#ASLI ENGINEERING

GitHub Outage: On switching a Master Database

SWIPE

BY

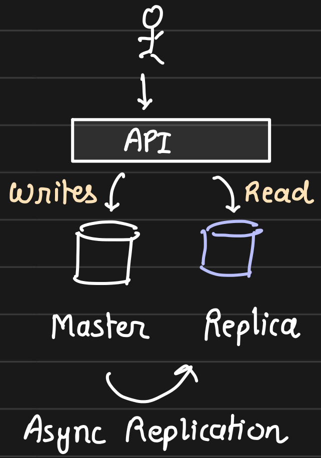
ARPIT BHAYANI

Dissecting GitHub Outage

Outage during switching Master database

GitHub had an outage ... during planned maintenance!!

What happened?



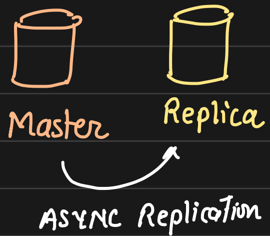
Users observed delays → in data being visible on the interface or API after it is being written on the database

Reads go to Replicas

Writes go to Master

Given that 1. data was written successfully but was not available for reads

↳ Place we store is different from the Place we read from



This is done through a Master Replica setup and is a popular way to handle large read load without affecting the write load.

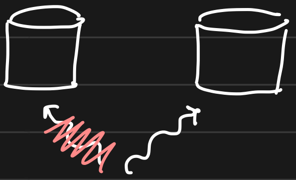
ARPIT BHAYANI

What happens in planned maintenance?

During a planned database maintenance,

we switch the database

- apply security patches
- version upgrades
- parameter tuning
- hardware replacement
- periodic reboots



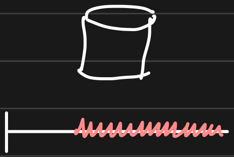
We switch the primary database from one machine to another

So, we keep another instance handy

and with a config change we route all traffic to new DB.

Hence, for a short duration the system might become unavailable.

So, what happened to GitHub?



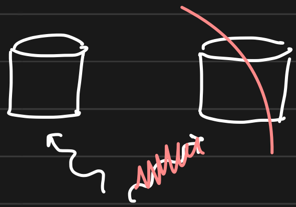
During planned maintenance, they switched the master and the mysqld process crashed!

on the newly promoted master server

How to mitigate?

The old database server was there,
so, because the new server crashed

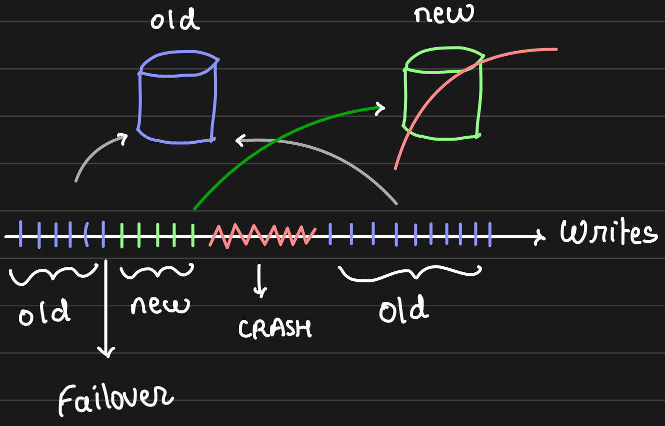
we quickly route traffic to old server
back



So, this should the problem..... wait....

Switching back to old server would definitely keep the system running as it can continue to process writes, but.....

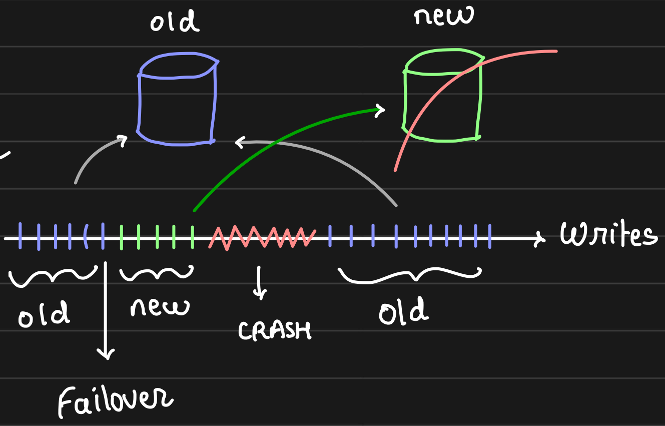
For GitHub, the crashed MySQL server, served the WRITE traffic for 6 seconds !!



Some writes went to
new database
and we switched back,
so, what would happen ??

Now, the current state of GitHub is

- new writes going to old
- some data only on the new database
- old data intact

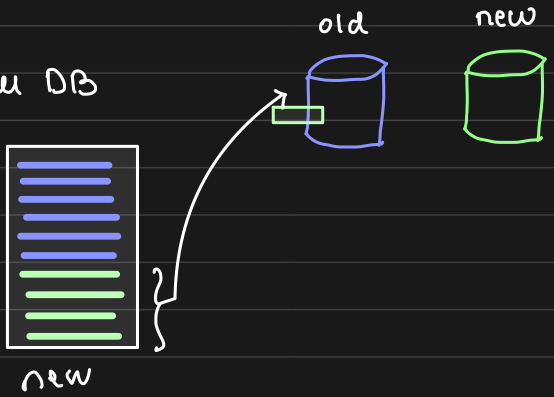


How do we remediate ?

Anytime we switch the database,
we should always note the BINLOG co-ordinates

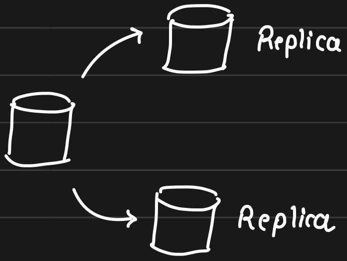
* Every company does this ↑

Using BINLOG we apply the changes that happened in new DB after first failover on the old DB



ARPIT BHAYANI

So, how reads got affected?



When we failover databases, specifically during outages, we create a new set of replicas - for a fresh start and clean consistency

Creating replicas took ~4 hours → Because dataset is HUGEEE !!

and manually configuring cluster took ~1 hour