

# **Pgweasel log parsing LT**

**Kaarel Moppel**

**Freelance PostgreSQL Consultant**

# Why look at Postgres logs ?

**The Postgres Stats Collector subsystem doesn't cover everything by far!**

- The obvious - get full details on PostgreSQL errors
- Slow queries with specific execution params
- Slow query plans (auto\_explain)
- Slow Autovacuum details
- Connection “spam”
- Detect unauthenticated access / brute force attack attempts
  - Sadly possible by default with Postgres ...
- Background processing details (e.g. autovacuum, 3rd party exts.)
- Lock wait details
- Temp file details
- Backend terminations / OOM

...

# Log management approaches

- Ad-hoc searching / grepping
  - grep, pgBadger & co
  - Exposing logfiles directly via file\_fdw for SQL power
- Continuous forwarding / analyzing
  - Loading into a DB (e.g. Postgres + ZFS)
  - Homegrown parsing (e.g. Cron+Python)
  - Filebeat / ELK (Elastic) pipeline
    - Sometimes via Syslog
  - Prometheus integration, e.g. pgwatch "server\_log\_event\_counts"
  - Generic framework (Nagios etc) Postgres plugins
  - Cloud SaaS / APM e.g. Loggly, DataDog, ...
- Hooking into the Postgres log emitting mechanism
  - Tapping into "emit\_log\_hook", a la "redislog" (unmaintained)
- ...

# pgweasel

- [pgweasel](#) is my new log parsing project
- That tries to be different, covering the Pareto DBA flow on the CLI
  - Simper to handle
  - Way faster, Golang (Rust?)
  - A single binary
  - Zero-config

```
kr1@e7420:~$ pgbadger --help | grep -E '^s+\-{1,2}' | wc -l  
106
```

# pgweasel - looking for contributors!

- One person has quite a narrow view on things...
- Plus the typical side-project time issue
- Also...to make it work really good under all conditions a lot of server log examples would be needed!



In case you have some large real-life logfiles without security risks, please send me some S3 etc link for private use or just open an Github issue 🙏

<https://github.com/kmoppel/pgweasel>

**Licence:** PostgreSQL license



All kinds of feedback, feature ideas /requests  
Or just a ★ would be very much appreciated!