



Vendor: IBM

Exam Code: 000-463

Exam Name: IBM InfoSphere Guardium Exam

Version: DEMO

QUESTION 1

Which consideration is true for a Vulnerability Assessment (VA) deployment?

- A. Collectors running VA cannot also perform database monitoring.
- B. Each collector can run up to 20 Vulnerability Assessments simultaneously.
- C. S-TAP must be running on the database server before VA is run for a database on that server.
- D. There is a need to create an account with appropriate privileges on the database for VA to work.

Answer: D

QUESTION 2

Which Guardium appliance cannot be managed?

- A. S-TAP
- B. Collector
- C. Aggregator
- D. Central manager

Answer: D

QUESTION 3

When planning the deployment for Data Activity Monitoring (DAM) there is a need to determine the location of the various Guardium solution components (I.e. Agents, appliances). Which statement is correct?

- A. S-TAP agents need to reside in the same data center the aggregators reside in.
- B. Collectors can report to aggregators that are located in data centers other than their own.
- C. Collectors can reside anywhere in the customer network regardless of database server location.
- D. Aggregators need to reside in the same data center the collectors that report to them (Aggregator) reside.

Answer: B

QUESTION 4

When sizing a Vulnerability Assessment solution, what is the recommendation for calculating the number of collectors needed?

- A. One collector for every 30K PVU.
- B. One collector for every data center.
- C. One collector for every 35 database servers.
- D. One collector for every 255 database instances.

Answer: D

QUESTION 5

What are the mechanisms used by UNIX S-TAP to capture database traffic?

- A. K-TAP, A-TAP, and PCAP
- B. K-TAP, LHMON, and PCAP
- C. PCAP, DB2TAP, and K-TAP

- D. A-TAP, Shared Memory Driver, and K-TAP
- E. Company

Answer: A

QUESTION 6

Which parameter should be used to enable K-TAP flex loading through GIM?

- A. KTAP_ENABLED set to "1"
- B. KTAP_LIVE_UPDATE set to "Y"
- C. KTAP_FAST_FILE_VERDICT set to "1"
- D. KTAP_ALLOW_MODULE_COMBOS set to "Y"

Answer: D

QUESTION 7

Before uninstalling A-TAP, which procedure must be done?

- A. K-TAP must be unloaded using guard_ktap_loader.
- B. A-TAP must be deactivated on all database instances.
- C. The Guardium group must be removed from the server.
- D. The sniffer must be stopped on the Guardium appliance.

Answer: B

QUESTION 8

Which guard_tap.ini parameter should be used to set the virtual IP of a Microsoft SQL Server cluster environment?

- A. tap_ip
- B. sqlguard_ip
- C. alternate_ips
- D. connect_to_ip

Answer: C

QUESTION 9

What statement is true regarding policy push down?

- A. Policy push down pushes a classification process into S-TAP for Z on IMS.
- B. Policy push down allows ZSecure to push policies into the Guardium appliance.
- C. Policy push down allows the Guardium appliance to identify sensitive objects inside the DB2 database.
- D. Policy-push-down enables policy push down of collected profiles, collection activation, and collection inactivation from the Guardium appliance.

Answer: D

QUESTION 10

What is the correct way to stop a UNIX S-TAP that was installed with a non-GIM installer?

- A. Use the Stop S-TAP button in the S-TAP Control window.
- B. Find the S-TAP Process ID and terminate with kill -9 command.
- C. Comment the U-TAP section of /etc/inittab, followed by the init q command.
- D. Under the Modules parameter in the Central Manager, set STAP_ENABLED = 0 for the appropriate S-TAP.

Answer: C

QUESTION 11

Which appliance type(s) can serve as a Guardium host for S-TAPs?

- A. A collector only.
- B. Collectors and Aggregators only.
- C. Collectors and standalone Central Managers.
- D. All appliance types can accept S-TAP connections.

Answer: A

QUESTION 12

In the Session level entity, how many UID Chain attribute(s) are there?

- A. 1 - UID Chain
- B. 2 - UID Chain & UID Chain Compressed
- C. 3 - UID Chain, UID Chain Compressed & UID Chain Expanded
- D. 4 - UID Chain, UID Chain Compressed, UID Chain Expanded & UID Chain for z/OS

Answer: B