Guardium Administration

Challenges and Options

Dec 15 2022 Sessions

CONTEXT 22 TECHNOLOGIES

Agenda

- Introduction by Omar Habbal, CEO of Context22 Technologies
- Technical Presentation by Frederic Petit, CTO :
  - Challenges managing Guardium Collectors
  - The importance of relying on the BUM data
  - Using DAM data to enhance the management of Guardium appliances
  - A path to lightweight and small footprint alternative to Aggregators
- Presentation of current offering and directions by our CEO
- Q&As

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 Volatility of Traffic : Spikes**

# **Signs of Unbalanced Traffic : Overloads/Underloads**

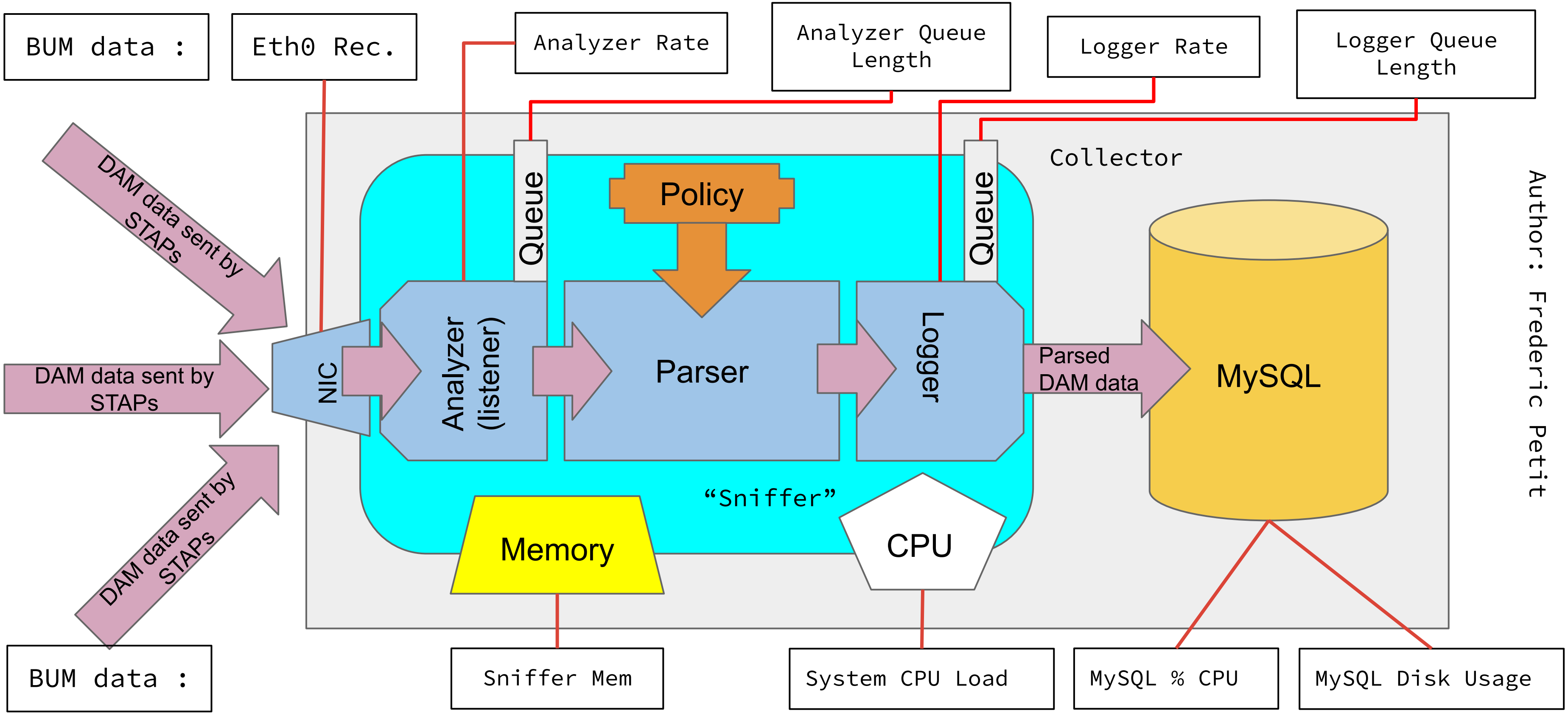
# **Signs of Reaching the Limits : in your Red Zone**

