IBM Security Guardium

S-TAP Severity 1 issues

Troubleshooting when S-TAP impacts the the DB or DB sever

-

Avi Walerius
Guardium Support

Contents

Introduction

“S-TAP impacts the DB or DB Server” what problems does this cover?

1. S-TAP process crashing
2. High CPU or memory usage of S-TAP on the database server
3. Database crashing
4. Availability or latency problems when accessing database
5. Server OS crash or hang

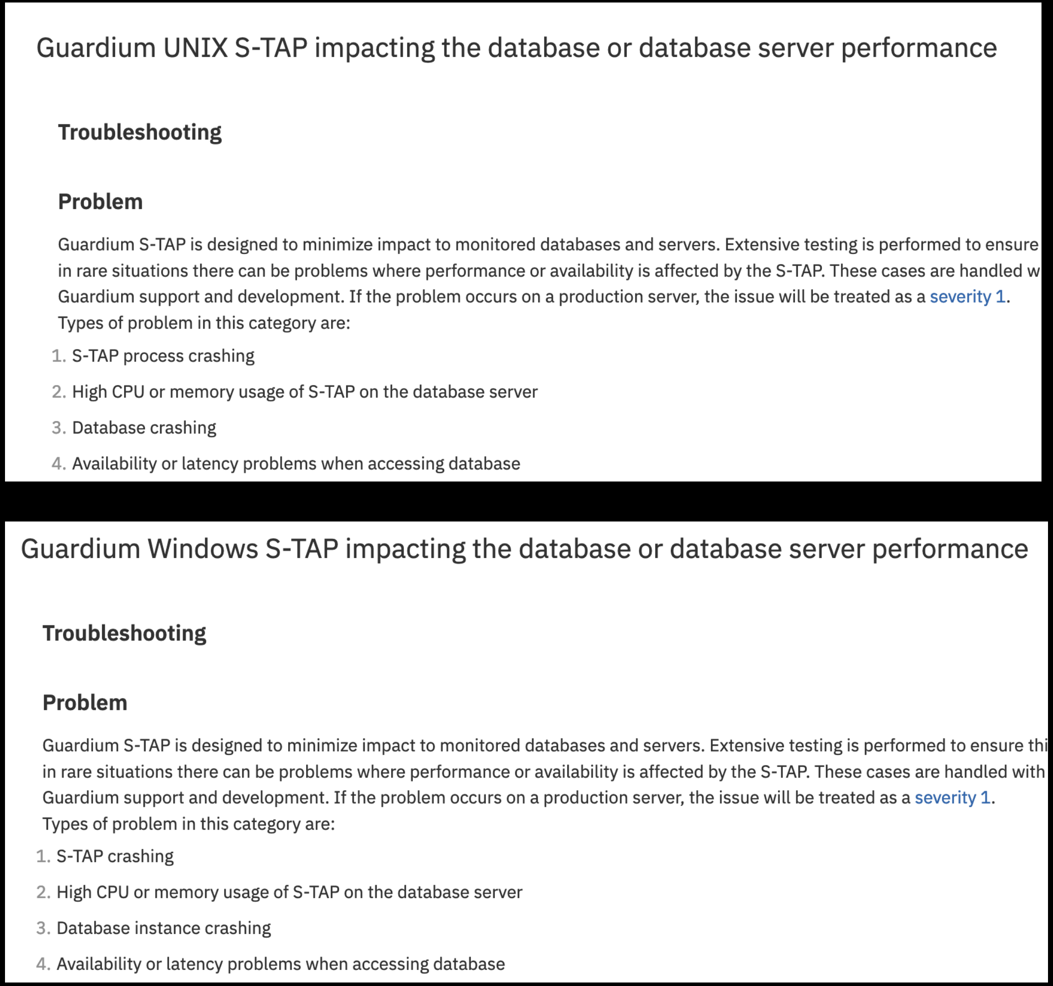
Reference technotes

UNIX (Focus of this training):

https://www.ibm.com/support/pages/guardium-unix-s-tap-impacting-database-or-database-server-performance

Windows:

https://www.ibm.com/support/pages/guardium-windows-s-tap-impacting-database-or-database-server-performance



Guardium UNIX S-TAP impacting the database or database server performance

Troubleshooting

Problem

Guardium S-TAP is designed to minimize impact to monitored databases and servers. Extensive testing is performed to ensure in rare situations there can be problems where performance or availability is affected by the S-TAP. These cases are handled w Guardium support and development. If the problem occurs on a production server, the issue will be treated as a severity 1. Types of problem in this category are:

1. S-TAP process crashing
2. High CPU or memory usage of S-TAP on the database server
3. Database crashing
4. Availability or latency problems when accessing database

Guardium Windows S-TAP impacting the database or database server performance

Troubleshooting

Problem

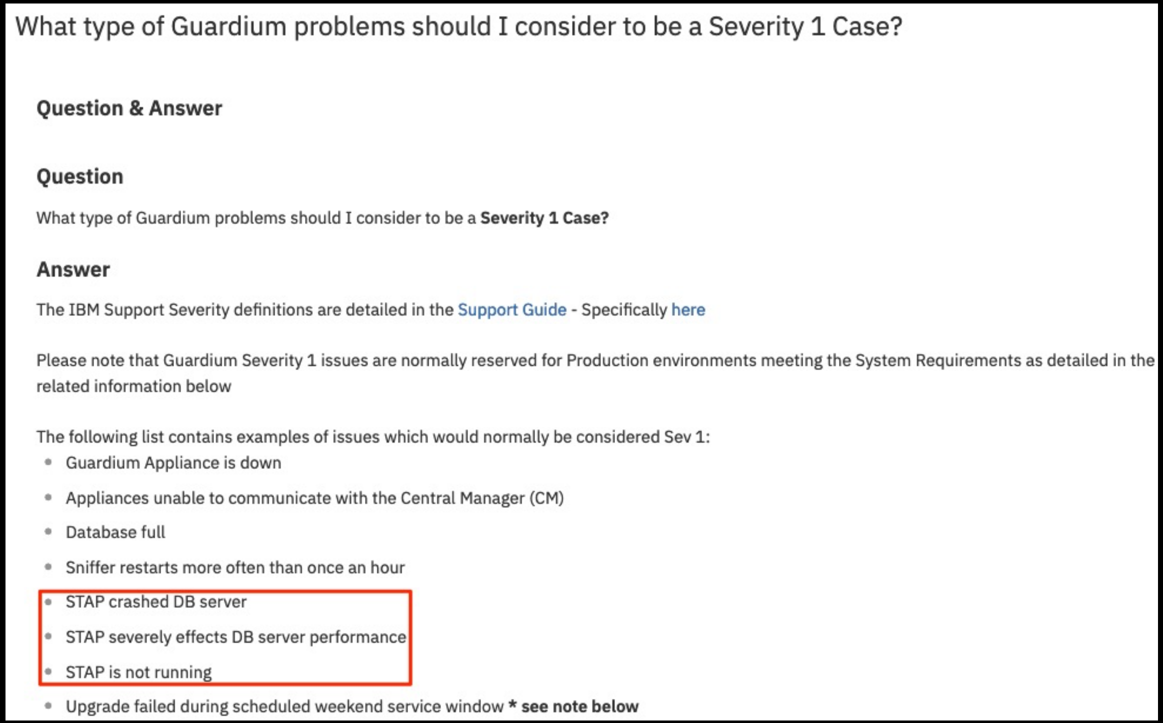
Guardium S-TAP is designed to minimize impact to monitored databases and servers. Extensive testing is performed to ensure thi in rare situations there can be problems where performance or availability is affected by the S-TAP. These cases are handled with Guardium support and development. If the problem occurs on a production server, the issue will be treated as a severity 1. Types of problem in this category are:

1. S-TAP crashing
2. High CPU or memory usage of S-TAP on the database server
3. Database instance crashing
4. Availability or latency problems when accessing database

UNIX and Windows troubleshooting technotes

How the Guardium team handles these problems

- Guardium S-TAP is designed to minimize impact to monitored databases and servers
- Extensive testing and QA is performed to ensure this is the case
- In **<u>rare</u>** situations there can be problems where performance or availability is affected by the S-TAP
- These cases are handled with the highest priority by Guardium support and development
- If the problem occurs on a production server, it is treated as a severity 1



What type of Guardium problems should I consider to be a Severity 1 Case?

