Guardium Administration

Second Installment - Part II.2 -

Maintaining a Balanced Environment

Handling Overloaded Collectors

#3.2 : How to Detect Contributing Servers/Agent

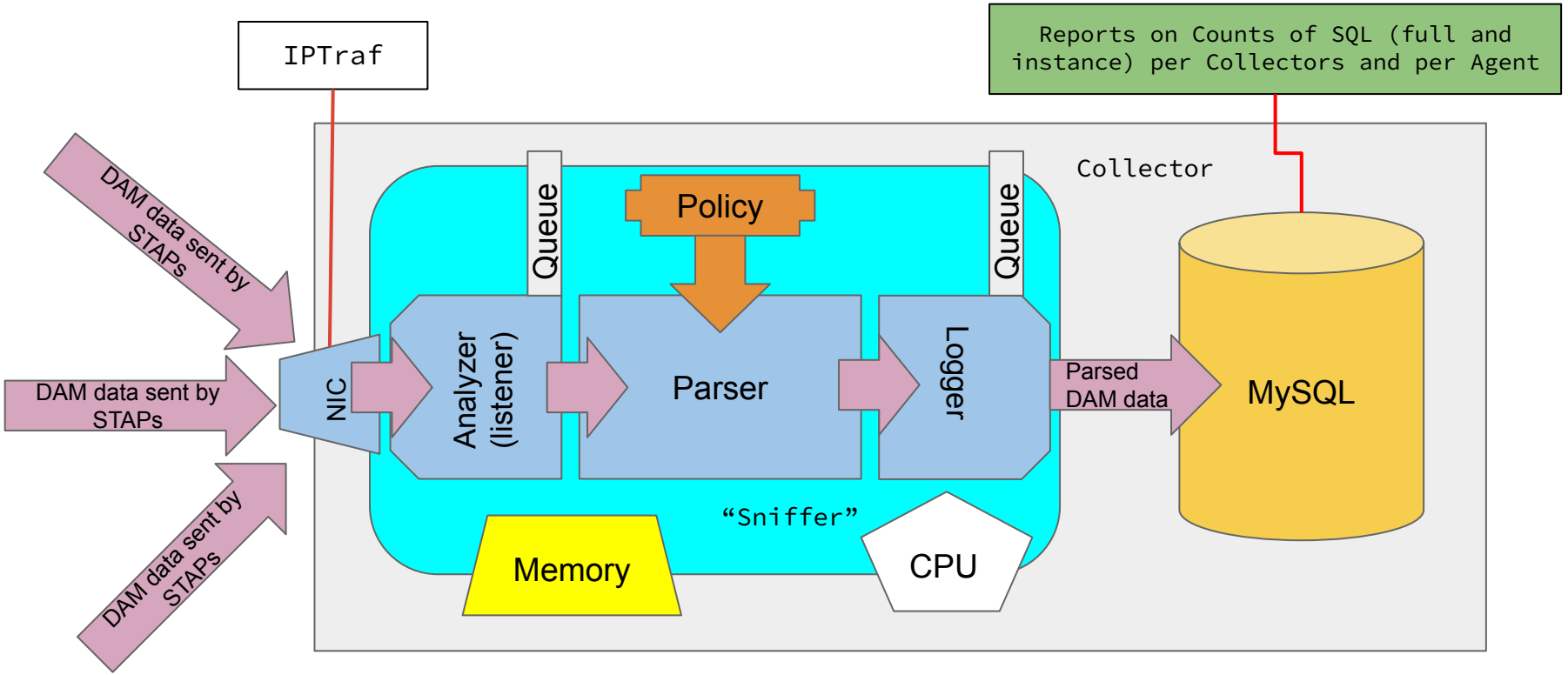
 # How to assess the contribution of each Agent ?

- **Unfortunately** the BUM gives ONLY global statistics -
- **Only 2 places : NIC and MySQL (see diagram)**
  - Option #1 : At the NIC level : IPTraf from CLI
  - Option #2 : At the MySQL Level : Statistical Reports counting the number of SQLs

 # What to do ?

- Do nothing is **rarely an option** in this case
- **Re-Assign** some Agents to underloaded collectors to reach a more balanced environment
- **Potentially** Activate the **E**nterprise **L**oad **B**alancing, but be careful, this too requires close monitoring and speedy reaction in case of trouble

3.2 : Assessing Contributing Agents (Not in the BUM)



