Selectel

Как вовремя разбудить дежурного администратора

Мониторинг инфраструктуры Облака Selectel

Александр Барсков

Системный администратор дежурной службы

О чем доклад

- Работа с алертами в Дежурной службе. Проблемы и их решения
- Как мы на рынок за Incident Management ходили
- Сложности перехода на Open Source
- Наш опыт интеграции Grafana Oncall OSS

О компании Selectel

40+
продуктовых решений

6
собственных дата-центров

800+
сотрудников

23 000+
клиентов

С 2008 года помогаем компаниям решать бизнес-задачи, создавая надежную IT-инфраструктуру для проектов любой сложности.

Про облака Selectel

С 2013 года строим облачную инфраструктуру для клиентов.

10 лет
опыта

13
пулов облака

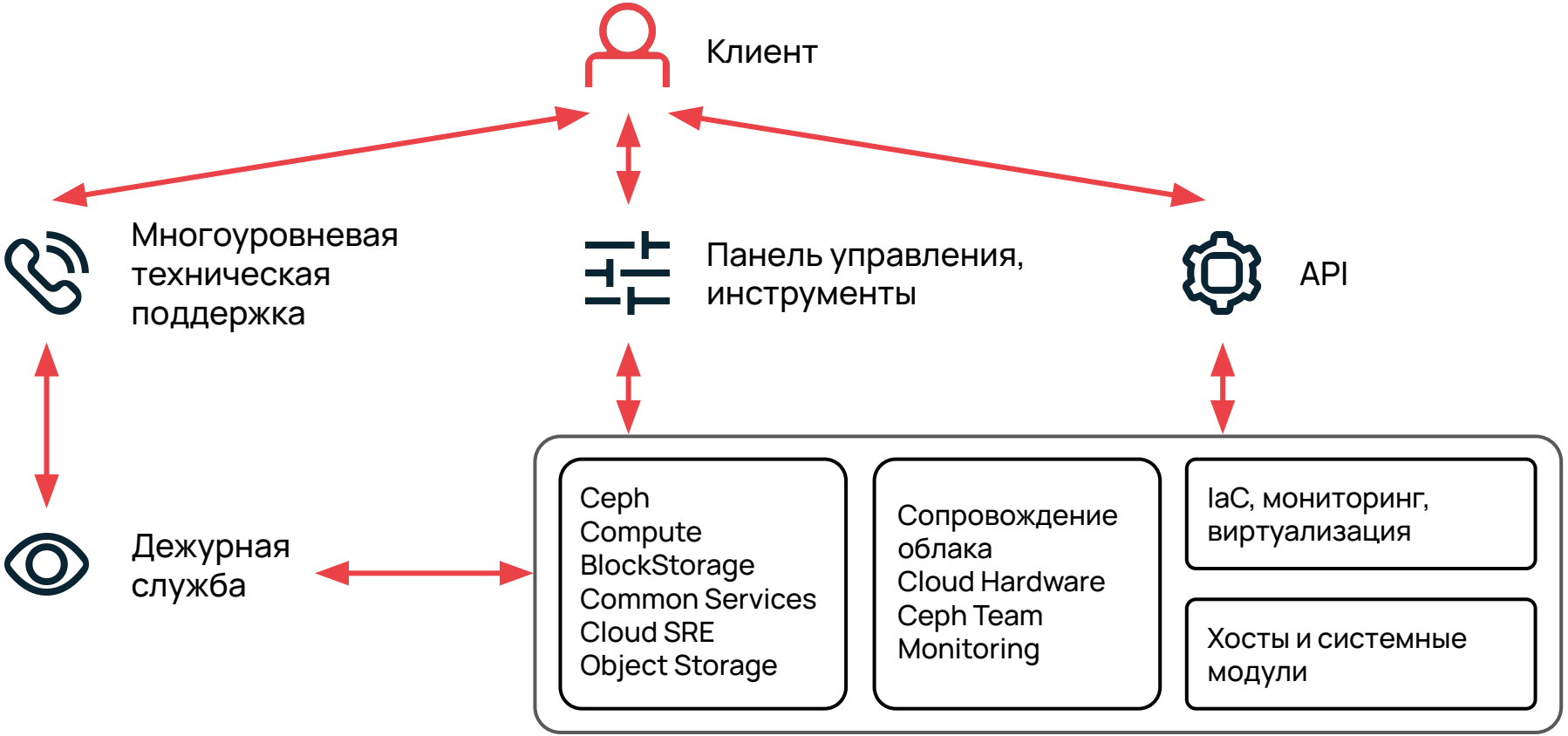
20+
петабайт клиентских данных

75 000
виртуальных машин

10
критичных алертов в день

Инфраструктура облака

Разработка и поддержка



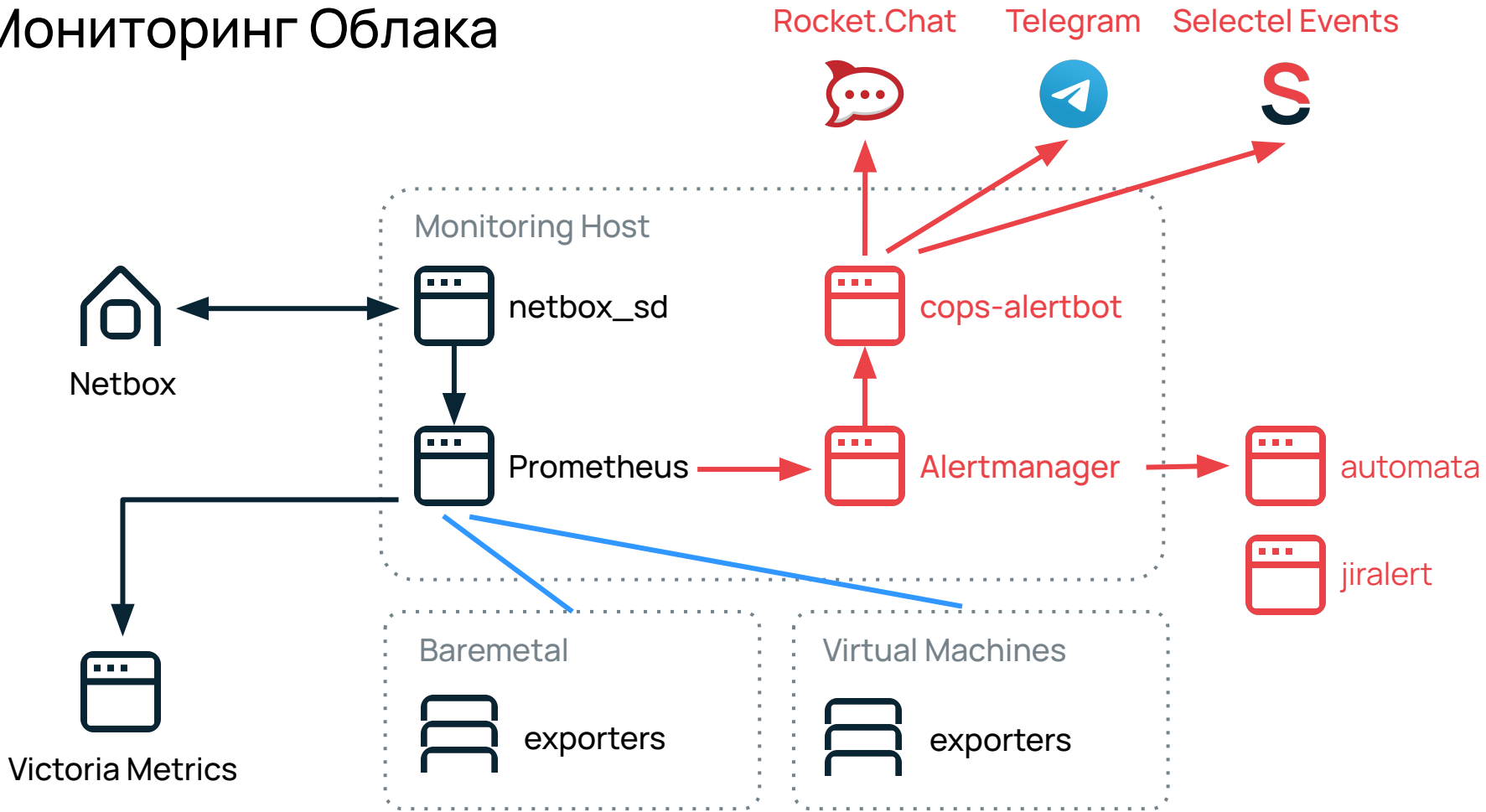
Дежурная служба

Работа
с сообщениями
мониторинга

Решение
инцидентов,
устранение аварий

Помощь саппорту
в дебаге сложных
кейсов

Мониторинг Облака

