IBM

Exam C2150-606

IBM Security Guardium V10.0 Administration

Verson: Demo

[Total Questions: 10]

Question No : 1

A Guardium administrator observes certain changes to the configuration and policies. How would the administrator identify the changes that were made and who made them?

A. Review the Audit Process Log report.
B. Review the sniffer buffer usage report.
C. Review the /var/log/messages log file.
D. Review the results of 'Detailed Guardium User Activity' report.

Answer: D

Question No : 2

A company wants to deploy S-TAPs for 2 groups of database servers located in 2 different data centers. The current set of Collectors are fully utilized. The Aggregators and Central Manager can handle more load.

What should a Guardium administrator recommend?

A. Deploy 2 new Collectors, 1 in each data center.
B. Connect S-TAPs directly to Aggregators to avoid network latency.
C. Connect S-TAPs directly to the Central Manager to avoid network latency.
D. Deploy 2 new Collectors in the third data center located in between the 2 data centers.

Answer: A

Question No : 3

A Guardium administrator noticed that while the data activity monitoring is working fine, the Guardium appliance is slower than usual. The administrator wants to check the current CPU load of the Guardium appliance.

Which predefined Guardium report(s) allows the administrator to determine the current system CPU load of the Guardium Appliance?

A. CPU Util report
B. CPU Tracker report
C. Unit summary and CPU Util report
D. Buff Usage Monitor and System monitor report

Answer: D

Question No : 4

A Guardium administrator installed the BUNDLE-STAP module and is monitoring the state of the install. Which state requires a database server reboot to complete the installation process?

A. Ip
B. IP-PR
C. FAILED
D. PENDING-UPDATE

Answer: B

Question No : 5

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.

Answer: D

Question No : 6

AGuardium administrator has rebuilt an appliance, and wants nowto restore a backup image of the entire database, audit data, and all definitions from Data backup.Which CLI command should the administrator use to accomplish this?

A. restore config
B. restore system
C. restore pre-patch-backup
D. restore certificate sniffer backup

Answer: B

Question No : 7

Auditors request a report of all unsuccessful login attempts to a database monitored by Guardium. How should a Guardium administrator create such a report?

A. Add a failed login rule to the policy.
B. Create a failed login query and report using access domain in Guardium.
C. Create a failed login query and report using exceptions domain in Guardium.
D. Create a failed login query and report using application data domain in Guardium.

Answer: C

Question No : 8

A Guardium administrator needs to configure EMC Centera for Archive and/or Backup.

In addition to the server IP address, what else is required to establish connection with an EMC Centera on the network?

A. ciipID
B. PEA file
C. Shared secret
D. Certificate signed request (CSR)

Answer: B

Question No : 9

A Guardium administrator is planning to build an environment that contains an S-TAP with one primary Collector and one failover Collector. What must the administrator ensure when setting up this environment?

A. Both Collectors are centrally managed.
B. There is network connectivity between the S-TAP and both Collectors.
C. Guardium Installation Manager (GIM) is installed on the Database Server.
D. in the guard_tap.ini file of the S-TAP set participate_in_load_balancing=1

Answer: B

Question No : 10

A Guardium administrator is setting up a Collector schedule to export data to an Aggregator and Archive its data to an Archive storage unit for additional data safety.

Given this scenario, which is true regarding the purge schedule?

A. The Archive and the Export have independent purge schedules but should not be run at the same time.
B. The Guardium unit would run the Export and Archive before any purge, so you would only see the last purge run each day.
C. it would not be possible to configure both on a Collector, the Aggregator should do the archiving and only export from the Collector.
D. Any time that Data Export and Data Archive are both configured, the purge age must be greater than both the ageat which to export and the ageat which to archive.

Answer: D