Author: Frederic Petit

Demo

Option #2 : Count of SQLs into MySQL - By Product of DAM

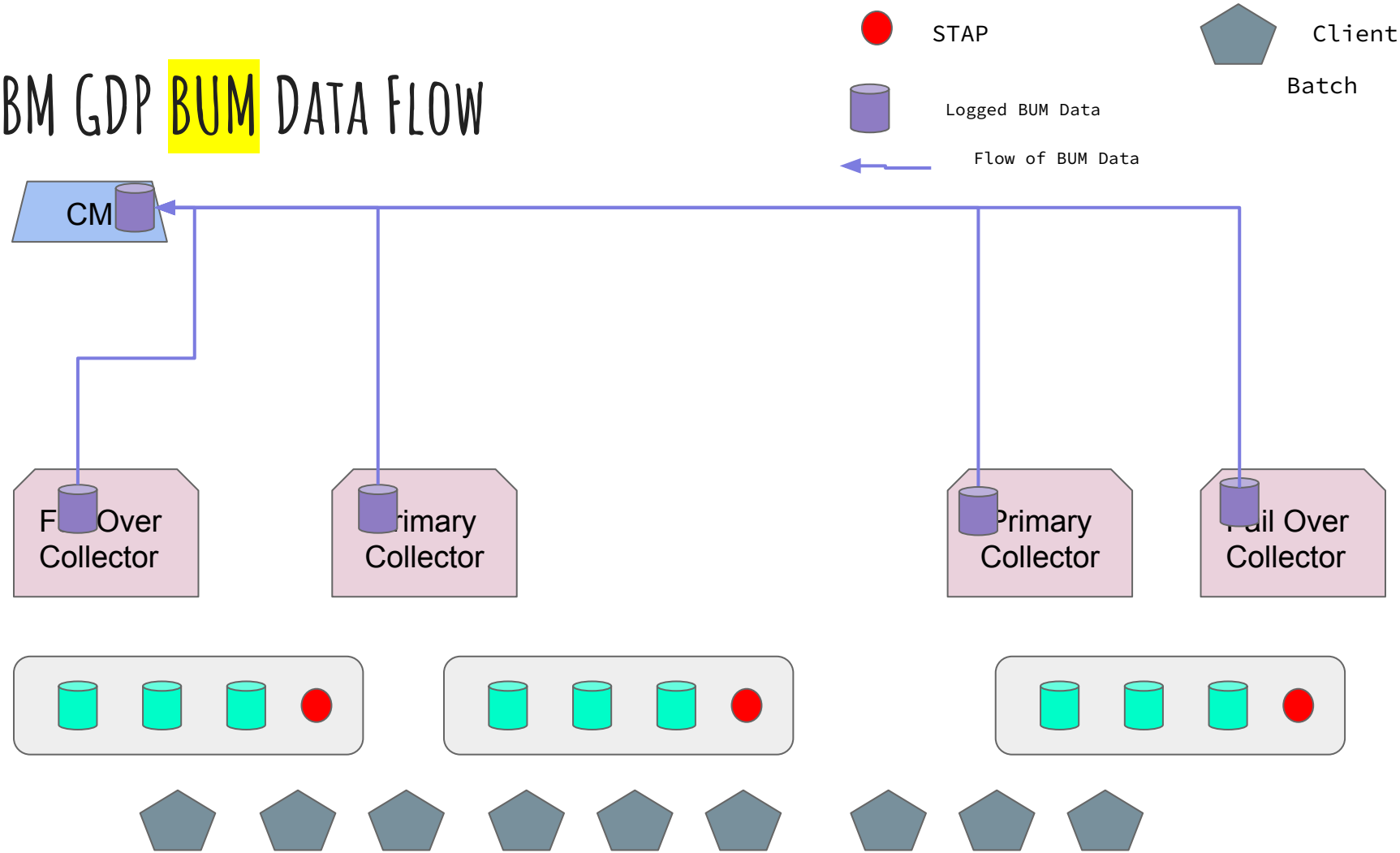
This is the tricky part :

- Requires centralization of the DAM data into an ELK instance
- Much heavier than centralizing and enriching the BUM

Our Solution :

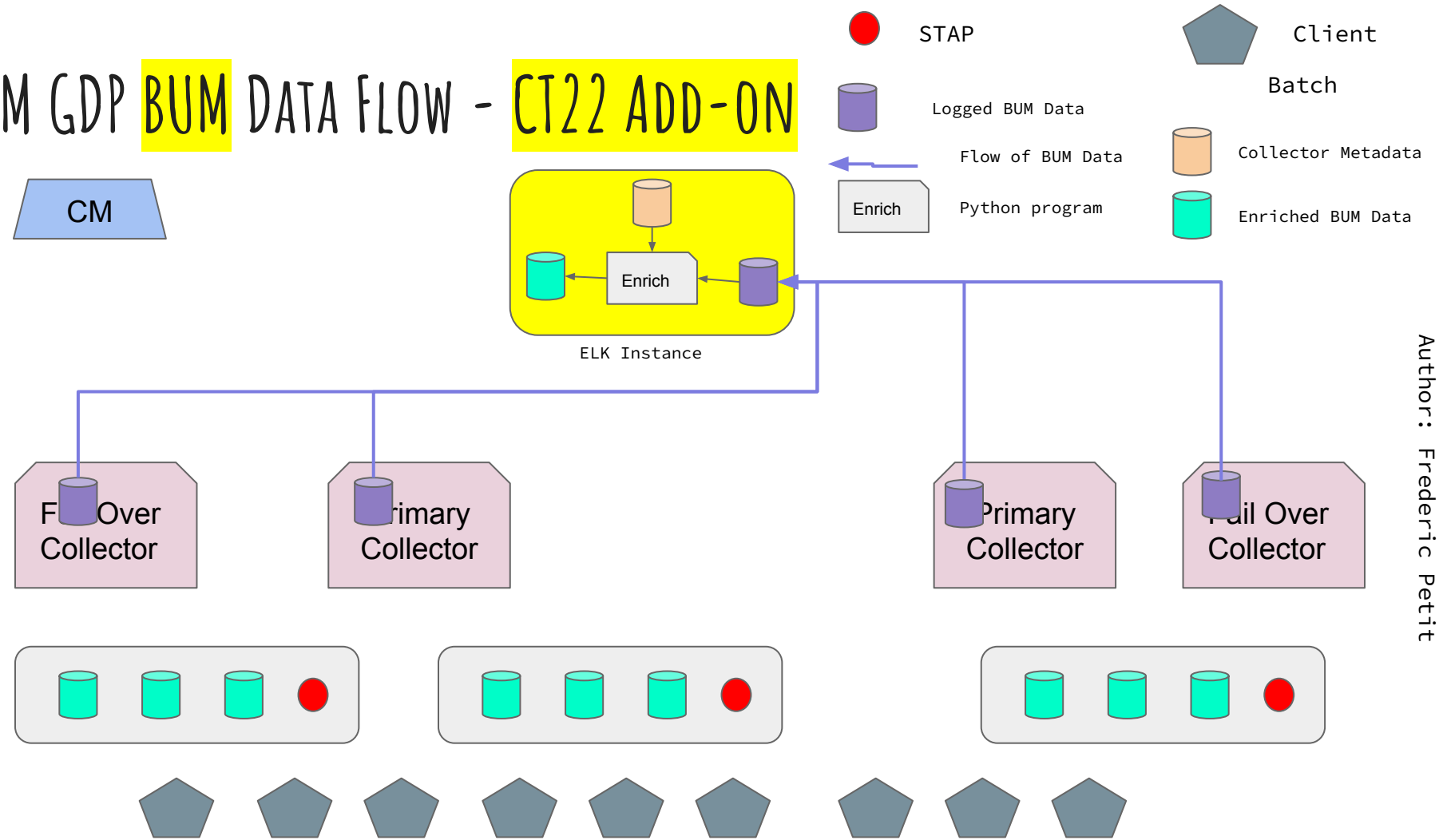
- Export PART of the DAM Traffic and send it to a ELK instance thru the **CT22T Enrichment process (see next slides)**

