PERCONA LIVE ONLINE MAY 12 - 13th 2021

Using Percona Audit plugin in daily operation

By Lenny Andersen, DBA

Disclaimer

Perhaps this session is a bit more detailed than planned at first.

But not rocket science.

What is it?

- The plugin is installed (but not enabled) with Percona servers.
- It will log all activity on the server.
- Can be configured to fit different use cases.
- Lightweight
- **Not** a log for performance tuning

Reasons to do audit logging

- The need for need for documentation on database usage.
- Having a documentation to do forencics in case of data theft.
- Getting a better understanding of data usage.
- Troubleshooting!
- I’m sure there’s a lot of other reasons.

Obsticals for making the logs useful.

- The raw output is bit verbose (xml, json, csv)
- Flat files are not very searchable
- Very storage consuming.


```
{"audit_record":{"name":"Query","record":"222_2021-04-08T14:06:26","timestamp":"2021-04-
08T14:34:40Z","command_class":"select","connection_id":"14","status":0,"sqltext":"select * from users","user":"root[root] @ localhost
[127.0.0.1]","host":"localhost","os_user":"","ip":"127.0.0.1","db":"website"}}
{"audit_record":{"name":"Query","record":"223_2021-04-08T14:06:26","timestamp":"2021-04-
08T14:34:40Z","command_class":"select","connection_id":"14","status":0,"sqltext":"select * from orders","user":"root[root] @ localhost
[127.0.0.1]","host":"localhost","os_user":"","ip":"127.0.0.1","db":"website"}}
{"audit_record":{"name":"Quit","record":"224_2021-04-08T14:06:26","timestamp":"2021-04-
08T14:34:41Z","connection_id":"11","status":0,"user":"root","priv_user":"root","os_login":"","proxy_user":"","host":"localhost","ip":"127.0.0.1","
db":"website"}}
```

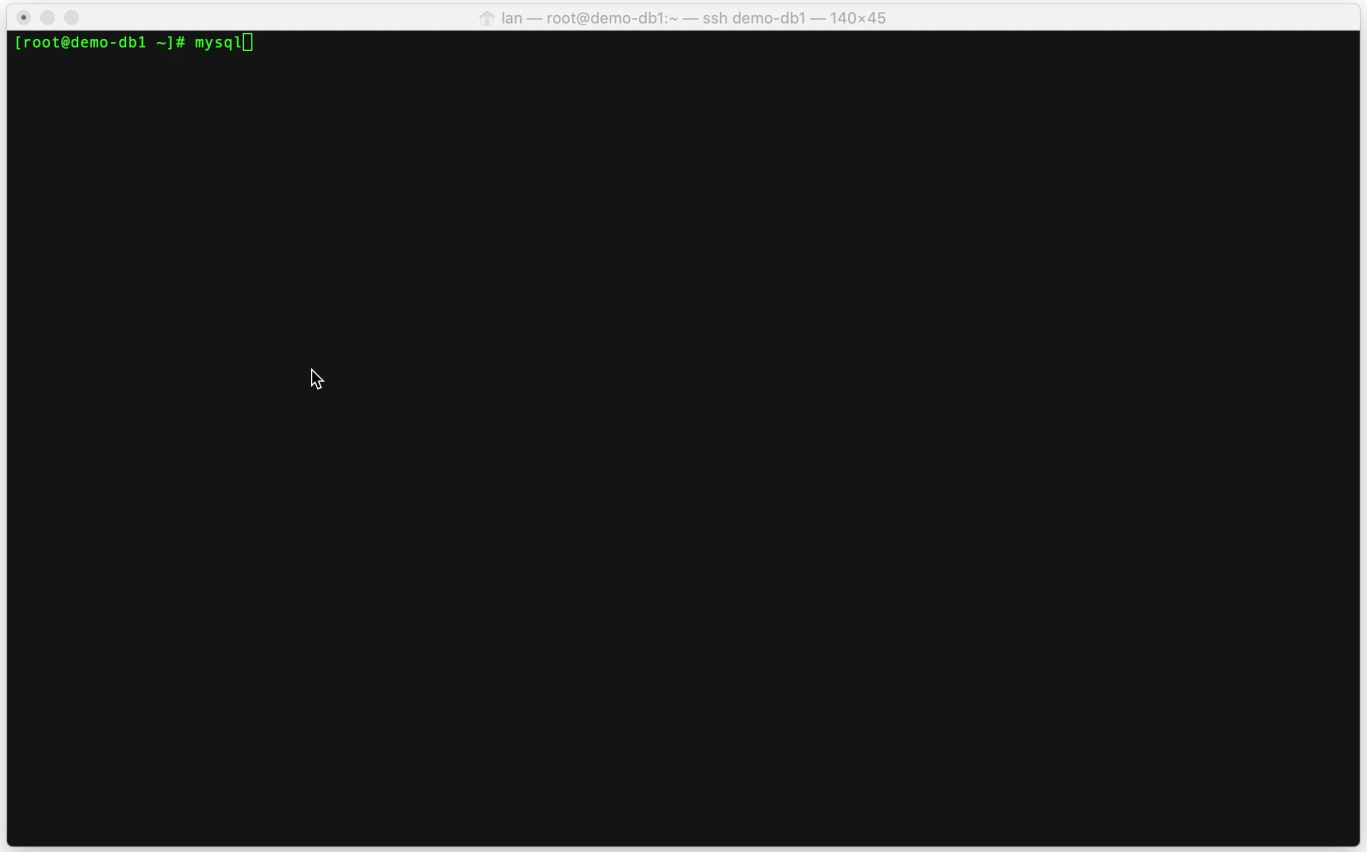

Solution

ClickHouse

- Data easiely structured in a table
- Very *very* quick when searching
- Very good compression ratio

Demo

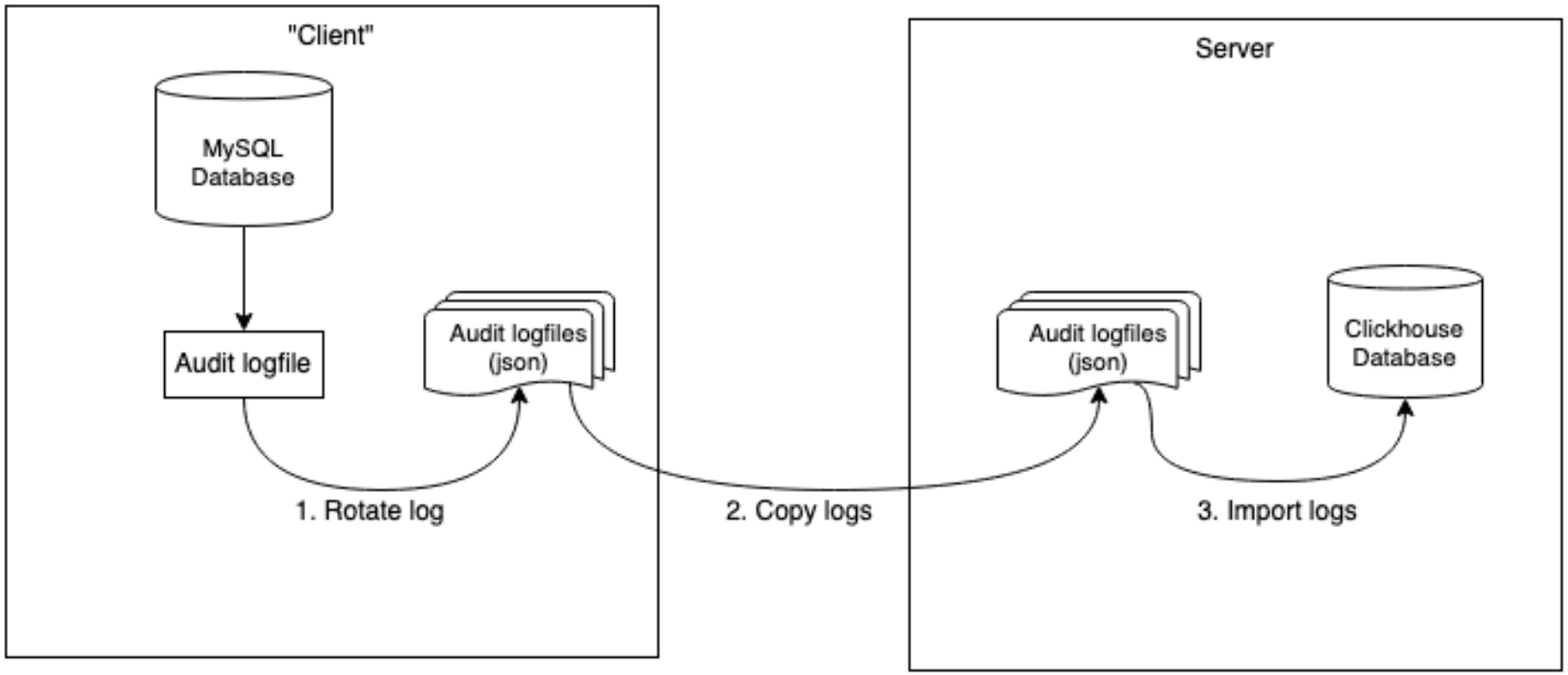
- Enable and configure Percona Audit Plugin


lan — root@demo-db1:~ — ssh demo-db1 — 140×45
[root@demo-db1 ~]# mysql

Considerations on the Plugin

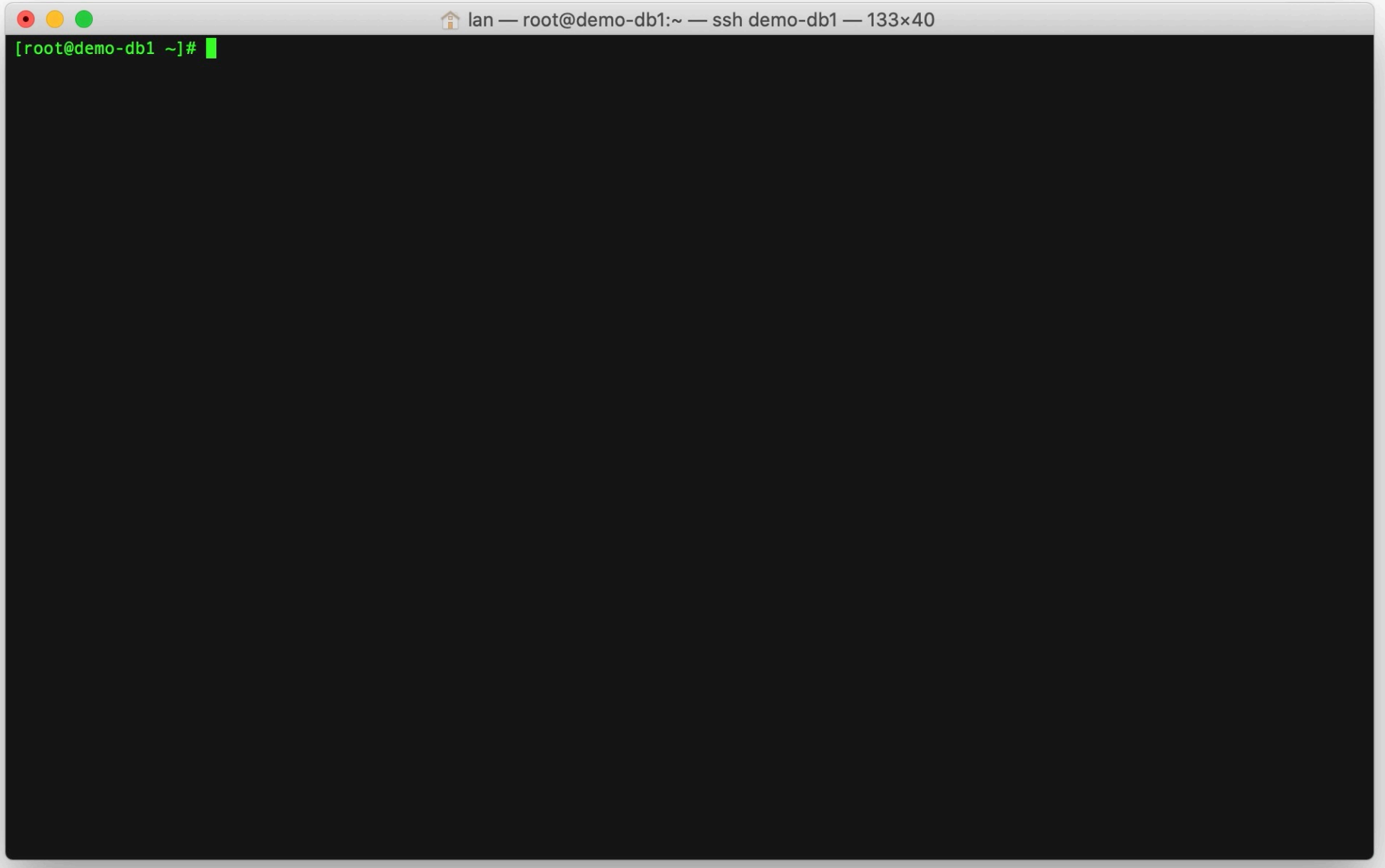
- Output format (CSV, JSON, XML)
- Syslog or to local disk
- Do you want to log EVERYTHING?
  - Remember the consequences
- All settings for the plugin are described at
  - https://www.percona.com/doc/percona-server/8.0/management/audit_log_plugin.html

Topology and Workflow



Demo

- Rotating and rsyncing the files


lan — root@demo-db1:~ — ssh demo-db1 — 133×40
[root@demo-db1 ~]#

Importing the files into ClickHouse Database

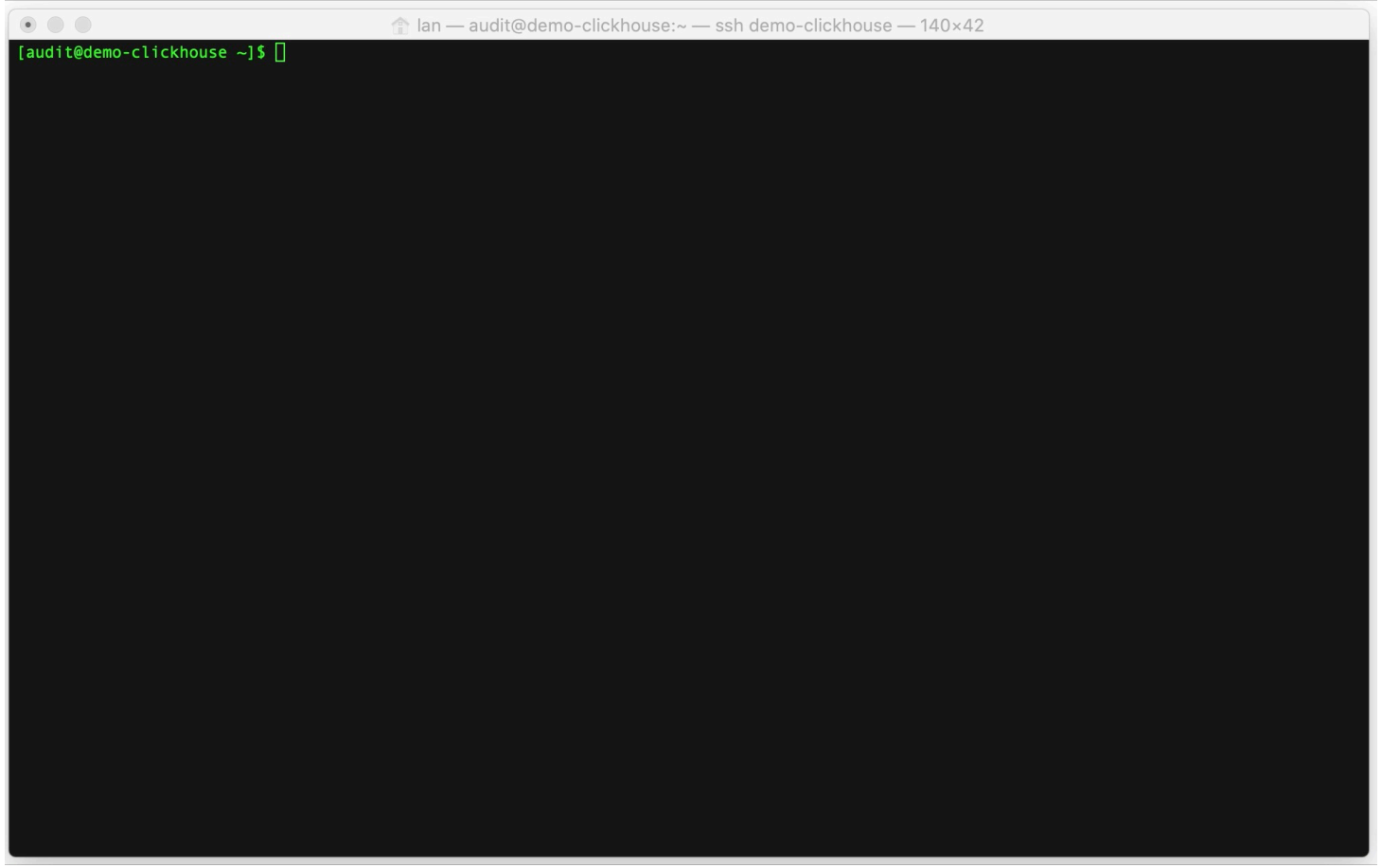
- Format is JSON. Easy but ….
- Not one JSON object. Each line is a JSON object
- The origin of the file is not included in the audit log

