Микросервис для агрегации логов

Курсовая работа Семёна Енцова, 3 курс ПМИ ВШЭ
Научный руководитель — Вячеслав Токарев

2023 год

Проблема
Observability

- Распределённые системы очень сложно отлаживать
- Важно развивать инфраструктуру для отладки
    A. логи
    B. метрики
    C. мониторинг

Проблема

Агрегация метрик по журналу доступа

- Журнал доступа — лог запросов к микросервисам
- Полезные метрики:
  - RPS запросов
  - Срез по коду ошибок
  - Тайминги запросов

```
timestamp=20220917T20:20:48 timezone=+0300 status=200
protocol=HTTP/1.1 method=GET request=/ping
timestamp=20220917T20:20:49 timezone=+0300 status=200
protocol=HTTP/1.1 method=GET request=/ping
timestamp=20220917T20:20:50 timezone=+0300 status=200
protocol=HTTP/1.1 method=GET request=/ping
```

Пример журнала доступа: три запроса по адресу /ping

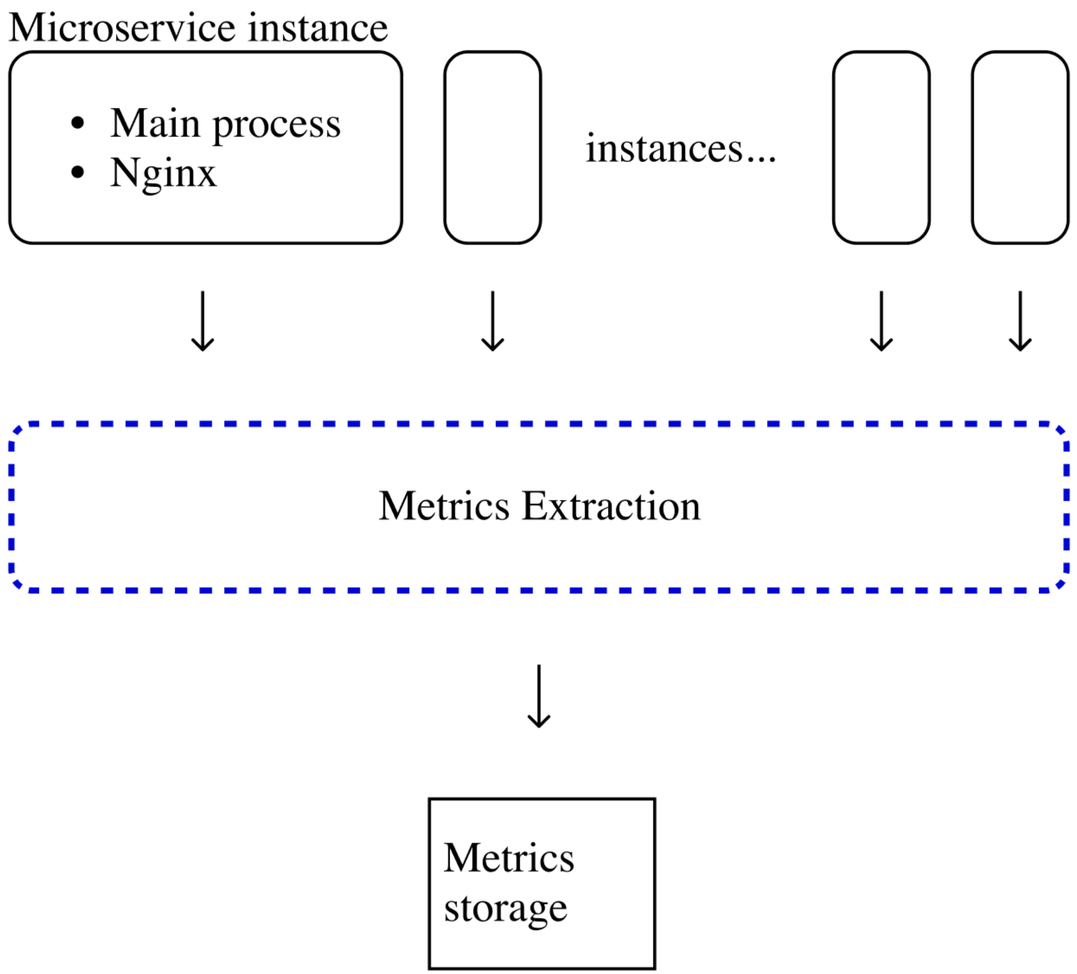
Задача

- Реализовать MVP сервиса для извлечения метрик из журнала доступа
- Требования:
  A. Масштабируемость: сервис должен обрабатывать поток логов в 200 МБ/сек с порядка 1000 машин
  B. Latency: задержка между событием и отражением его на графике меньше 20 секунд
  C. Данные не критичные. Допустимо потерять часть логов