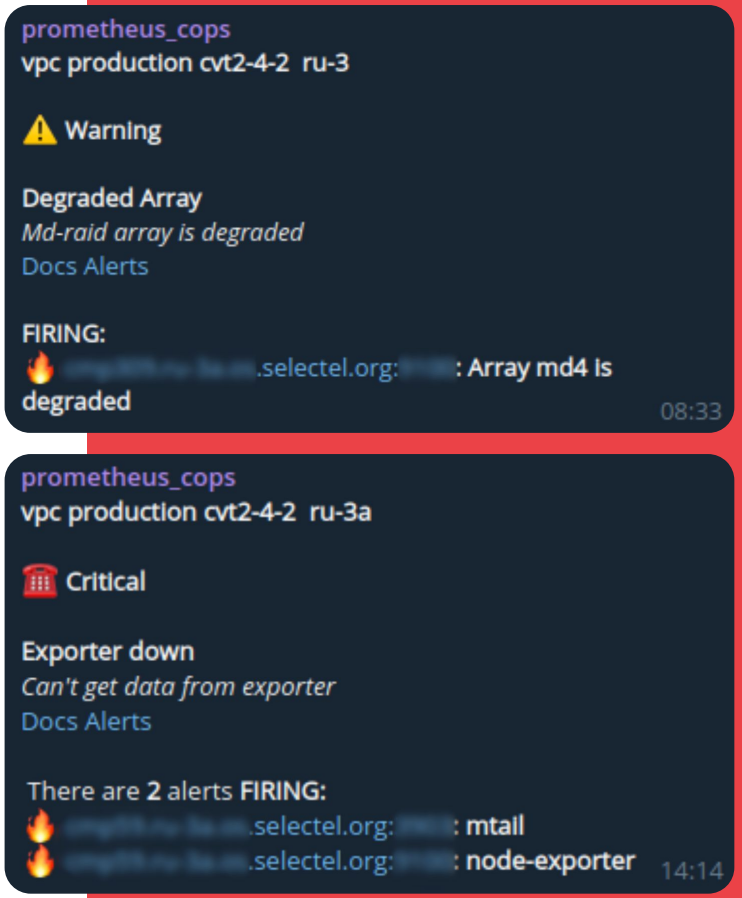


Требования к системе мониторинга

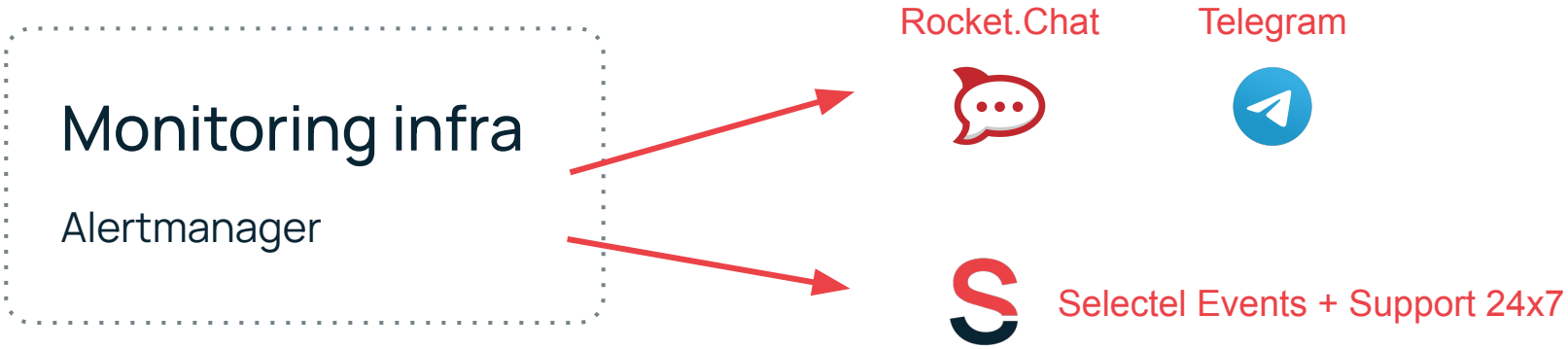
- Скорость доставки уведомлений
- Читаемые сообщения, удобный формат
- Инструкции и документация
- Агрегация уведомлений в очередь
- Связи между зависимыми сервисами
- Сбор данных для анализа

Требования к системе мониторинга

- Скорость доставки уведомлений
- Читаемые сообщения, удобный формат
- Инструкции и документация
- Агрегация уведомлений в очередь
- Связи между зависимыми сервисами
- Сбор данных для анализа



А что на практике?