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

Author: Frederic Petit

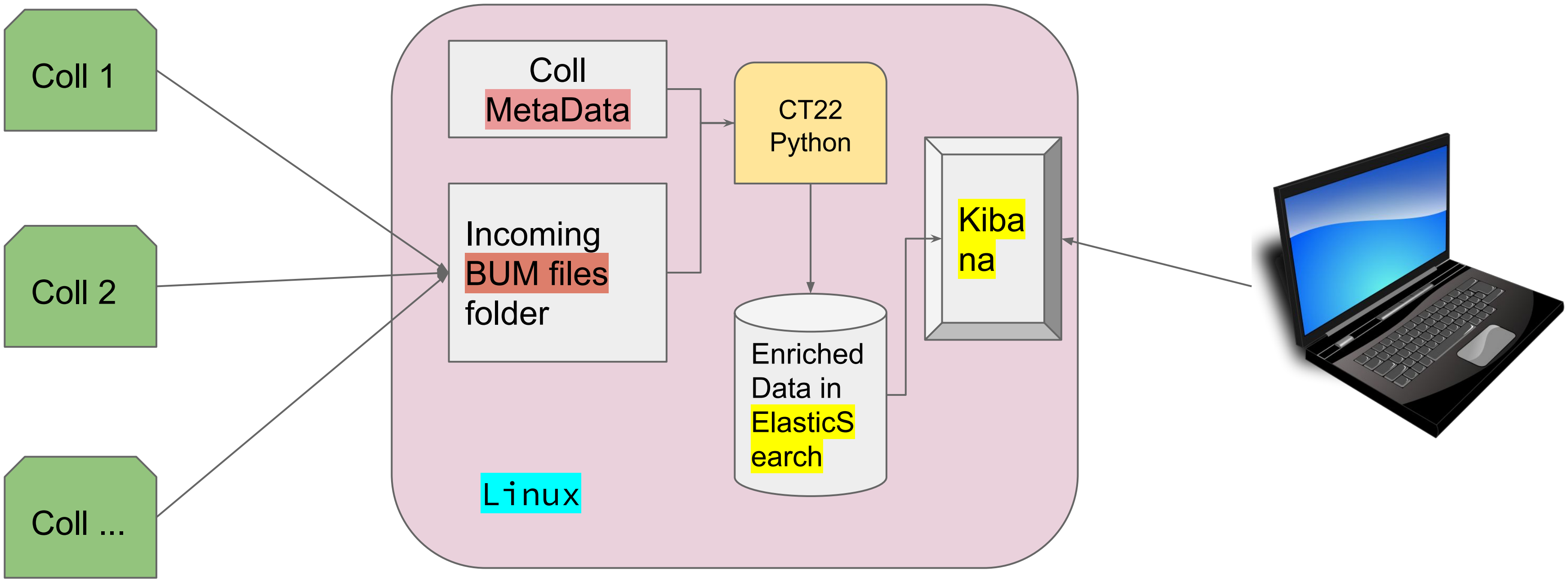
Importance of the BUM and its Enrichment with Collector Metadata

Guardium Collectors Internal Architecture and the BUM



Author: Frederic Petit

CT22 Overall Architecture : ElasticSearch, Kibana, Python, Linux



Why ELK and OpenSource Python programs ?

- Why ELK ?
  - Widely deployed - Like a Standard - Skills wisely available -
  - ELK = Data Engineering - Not a concern anymore - Companies may already have an ELK environment and just piggyback on it - No system management concern as managed by the ELK team - May be cost effective
  - ElasticSearch is quite efficient
  - Kibana is one of the best Analytics GUI with a lot of versatile capabilities
- Why OpenSource Python programs ?
  - Standard -
  - Non-proprietary system - Long-Term guarantees of sustainability
- Why Linux : OpenSource
- What about the Cloud ? Under Development