IBM GDP BUM Data Flow



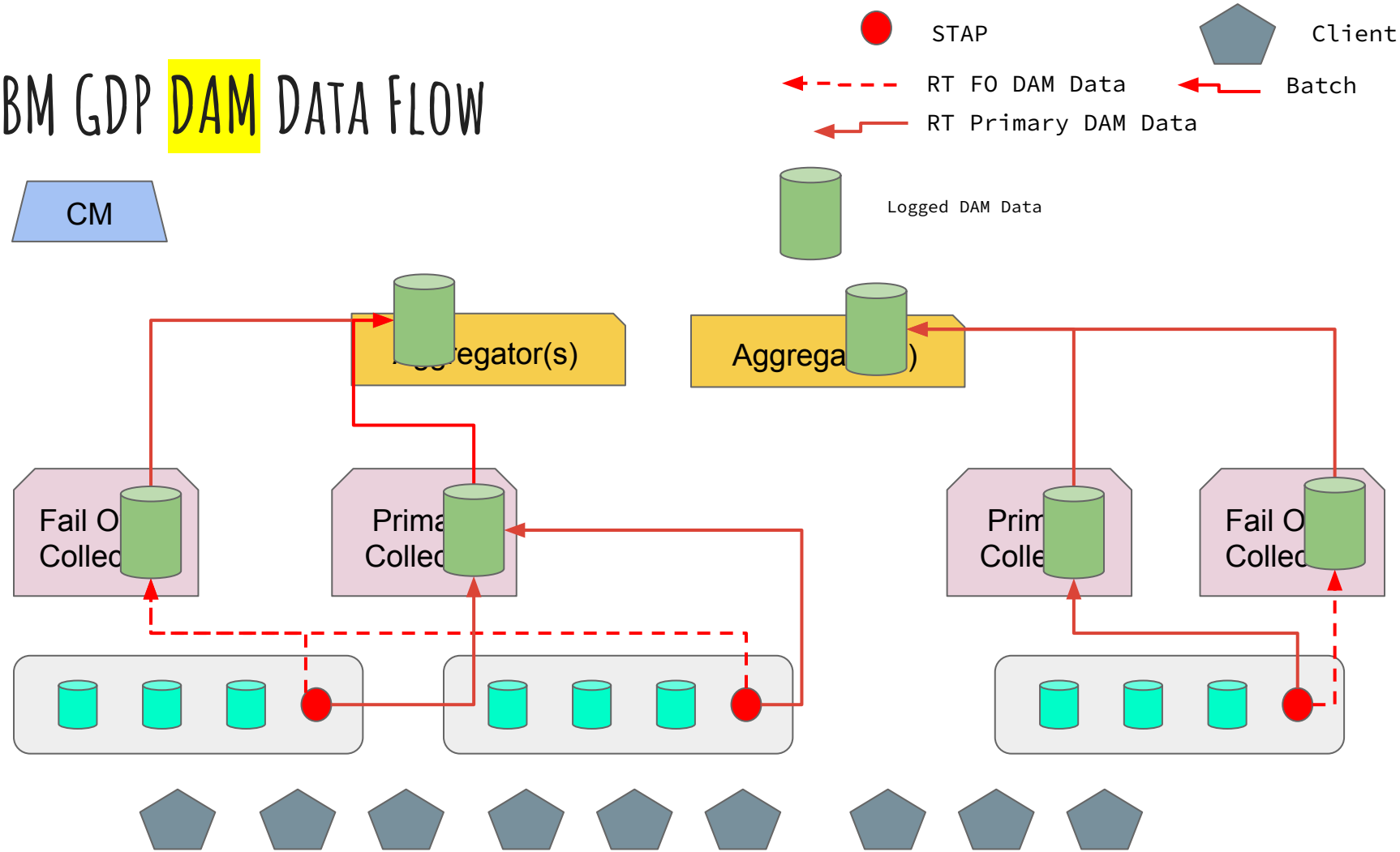
Author: Frederic Petit

IBM GDP BUM Data Flow - CT22 ADD-ON



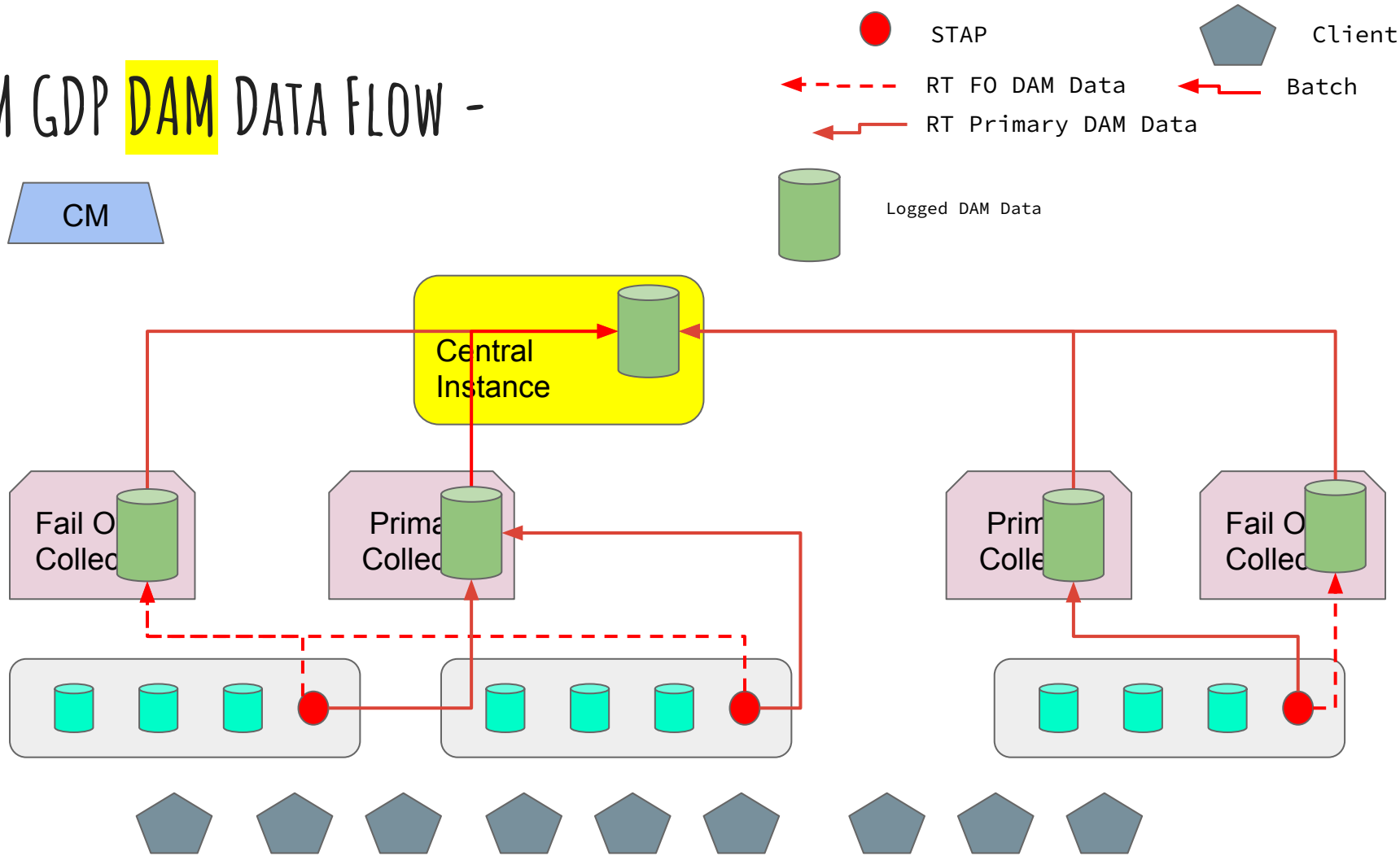
Author: Frederic Petit

IBM GDP DAM Data Flow



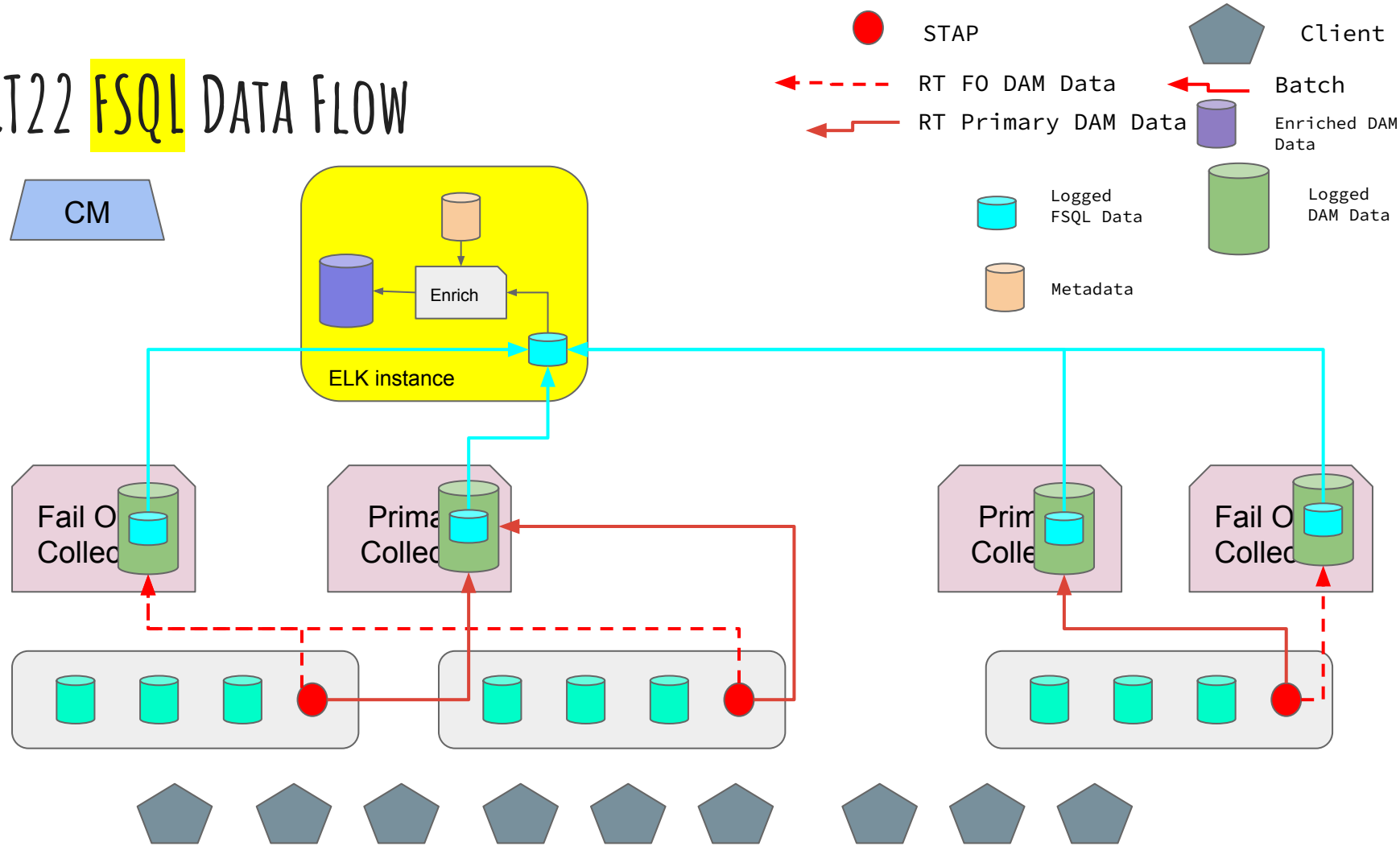
Author: Frederic Petit

IBM GDP DAM Data Flow -



Author: Frederic Petit

CT22 FSQL Data Flow



Author: Frederic Petit

FSQL vs. DAM Data

DAM Data in Guardium

- **Sessions** : (logins + connection time)
- **Instance** : SQL with a count per hours and per session
- **Full SQL** : Individual SQLs
- **Exceptions** : Failed Logins + SQL errors

Full SQL in CT22

-

-

- **Part of Full SQL :** SQLs extracting sensitive data

-

FSQL in CT22T is only a part of Full SQL but is representative enough to get the proportion of Traffic sent by each Agent

Why Did We Originally Develop this FSQL Enrich Module ?