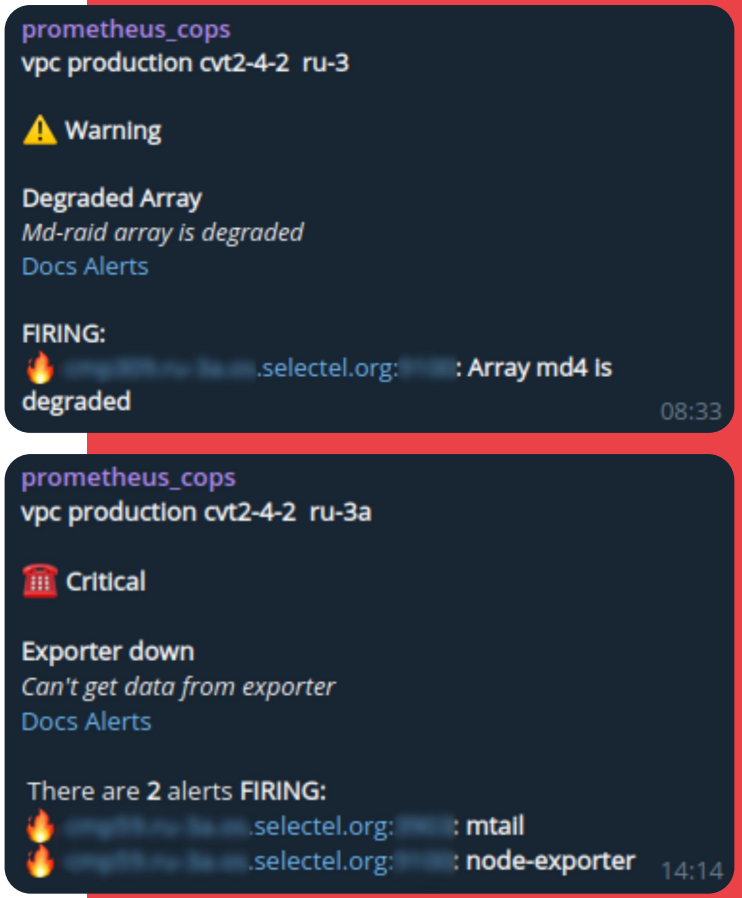


- Все алерты приходили в несколько каналов Rocket.Chat и Telegram
- Критичные алерты подсвечивались в Selectel Events
- Саппорт 24/7 отслеживали алерты
- Саппорт 24/7 звонили дежурным администраторам Облака

А что на практике?

Сотрудники

- Бесконечные окна, интерфейсы и чаты
- Нет связи между алертами разных сервисов
- Человеческий фактор, ошибки



А что на практике?

Сотрудники

— Бесконечные окна, интерфейсы и чаты

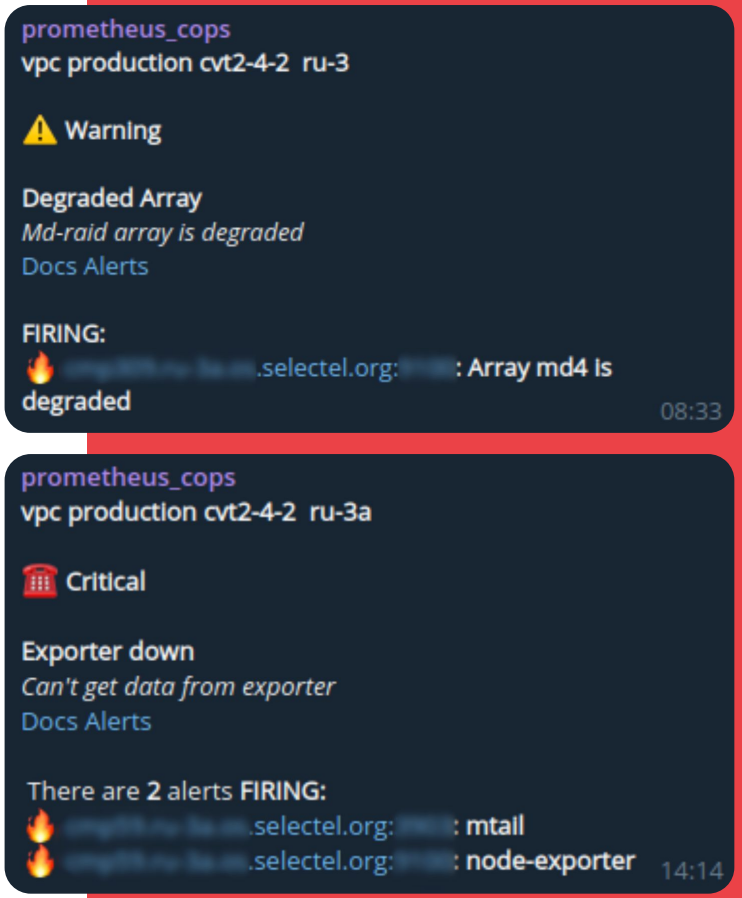
— Нет связи между алертами разных сервисов

— Человеческий фактор, ошибки

Менеджмент

— Сложно понять ход работы и найти ответственных

— Отсутствие сбора данных для анализа



А что на практике?

