C2150-606^{Q&As}

IBM Security Guardium V10.0 Administration

Pass IBM C2150-606 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/c2150-606.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A Guardium administrator needs to monitor changes to the Oracle configuration file on a production Oracle database server. Assuming all valid licenses are applied, which Guardium component does the administrator need to install and where?

A. Guardium Installation Manager (GIM) on the Database Server

B. Configuration Auditing System (CAS) on the Database Server.

C. Configuration Auditing System (CAS) on the Guardium Collector.

D. Configuration Auditing System (CAS) on the Database Server and on the Guardium Collector.

Correct Answer: D

QUESTION 2

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.

Correct Answer: D

QUESTION 3

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.

Rule 1:

Record Rule Description	Cat.	Classif.	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Src App.	DB Name	DB User	App. User	Client IP/Src App./DB User/Server IP/Svc. Name
☑	ANY	ANY	①	9.9.8.7 / 255.255.255.255	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Svc. Name	OS User	Net Protocol	Field	Pattern	XML Pattern	Client MAC	DB Type
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Object	Command	Object/Command Group	Object/Field Group	Records Affected Threshold	Trigger Once Per Session	Masking Pattern	Replacement Character	Min. Ct.	Reset Int.	Quarantine Min.	Rec. Vals.	Cont.	Period	Action
ANY	ANY	ANY	ANY	0	☑	ANY	*	0	0	0	☑	☑	ANY	▮▮▮

App Event Exists	Event Type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.
☐	ANY	ANY	ANY	ANY	ANY

Rule 2:

Record Rule Description	Cat.	Classif.	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Src App.	DB Name	DB User	App. User	Client IP/Src App./DB User/Server IP/Svc. Name
☑	ANY	ANY	①	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Svc. Name	OS User	Net Protocol	Field	Pattern	XML Pattern	Client MAC	DB Type
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Object	Command	Object/Command Group	Object/Field Group	Records Affected Threshold	Trigger Once Per Session	Masking Pattern	Replacement Character	Min. Ct.	Reset Int.	Quarantine Min.	Rec. Vals.	Cont.	Period	Action
ANY	DELETE	ANY	ANY	0	☑	ANY	*	0	0	0	☑	☐	ANY	▮▮▮

App Event Exists	Event Type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.
☐	ANY	ANY	ANY	ANY	ANY

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

Correct Answer: A

QUESTION 4

A Guardium administrator installed an S-TAP but is not seeing any data in reports on the collector. The administrator discovered that an Inspection Engine is not configured for that S-TAP.

What is an Inspection Engine?

A. A piece of software residing on the Collectors.

B. Another software to be installed on the Database server.

C. The same thing as the policy and it runs on the S-TAP to inspect the traffic in real-time.

D. A set of parameters needed for the S-TAP to define how to monitor traffic for a particular database instance on a server.

Correct Answer: C

QUESTION 5

A Guardium administrator needs to monitor an Oracle database on a production database server.

Which component does the administrator need to install on this database server that will monitor the traffic?

A. S-TAP

B. Guardium Collector

C. Guardium Installation Manager (GIM)

D. Configuration Auditing System (CAS)

Correct Answer: D