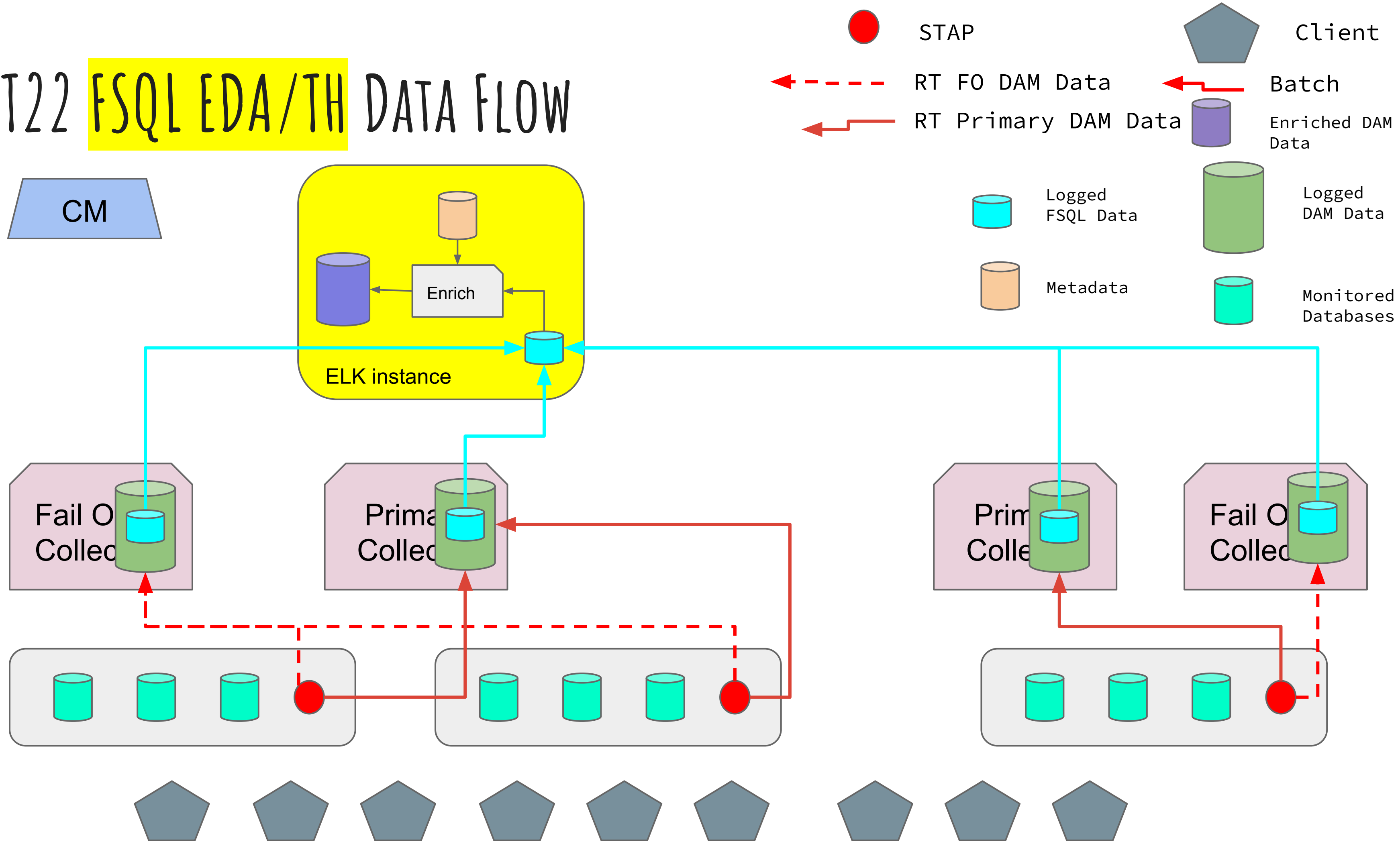
BUM
Quick Demo

Using DAM Data for the Management of Guardium Appliances

Re-Using a Functionality Developed for Threat Hunting

- CT22T developed a Functionality for EDA/Threat Hunting
- Description:
    - Taking part of the Full SQL data and Enrich them
    - Upload them into ES
    - Perform Exploratory Data Analysis (EDA) with Kibana by “playing” with the Metadata
    - EDA = Threat Hunting
- This Feature can be re-used or piggybacked for Guardium Appliances Management by providing volumes information on Agents which the BUM cannot provide

CT22 FSQL EDA/TH Data Flow



Author: Frederic Petit

Value and Challenges

Values

- Provide Volume Data per Agents
- Act as a Sample:
  - Representative enough (we need ranking more than proportion)
  - Smaller Amount of Data

Challenges

- Smaller than Total Full SQL as but potentially still large
- Volumes :
  - BUM : 1440 records a day per collectors
  - FSQL : Possibly several tens of thousand records per day and per Agents
- More Challenging in terms of Volumes for Guardium Administration than the BUM

You should do Threat Hunting as well

FSQL
Quick Demo

A Path to Threat hunting

Enriched FSQL
Quick Demo
Threat Hunting

Demo - plan -

A Whole demo next month with Metadata, Time Series, Confidence level computation, Predictive Analytics, anomalies detection, outliers and more