Question & Answer

Question

What type of Guardium problems should I consider to be a **Severity 1 Case?**

Answer

The IBM Support Severity definitions are detailed in the Support Guide - Specifically here

Please note that Guardium Severity 1 issues are normally reserved for Production environments meeting the System Requirements as detailed in the related information below

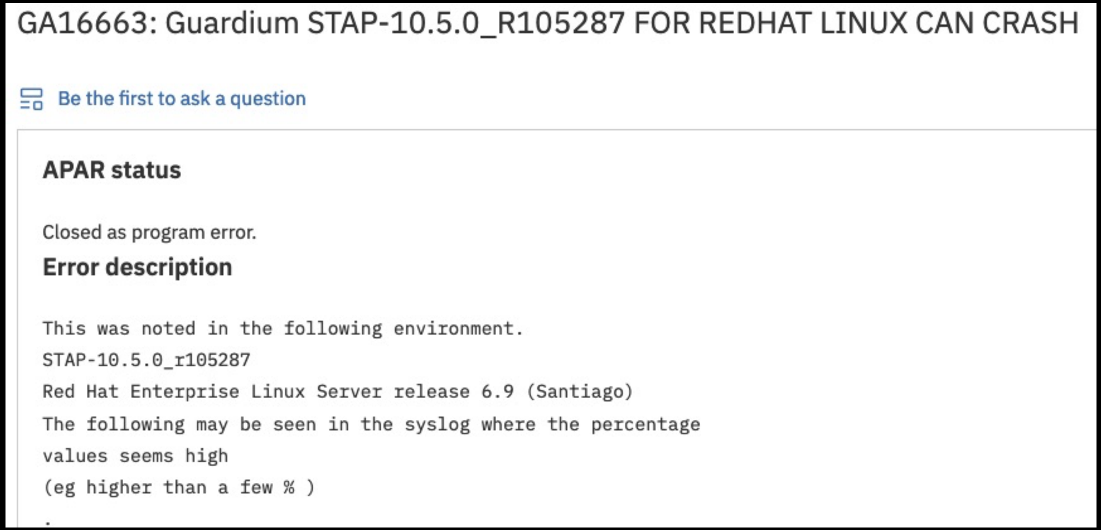
The following list contains examples of issues which would normally be considered Sev 1:

- Guardium Appliance is down
- Appliances unable to communicate with the Central Manager (CM)
- Database full
- Sniffer restarts more often than once an hour
- STAP crashed DB server
- STAP severely effects DB server performance
- STAP is not running
- Upgrade failed during scheduled weekend service window *** see note below**

Severity 1 guidelines technote
https://www.ibm.com/support/pages/what-type-guardium-problems-should-i-consider-be-severity-1-case

Typical problem causes

1. Defects in Guardium S-TAP code
   - S-TAP is designed to limit impact on DBs and servers so majority of cases involve a defect
   - Known defects are tracked in APARs
2. Configuration issues
   - SGATE and Query Rewrite common cause of latency if configuration is not set well
3. Environmental factors combined with 1 and/or 2 (most common)
   - Specific traffic may trigger defect in S-TAP
   - 3rd party products may conflict with S-TAP
   - Specific traffic may trigger SGATE rules in unexpected way



GA16663: Guardium STAP-10.5.0_R105287 FOR REDHAT LINUX CAN CRASH

Be the first to ask a question

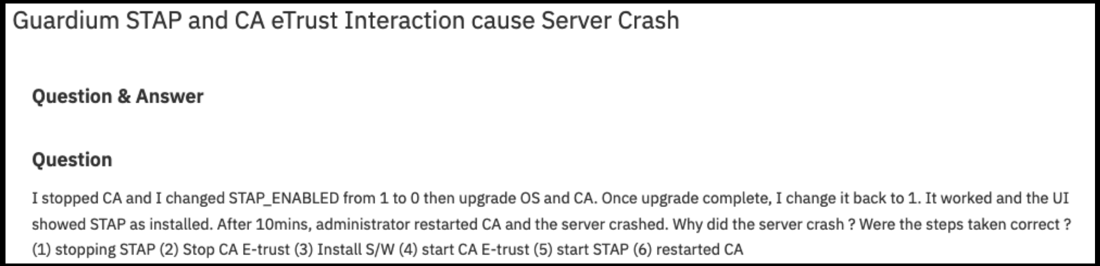
APAR status

Closed as program error.

Error description

```
This was noted in the following environment.
STAP-10.5.0_r105287
Red Hat Enterprise Linux Server release 6.9 (Santiago)
The following may be seen in the syslog where the percentage
values seems high
(eg higher than a few % )
```

Example APAR



Guardium STAP and CA eTrust Interaction cause Server Crash

Question & Answer

Question

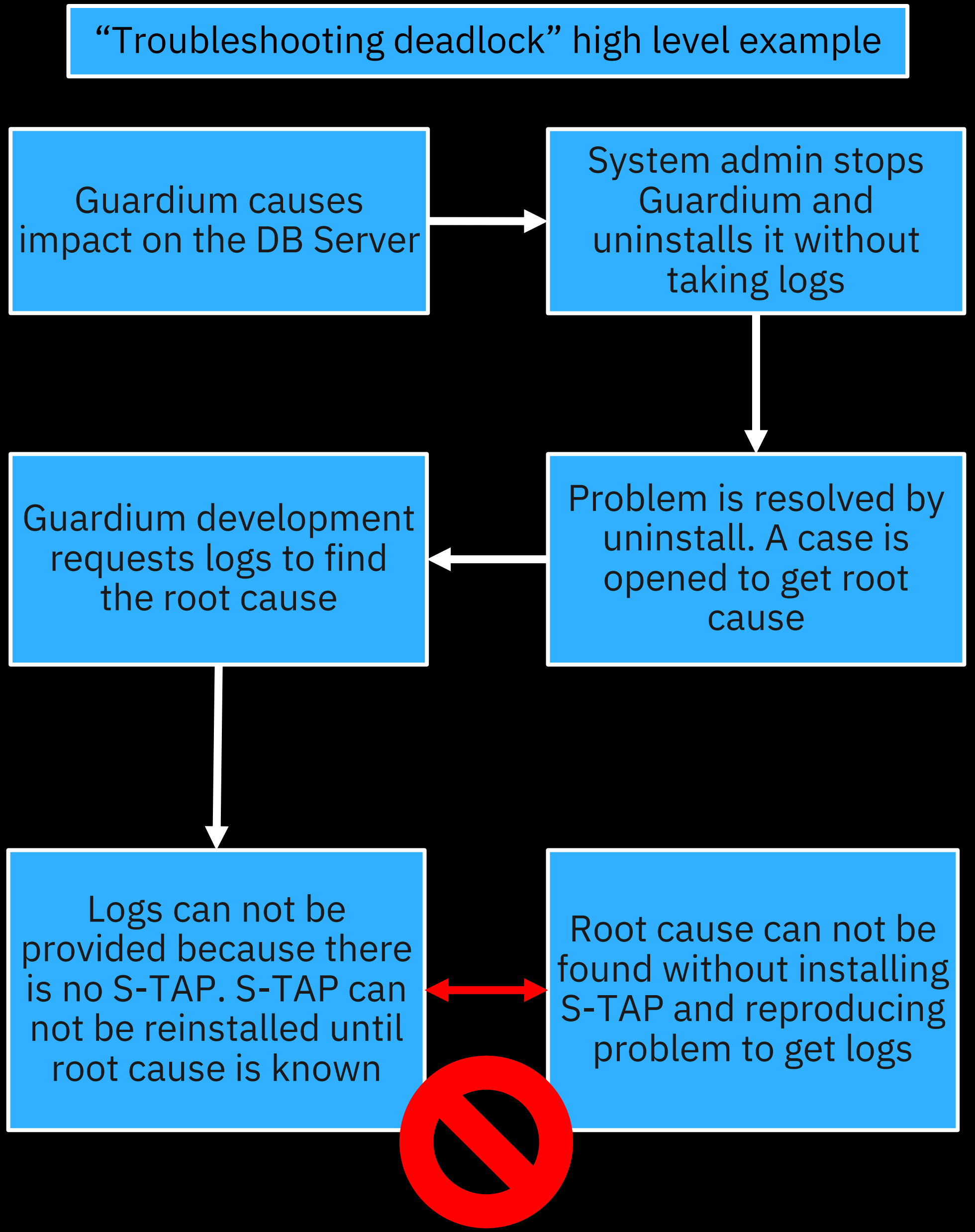
I stopped CA and I changed STAP_ENABLED from 1 to 0 then upgrade OS and CA. Once upgrade complete, I change it back to 1. It worked and the UI showed STAP as installed. After 10mins, administrator restarted CA and the server crashed. Why did the server crash ? Were the steps taken correct ? (1) stopping STAP (2) Stop CA E-trust (3) Install S/W (4) start CA E-trust (5) start STAP (6) restarted CA

Technote describing conflict between CA eTrust and S-TAP and solution
https://www.ibm.com/support/pages/guardium-stap-and-ca-etrust-interaction-cause-server-crash

Troubleshooting aims for Guardium admin

- Often Guardium admin can not resolve *new* issues without input from server admins and Guardium support/development

- Aim of this training for Guardium admins
  - Identify cases when admin *can* resolve issues
  - Understand what logs are required for Guardium team to investigate
  - Understand importance of logs currency and timing
  - Act as an intermediary in your organization so the correct actions are taken at the right times
  - Help avoid "troubleshooting deadlock" type situations


"Troubleshooting deadlock" high level example

Guardium causes impact on the DB Server

System admin stops Guardium and uninstalls it without taking logs

Problem is resolved by uninstall. A case is opened to get root cause

Guardium development requests logs to find the root cause

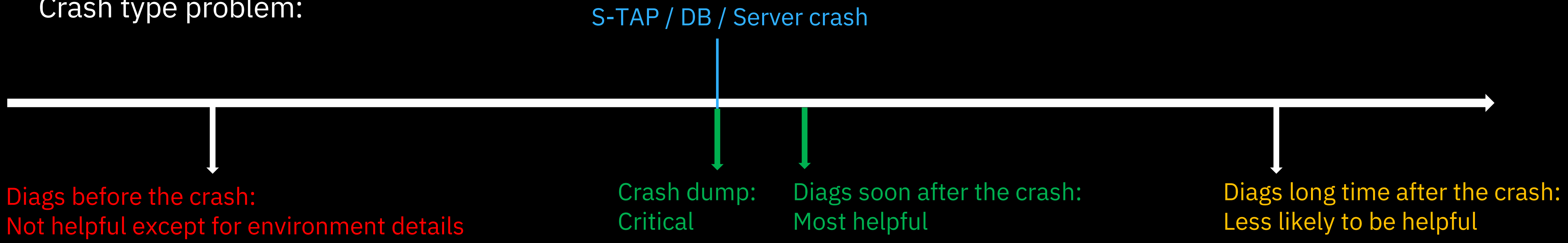
Logs can not be provided because there is no S-TAP. S-TAP can not be reinstalled until root cause is known

Root cause can not be found without installing S-TAP and reproducing problem to get logs

Key troubleshooting points for all problems

Diagnostic timing

- Diagnostic timing is crucial to investigation
- Crash type problem:



S-TAP / DB / Server crash

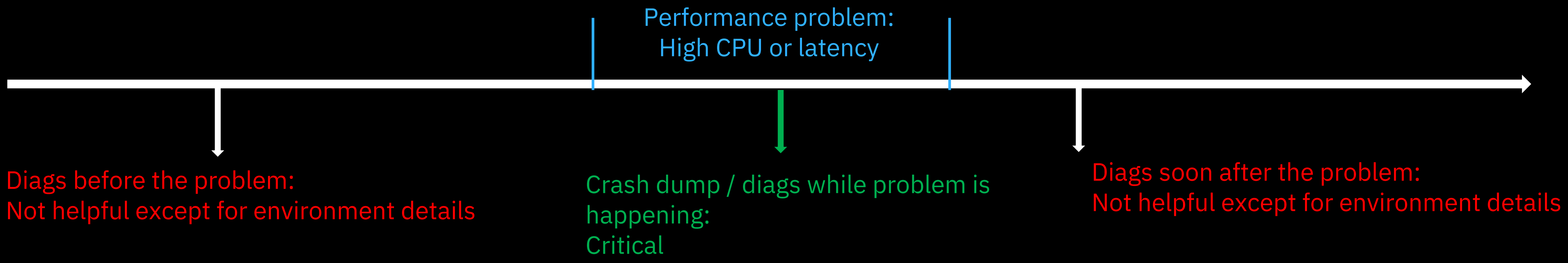
Diags before the crash:
Not helpful except for environment details

Crash dump:
Critical

Diags soon after the crash:
Most helpful

Diags long time after the crash:
Less likely to be helpful

- Performance type problem:



Performance problem:
High CPU or latency

Diags before the problem:
Not helpful except for environment details

Crash dump / diags while problem is happening:
Critical

Diags soon after the problem:
Not helpful except for environment details

Crash dump file collection and vendor analysis

- When S-TAP, database or server OS crashes a dump file is required to be *certain* of the root cause
- If no dump file is available Guardium team will work on a best effort basis to find the root cause
- The server or database admin should provide the core dumps required based on vendor best practices
- Guardium team has collated some vendor documentation to be used as a reference if there is uncertainty about how to collect dump files
- When database or server crashes it is recommended to provide the dump file to the vendor to provide their analysis, then send that to Guardium support
- In some cases Guardium team and vendor team will work together to find root cause

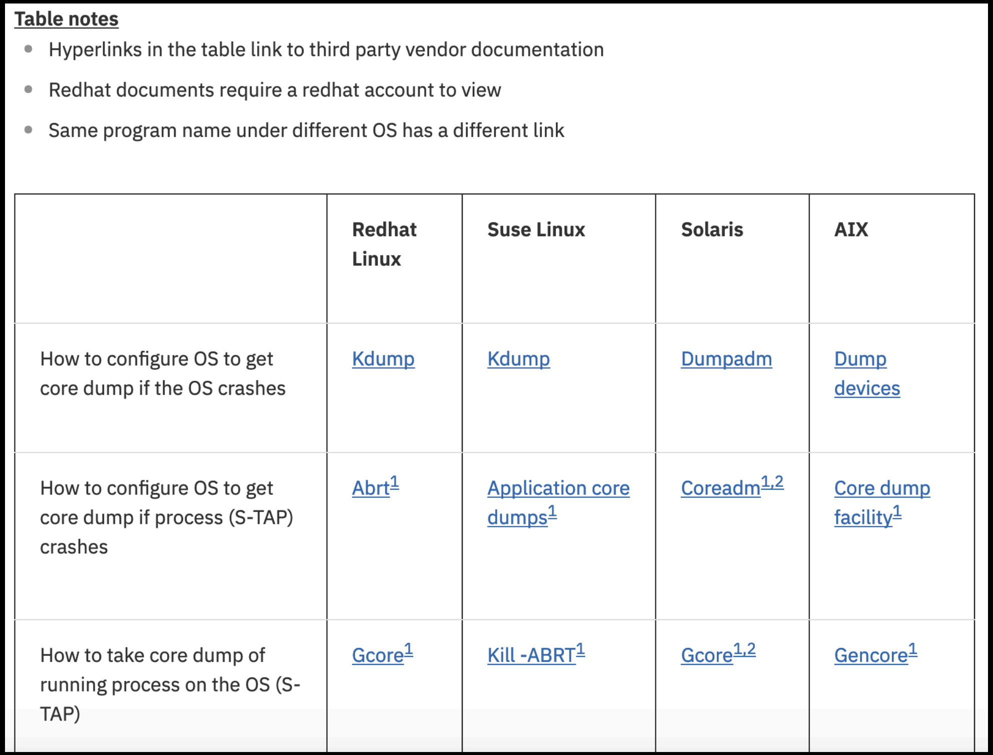


Table notes

- Hyperlinks in the table link to third party vendor documentation
- Redhat documents require a redhat account to view
- Same program name under different OS has a different link

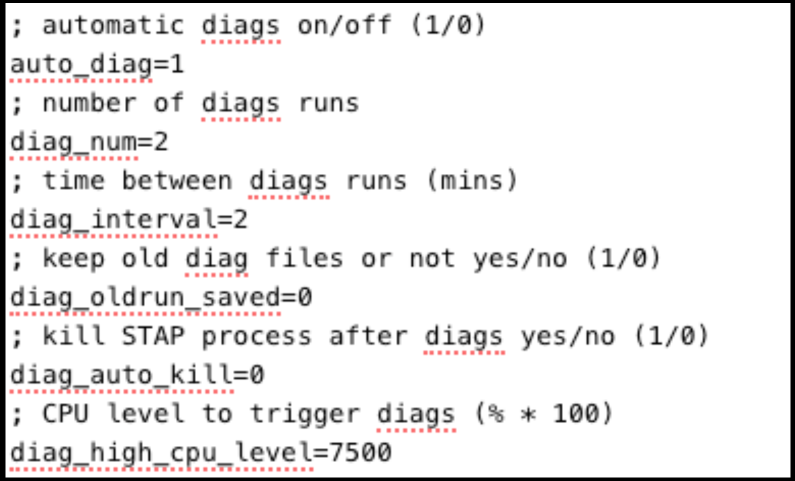
	Redhat Linux	Suse Linux	Solaris	AIX
How to configure OS to get core dump if the OS crashes	Kdump	Kdump	Dumpadm	Dump devices
How to configure OS to get core dump if process (S-TAP) crashes	Abrt[1]	Application core dumps[1]	Coreadm[1,2]	Core dump facility[1]
How to take core dump of running process on the OS (S-TAP)	Gcore[1]	Kill -ABRT[1]	Gcore[1,2]	Gencore[1]

Part of the technote - "How to collect core dumps if Guardium UNIX S-TAP is impacting the database or database server". Links to examples of how to collect appropriate core dumps, but should not override the expertise of the server admin. *https://www.ibm.com/support/pages/node/1169620*

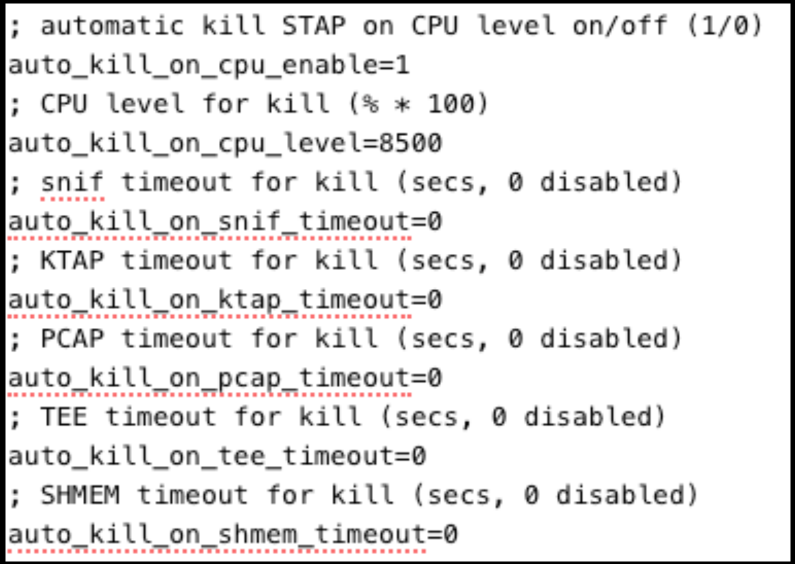
Guard_monitor

- A UNIX utility to monitor the S-TAP performance. Equivalent also exists for Windows.
- Can take actions automatically when conditions are met
- Conditions:
  - CPU Utilization
  - S-TAP responsiveness to polling
- Actions:
  - Run guard_diag
  - Kill S-TAP
  - Core dump and kill S-TAP
  - Start trace