The FSQL Enrich Module was not developed originally to help managing Guardium appliances and their load

The help to **managing the load of appliances** is only a by-product of this Module

The FSQL Enrich Module purpose is to offer a **workbench for security analysis** of the DAM traffic

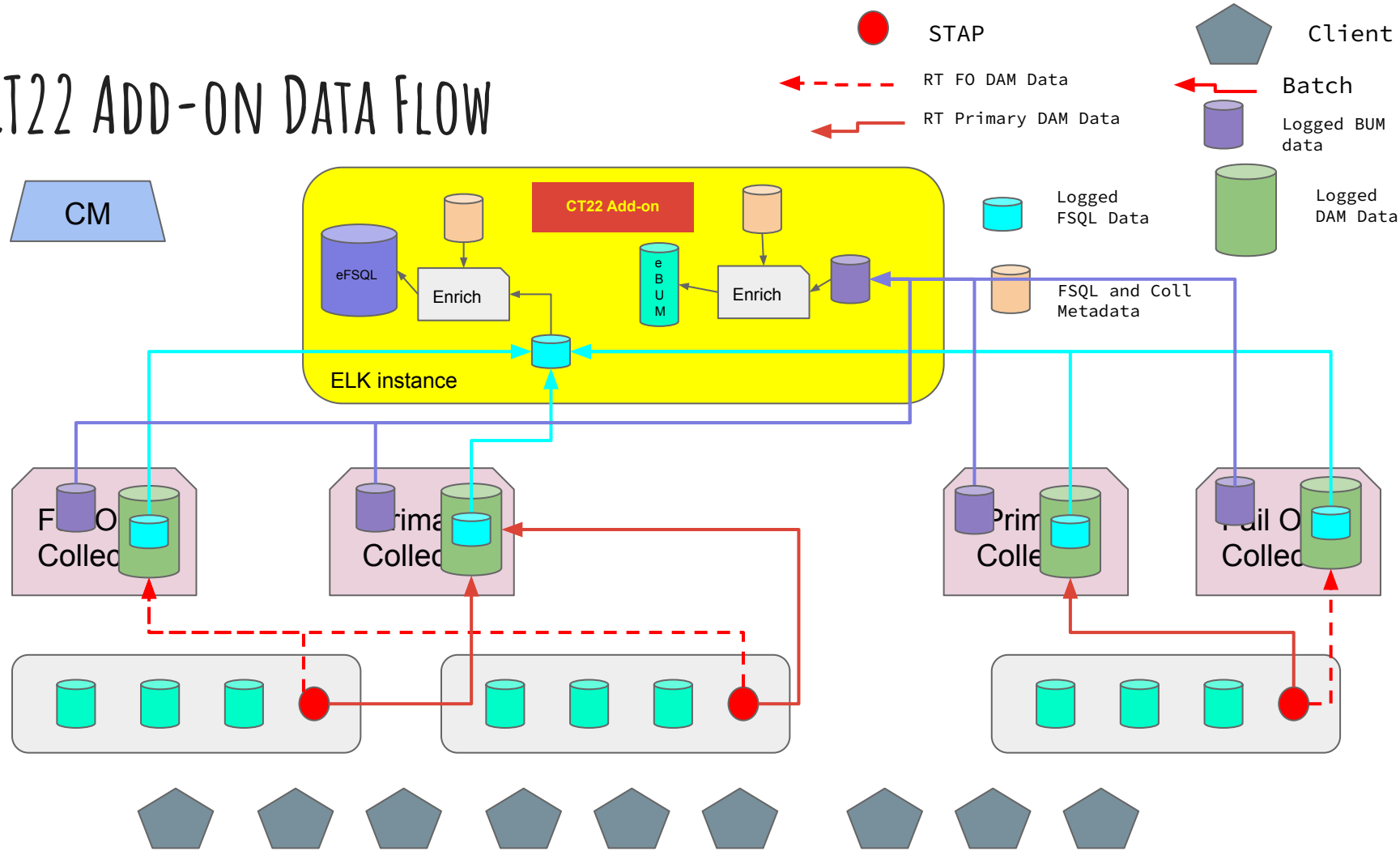
Basically by installing this add-on, not only you can ease the management of your appliances but also start security analysis

It’s 1 module for 2 functions

The Security Analysis functionality was presented in several articles on LinkedIn and in videos on the Context22 YouTube channel

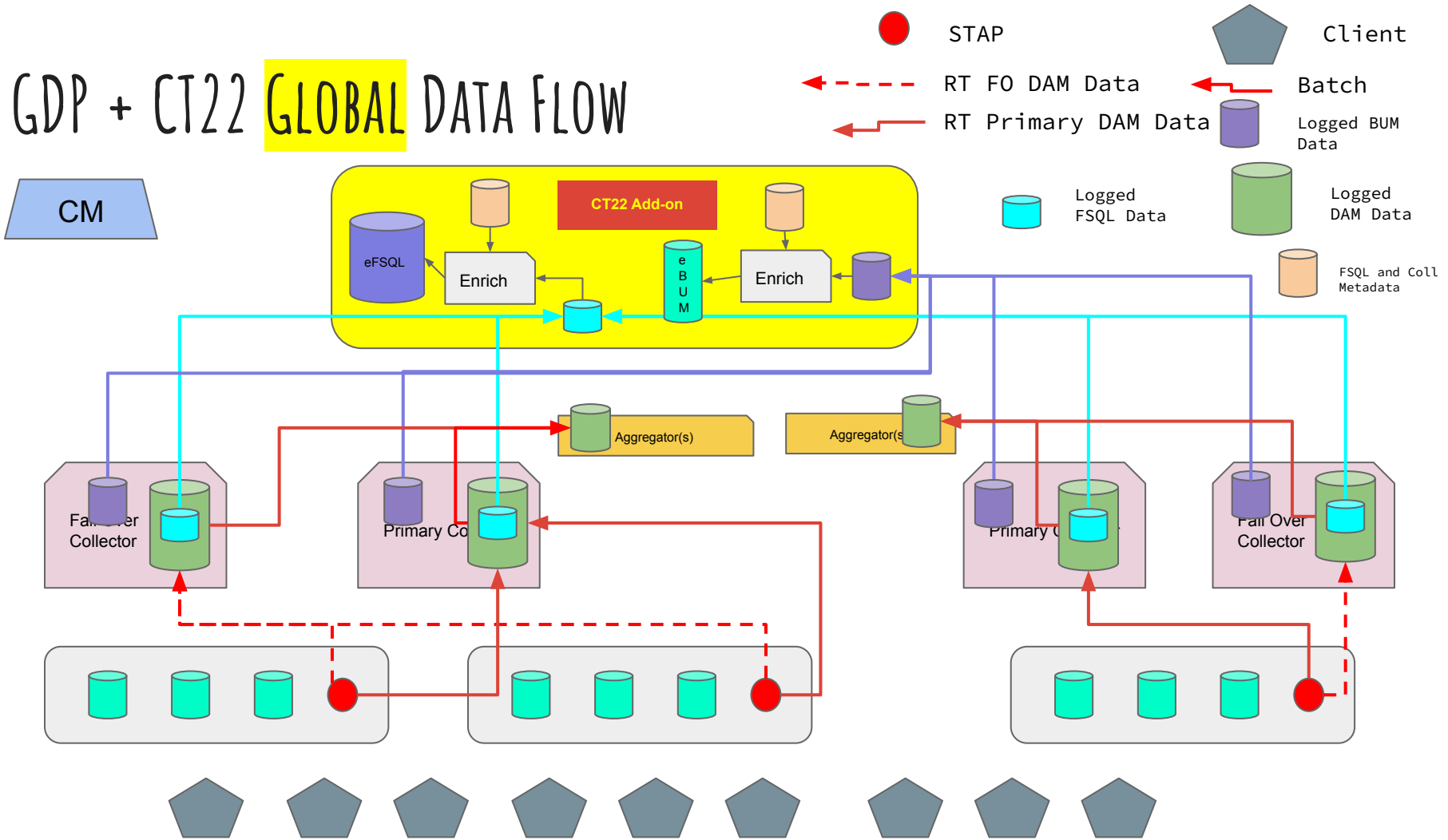
We keep developing this security capability in particular around Time Series Analysis and Predictive Analytics

