ecwid

20Tb логов в ClickHouse

Василий Васильков, Ecwid

Ecwid

- E-commerce SaaS-платформа
- Миллионы клиентов
- 150+ человек в команде
- Ульяновск, Самара, Владивосток, San Diego

Давным-давно

- 2009 год
- Первый релиз
- Хочешь логи – зайди на нужный сервер и почитай, не барин
- И вообще не до логов, сели ждать клиентов

Проблемы

- Сервер внезапно умер – логов нет
- Надо бегать по серверам
- Сложно исследовать проблемы

Syslog

- Доставляем все логи на один сервер
- По файлу на сервис
- Вся мощь Unix-утилит (grep, awk, sed, sort, uniq etc.)

ELK?

- Была попытка внедрить ELK
- ~~Это какое-то говно~~ Не понравилось

Наши дни

- 100 гигабайт логов (текстовых) в сутки
- 200 миллионов строк (тоже в сутки)
- Другими словами – 3 терабайта в месяц
- grep уже как-то не очень

Немного о ClickHouse

- Просто охеренная база
- Рекомендую хотя бы посмотреть
- Колоночная
- Феерически быстрая

```
create table log(
  date_time DateTime,
  service String,
  level Enum8('info' = 0, 'warn' = 1, 'error' = 2),
  version String,
  class_name String,
  method_name String,
  ip_address UInt32,
  message String,
) ENGINE = MergeTree()
    PARTITION BY toYYYYMMDD(date_time)
    ORDER BY (service);
```

Индексатор

- У нас уже есть файлы с логами
- В Unix есть `tail -F`
- Отлично, половина уже готова

```
tail -F billing.log |
 java -jar indexer.jar |
  clickhouse-client
```

```
info 2019.04.26 00:17:33.180 billing c55a13b77c8
BillingService subscribe 172.30.1.2 Subscribe
client #123123 to paid subscription
```

```
insert into log(date_time,service,level,version,
    class_name,method_name,ip_address,message)
values('2019.04.26 00:17:33.180', 'billing','info',
    'c55a13b77c8','BillingService','subscribe',
    '172.30.1.2', 'info 2019.04.26 00:17:33.180 billing
    c55a13b77c8 BillingService subscribe 172.30.1.2
    Subscribe client #123123 to paid subscription')
```

Поисковик

- Все данные есть в ClickHouse
- Однако, заставлять писать SQL негуманно

```
select message from log where
    level='error' and
    service='billing' and
    version='c55a13b77c8' and
    class_name='BillingService' and
    date_time>'2019.04.20 00:00:00'
```

А давайте DSL

- Хочется что-то тупое
- Как и всегда, впрочем

```
level:error service:billing
date:2019.04.20..now
```

Unix pipes

```
echo "level:error date:2019.04.01" |
 java -jar finder.jar |
  clickhouse-client
```

level:error service:billing
version:c55a13b77c8 class:BillingService
date:2019.04.20..now

```
select message from log where
    level='error' and
    service='billing' and
    version='c55a13b77c8' and
    class_name='BillingService' and
    date_time>'2019.04.20 00:00:00'
```

Готово

- Написали два обработчика строк туда-сюда
- Завязали с уже готовыми утилитами через pipes
- Скорость выросла (100-1000x)
- Все остальные утилиты этого не заметили

Немного результатов

- За сутки все записи с уровнем error в конкретном сервисе

  Время поиска – 1.2s, обработано ~90mln lines

- За всю историю, поиск по пяти text-полям

  Время поиска – 4min, обработано ~36bln lines

Василий Васильков

vgv@ecwid.com

https://github.com/ecwid/new-job