Задача

Инфраструктура

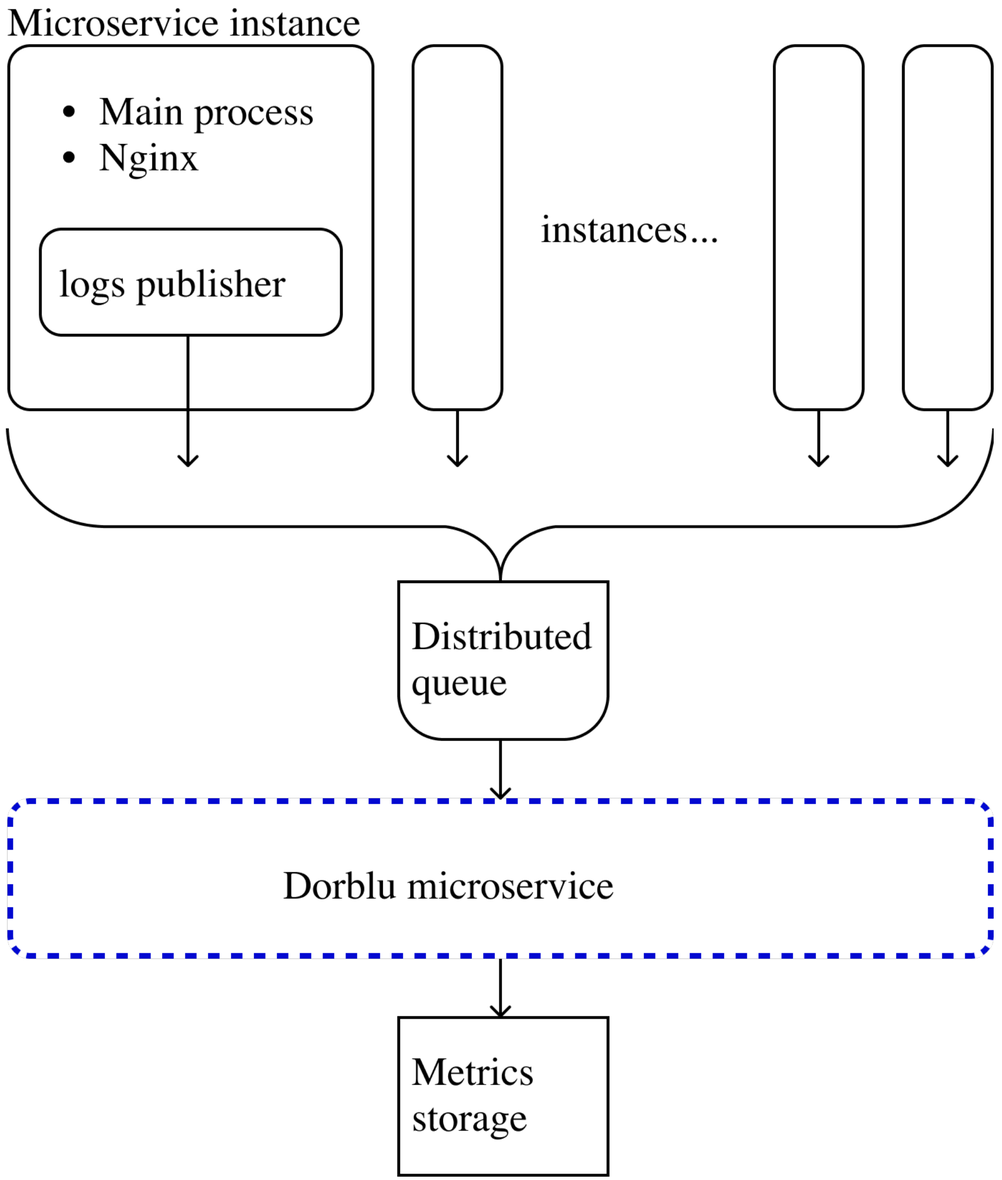
- Микросервисная архитектура
- Nginx ведёт журнал доступа на каждой виртуальной машине
- Подсчитываются значения метрик внутри интервала
- Итоговые метрики отправляются в хранилище



Реализация

Обзор решения

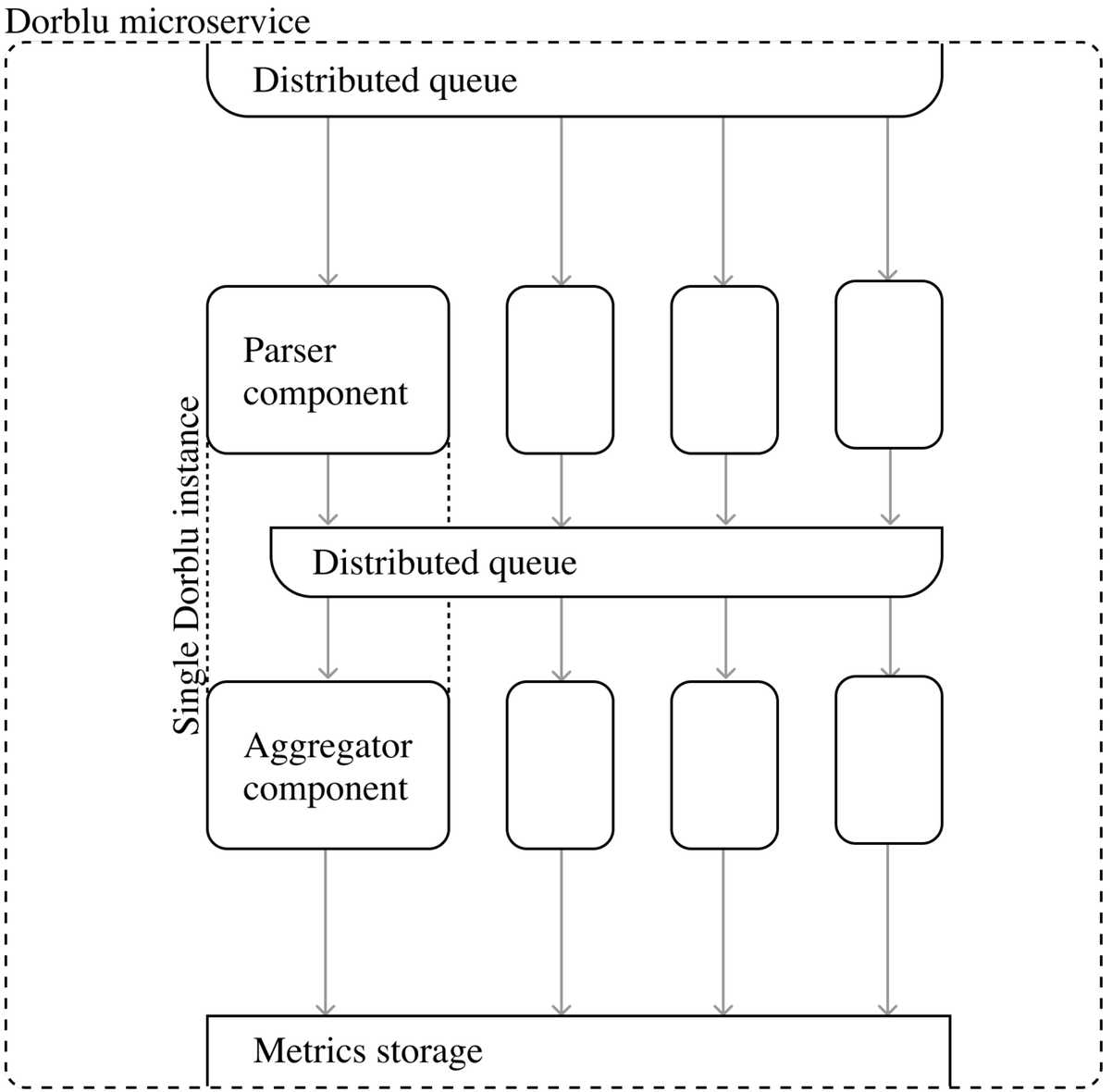
- Логи отправляются в распределённую очередь
- Микросервис выполняет всю обработку логов
- Метрики отправляются в хранилище



Реализация

Архитектура микросервиса

- Из логов извлекаются метрики, применяется конфигурация
- Промежуточные значения отправляются в распределённую очередь
- Метрики объединяются, подсчитываются итоговые значения за интервал



Реализация

Особенности

- Данные перераспределяются между этапами обработки
  A. Два воркера могут получить строчки логов одного микросервиса
  B. Но один воркер должен объединить все метрики из одного источника