Сотрудники

— Бесконечные окна, интерфейсы и чаты

— Нет связи между алертами разных сервисов

— Человеческий фактор, ошибки

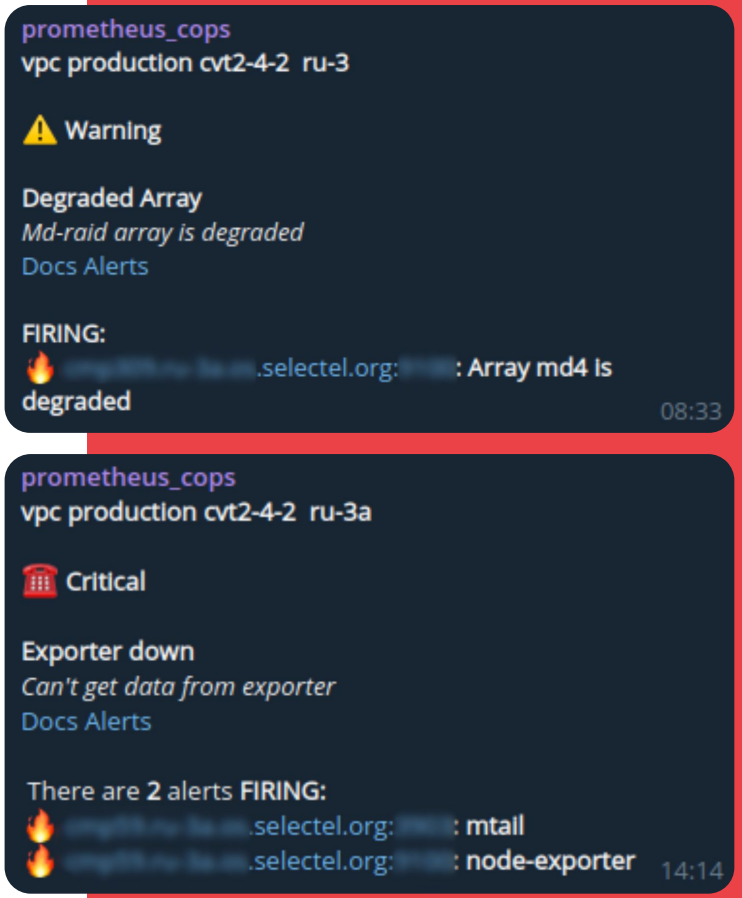
Менеджмент

— Сложно понять ход работы и найти ответственных

— Отсутствие сбора данных для анализа

Бизнес

— Время реакции на инцидент и его решения



Мониторинг. Алерты, чаты. Инциденты. Постмортем

Формулируем задачи

- Ускорить время реакции на инциденты
- Автоматизировать звонок дежурному
- Выделить единое окно, очередь алертов
- Наладить воркфлоу работы с алертами: ответственный, комментарии, история
- Прояснить взаимосвязи между сервисами: где причина, а где следствие
- Собирать данные, анализировать и прогнозировать их

Ищем систему управления инцидентами

Opensource — очень сырые решения, требующие значительного объема работ для запуска с минимальными функциями:

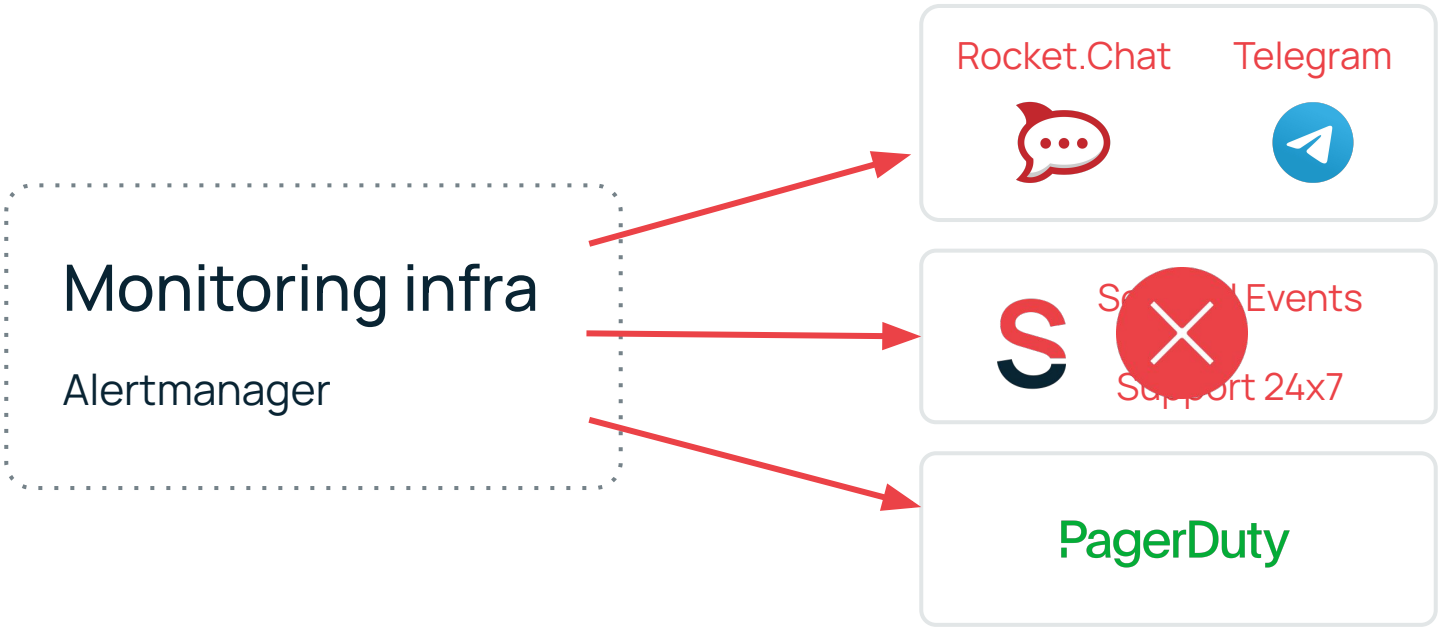
- Dispatch от Netflix
- Oncall от LinkedIn

Ищем систему управления инцидентами

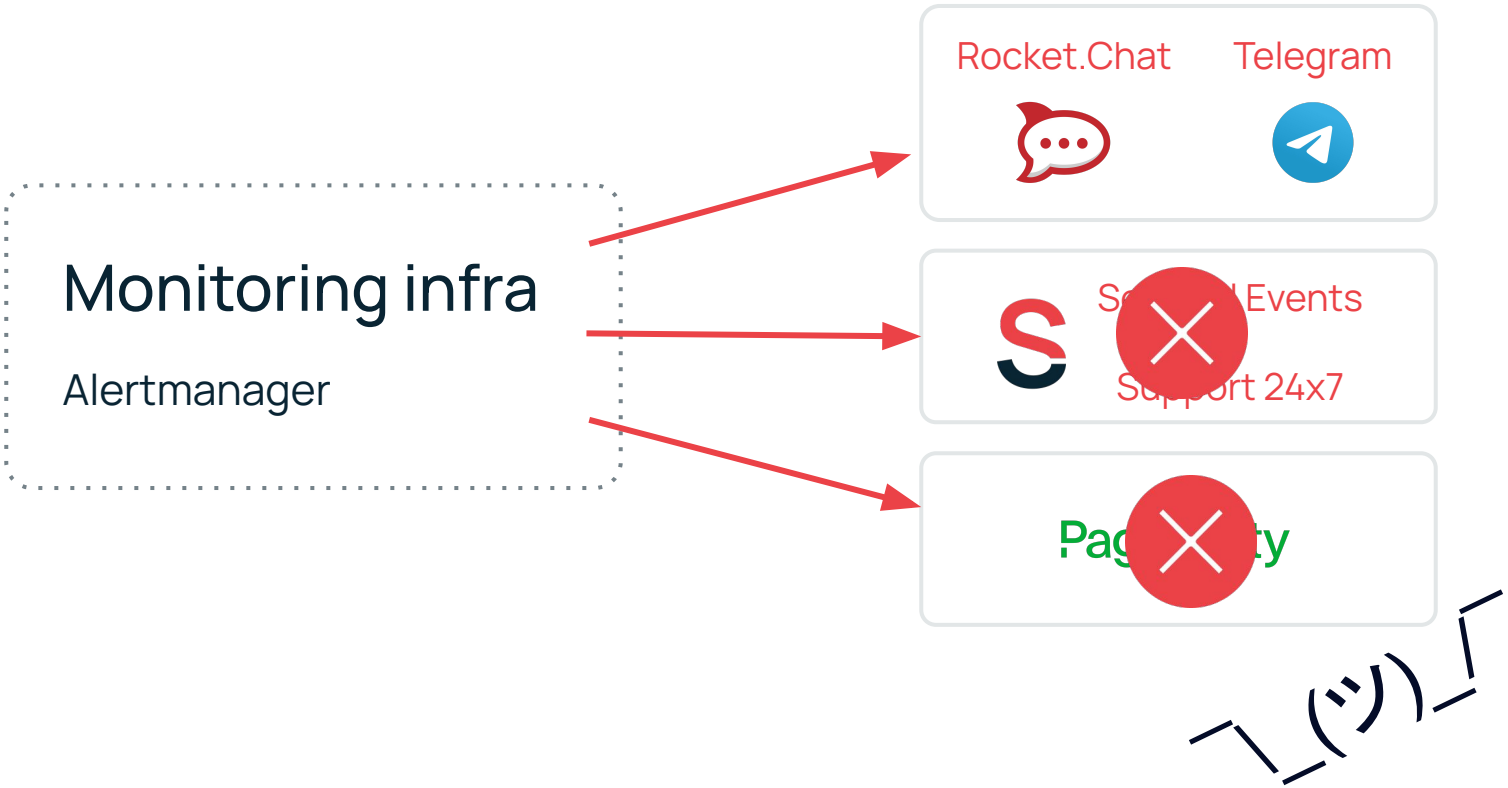
Проприетарные коммерческие решения — широкий набор инструментов, быстрый запуск:

- **OPSGENIE** от Atlassian: глубокая интеграция с Jira — это плюс… и минус
- **Datadog** — непростой в использовании, нужно правильно готовить
- **amixr** — отечественный чатопс на базе Slack и Telegram. Новые регистрации уже были закрыты, но сервис все равно не подходит, т.к. не поддерживает звонки на мобильные
- **VictorOps / Splunk On-Call** — официально в стране не продается
- **PagerDuty** — дорогой, но удобный и функциональный

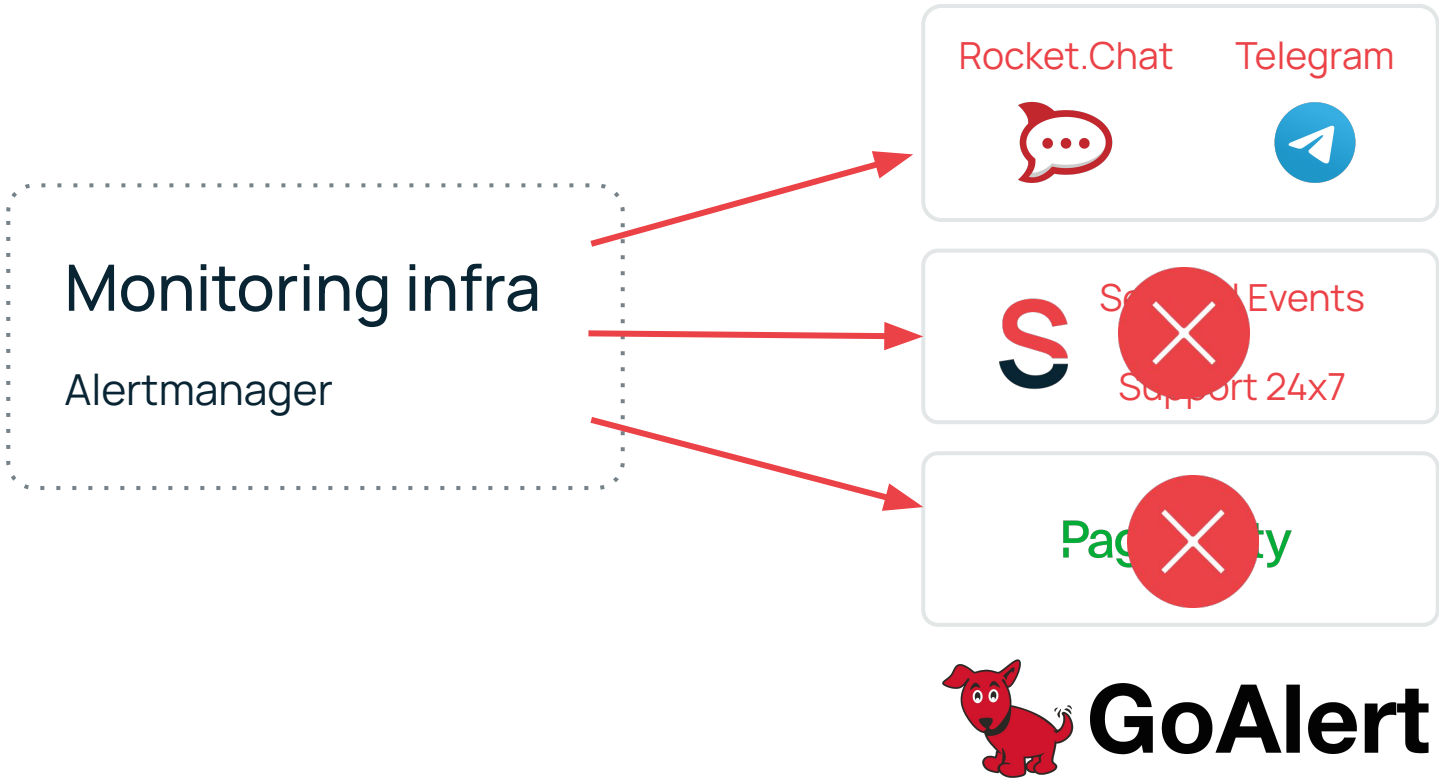
Мониторинг в облаке Selectel. Pager Duty



Мониторинг в облаке Selectel. А что случилось?