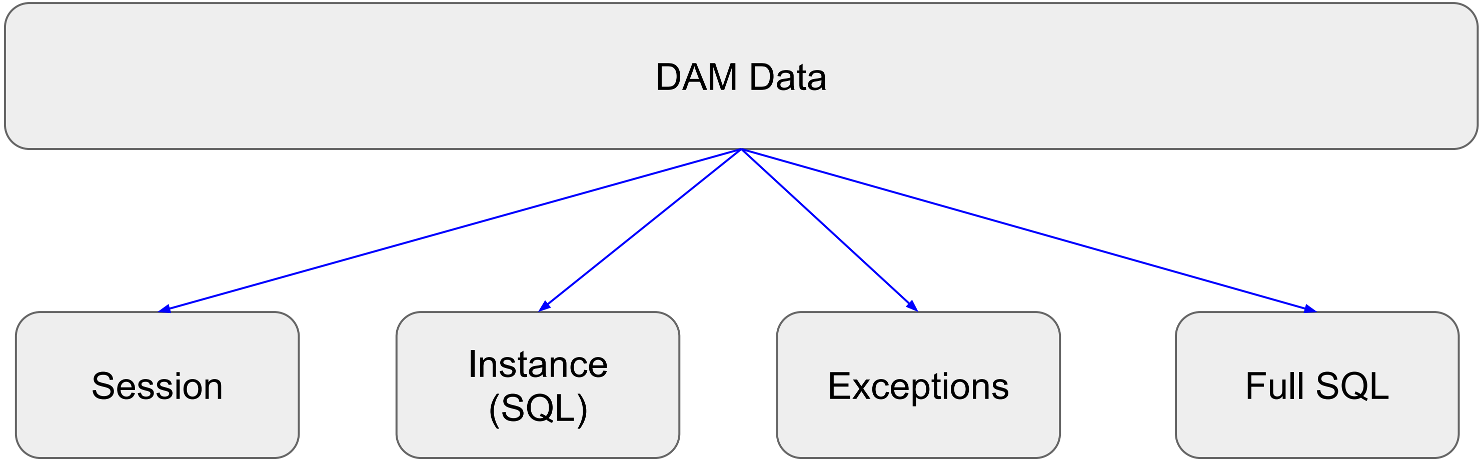
See also my YouTube Channel Context22 for numerous videos

Tentative Date : 3rd week of January

- For now :
  - Enriched Full SQL Index
  - Metadata
  - Threat Hunting

A Path to Light weight and Small Footprint Alternative to Aggregators

The 4 Components of the DAM Data

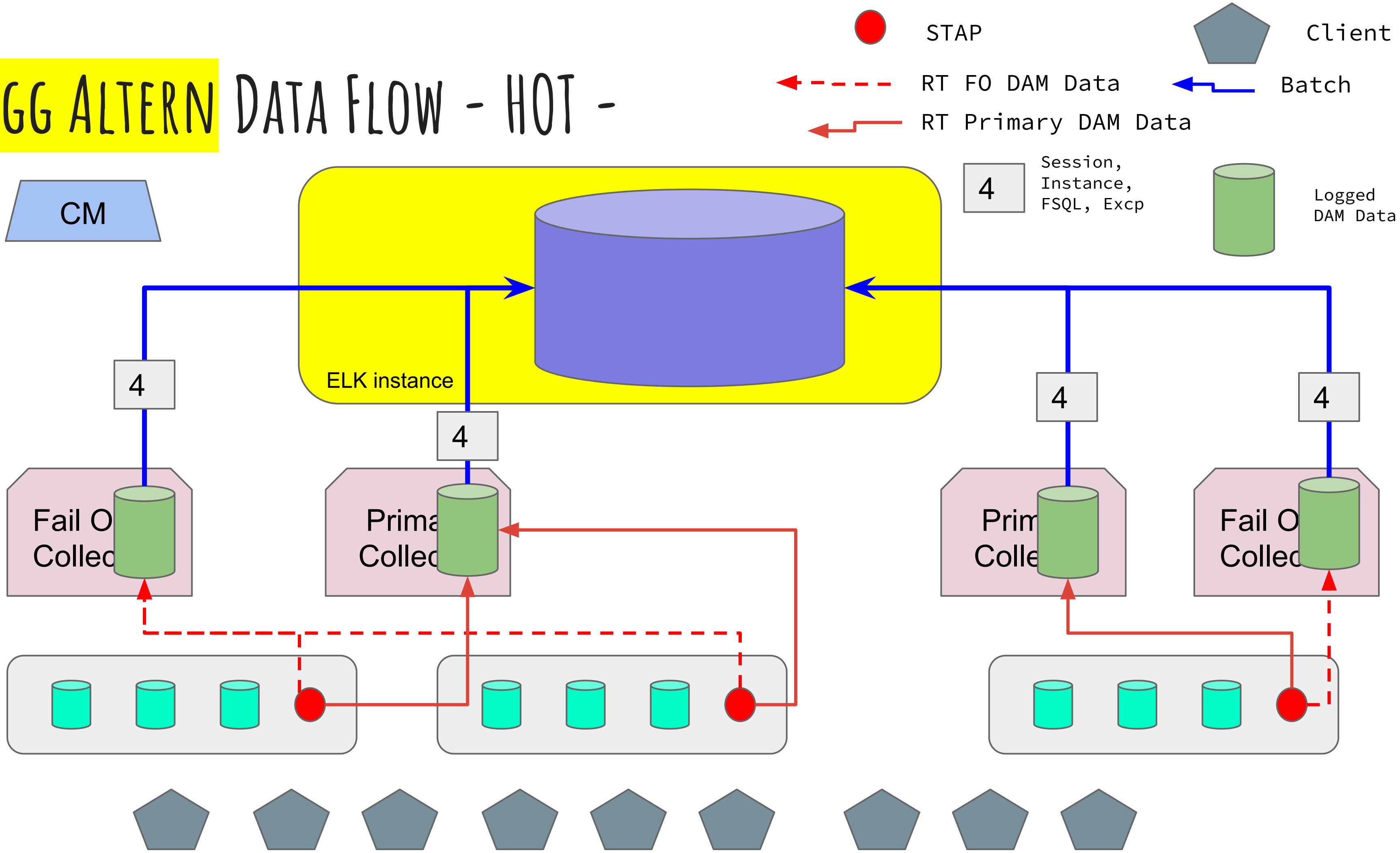


The 4 Components can be transferred to the DW Separately using the standard Guardium Data Mart feature

