IBM 000-463

IBM InfoSphere Guardium

Version: 4.0

QUESTION NO: 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
Explanation:

QUESTION NO: 2

Which Guardium appliance cannot be managed?

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

Answer: D
Explanation:

QUESTION NO: 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 then 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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

Answer: A
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 13

What is the main command line utility to control and configure A-TAP on all platforms?

A. guardctl
B. guard-atap-ctl
C. guard-ktap-ctl
D. guard-executor-32

Answer: A
Explanation:

QUESTION NO: 14

What is the documented procedure for handling delayed cluster disk mounting?

A. Manually restart the S-TAP process after mounting the database server directory.
B. Configure the wait_for_db_exec parameter in the guard_tap.ini with an appropriate delay.
C. Ensure that the S-TAP process is started only after the database installation directory is available.
D. There is no special procedure, S-TAP can automatically detect when the database directory becomes available.

Answer: B
Explanation:

QUESTION NO: 15

Which GIM component controls starting and stopping managed agents on UNIX?

A. gim_client.pl
B. guardium_stap
C. guard_supervisor
D. guard_ktap_loader

Answer: C
Explanation:

QUESTION NO: 16

What is the correct way to stop S-TAP that is managed by GIM?

A. Uninstall S-TAP.
B. Use kill -9 on S-TAP process.
C. Comment S-TAP entry in /etc/inittab.
D. Set STAP_ENABLED to "0" in GIM parameters.

Answer: D
Explanation:

QUESTION NO: 17

Where are DB2 z audit rules stored?

A. Collection profiles
B. CICS audit profiles
C. Group audit profiles
D. VSAM audit profiles

Answer: A
Explanation:

QUESTION NO: 18

Which ports are used by UNIX S-TAP?

A. 9500 TCP (unencrypted) and 8075 TCP (encrypted)
B. 16016 TCP (unencrypted) and 16018 TCP (encrypted)
C. 9500 TCP (unencrypted) and 8075 UDP (heartbeat signal)
D. 16016 TCP (unencrypted) and 16018 UDP (hearbeat signal)

Answer: B
Explanation:

QUESTION NO: 19

Which mechanism is used to intercept DB2 and Informix shared memory traffic on all UNIX platforms except Linux?

A. TEE
B. PCAP
C. A-TAP
D. K-TAP

Answer: D
Explanation:

QUESTION NO: 20

What is the purpose of K-TAP flex load in Linux installations?

A. Allows upgrade of the K-TAP module without requiring a reboot of the host operating system.
B. Give the system administrator the ability to stop traffic interception by manually unloading the K-TAP module.
C. Allows installation of K-TAP module with closest match in cases where an exact kernel match is not available.
D. Allows the system administrator to upgrade the K-TAP module directly from GIM interface on Central Manager.

Answer: C
Explanation:

QUESTION NO: 21

Which statement about Configuration Audit System (CAS) is true?

A. It does not support windows platform.
B. It supports running operating system shell scripts.
C. It does not support monitoring of file permissions (rwxrwxrwx).
D. It supports vulnerability assessment tests using observed behavior.

Answer: B
Explanation:

QUESTION NO: 22

What is the primary purpose of Group Builder?

A. To update vulnerability assessment rules.
B. To trigger compliance workflow automation.
C. To adapt to the dynamic needs of the business.
D. To associate policy rules with audit process results.

Answer: C
Explanation:

QUESTION NO: 23

What query change requires the report portlet to be regenerated?

A. Main entity
B. Query fields
C. Runtime parameters
D. Timestamp attributes

Answer: C
Explanation:

QUESTION NO: 24

In a rule definition, what DB User field value would test for a blank database user name in the traffic?

A. %
B. NULL
C. guardium://empty
D. Leaving the field blank

Answer: C
Explanation: