# Guardium Administration

Fourth Installment

## Fixing an Overwhelmed (down) Environment

## Handling Full Collectors

# #1 : Why Do Guardium Collectors Get Under Stress ?

# **Database Traffic is hectic by nature** and no one controls it. Therefore Guardium teams need to adapt to it.

# **Hectic traffic does put stress on appliances.** Here are the 4 major ones:

# **Signs of Hyper Variation of Traffic : Spikes**

- Large Variations on Eth0 Rec., Analyzer Rate, Analyzer Queue Length
- Spikes on increases in MySQL Disk Usage

# **Signs of Unbalanced Traffic : Overloads**

- Large differences among appliances on Eth0 Rec, Analyzer Rate, Logger Rate
- Large differences among appliances on System CPU Loads, MySQL Disk Usage

# **Signs of Reaching the Limits : in your Red Zone**

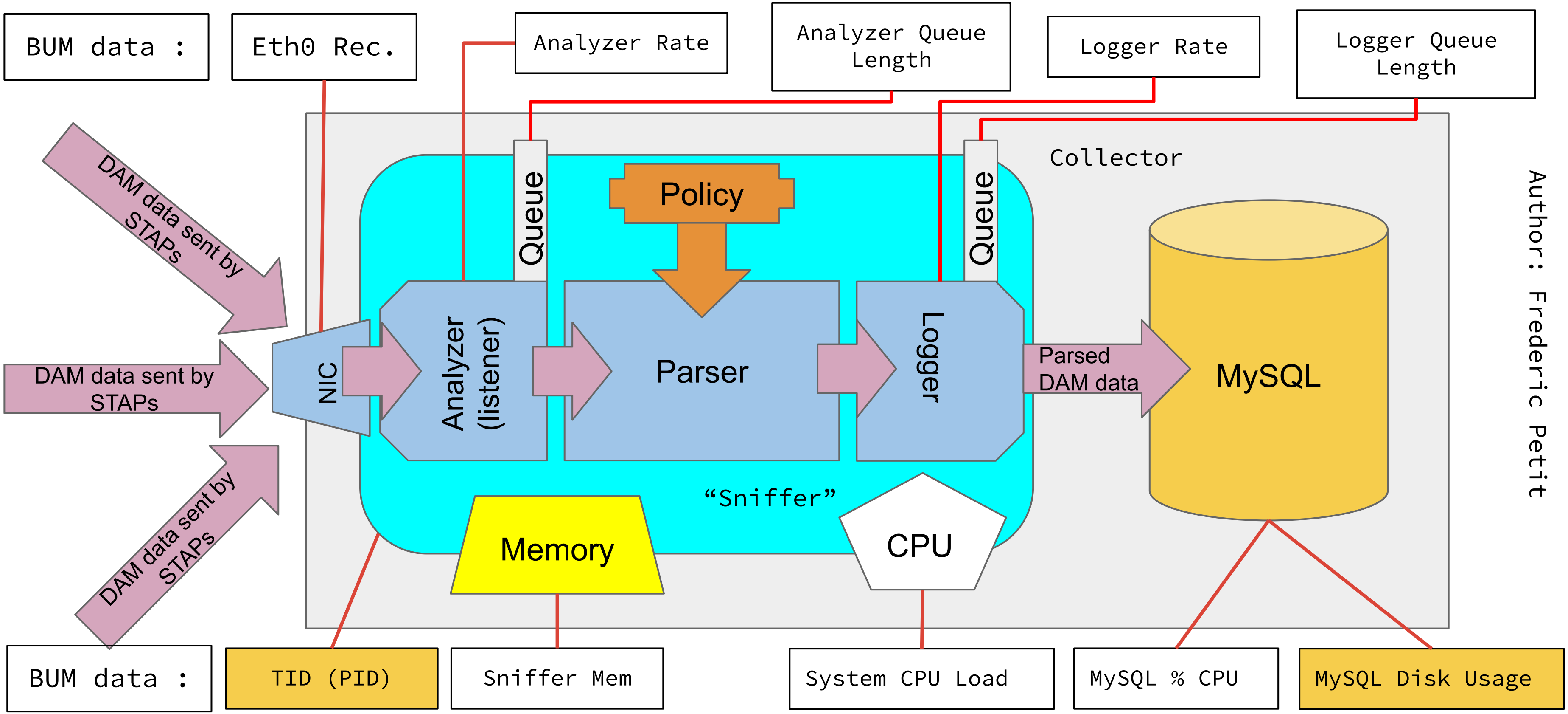
- Sniffer Memory close to ⅓ of total memory
- Mysql Disk Usage close to 90%

# **Signs of Being Beyond the Limits: you got outscored**

- Sniffer restarts frequently (many times a day)
- MySQL has reached 90% and the sniffer is down

Author: Frederic Petit

# Guardium Collectors Internal Architecture and the BUM



# Meaning of TID & MySQL Disk Usage

**TID : Process ID**

- Each time the sniffer shuts down and restarts (re-spawns) a new Process ID (TID) is generated
- The number of TID over a period of time tells us how many times the Sniffer shut down
- A sniffer shutdown and restart is a sign of major stress if it is repeated frequently

