Monitoring and Observability

Павел Селиванов
SRE

slurm.io

Мониторинг

Мониторинг: зачем?

- Наблюдать состояние системы

  В настоящий момент и с течением времени
- Уведомлять об аномалиях
- Анализировать тренды
- Проводить ретроспективный анализ

СЛЁРМ

Симптомы и причины

Симптомы и причины

- Симптом: что сломано?
- Причина: почему сломано?

СЛЁРМ

Симптомы и причины

- Симптом: нет соединения с домашним NAS
- Причина: кот перегрыз сетевой кабель

СЛЁРМ

Симптомы и причины

- Мониторинг: преимущественно на симптомах
- Алертинг: почти всегда на симптомах
- Анализ: контекст дополняется причинами

СЛЁРМ

White Box / Black Box

Black Box Monitoring

- Поведение, видимое извне (пользователями)
- Преимущественно ориентирован на симптомы
- Что сломано у пользователей прямо сейчас?

СЛЁРМ

White Box Monitoring

- Внутреннее состояние системы
- Необходим для определения причин
- На каком уровне системы поломка?
- Что может сломаться в ближайшем будущем?

СЛЁРМ

Golden Signals

Golden Signals

- Задержка (latency)
- Трафик (traffic)
- Ошибки (errors)
- Загруженность (saturation)

СЛЁРМ

Latency

- Время на обработку запроса
- Стоит измерять latency успешных запросов

  ...и отдельно измерять latency ошибок

Traffic

- Поток обращений к системе
- Специфичная высокоуровневая метрика
  - HTTP-запросы в секунду?
  - Транзакции в секунду?
  - Одновременные подключения?

СЛЁРМ

Errors

- Явные ошибки (HTTP 500)
- Неявные ошибки (HTTP 200, неверный контент)
- Нарушения SLA (HTTP 200, но дольше 3 секунд)

СЛЁРМ

Saturation

- Загруженность системы
  - CPU
  - Memory
  - I/O
  - Network Bandwidth

СЛЁРМ

Ловим за хвост

Средние значения

- Александр: $8,000
- Елена: $8,500
- Владимир: $7,500

- Среднее: $8,000

Средние значения

- Александр: $30
- Елена: $120
- Владимир: $23,850

- Среднее: $8,000

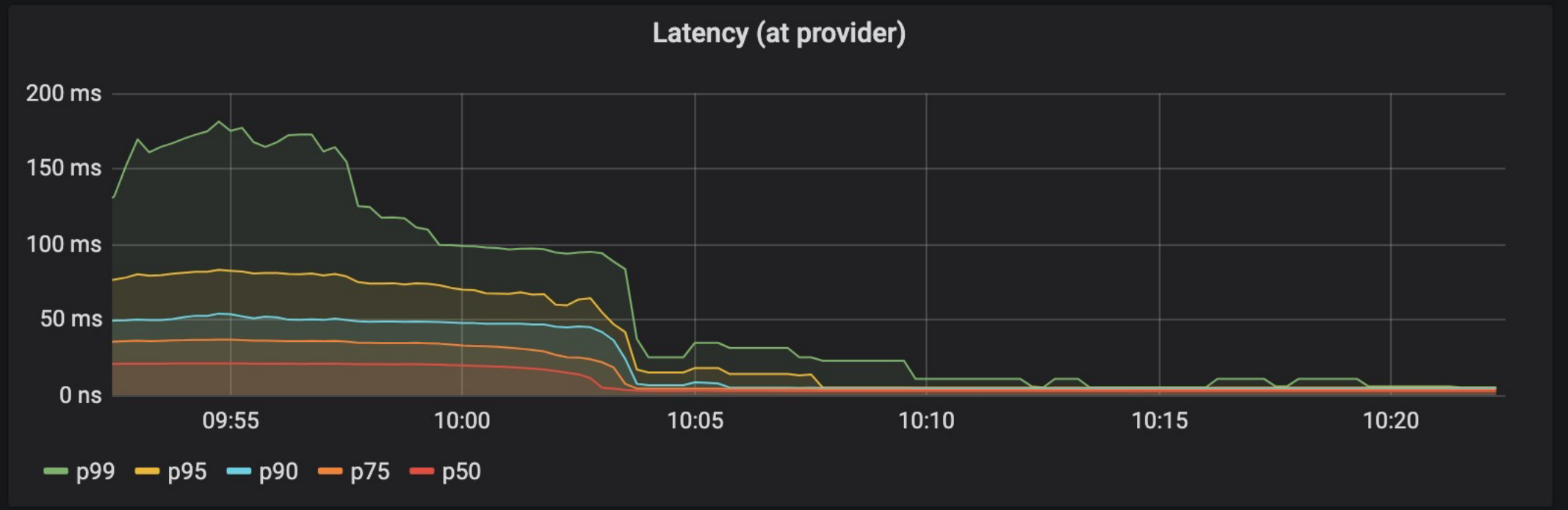
СЛЁРМ

Перцентили

- 90-й перцентиль (p90): наибольшее значение из 90% наименьших

- p90 = 125мс: 90% запросов обрабатываются за 125мс или меньше

СЛЁРМ


Latency (at provider)
200 ms
150 ms
100 ms
50 ms
0 ns
09:55
10:00
10:05
10:10
10:15
10:20
p99
p95
p90
p75
p50

Алертинг

Алерты

- *Каждый* алерт должен быть важным
- Если алерт возможно проигнорировать, его обязательно проигнорируют

СЛЁРМ

Хорошие алерты

- Приходят *только* нужному человеку
- Отражают проблемы *у пользователей*
- Подразумевают *немедленные действия*
- Не могут быть легко автоматизированы

СЛЁРМ

Observability

Observability

- Observability — качество системы, которое отражает, насколько подробно можно узнать о её внутреннем состоянии снаружи
- Observability включает в себя мониторинг
- Мы не можем мониторить метрики, которых нет

СЛЁРМ

Компоненты observability

- Метрики
- Трассировка
- Логи
- Алерты

СЛЁРМ

(Un)known unknowns

- Мониторинг помогает справляться с проблемами, которые мы ожидаем
- Observability помогает справляться с проблемами, которые мы *не* ожидаем

СЛЁРМ

Практика

https://gitlab.slurm.io/-/snippets/79

СЛЁРМ