CT22 Add-on Data Flow



Author: Frederic Petit

GDP + CT22 GLOBAL DATA FLOW



Author: Frederic Petit

Functionalities of the [GDP + CT22 add-on] Components

Components	Functionalities	
Guardium Agents	Capture Traffic	
Guardium Collectors	Parse and Store Traffic	
Guardium Aggregators	Reporting / Auditing	
CT22 Add-on Enrich BUM	Appliances Management	
CT22 Add-on Enrich FSQL	Appliances & Agents Management	Security Analysis of the DB Traffic
Guardium CM	Configuration of Appliances & Agents	

Architecture Options

Approach : Keep the Aggregators - Not moving to SonarG/Insights -

CT22 add-on as add-on to GDP:

- Get a quick return on Appliances admin due to ease of deployment of the Add-on
- Aggregators stay centered on reporting for auditing
- Platform for Security analysis
  - Enrich FSQL makes FSQL meaningful
  - Threat detection becomes available
- CT22 add-on : gateway to security analysis

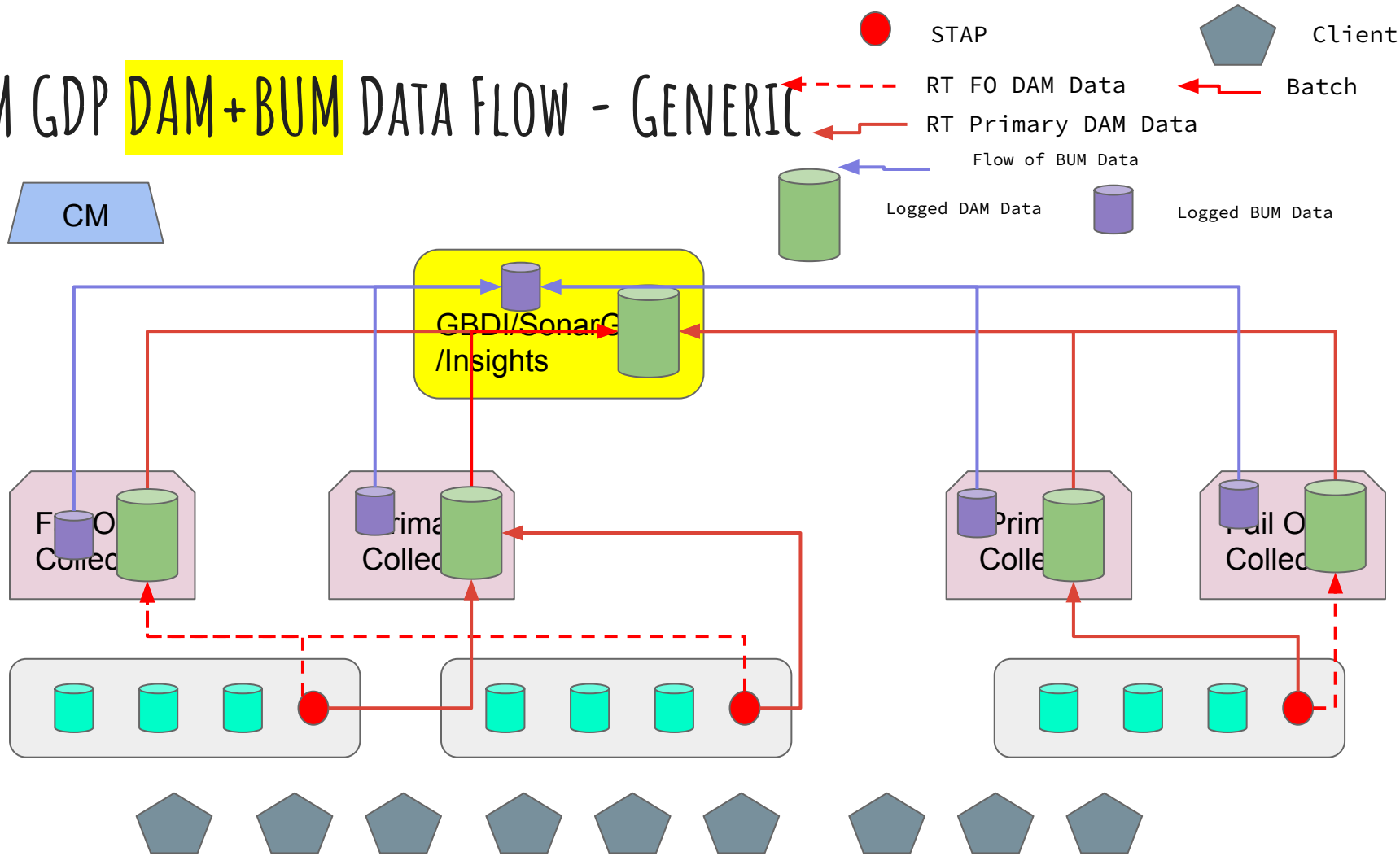
Approach : CT22 Add-on as path to Sonarg/Insights