Features of an Alternative to Aggregators

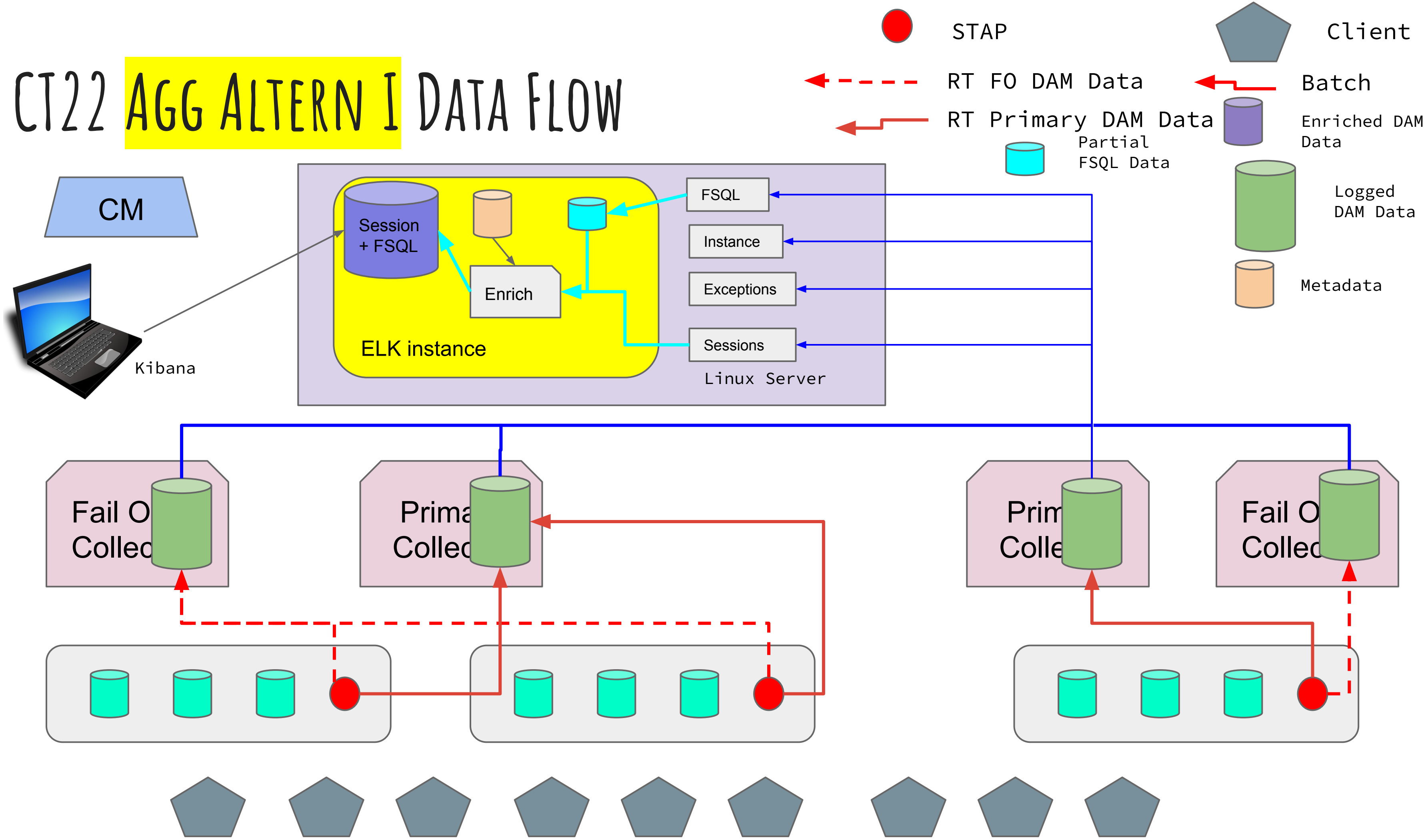
- **Main Idea :**
    - **There is NO NEED for keeping on-line ALL DAM Data in a DW (here ES) as needed only occasionally by Auditors**
    - **We can leverage the EDA/TH Capability to build a Lightweight Alternative to Aggregators**
- **HOT vs. WARM**
    - HOT : ALL DAM Data uploaded into a DW (ES)
    - WARM : Not ALL DAM Data uploaded into a DW BUT ready to be easily
- **WARM :**
    - Delaying the Upload (w/ or w/o enrichment) of the DAM data for when the need arises
    - When needed ? In general, when auditors make a request, which is rare in general
    - Keep DORMANT the DAM Data NOT used for Threat Hunting
- **Technically:**
    - We consider the DAM Data as being 2 groups:
    - Data needed for Threat Hunting and Guardium Management -> **HOT** - on-line in the DW
    - Data occasionally needed by Auditors :
        - **Sessions** : Can be kept **HOT** w/ Enrichment - Low volumes
        - **Remaining DAM Data** :
            - No need to be uploaded until requested by the Auditors - Can be kept as csv files, READY to be uploaded in DW on-demand - **WARM**
            - **Procedure to upload data requested by Auditors from csv files**

