Guardium Administration

How To Fix The Problem of Full Collectors ?

There are 2 cases of a COLLECTOR filling up

 # CASE 1 : Some Logs have filled up the Disk itself. There is no mechanism in Guardium for preventing this. This is a Linux issue to be treated at the OS level, root actually. Therefore the only option is to **open a ticket** and let Support fix it

 # CASE 2 : MySQL gets full, reaches 90% and the traffic collection stops. This is what we are treating here and there is **NO need to call Guardium Support**. Guardium provides every data you need to prevent and/or address the issue

FIRST thing First, Collectors Full are NOT Policies Related

Let's be clear, a Collector Full has NOTHING to do with Policies

- Policies MUST be designed and implemented to MEET the company's Security Requirements. That's it.
- As a Guardium admin, you CANNOT tweak a policy to "fix" a Collector full. If you do so, you are ALTERING the Security Requirements which is NOT in the power of Guardium Admins but in the power of your CISO.You CANNOT alter the Security posture of your company.

Therefore there are only 2 kinds of Policies:

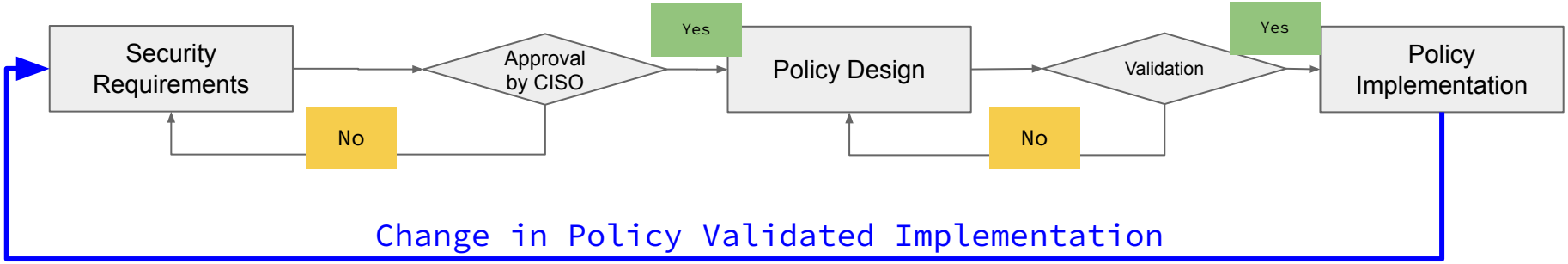
- Policies that MEET your company's Security Requirements
- Policies that do NOT meet your company's Security Requirements

Yes, the Guardium environment MUST be sized to support the volumes of traffic generated by the Security requirements and we have to assume it is unless proven otherwise. But one CANNOT assume by default that a collectors full is due to the policy. It is NOT.

Collectors Full are a Capacity Management Issue. Nothing else.

Policy Design Process and State of Collectors

The ONLY question is : Has your Guardium environment been sized to support your company's Security Requirements or not. If not, as a Guardium Admin you have to demonstrate and prove to your management. But tweaking the policy to "fix" volumes issues is out of question.



Validation of policy design :

- Verifying the policy implements the Security Requirements
- Verification can be done by some Professional Services or/and by Auditors (the best)

#1 - First, Fixing a MySQL Full db

#2 - Preventing It From Happening Again.

Immediate Fix

- Status :
  - MySQL has reached 90%
  - Sniffer (collection) has stopped
  - Agents should have been diverted to their Failover Collectors which are starting to fill up as well . . .
- What to do ?
  - Nothing worse will happen on the primary collector
  - However, the Failover collector may itself be in bad shape and may be filling up quickly
  - And if the Failover fills up, agents have no place to go and therefore the traffic will be lost …
  - Therefore, the FIRST thing is to look at the state of the Failover and assess how long it will take to fill up : this is the time you have to fix the Primary
  - On the Primary: You must fix the problem BEFORE the Failover fills up.

Options for Immediate and longer-Term Fix

#1 : Reduce the Retention Period and Purge immediately, but this ONLY delays the issue.It does NOT fix it.

#2 : Identify the cause of the amount of Traffic filling up the Collector and acting accordingly to **put the Collector in a sustainable state**

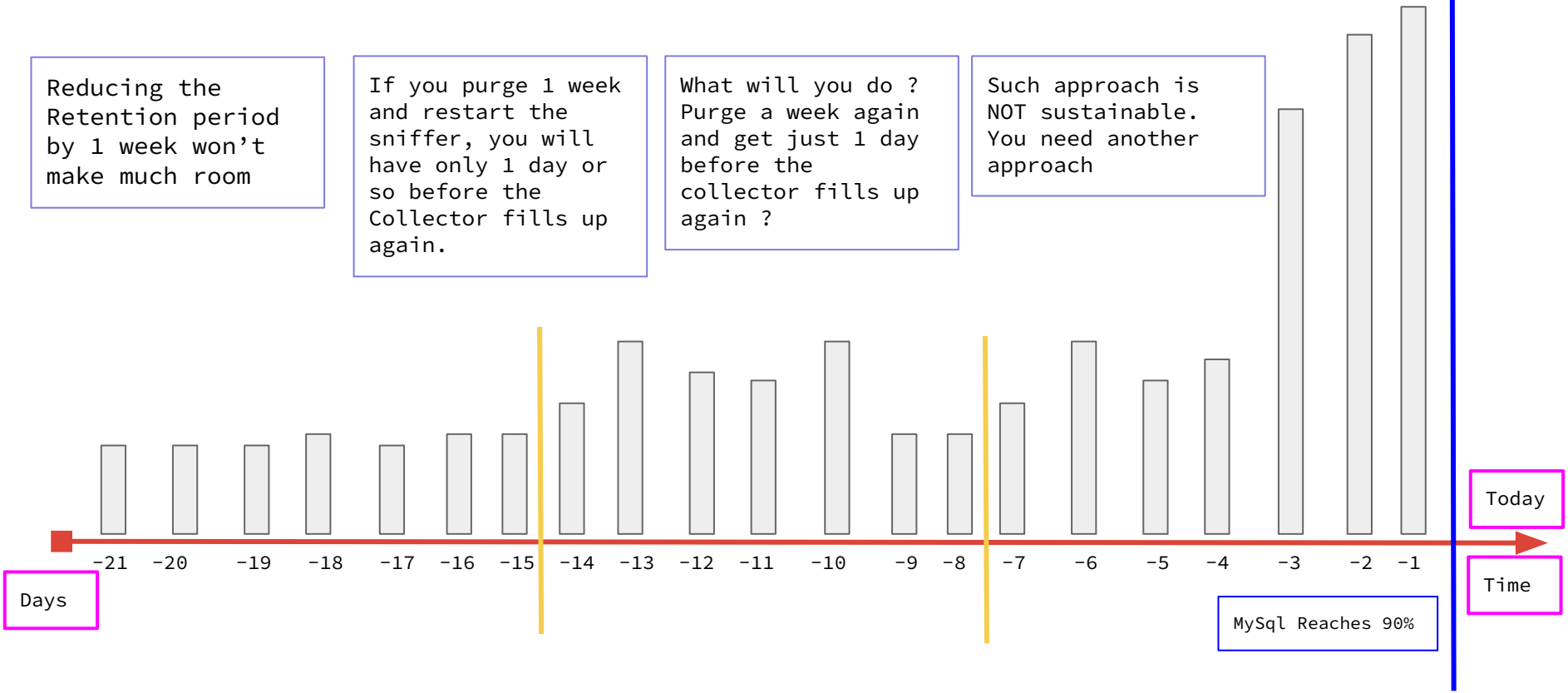
#1.1 Randomly Reduce the Retention Period and Purge

Reducing the Retention period by 1 week won't make much room

If you purge 1 week and restart the sniffer, you will have only 1 day or so before the Collector fills up again.

What will you do ? Purge a week again and get just 1 day before the collector fills up again ?

Such approach is NOT sustainable. You need another approach



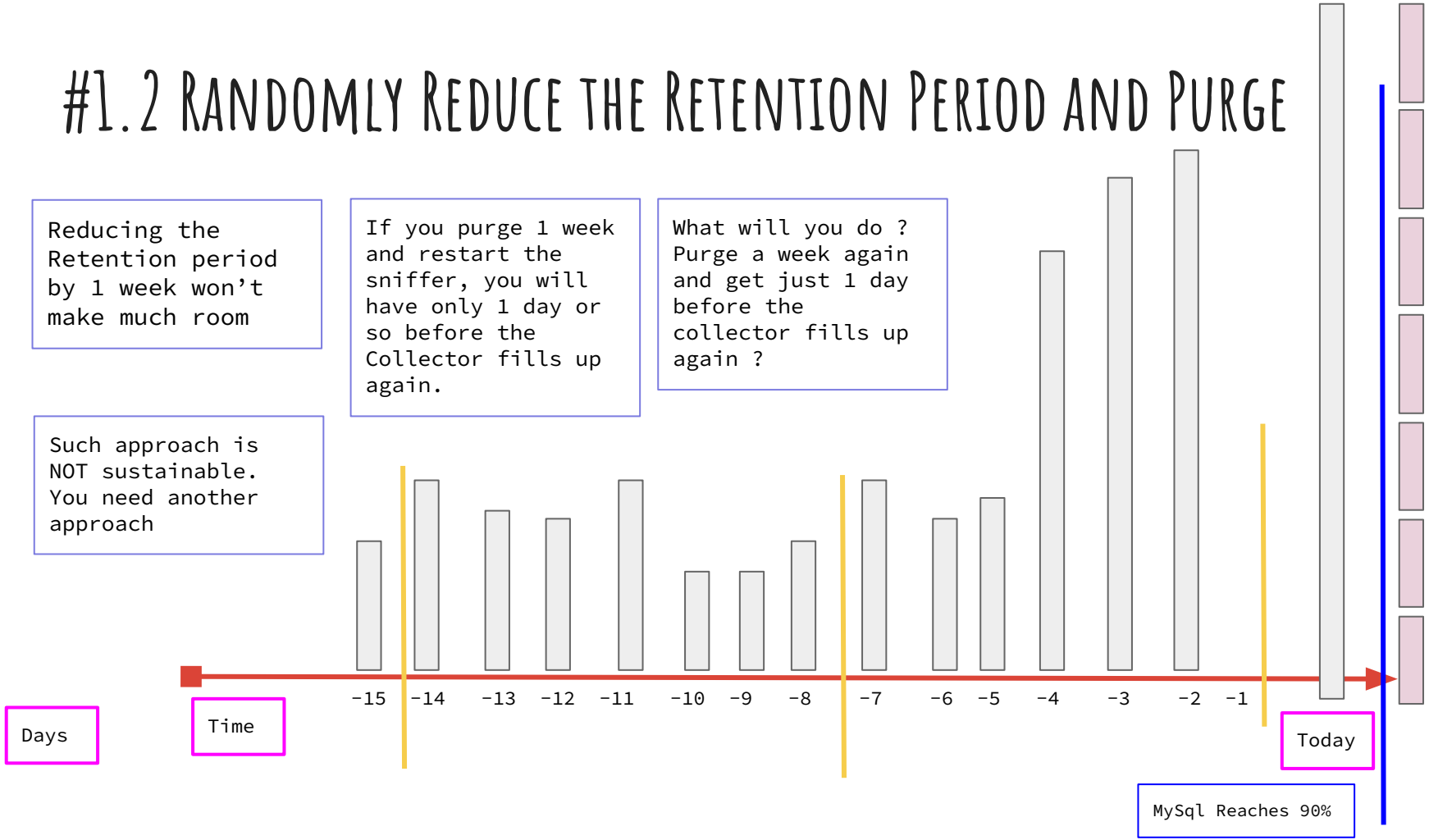
#1.2 Randomly Reduce the Retention Period and Purge

Reducing the Retention period by 1 week won't make much room

If you purge 1 week and restart the sniffer, you will have only 1 day or so before the Collector fills up again.

What will you do ? Purge a week again and get just 1 day before the collector fills up again ?