**MySQL Disk Usage @ 90%**

- When the DB reaches 90% full, the sniffer shuts down permanently
- The collection of traffic STOPS
- Agents will be redirected to a Fail-Over(FO) Collector if set up
- If 2 collectors reach 90% and their agents use the SAME FO, this FO is going to receive the traffic of 2 collectors and be overwhelmed

Both, frequent shut downs and restarts of sniffer and Full DB MUST be avoided

# The case of ALP

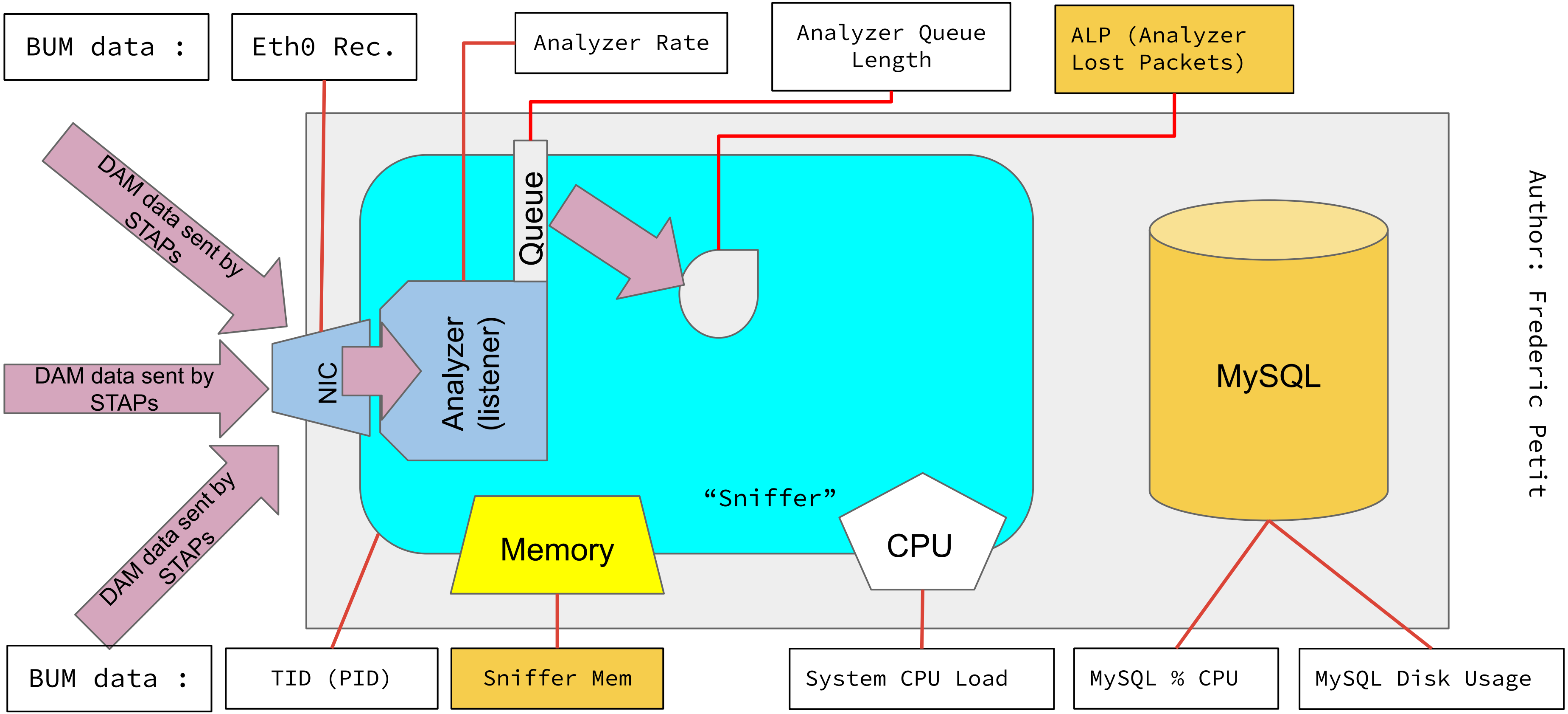
ALP : Analyzer Lost Packet - As the name says, when the Analyzer loses packets

ALP > 0, actually means DEEP trouble

Here is why :

- When the sniffer is asking for memory over a ⅓ of the total memory, the nanny (watchdog) is supposed to kill it.
- When the sniffer gets killed, if nothing is done, the data in memory AND in the queue get lost.
- To avoid this, the nanny,prior to killing the sniffer, makes it write the data into an OS file on disk.
- When the sniffer restarts, the process called Flat Log Process, if activated, feeds the sniffer with those data. That way there is NO Analyzer Lost Packet and NO traffic is lost.
- But the size on the file on the disk is limited too, and if that limit is reached, NO packets can be written anymore and therefore get lost, making the ALP > 0
- You NEVER want to let this happen.

# Guardium Collectors Internal Architecture and the BUM



Author: Frederic Petit

# Recognizing the System Went Beyond the Limits

- Guardium Appliances like ANY Computing system has limits
- Don’t let them get crossed
- There is no solution when the system goes beyond the limits
- Only option is fixing the machine which is difficult and resources consuming
- Proactivity as described in Installments I, II & III should prevent going beyond the limits.

# Demo

# The End

info@context22.com