Solution

- Fairly simple JSON parser (binary written in Go)
- Wrapped into a bash script
- Reading the ingress dir one file at a time.
- Available at Github (binary and sourcecode)

Demo

- Importing the files into ClickHouse


lan — audit@demo-clickhouse:~ — ssh demo-clickhouse — 140×42
[audit@demo-clickhouse ~]$

Using the data

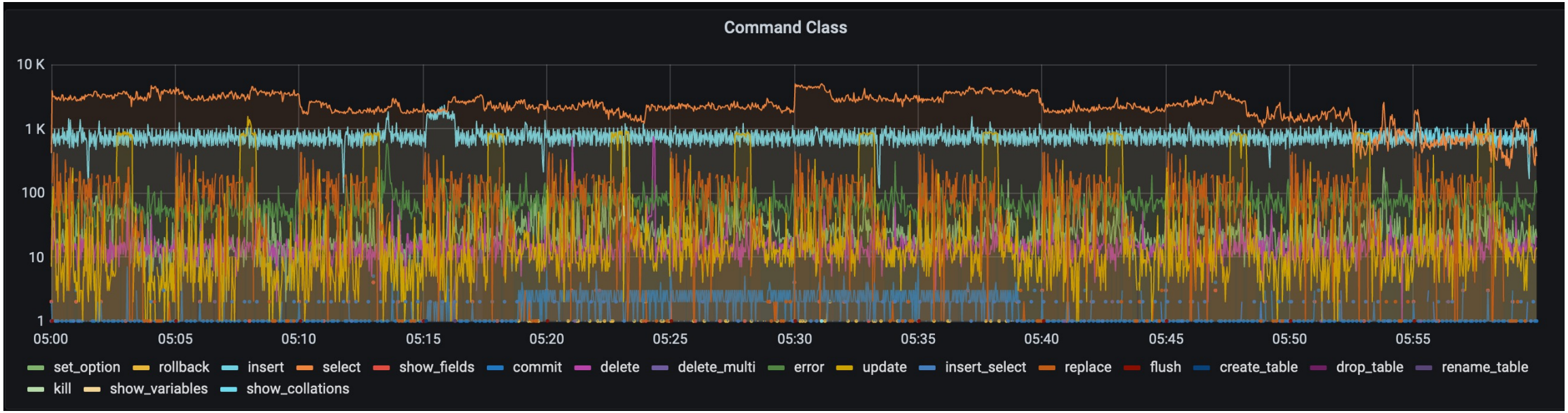
- ClickHouse CLI gives easy access
- Investigate a timestamp query by query
- Follow a user
- Follow a host
- Follow a connection