- Important! guard_monitor can automatically stop or restart the S-TAP. Careful consideration and testing of the settings should be done before starting it in production environment.



```
; automatic diags on/off (1/0)
auto_diag=1
; number of diags runs
diag_num=2
; time between diags runs (mins)
diag_interval=2
; keep old diag files or not yes/no (1/0)
diag_oldrun_saved=0
; kill STAP process after diags yes/no (1/0)
diag_auto_kill=0
; CPU level to trigger diags (% * 100)
diag_high_cpu_level=7500
```

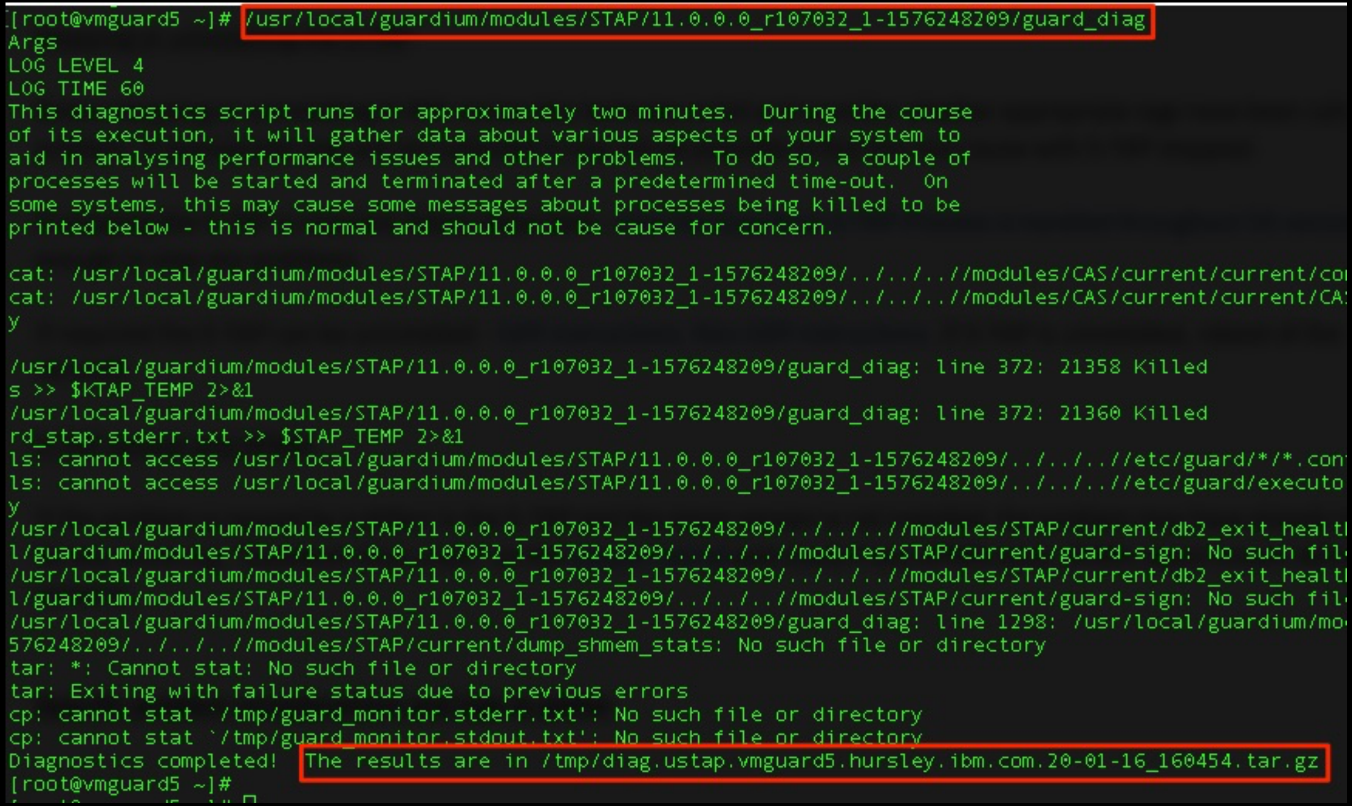


```
; automatic kill STAP on CPU level on/off (1/0)
auto_kill_on_cpu_enable=1
; CPU level for kill (% * 100)
auto_kill_on_cpu_level=8500
; snif timeout for kill (secs, 0 disabled)
auto_kill_on_snif_timeout=0
; KTAP timeout for kill (secs, 0 disabled)
auto_kill_on_ktap_timeout=0
; PCAP timeout for kill (secs, 0 disabled)
auto_kill_on_pcap_timeout=0
; TEE timeout for kill (secs, 0 disabled)
auto_kill_on_tee_timeout=0
; SHMEM timeout for kill (secs, 0 disabled)
auto_kill_on_shmem_timeout=0
```

Example snippets from guard_monitor.ini. Full UNIX documentation: https://www.ibm.com/support/knowledgecenter/SSMPHH_11.1.0/com.ibm.guardium.doc.stap/stap/unix_stap_guard_monitor.html

Guard_diag

- Guard_diag is a script to gather detailed troubleshooting information about the system and installed agents
- Should be provided for all issues involving UNIX S-TAP
- <stap install dir>/guard_diag
- Contains server syslog, which may rotate. Should be run during or soon after the problem reproduction
- Equivalent also exists for Windows (Windows S-TAP must gather)

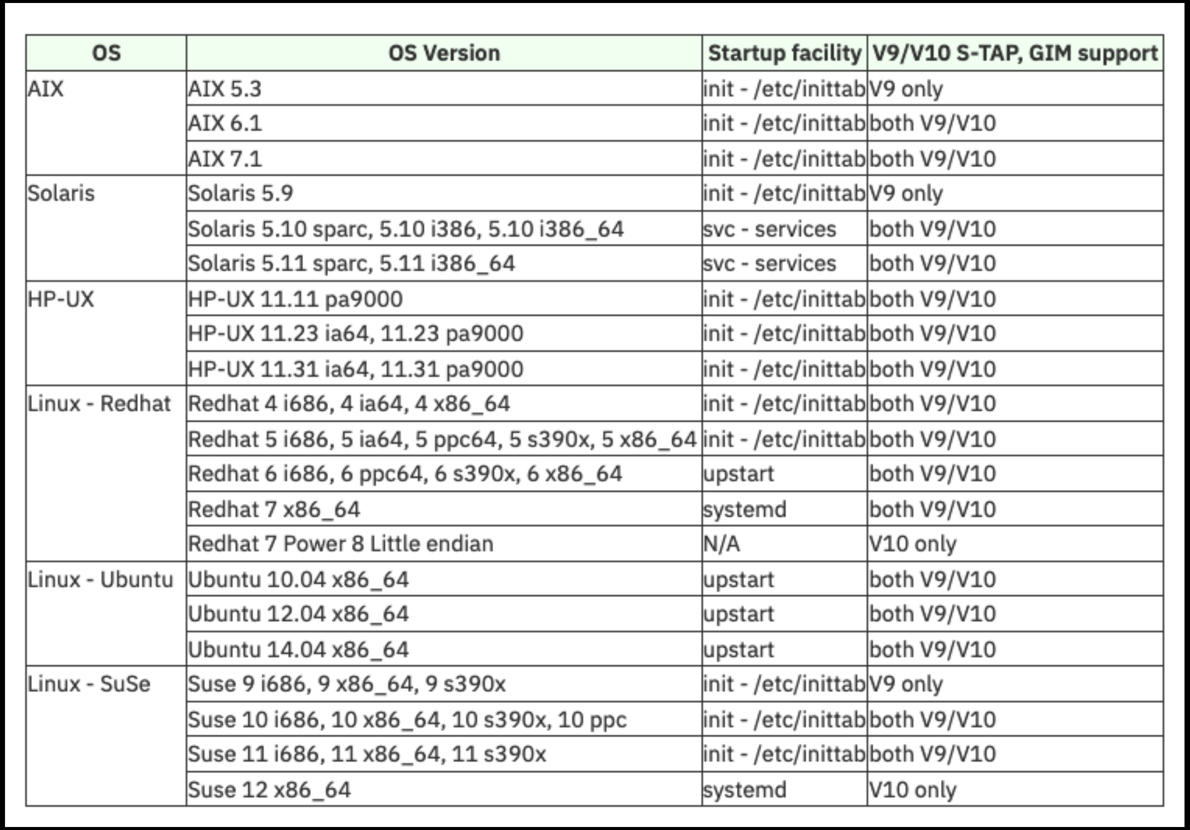


```
[root@vmguard5 ~]# /usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/guard_diag
Args
LOG LEVEL 4
LOG TIME 60
This diagnostics script runs for approximately two minutes.  During the course
of its execution, it will gather data about various aspects of your system to
aid in analysing performance issues and other problems.  To do so, a couple of
processes will be started and terminated after a predetermined time-out.  On
some systems, this may cause some messages about processes being killed to be
printed below - this is normal and should not be cause for concern.

cat: /usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//modules/CAS/current/current/co
cat: /usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//modules/CAS/current/current/CA
y

/usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/guard_diag: line 372: 21358 Killed
s >> $KTAP_TEMP 2>&1
/usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/guard_diag: line 372: 21360 Killed
rd_stap.stderr.txt >> $STAP_TEMP 2>&1
ls: cannot access /usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//etc/guard/*/*.con
ls: cannot access /usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//etc/guard/executo
y
/usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//modules/STAP/current/db2_exit_healt
l/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//modules/STAP/current/guard-sign: No such fil
/usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//modules/STAP/current/db2_exit_healt
l/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/../../..//modules/STAP/current/guard-sign: No such fil
/usr/local/guardium/modules/STAP/11.0.0.0_r107032_1-1576248209/guard_diag: line 1298: /usr/local/guardium/mo
576248209/../../..//modules/STAP/current/dump_shmem_stats: No such file or directory
tar: *: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
cp: cannot stat `/tmp/guard_monitor.stderr.txt': No such file or directory
cp: cannot stat `/tmp/guard_monitor.stdout.txt': No such file or directory
Diagnostics completed!  The results are in /tmp/diag.ustap.vmguard5.hursley.ibm.com.20-01-16_160454.tar.gz
[root@vmguard5 ~]#
```