- Prototype the migration
- Testing Enrichment
- Get a quick return on Appliances admin due to ease of deployment of the Add-on
- Enrichment can be ported to Sonar and/or Insights

The End

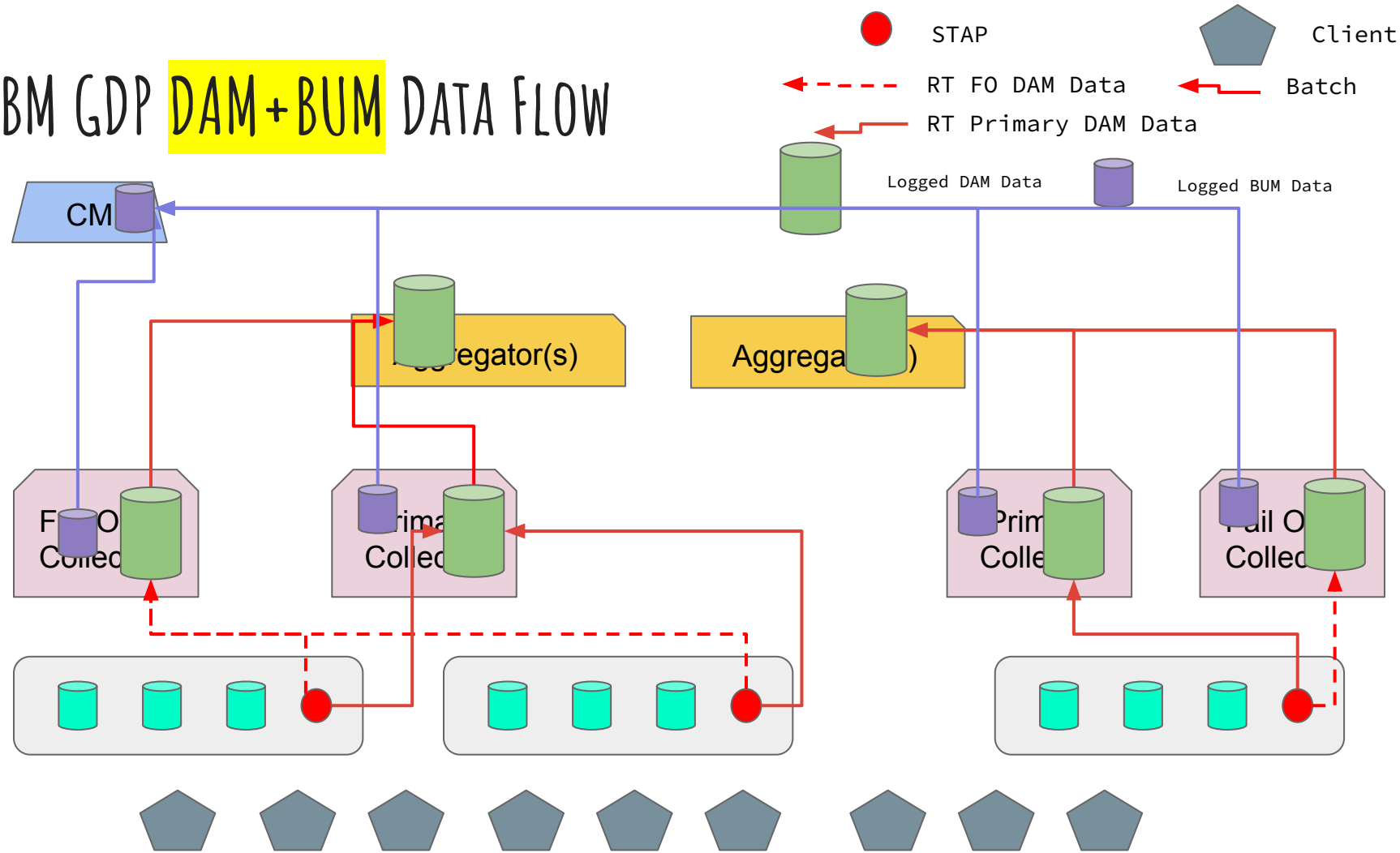
info@context22.com

IBM GDP DAM+BUM Data Flow - Generic