Agg Altern Data Flow - HOT -



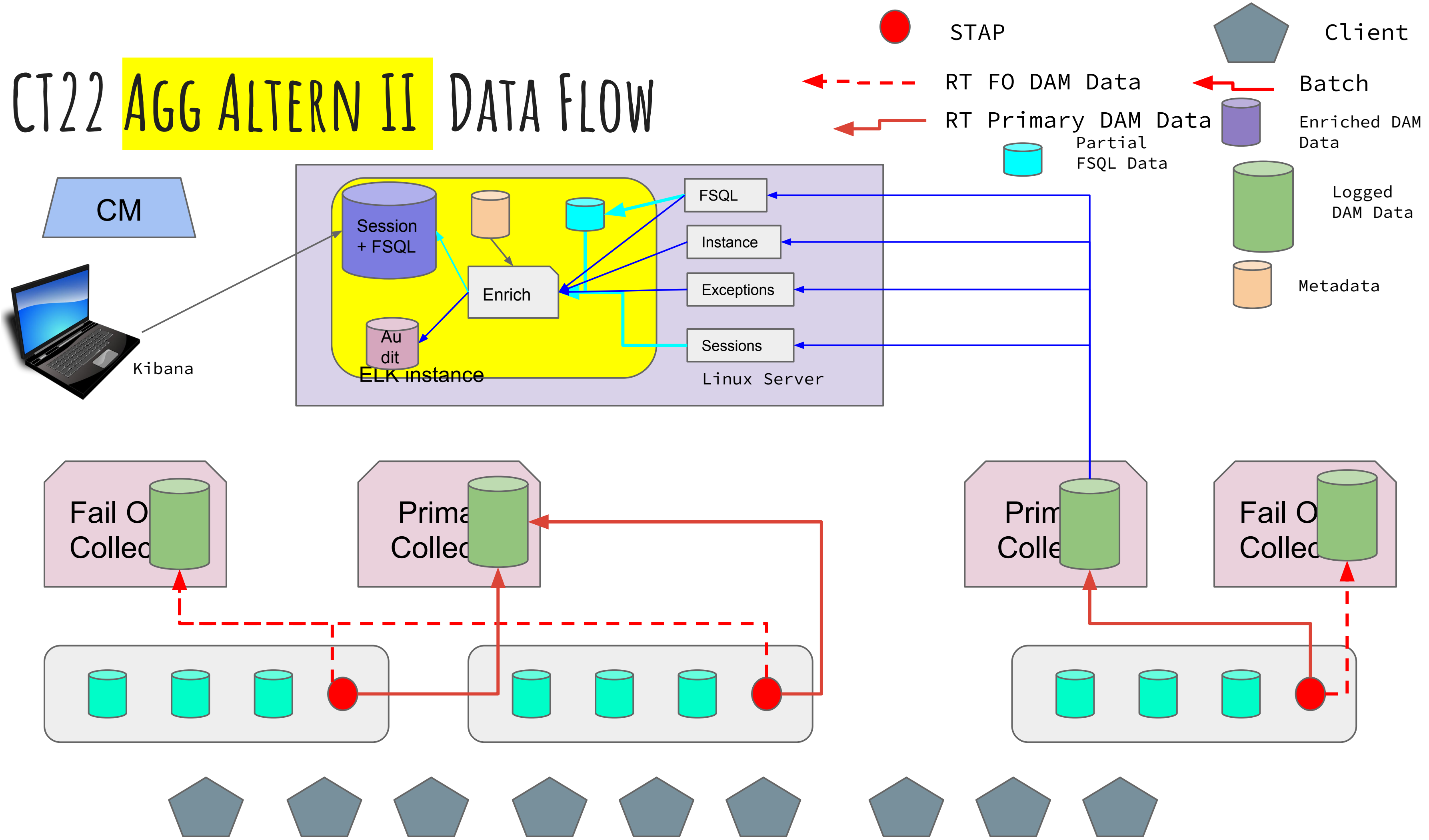
Author: Frederic Petit

CT22 Agg Altern I Data Flow



Author: Frederic Petit

CT22 Agg Altern II Data Flow



STAP

Client

RT FO DAM Data

Batch

RT Primary DAM Data

Enriched DAM Data

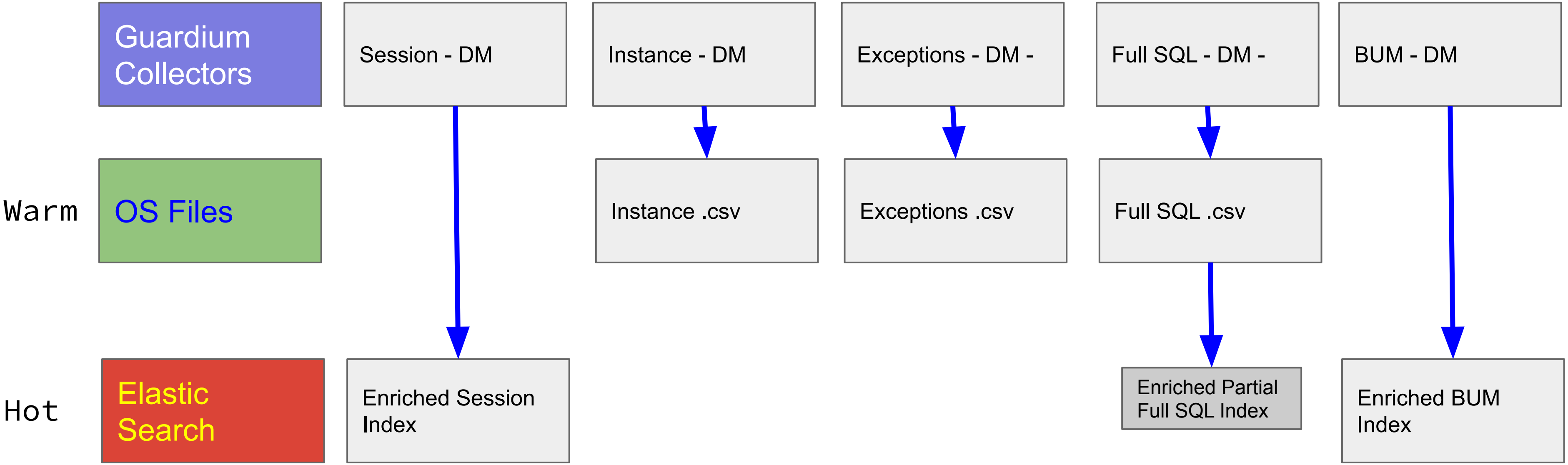
Partial FSQL Data

Logged DAM Data

Metadata

Author: Frederic Petit

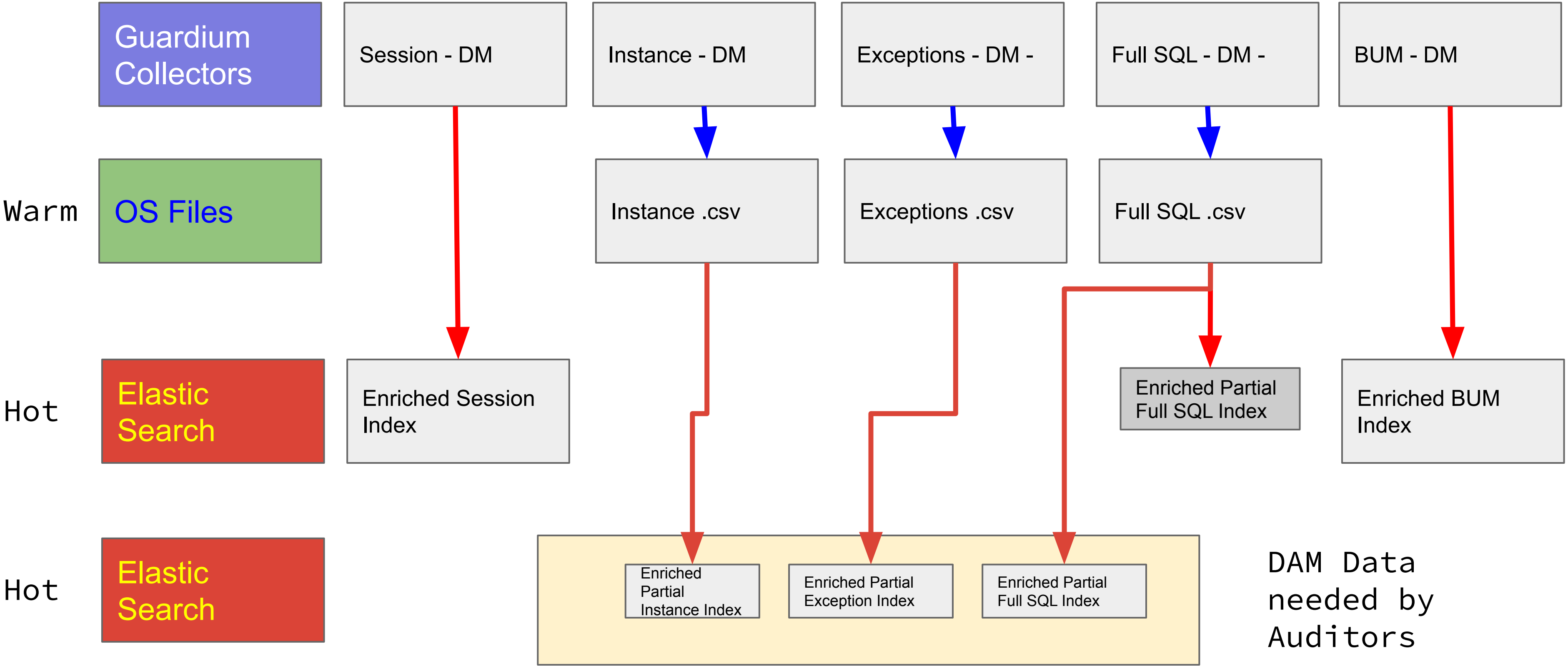
STATE 1 : THREAT HUNTING + GUARDIUM MGT ONLY



Warm On-line storage:

- All DAM data stored in ElasticSearch
- **Issues** : Large Environment or maintain for limited use

State II + Targeted Audit