Guard_diag collection including some errors. In most cases any errors can be ignored as long as the output file is created

Stopping or uninstalling the S-TAP

- Important! Before stopping or uninstalling S-TAP be sure that appropriate logs have been taken
- Usually stopping the S-TAP will be enough to stop problems caused by S-TAP
- See ‘How S-TAP process is handled throughout OS versions’ for stopping steps per OS
- If uninstall is required see: https://www.ibm.com/support/knowledgecenter/en/SSMPHH_11.1.0/com.ibm.guardium.doc.stap/stap/gim_install_upgrade_uninstall.html
- If S-TAP is uninstalled when KTAP loaded, server must be rebooted before reinstalling

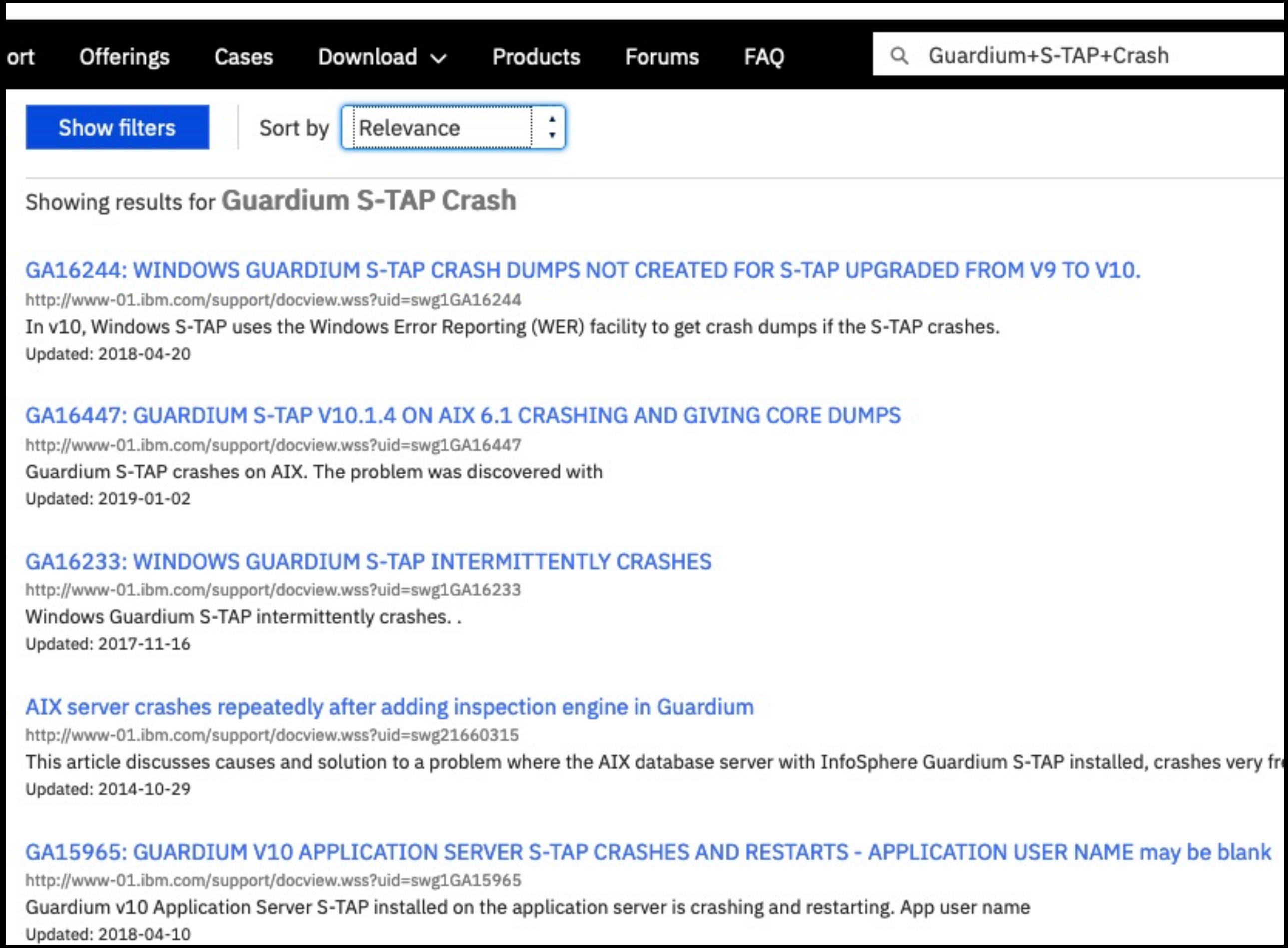


OS	OS Version	Startup facility	V9/V10 S-TAP, GIM support
AIX	AIX 5.3	init - /etc/inittab	V9 only
	AIX 6.1	init - /etc/inittab	both V9/V10
	AIX 7.1	init - /etc/inittab	both V9/V10
Solaris	Solaris 5.9	init - /etc/inittab	V9 only
	Solaris 5.10 sparc, 5.10 i386, 5.10 i386_64	svc - services	both V9/V10
	Solaris 5.11 sparc, 5.11 i386_64	svc - services	both V9/V10
HP-UX	HP-UX 11.11 pa9000	init - /etc/inittab	both V9/V10
	HP-UX 11.23 ia64, 11.23 pa9000	init - /etc/inittab	both V9/V10
	HP-UX 11.31 ia64, 11.31 pa9000	init - /etc/inittab	both V9/V10
Linux - Redhat	Redhat 4 i686, 4 ia64, 4 x86_64	init - /etc/inittab	both V9/V10
	Redhat 5 i686, 5 ia64, 5 ppc64, 5 s390x, 5 x86_64	init - /etc/inittab	both V9/V10
	Redhat 6 i686, 6 ppc64, 6 s390x, 6 x86_64	upstart	both V9/V10
	Redhat 7 x86_64	systemd	both V9/V10
	Redhat 7 Power 8 Little endian	N/A	V10 only
Linux - Ubuntu	Ubuntu 10.04 x86_64	upstart	both V9/V10
	Ubuntu 12.04 x86_64	upstart	both V9/V10
	Ubuntu 14.04 x86_64	upstart	both V9/V10
Linux - SuSe	Suse 9 i686, 9 x86_64, 9 s390x	init - /etc/inittab	V9 only
	Suse 10 i686, 10 x86_64, 10 s390x, 10 ppc	init - /etc/inittab	both V9/V10
	Suse 11 i686, 11 x86_64, 11 s390x	init - /etc/inittab	both V9/V10
	Suse 12 x86_64	systemd	V10 only

Startup facility for UNIX S-TAP for different OS. Full details: https://www.ibm.com/support/pages/how-guardium-s-tap-process-handled-throughout-os-versions

S-TAP version and APARs

- In case of these problems check your S-TAP version
- Compare against latest version on fix central
- If you have an older version your issue may be a defect resolved in the latest version
- APARs track code defects that have been fixed
  - Check release notes of new S-TAPs on fix central
  - Search for APARs from support portal: https://www.ibm.com/mysupport/s/?language=en_US



Showing results for **Guardium S-TAP Crash**

GA16244: WINDOWS GUARDIUM S-TAP CRASH DUMPS NOT CREATED FOR S-TAP UPGRADED FROM V9 TO V10.
http://www-01.ibm.com/support/docview.wss?uid=swg1GA16244
In v10, Windows S-TAP uses the Windows Error Reporting (WER) facility to get crash dumps if the S-TAP crashes.
Updated: 2018-04-20

GA16447: GUARDIUM S-TAP V10.1.4 ON AIX 6.1 CRASHING AND GIVING CORE DUMPS
http://www-01.ibm.com/support/docview.wss?uid=swg1GA16447
Guardium S-TAP crashes on AIX. The problem was discovered with
Updated: 2019-01-02

GA16233: WINDOWS GUARDIUM S-TAP INTERMITTENTLY CRASHES
http://www-01.ibm.com/support/docview.wss?uid=swg1GA16233
Windows Guardium S-TAP intermittently crashes. .
Updated: 2017-11-16

AIX server crashes repeatedly after adding inspection engine in Guardium
http://www-01.ibm.com/support/docview.wss?uid=swg21660315
This article discusses causes and solution to a problem where the AIX database server with InfoSphere Guardium S-TAP installed, crashes very fr
Updated: 2014-10-29