Such approach is NOT sustainable. You need another approach



#2 : Know your Traffic Volumes and Act accordingly

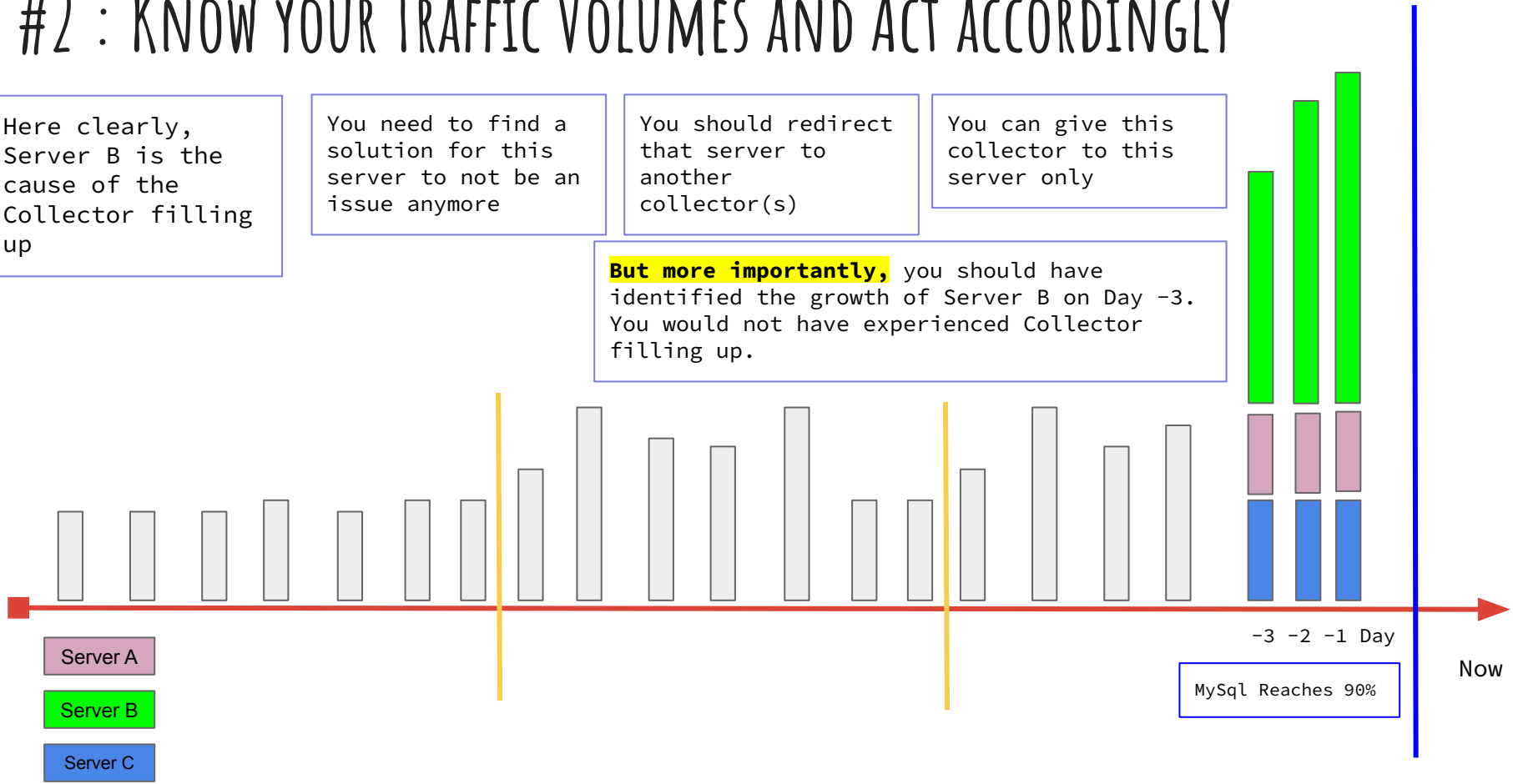
Here clearly, Server B is the cause of the Collector filling up

You need to find a solution for this server to not be an issue anymore

You should redirect that server to another collector(s)

You can give this collector to this server only

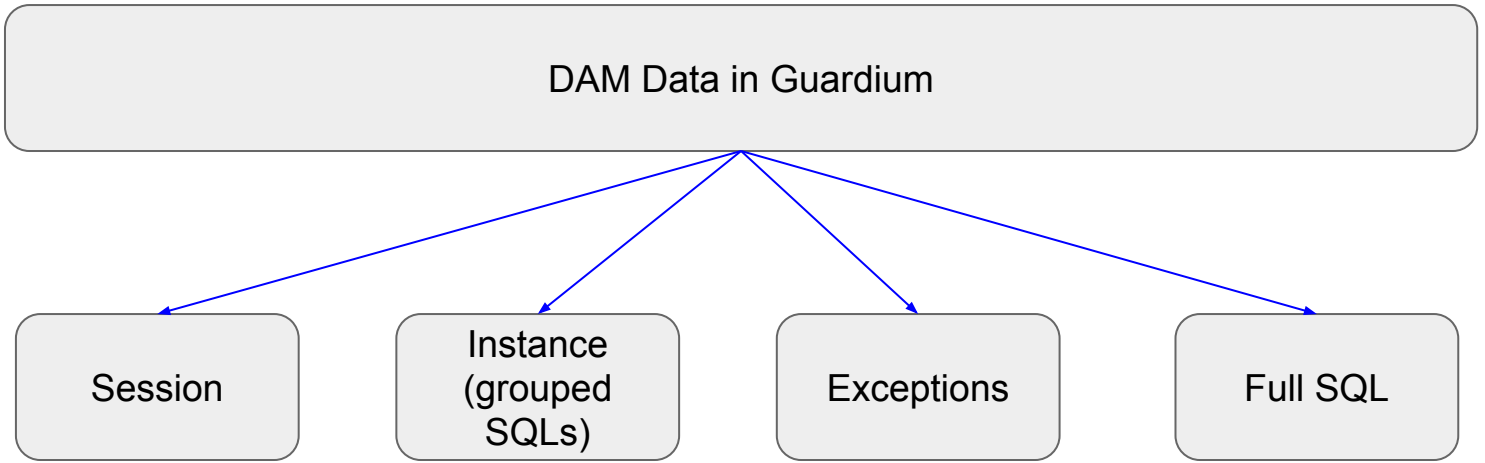
But more importantly, you should have identified the growth of Server B on Day -3. You would not have experienced Collector filling up.



