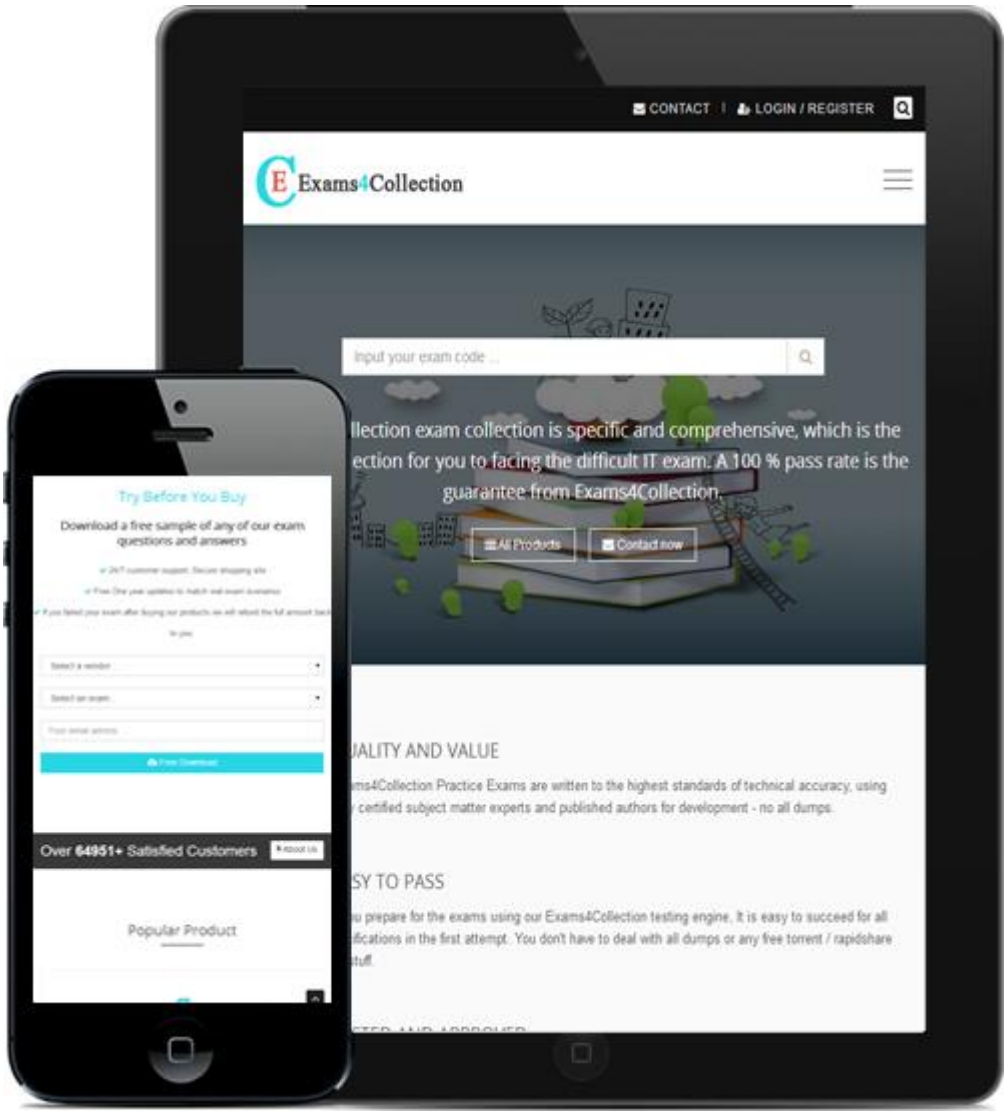
Exams4Collection



http://www.exams4collection.com

Exams4Collection exam dumps & Exams4Collection exam study material

Exam : **C2150-606**

Title : IBM Security Guardium V10.0 Administration

Vendor : IBM

Version : DEMO

NO.1 AGuardium administrator must configure a policy to ignore all traffic from an application with a known client IP. Due to the high amount of traffic from this application, performance of the S-TAP and sniffer is a concern.
What action should the administrator use in the rule?
A. Ignore Session
B. ignore S-TAP Session
C. ignore SQL per Session
D. ignore Responses per Session
Answer: B

NO.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.
Answer: C

NO.3 During a Guardium deployment planning meeting, a database administrator indicated that the mission critical databases were clustered. How should the Guardium administrator handle S-TAP installation and configuration with respect to clustered databases?
A. Install S-TAP agents on all active nodes. Set ALL_CAN_CONTROL=1 to failover the STAP process to the passive nodes when a database failover occurs.
B. install S-TAP agents on all active nodes Set WAIT_FOR_DB_EXEC=-1 to set the agent process to failover to the passive node when a database failover occurs.
C. Install S-TAP agents on all active and passive nodes. Set ALL_CAN_CONTROL=0 to disable all passive nodes until a database failover occurs.
D. Install S-TAP agents on all active and passive nodes: Set WAIT_FOR_DB_EXEC>0 on all nodes to start S-TAP processes without waiting for a correct DB home.
Answer: A

NO.4 An administrator manages a Guardium environment including 4 Collectors exporting data to an Aggregator. The Collectors export their data daily at 2, 3, 4 and 5 am Eastern Standard Time (EST) respectively. The Collectors receive traffic every day. The logs on all the Collectors confirm data is exported daily without errors, and all the exported files always have data. A Session report is run on the Aggregator at noon EST for data from the last day.
Which of the following will ensure there is data in the report?
A. Schedule Data Purge on the Aggregator to run every day after 5 am EST.
B. Schedule Data Import on the Aggregator to run at any time of the day.
C. Schedule Data Import in the Aggregator to run every day before 2 am EST.
D. Schedule Data Import on the Aggregator to run every day at 6 am EST or later.
Answer: C

NO.5 AGuardium administrator is registering a new Collector to a Central Manager (CM). The registration failed. As part of the investigation, the administrator wants to identify if the firewall ports are open-How can the administrator do this?
A. Ask the company's network administrators.
B. Ask IBM technical support to login as root and verify.
C. Login as CLI and execute telnet <ip address> <port number>
D. Login as CLI and execute support show port open <ip address> <port number>
Answer: D

NO.6 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
Answer: A