Реализация

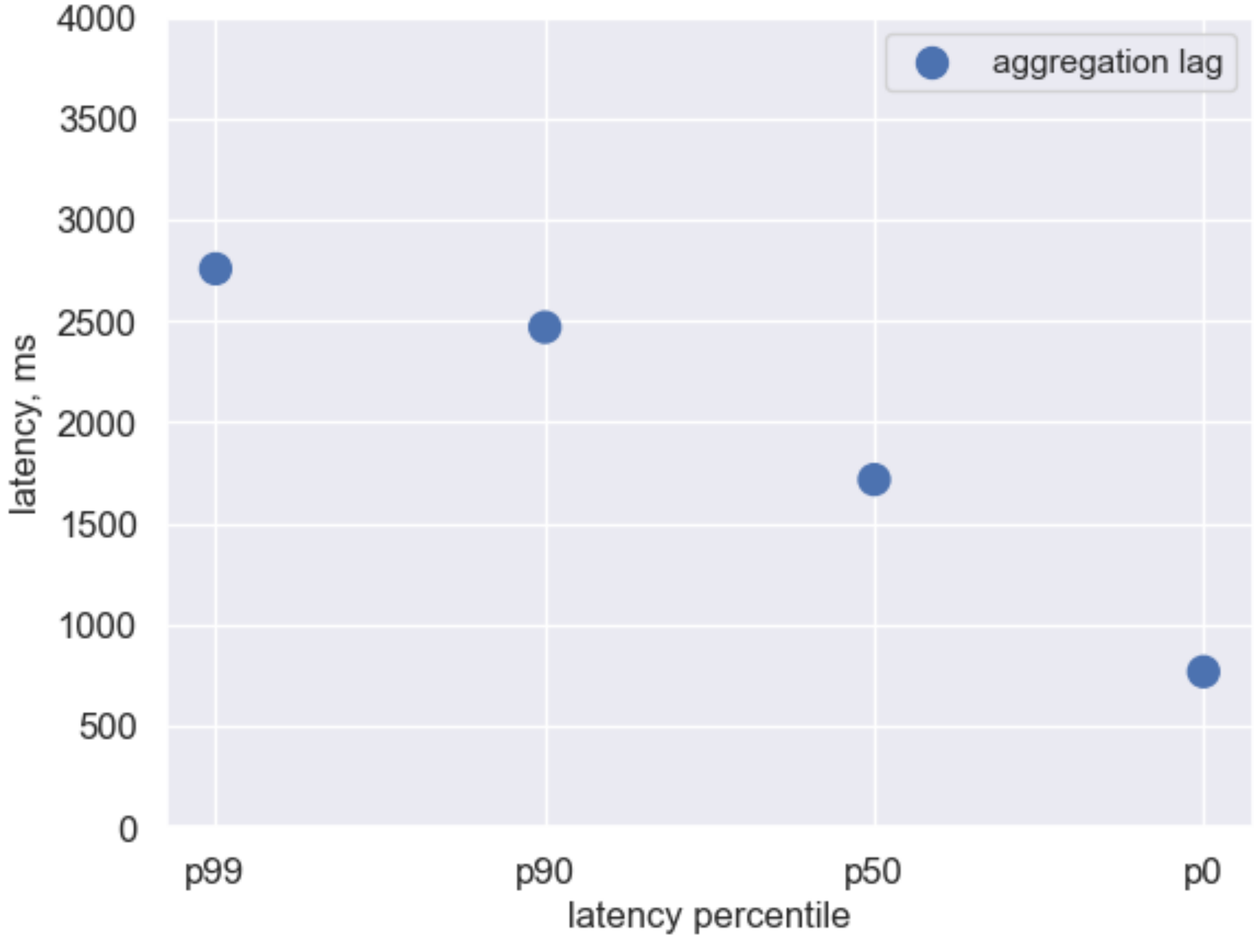
Особенности

- На этапе парсинга применяется конфигурация, которая хранится в базе данных
- Для низкого latency, опоздавшие данные игнорируются
- Так как часть данных теряется, итоговые значения метрик аппроксимируются по имеющимся данным

Результаты

Latency

- **3 секунды** с окончания интервала до отправки метрик в хранилище
- Опоздавшие данные игнорируются



Результаты

- В рамках курсовой, **реализован MVP сервиса** для агрегации метрик по журналу доступа
- Сервис обрабатывает больше **200 МБ логов в секунду**
- Latency в пределах **5 секунд**
- Сервис **хорошо масштабируется** и предоставляет **сильные гарантии на latency**
- Новый сервис позволил сократить интервал сбора метрик с минуты до 10 секунд в Яндекс Такси