GA15965: GUARDIUM V10 APPLICATION SERVER S-TAP CRASHES AND RESTARTS - APPLICATION USER NAME may be blank
http://www-01.ibm.com/support/docview.wss?uid=swg1GA15965
Guardium v10 Application Server S-TAP installed on the application server is crashing and restarting. App user name
Updated: 2018-04-10

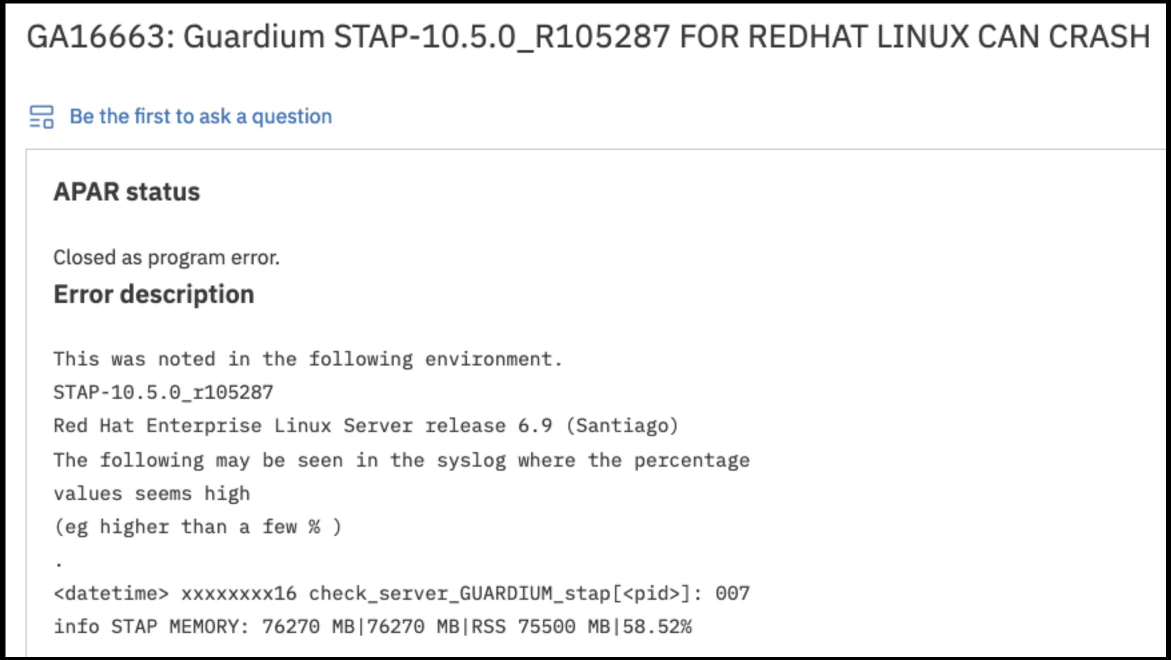
Searching for issues in support portal. Items starting with GA are APARs. Technotes and documentation also appear

Problem specifics

S-TAP Process Crashing

Logs to collect

- guard_diag while the S-TAP is installed and soon after the crash happens
- S-TAP process crash dump
  - Steps to enable automatic process crash dump vary between different OS. Check with the server administrator to confirm exact steps in your environment. Use crash dump reference if needed.
- Timing of the crashes, is it correlated to any other event?
  - Specific traffic?
  - Regular timing?



GA16663: Guardium STAP-10.5.0_R105287 FOR REDHAT LINUX CAN CRASH

Be the first to ask a question

APAR status

Closed as program error.

Error description

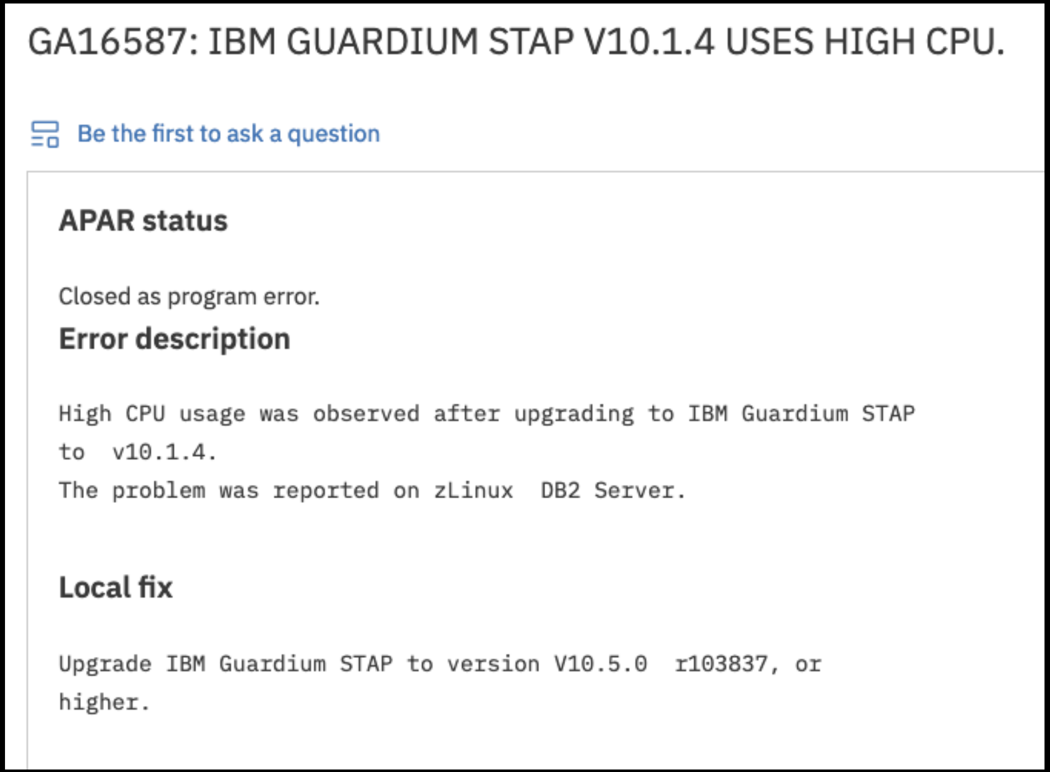
```
This was noted in the following environment.
STAP-10.5.0_r105287
Red Hat Enterprise Linux Server release 6.9 (Santiago)
The following may be seen in the syslog where the percentage
values seems high
(eg higher than a few % )
.
<datetime> xxxxxxxx16 check_server_GUARDIUM_stap[<pid>]: 007
info STAP MEMORY: 76270 MB|76270 MB|RSS 75500 MB|58.52%
```

APAR GA16663

High CPU or memory usage of S-TAP

Logs to collect

- At least one S-TAP process dump, triggered manually on server when CPU/memory is high
  - Commands to trigger process dump vary between OS, check with server admin to confirm exact steps in your environment. Use crash dump reference if needed
- guard_diag taken when CPU/Memory is high
- Timing of problem, is it correlated to any other event?
  - Batch jobs or other specific traffic?
  - Regular timing?
- Guard_monitor can be used to take automatic actions



GA16587: IBM GUARDIUM STAP V10.1.4 USES HIGH CPU.

APAR status

Closed as program error.

Error description

```
High CPU usage was observed after upgrading to IBM Guardium STAP
to  v10.1.4.
The problem was reported on zLinux  DB2 Server.
```

Local fix

```
Upgrade IBM Guardium STAP to version V10.5.0  r103837, or
higher.
```

APAR GA16587

How much CPU can S-TAP use?

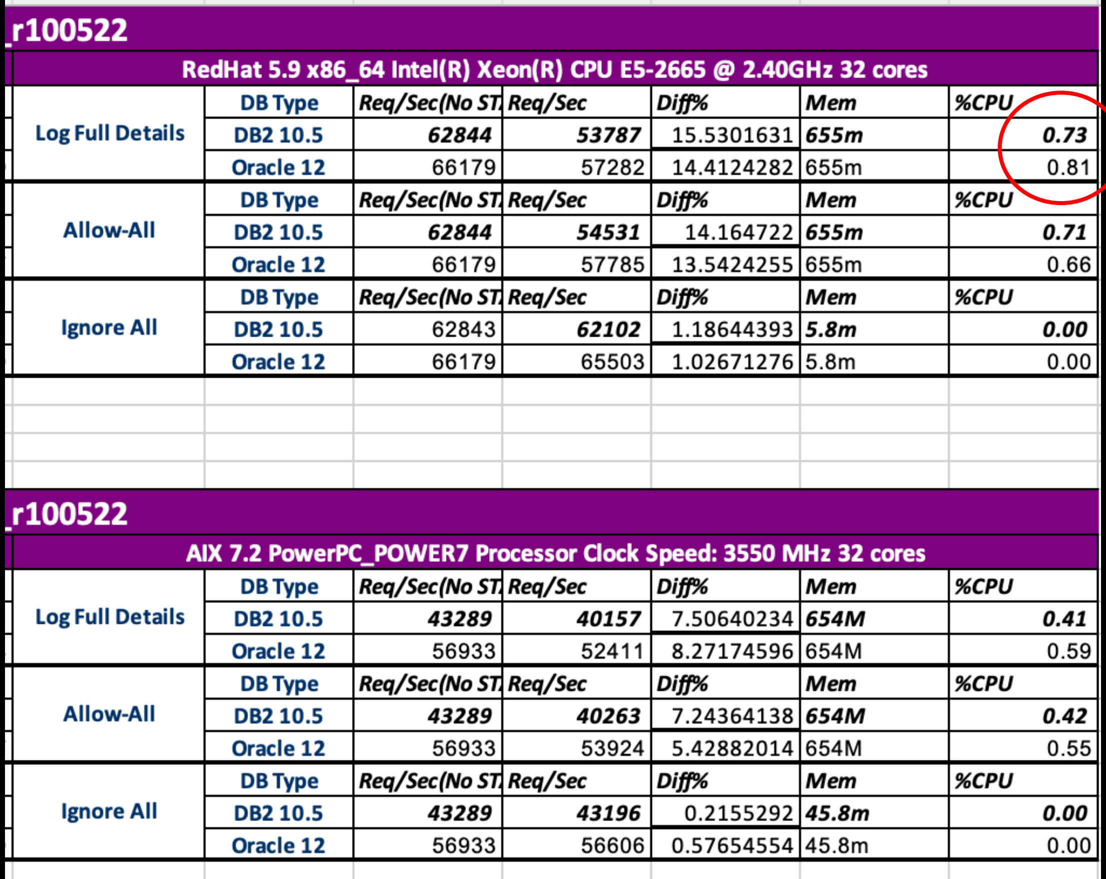
- Common question – Answer depends on the number of threads used by the KTAP. Default 1, max 5.