DAM Data needed by Auditors

Comparison Full HOT vs. WARM

Audit Procedure in HOT State :

- Scan over large amount of data.
- Will take time
- Heavy management of the DW (ES)
- Data most of the time not used

Audit Procedure in WARM State :

- Upload of selected DAM data from OS files
- Small amount
- Light management of the DW
- ALL Uploaded Data are used

Claim : Uploading of WARM DAM Data for auditors is EQUIVALENT to scanning HOT DAM Data. Going WARM does NOT negatively impact. Simpler management

How to contact us

info@context22.com
Support@context22.com
www.context22.com
(under construction)

CONTEXT 22
TECHNOLOGIES

#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**

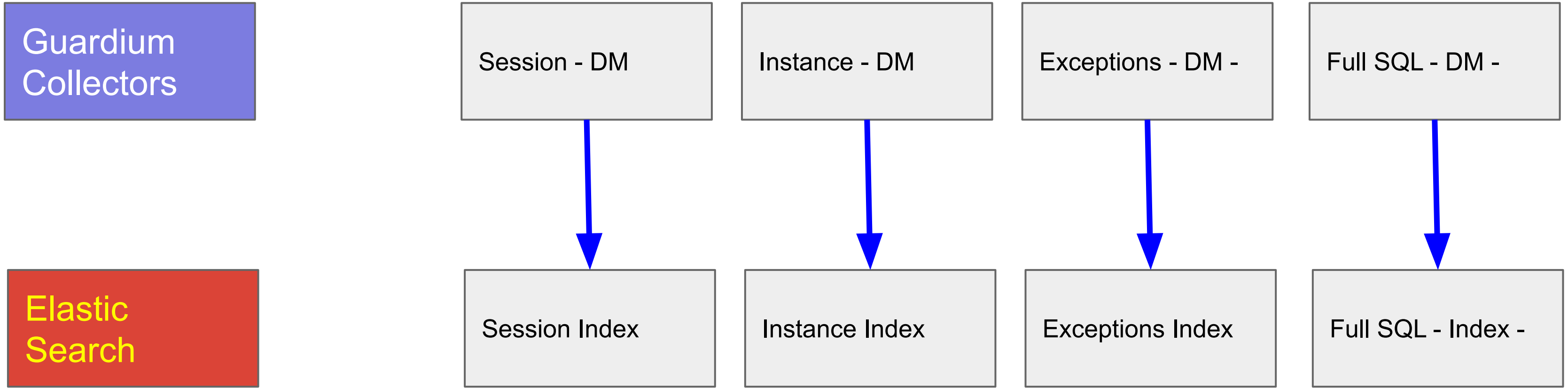
- Sniffer Memory close to ⅓ of total memory
- Mysql Disk Usage close to 90%

# **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

Replacement of Aggregators we are NOT advocating (Hot)



Guardium Collectors

Session - DM

Instance - DM

Exceptions - DM -

Full SQL - DM -

Elastic Search

Session Index

Instance Index

Exceptions Index

Full SQL - Index -

Hot On-line storage :

- All DAM data stored in ElasticSearch
- **Issues** :
    - Large Environment or maintain for limited use
    - Hot but NOT Enriched