Guardium Administration

Third Installment

Maintaining a Growing Environment

Handling Growing Traffic on 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 ½ of total memory
- Mysql Disk Usage close to 90%

 # Signs of Being Beyond the Limits: you got outscored

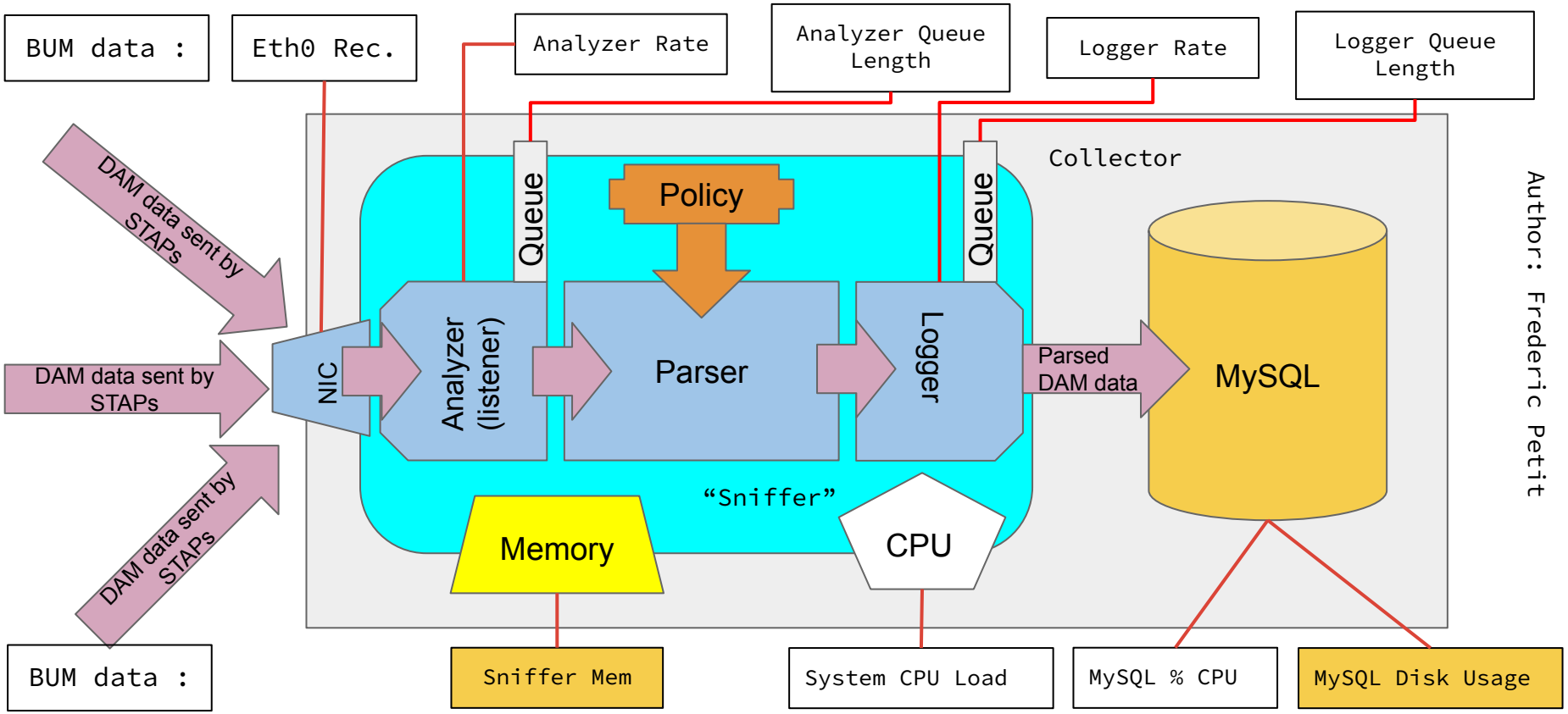
- Sniffer restarts frequently (many times a day)
- MySQL has reached 90% and the sniffer is down

Author: Frederic Petit

How to detect Growing Traffic Hitting Appliances ?

- In the detection of consistently overloaded appliances we used **Averages**
- To detect growing traffic we need to use **Time Series**, meaning evolution of variables over time.
- An appliance may be overloaded but under a trend of reducing amount of traffic. In that case the overload may take care of itself
- An appliance may not be overloaded at this time, but the trend the appliance is under, is a growing amount of traffic. This appliance may become stressed
- The 2 variables we recommend to look at are : Sniffer Mem and MySQL Disk Usage

Guardium Collectors Internal Architecture and the BUM



Meaning of Sniffer Mem & MySQL Disk Usage

Sniffer Mem

- Global Memory of the Collector is divided into 3 equal parts:
  - ⅓ for the OS
  - ⅓ for the MySQL DB
  - **⅓ for the Sniffer**
- The sniffer is not allocated that amount of memory by default
- The Sniffer “requests” additional as it goes.
- **Within a limit :** If the Sniffer makes a request that would give it more than ⅓ , the nanny (a watchdog) will kill it
- The sniffer rarely “releases” memory. Therefore the memory used by the sniffer always grows.
- You want to keep it UNDER a 1/3

MySQL Disk Usage

- For a given Retention Period, the amount of traffic handled by a collector is stable if MySQL size is stable
- A growing size of MySQL is a good indication of growing amount of traffic being handled by the Collector
- Reducing the Retention Period is a temporary solution

Options to Address Growing Traffic

Sooner or later, you will need to add Collectors

Demo

The End

info@context22.com