- Total <u>maximum possible</u> CPU usage of the S-TAP

$$PercentServerCPU = \left(\frac{KtapThreads}{TotalServerCPUCores}\right)100$$

- Example for default S-TAP on 32 core server

$$PercentServerCPU = (\frac{1}{32})100 = 3.125$$



r100522

RedHat 5.9 x86_64 Intel(R) Xeon(R) CPU E5-2665 @ 2.40GHz 32 cores

	DB Type	Req/Sec(No ST	Req/Sec	Diff%	Mem	%CPU
Log Full Details	DB2 10.5	***62844***	***53787***	15.5301631	***655m***	***0.73***
	Oracle 12	66179	57282	14.4124282	655m	0.81
	DB Type	Req/Sec(No ST	Req/Sec	Diff%	Mem	%CPU
Allow-All	DB2 10.5	***62844***	***54531***	14.164722	***655m***	***0.71***
	Oracle 12	66179	57785	13.5424255	655m	0.66
	DB Type	Req/Sec(No ST	Req/Sec	Diff%	Mem	%CPU
Ignore All	DB2 10.5	62843	***62102***	1.18644393	***5.8m***	***0.00***
	Oracle 12	66179	65503	1.02671276	5.8m	0.00

r100522

AIX 7.2 PowerPC_POWER7 Processor Clock Speed: 3550 MHz 32 cores

	DB Type	Req/Sec(No ST	Req/Sec	Diff%	Mem	%CPU
Log Full Details	DB2 10.5	***43289***	***40157***	7.50640234	***654M***	***0.41***
	Oracle 12	56933	52411	8.27174596	654M	0.59
	DB Type	Req/Sec(No ST	Req/Sec	Diff%	Mem	%CPU
Allow-All	DB2 10.5	***43289***	***40263***	7.24364138	***654M***	***0.42***
	Oracle 12	56933	53924	5.42882014	654M	0.55
	DB Type	Req/Sec(No ST	Req/Sec	Diff%	Mem	%CPU
Ignore All	DB2 10.5	***43289***	***43196***	0.2155292	***45.8m***	***0.00***
	Oracle 12	56933	56606	0.57654554	45.8m	0.00

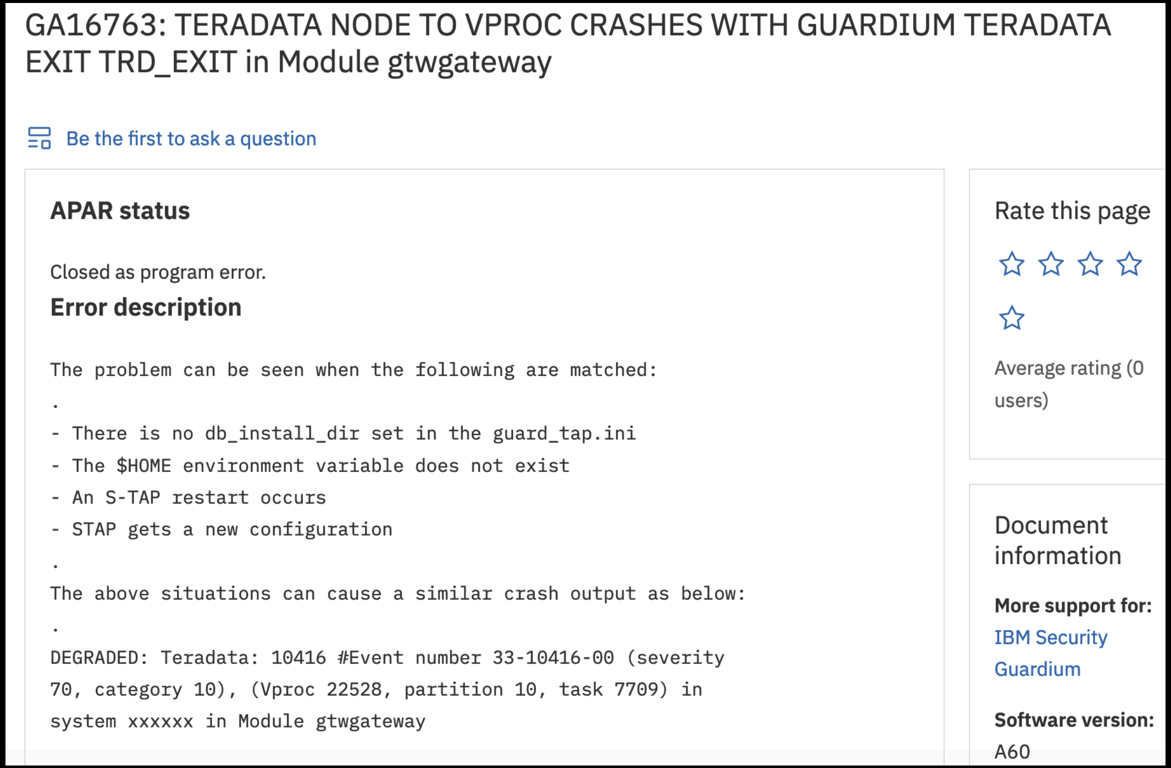
Actual published v10.1.2 S-TAP CPU benchmarks. Actual usage depends on policy, configuration and traffic profile. There is no single 'correct' value for actual usage.

Database Crashing

Database crash can only be caused when ATAP or EXIT are in use.

Logs to collect

- Database crash dump
- Database vendor analysis
- Guard_diag soon after the crash
- Timing of problem, is it correlated to any other event?
    - ATAP or EXIT related activities?



GA16763: TERADATA NODE TO VPROC CRASHES WITH GUARDIUM TERADATA EXIT TRD_EXIT in Module gtwgateway

Be the first to ask a question

APAR status

Closed as program error.

Error description

```
The problem can be seen when the following are matched:
.
- There is no db_install_dir set in the guard_tap.ini
- The $HOME environment variable does not exist
- An S-TAP restart occurs
- STAP gets a new configuration
.
The above situations can cause a similar crash output as below:
.
DEGRADED: Teradata: 10416 #Event number 33-10416-00 (severity
70, category 10), (Vproc 22528, partition 10, task 7709) in
system xxxxxx in Module gtwgateway
```

Rate this page

☆ ☆ ☆ ☆ ☆

Average rating (0 users)

Document information

More support for: IBM Security Guardium

Software version: A60

APAR GA16763

Availability or latency problems accessing the DB

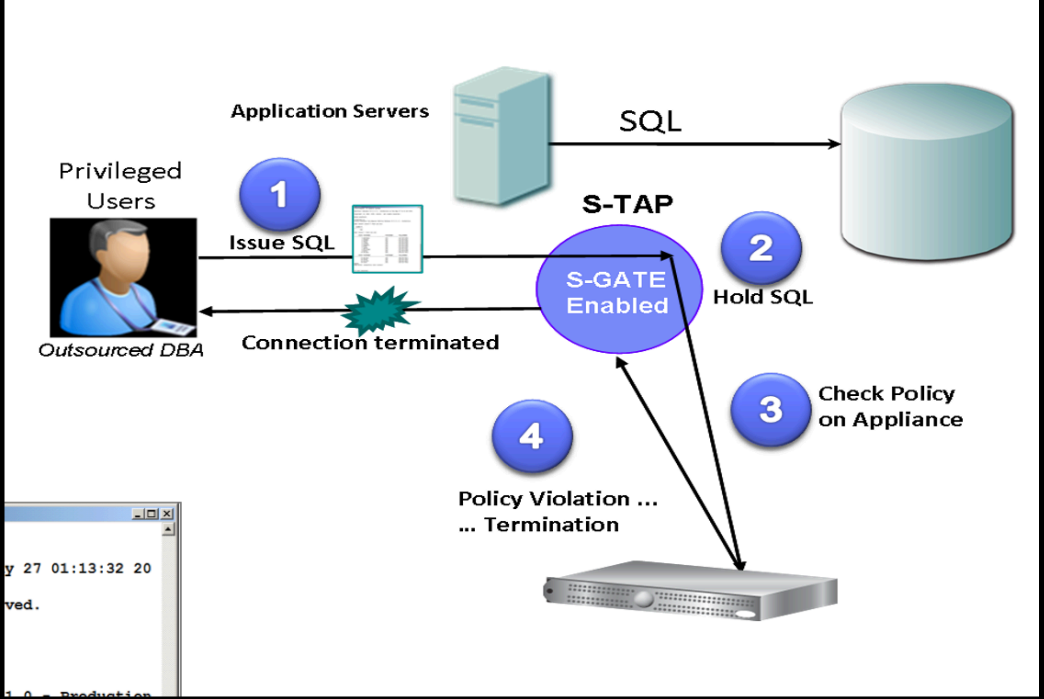
SGATE or Query rewrite (QRW) almost always the source of latency issues or timeout when trying to access the DB.