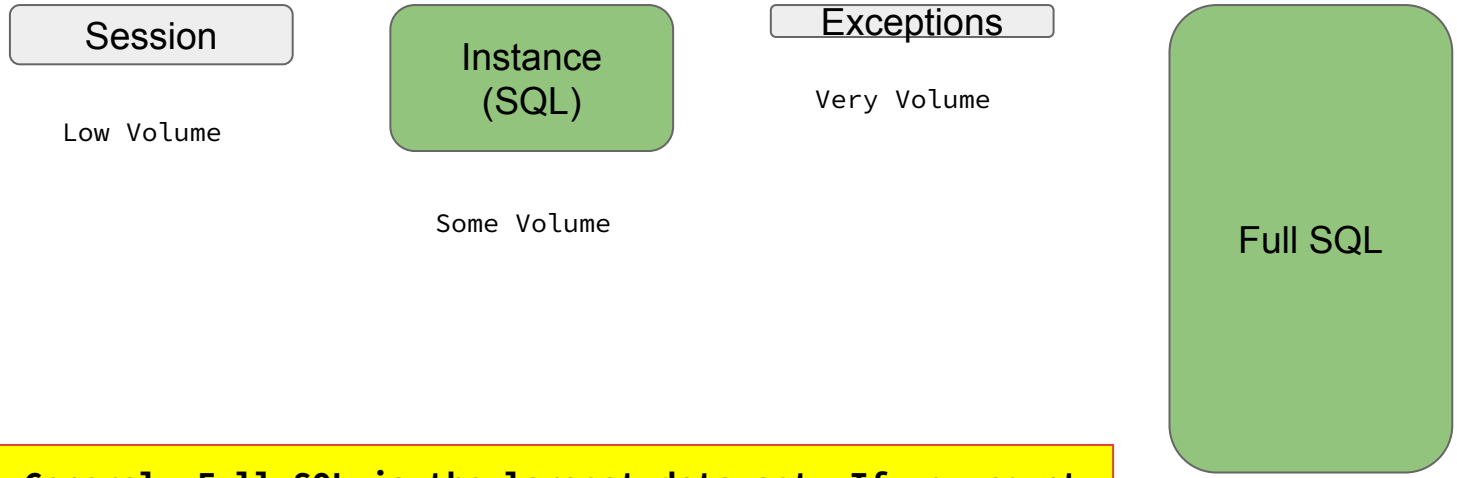
How to Know the Amount of Data per Day and per Server

The 4 Components of the DAM Data

We need to use the DAM Data as the BUM does not provide that information



In General What is the relative Importance of Each Component



In General, Full SQL is the largest data set. If you count the number of records per day and per agent (not per server as some may be VIPs), you will get a good idea of the respective contribution of the different agents.

How to get this count ?
Write a report on Full SQL or use the CT22T Add-on for Guardium

The 2 tools to fix a MySQL DB Full Issue on Collectors

#1 - Reduce the retention period and purge. This will make room TEMPORARILY

#2 - Reassign some of the Agents currently on the Full Collector to a different collector

If this is not enough, you may have an undersized environment and you may need additional collectors. You get that by **going back to your management** and present to it **a clear picture** of the undersizing **with numbers**. And you should NOT have underused collectors. If so, your management will make a decision and if they decide to change the policy to reduce the amount of traffic collected, it will be their executive decision, the only one acceptable in that case.

Conclusion :

- You can start by purging but it will NOT fix the issue, it will just delays it from happening again. And it will very soon.
- You need instead to figure out the contributing volumes of each agents, then get a new Collector(s) or identify underused collectors and re-assign some agents to them, then execute the change and purge. At that time ONLY you can restart the sniffer on the full collector

You can still purge first, just to give MySQL some space and be able to run reports counting records better. **But don’t restart the sniffer before re-assigning some agents** or you will get the collector full again very soon. You will be back at square 1 without any sustainable solution in sight.

How to contact us

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

Thank youtube to Akash Parmar for his review