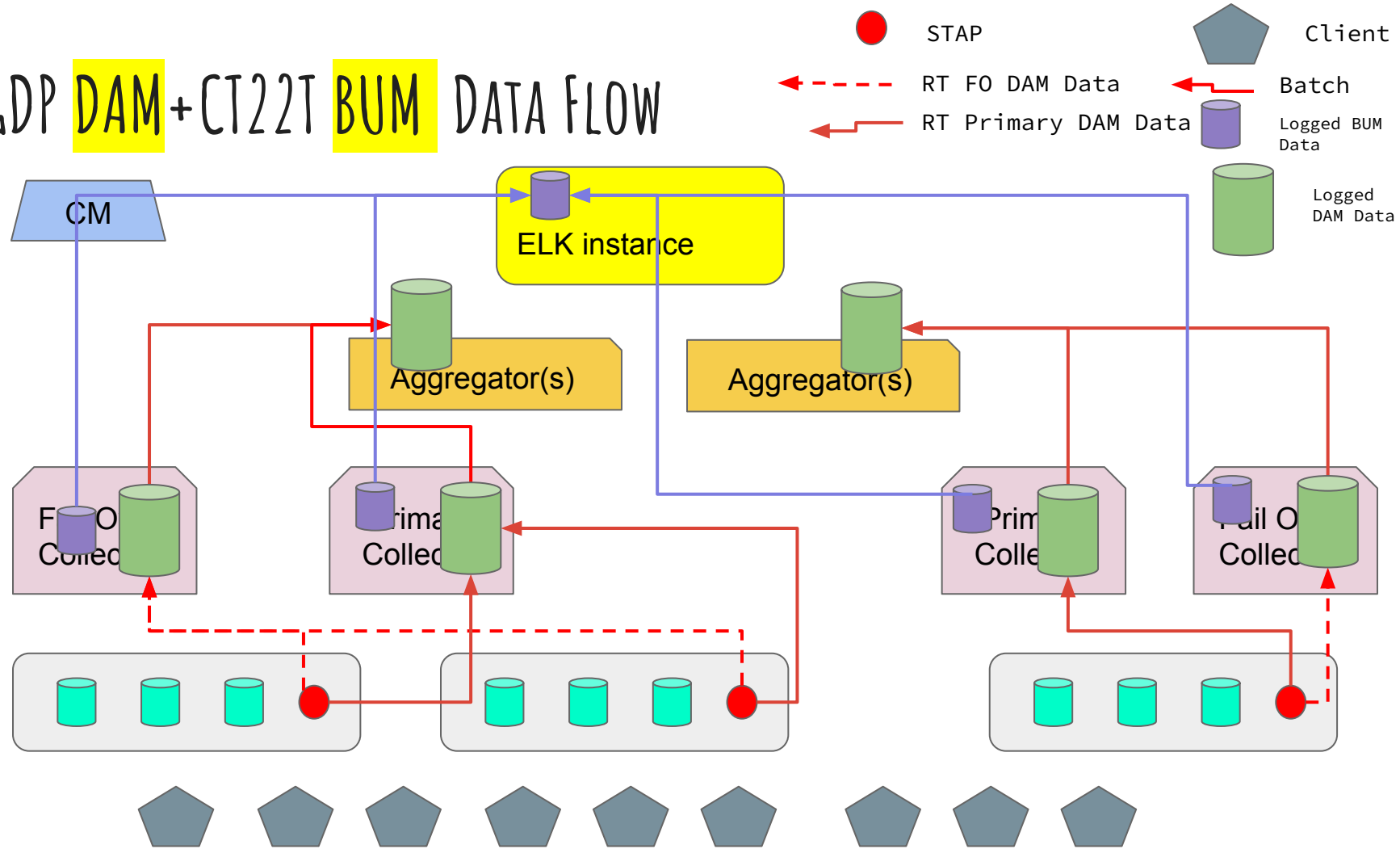


Author: Frederic Petit

IBM GDP DAM+BUM Data Flow

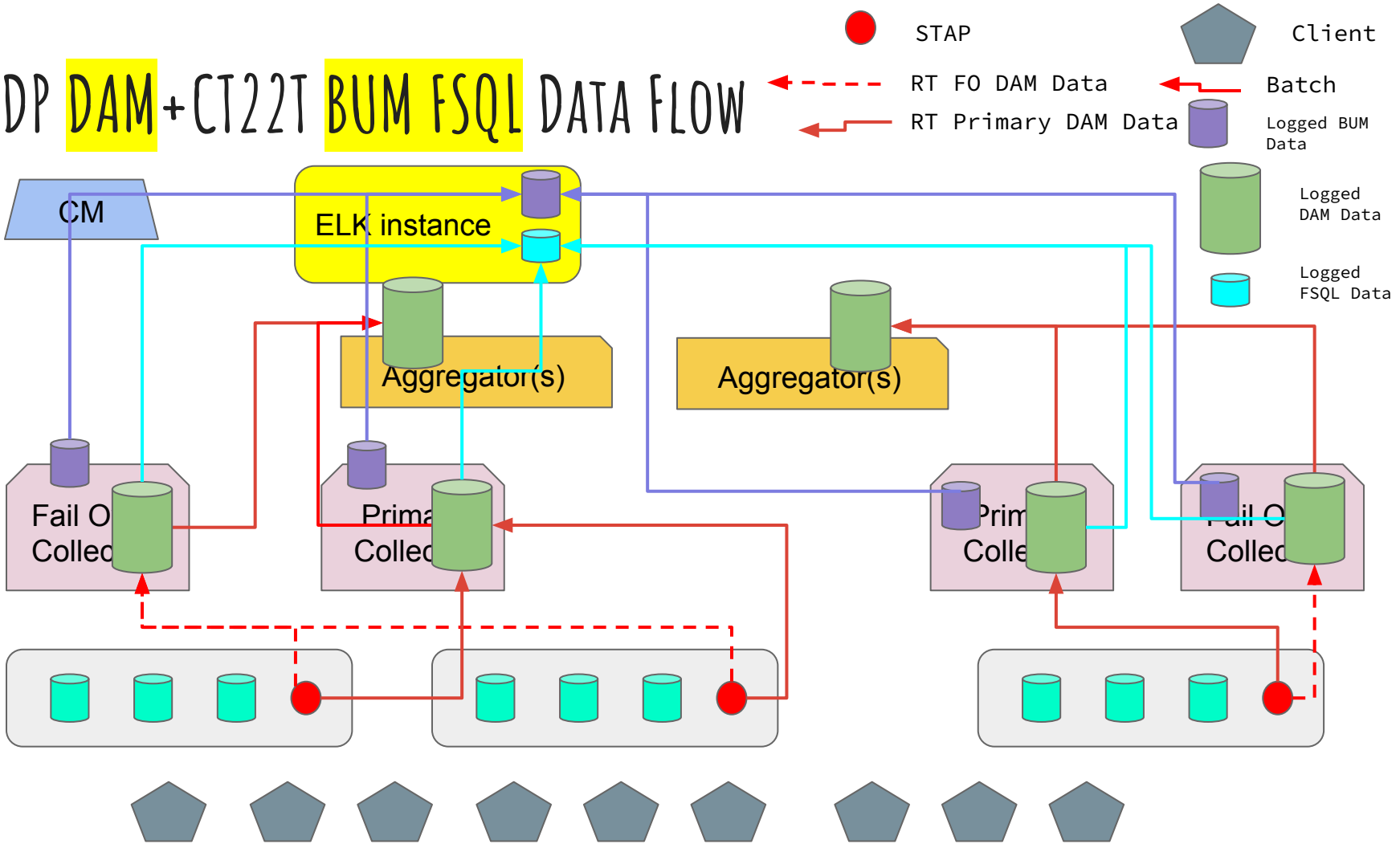


GDP DAM+CT22T BUM Data Flow



Author: Frederic Petit

GDP DAM+CT22T BUM FSQL Data Flow



Author: Frederic Petit

Demo