IBM

Exam C2150-463

IBM InfoSphere Guardium

Version: 6.0

[Total Questions: 130]

Question No : 1

When creating a new report there is a need to choose a main entity. There are six levels in the entity hierarchy for the access domain. Which of the following represents the correct hierarchy order (top to bottom)?

A. SQL, Client/Server By Session, Application Event, Command, Object, Field
B. Command, Object, SQL, Field, Client/Server By Session, Application Event
C. Object, Command, SQL, Field, Client/Server By Session, Application Event
D. Client/Server By Session, Application Event, SQL, Command, Object, Field

Answer: D

Question No : 2

Which Guardium Feature can be used to extract Application End User information from a stored procedure call?

A. Tuple Groups
B. Custom ID procedures
C. ABAP Import procedures
D. SIEM Integration with Message Templates

Answer: B

Question No : 3

Which command sets the eth0 network IP address to 192.168.1.54?

A. store network ip 0 192.168.1.54
B. store network resolver 1 192.168.1.54
C. store network interface ip 192.168.1.54
D. store network routes static 192.168.1.54

Answer: C

Question No : 4

What is the default policy of a new appliance?

A. PCI policy
B. SOX Policy
C. allow all policy
D. selective audit policy

Answer: C

Question No : 5

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 No : 6

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

Question No : 7

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

Question No : 8

What is the default time of the command "store uid_chain_polling_interval <N>" where N is time in minutes?

A. 2 minutes
B. 30 minutes
C. 60 minutes
D. 720 minutes

Answer: A

Question No : 9

Which log is the most relevant for data restore troubleshooting on an aggregator?

A. syslog
B. sql_err.log
C. snif_stderr.txt
D. agg_progress.log

Answer: D

Question No : 10

Which guard_tap.ini parameter is configured to set User ID (UID) chain logging?

A. hunt
B. uid_chain

C. hunter_trace
D. Specify "user" in Intercept Types

Answer: C

Question No : 11

When attempting to quarantine a connection, what is needed to create a rule within the security policy?

A. Fill out the DB User and identify the "command" as Quarantine.
B. Fill out the "Quarantine for xx" minutes section of the Admin Quarantine tab.
C. Fill out the "reset Interval" to identify when the Quarantined user will become active.
D. Fill out the "Quarantine for xx" minutes section of the policy and create a rule action of "Quarantine".

Answer: D

Question No : 12

Guardium supports what databases platforms for entitlement reports?

A. DB2
Informix
MS-SQL
MySQL
Netezza
PostgreSQL
B. DB2
Informix
MS-SQL
Oracle
PostgreSQL
Sybase
C. DB2
Informix
MS-SQL
MySQL
Netezza
Oracle

PostgreSQL
Sybase
Teradata
D. Netezza
Oracle
PostgreSQL
Sybase
Teradata

Answer: C

Question No : 13

Which component of the Guardium solution makes a decision to terminate database connection as part of Data access level control / blocking functionality?

A. Functionality within policy running on Guardium collector.
B. Functionality within CAS agent running on the database server.
C. Functionality within S-GATE agent running on database server.
D. Functionality within S-TAP process running on database server.

Answer: A

Question No : 14

A customer is deploying InfoSphere Guardium for Data Activity Monitoring (DAM) & Data Level Access Control (DLAC). They are not sure where to locate their collector appliances with respect to the database server that needs to be monitored & protected. Which response is correct?

A. The collectors can be located anywhere on the network.
B. The collectors should be located in the same data center the database servers they monitor & protect reside.
C. The S-TAP must reside in the same data center the databases servers are at but the collectors can be anywhere.
D. The collectors and aggregators need to reside in the same location regardless of were the database servers reside.

Answer: B

Question No : 15

An audit workflow process may contain any number of audit tasks. Which is NOT a valid audit task?

A. a privacy set
B. a policy process
C. a security assessment
D. a classification process

Answer: B

Question No : 16

Which method stops a non-GIM installed Windows S-TAP?

A. Invoking the "stop winstap" command.
B. Stopping the GUARDIUM_STAP service.
C. Ending Guardium S-TAP process through Task Manager.
D. Removing S-TAP from startup programs and rebooting server.

Answer: B

Question No : 17

Which statement is true in a centrally managed environment?

A. Policies can be created and installed only on Central Manager.
B. Policy should be created and installed on collector.
C. Policy installed on one collector will automatically propagate to other collectors.
D. Policy can be created on Central Manager or managed unit but need to be installed on the relevant collector.

Answer: D

Question No : 18

Quarantine is available for which types of rule(s) in the policy?

A. access rule only
B. access and exception rules
C. access, exception and extrusion rules
D. access, exception, extrusion and ignore rules

Answer: C

Question No : 19

What could cause all the S-TAPs on a particular collector to turn red (in S-TAP Control)?

A. The GUI is down (port 8443 unavailable).
B. The SSH daemon on appliance is down (port 22 unavailable).
C. The GIM server on the appliance is down (port 8081 unavailable).
D. The inspection core was stopped (ports 9500 and 16016 unavailable).

Answer: D

Question No : 20

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 No : 21

What is the difference between real time alerts and correlation alerts?

A. There is no difference, terminology is used interchangeably.

B. Real time alerts are based on policy rules. Correlation alerts are Query based.
C. Real time alerts are driven by anomaly detection. Correlation alerts are policy driven.
D. Real time alerts could only be run on the Managed Units. Correlation alerts can only be run on Central Manager.

Answer: B

Question No : 22

Which report allows you to monitor Guardium user activities?

A. Audit Process Log
B. User Activity Audit Trail
C. Guardium Users Report
D. Default DB Users Enabled

Answer: B

Question No : 23

For an SQL Server 2005 environment using encryption, what can cause DB User and Source Program information to show up blank in the Guardium reports?

A. A-TAP is not installed.
B. The port range specified in the inspection engines is not correct.
C. There is a policy with Ignore S-TAP Session rule blocking the users.
D. The Instance Name parameter in the inspection engines is not correct.

Answer: D

Question No : 24

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.