



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

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.

Correct Answer: D

QUESTION 2

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.	Sec.	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		
<input checked="" type="checkbox"/>	ANY	ANY	(1)	9.9.8.7 265.265.255.265	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	<input checked="" type="checkbox"/>	ANY	-	0	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ANY	<input checked="" type="checkbox"/>
App Event Exists	Event type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.									
<input checked="" type="checkbox"/>	ANY	ANY	ANY	ANY	ANY									

Rule 2:

Record Rule Description	Cat.	Classif.	Sec.	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		
<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	ANY	-	0	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ANY	<input checked="" type="checkbox"/>
App Event Exists	Event type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.									
<input checked="" type="checkbox"/>	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 3

A company is installing S-TAPS on new Database Clusters. The Guardium administrator was provided with the PVU load of each node. The clusters are in active/passive mode. The administrator is associating S-TAPs to Collectors using the PVU count.

How should the administrator treat the PVUs of passive nodes?

- A. include the PVU load of passive nodes.
- B. include half of the passive nodes PVU load.
- C. include a third of the passive nodes PVU load.
- D. Not include the PVU load of passive nodes.

Correct Answer: D

QUESTION 4

A Guardium policy has been configured with the following two rules:

Rule 1:

Record Rule Description	Cat.	ClassID	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Svc. App.	DB Name	DB User	App. User	Client IP/Svc. App./DB User/Server IP/Svc. Name		
<input checked="" type="checkbox"/>	ANY	ANY	1	9 4 5 6 / 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. Cl.	Reset Int.	Quarantine Min.	Rec. Val.	Cont.	Period	Action
TABLE1	ANY	ANY	ANY	0	<input type="checkbox"/>	ANY		0	0	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ANY	ALERT PER MATCH (Default)
App Event Exists	Event Type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.									
<input type="checkbox"/>	ANY	ANY	ANY	ANY	ANY									

Rule 2:

Record Rule Description	Cat.	ClassID	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Svc. App.	DB Name	DB User	App. User	Client IP/Svc. App./DB User/Server IP/Svc. Name		
<input checked="" type="checkbox"/>	ANY	ANY	1	9 4 5 6 / 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. Cl.	Reset Int.	Quarantine Min.	Rec. Val.	Cont.	Period	Action
TABLE1	ANY	ANY	ANY	0	<input type="checkbox"/>	ANY		0	0	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ANY	LOG FULL DETAILS
App Event Exists	Event Type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.									
<input type="checkbox"/>	ANY	ANY	ANY	ANY	ANY									



A Guardium administrator is required to check for SQL statements from client IP 9.4.5.6 executed on object "TABLET". What domain(s) can the administrator create a report in to see the SQL?

- A. Access
- B. Policy Violations
- C. Access and Access Policy
- D. Access and Policy Violations

Correct Answer: A

QUESTION 5

A Guardium administrator needs to build new appliances with the latest version of Guardium. How should the administrator obtain the ISO image?

- A. Contact IBM Support.
- B. Download from ibm.com
- C. Download from IBM Fix Central.
- D. Download from IBM Passport Advantage.

Correct Answer: D

[C2150-606 Practice Test](#)

[C2150-606 Study Guide](#)

[C2150-606 Braindumps](#)