With sessions attached in the firewall, latency is expected. Misconfiguration can cause too many or unwanted sessions to be attached and slow down DB. **Guardium admin can resolve these kind of problems.**

Simple check: Disable firewall - Does problem go away?

If yes, troubleshoot firewall configuration:

- What is the firewall or QRW default_state?
  - Default_state=1 means all sessions attached by default
- What sessions is my policy attaching?
  - SGATE or QRW ATTACH action puts them into attached state
- If you are struggling with security v latency tradeoff check out firewall_default_state=2 and Firewall optimization: https://www.ibm.com/support/knowledgecenter/SSMPHH_11.1.0/com.ibm.guardium.doc/protect/session_level_policies_actions.html



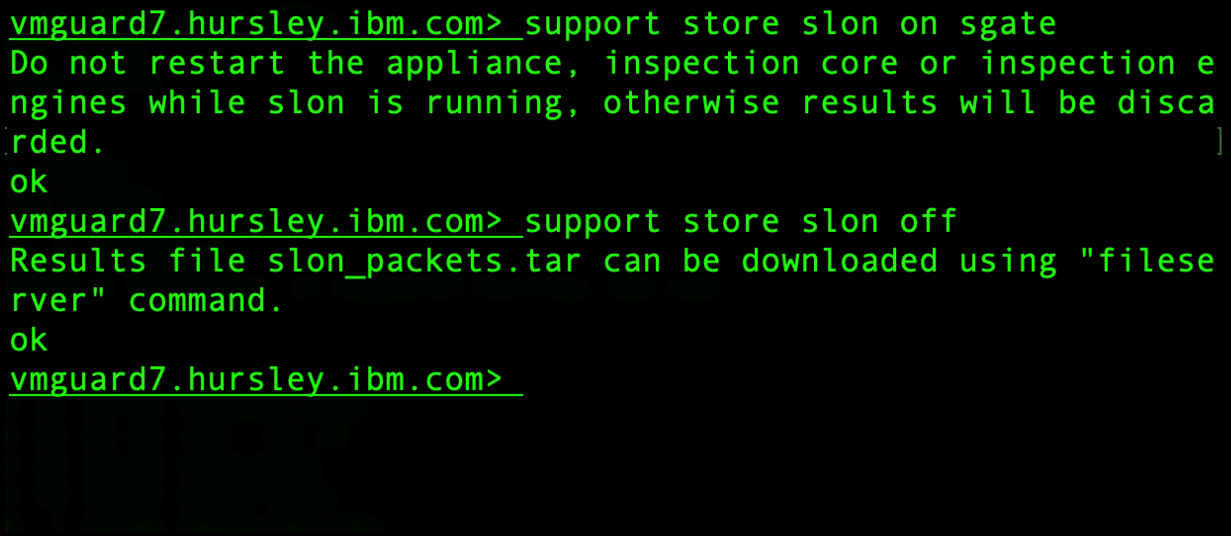
SGATE in closed mode diagram. See full explanation of SGATE in learning academy: *https://www.securitylearningacademy.com/course/view.php?id=2893*

Availability or latency problems accessing the DB

If the problem can not be determined from troubleshooting configuration and policy.

Logs to collect:

- Guard_diag when latency happening
- Slon with ‘sgate’ option containing sessions that reproduce issue
- Explanation of exact symptom. E.g.
  - Latency on certain / all commands (how much latency)
  - Certain / all users can't login
- Explanation of what kind of sessions produce symptom
- Sniffer must gather
- If SGATE/QRW not in use – S-TAP process core dump when latency is happening



```
vmguard7.hursley.ibm.com> support store slon on sgate
Do not restart the appliance, inspection core or inspection e
ngines while slon is running, otherwise results will be disca
rded.
ok
vmguard7.hursley.ibm.com> support store slon off
Results file slon_packets.tar can be downloaded using "filese
rver" command.
ok
vmguard7.hursley.ibm.com> 
```

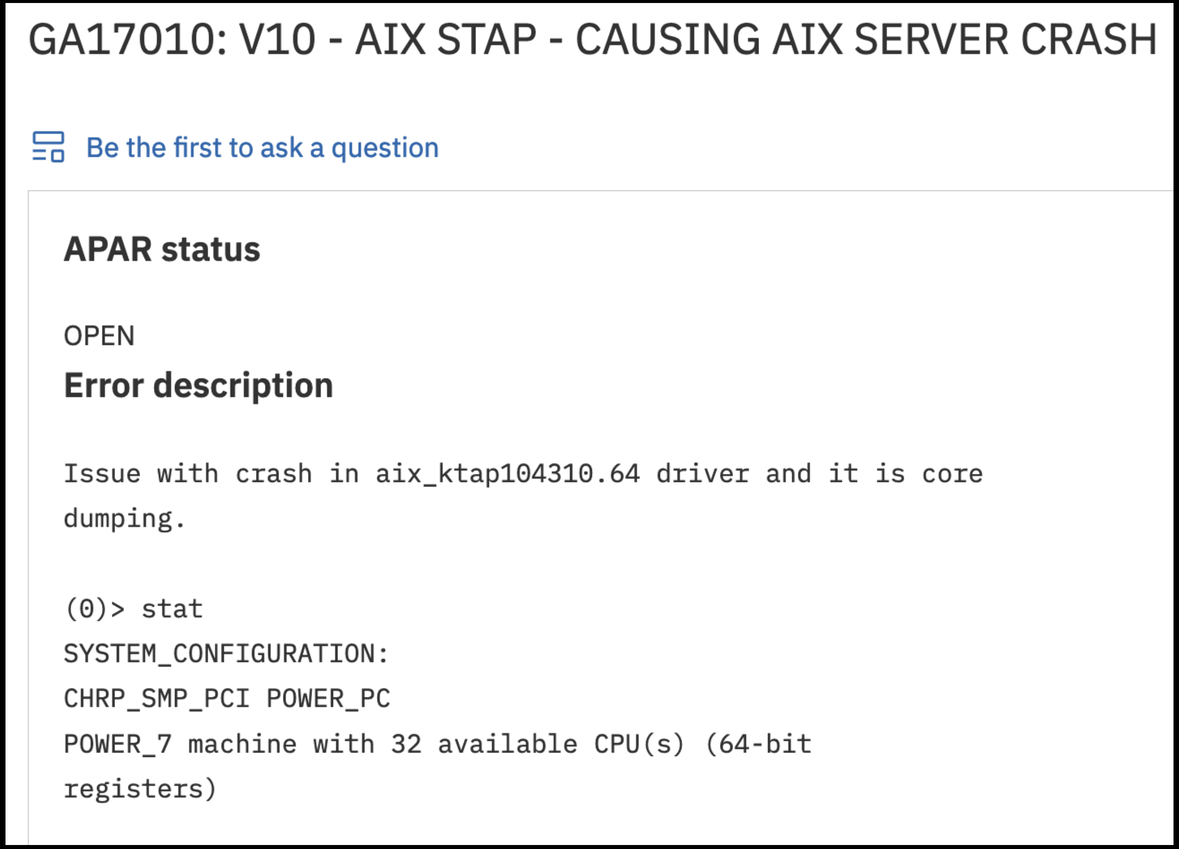
Slon command with sgate option. Use support store slon off to stop the capture after the problem is reproduced.

Server OS crash or hang

This problem can only be caused by Guardium if KTAP is loaded.

Logs to collect

- Server crash dump. Even more critical for these problems
- Server vendor analysis
- Guard_diag soon after the crash if possible
- If server can not boot at all, special steps are required. See main technote: https://www.ibm.com/support/pages/guardium-unix-s-tap-impacting-database-or-database-server-performance



GA17010: V10 - AIX STAP - CAUSING AIX SERVER CRASH

APAR status

OPEN

Error description

```
Issue with crash in aix_ktap104310.64 driver and it is core
dumping.

(0)> stat
SYSTEM_CONFIGURATION:
CHRP_SMP_PCI POWER_PC
POWER_7 machine with 32 available CPU(s) (64-bit
registers)
```

APAR GA17010

Summary

Summary

- “S-TAP impacts the DB or Server” issues have several main symptoms – S-TAP process crashing, High CPU or Memory usage, Database crashing, Latency accessing DB, Server OS crash
- Root cause of these issues (except latency) is usually defect in Guardium S-TAP combined with specific environmental factor
- Latency issues are usually caused by SGATE/QRW configuration that can be corrected by Guardium admin
- Latest S-TAPs and APARs should be checked for duplicate problems
- Timely collection of the correct logs is critical to resolving issues successfully when working with support
- Crash dumps and diag soon after the crash for crashing issues
- Vendor analysis for 3rd party product crashes
- Dumps and logs while the problem is happening for performance issues

- Use reference technotes from slide 5

Questions?