- Obvious to implement into Grafana

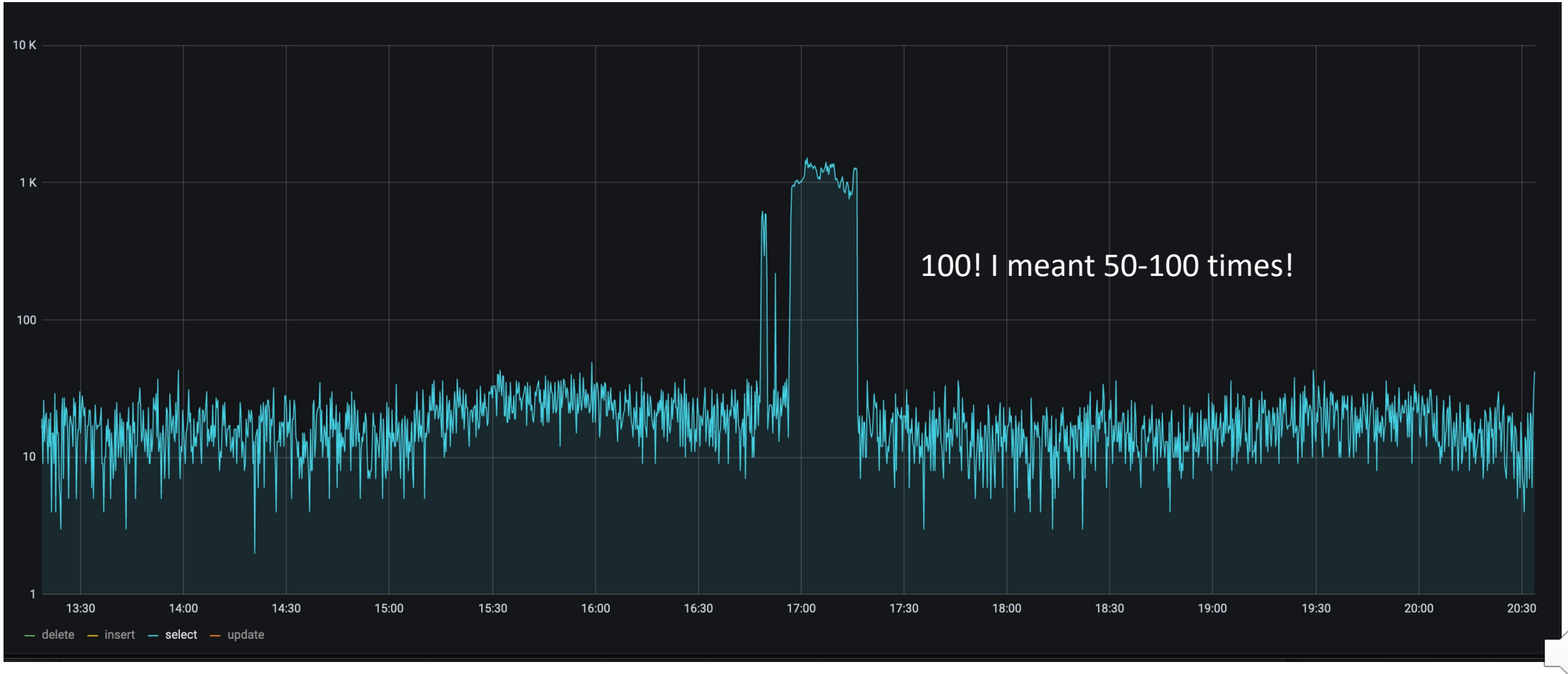
Story time

Tellings from the trenches

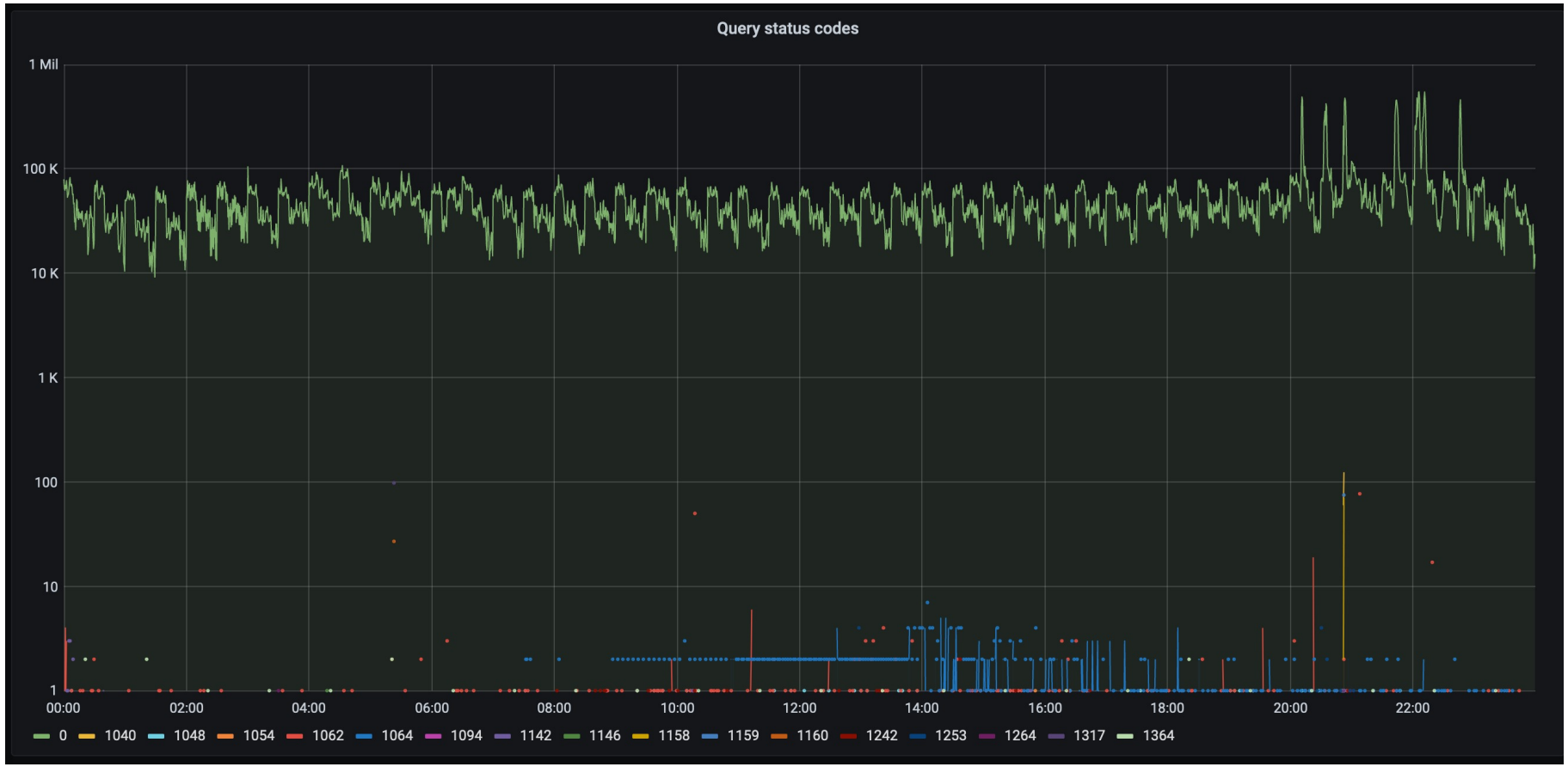
What the heck is going on?



Security incidents



There is something wrong with the database



There is something wrong with the database

```
| 2021-02-17 10:44:38 | select         | select blah blah from table blah blah|
```

```
┌─────────────────────time─┬─command_class─┬─sqltext──────────────────────────────────────────────────────┐
| 2021-02-17 09:43:27 | set_option    | SET NAMES utf8 COLLATE 'utf8_general_ci'                     |
| 2021-02-17 09:43:27 | set_option    | SET sql_select_limit=1                                       |
| 2021-02-17 09:43:27 | set_option    | SET SESSION TRANSACTION ISOLATION LEVEL READ COMMITTED       |
| 2021-02-17 09:43:27 | set_option    | SET SESSION TRANSACTION READ WRITE                           |
| 2021-02-17 09:43:27 | set_option    | SET character_set_results=NULL                               |
| 2021-02-17 09:43:27 | set_option    | SET character_set_connection=utf8mb4                         |
| 2021-02-17 09:43:27 | set_option    | SET character_set_client=utf8mb4                             |
| 2021-02-17 09:43:27 | set_option    | SET collation_connection='utf8mb4_general_ci'                |
└─────────────────────┴───────────────┴──────────────────────────────────────────────────────────────┘
```

Useful links

- Percona Audit Plugin documentation
  - https://www.percona.com/doc/percona-server/8.0/management/audit_log_plugin.html
- Log importer
  - https://github.com/LennyAndersen/clickhouse-audit-import
- Grafana Clickhouse plugin
  - https://grafana.com/grafana/plugins/vertamedia-clickhouse-datasource/

Thanks!

Any questions?

You can find me at:

lenny@bdbafh.dk