Мониторинг в облаке Selectel. GoAlert



Goalert. Необходимый минимум

- Подключили к Prometheus: доступно «из коробки»
- Написали прослойку между GoAlert и API сервиса телефонии
- Получили автоматический дозвон дежурному, согласно графику дежурств

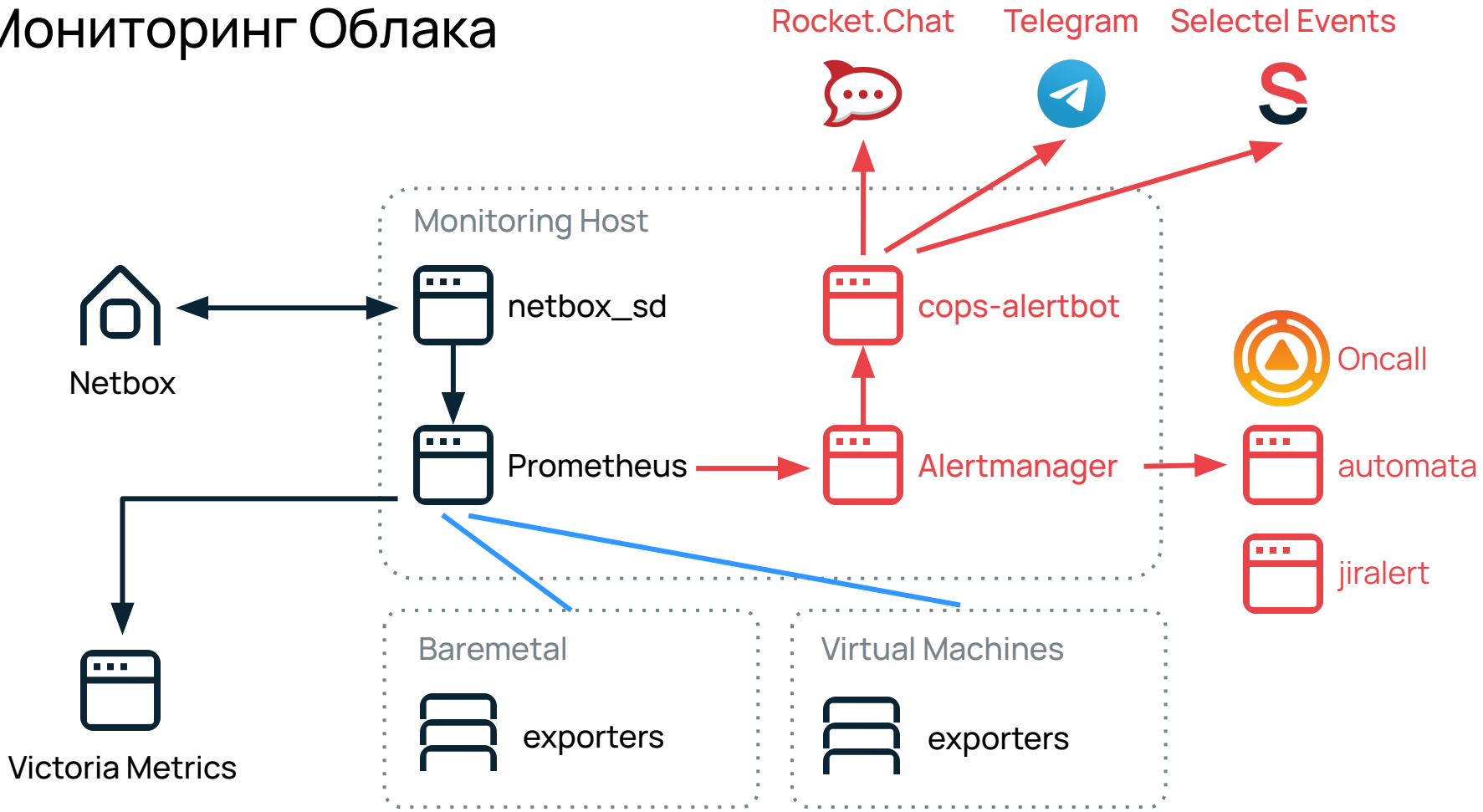
Но у нас еще болело:

- Не хватало прозрачного флоу работы
- Не было истории и комментариев
- Не собирались данные для анализа
- График дежурств — отдельное удовольствие

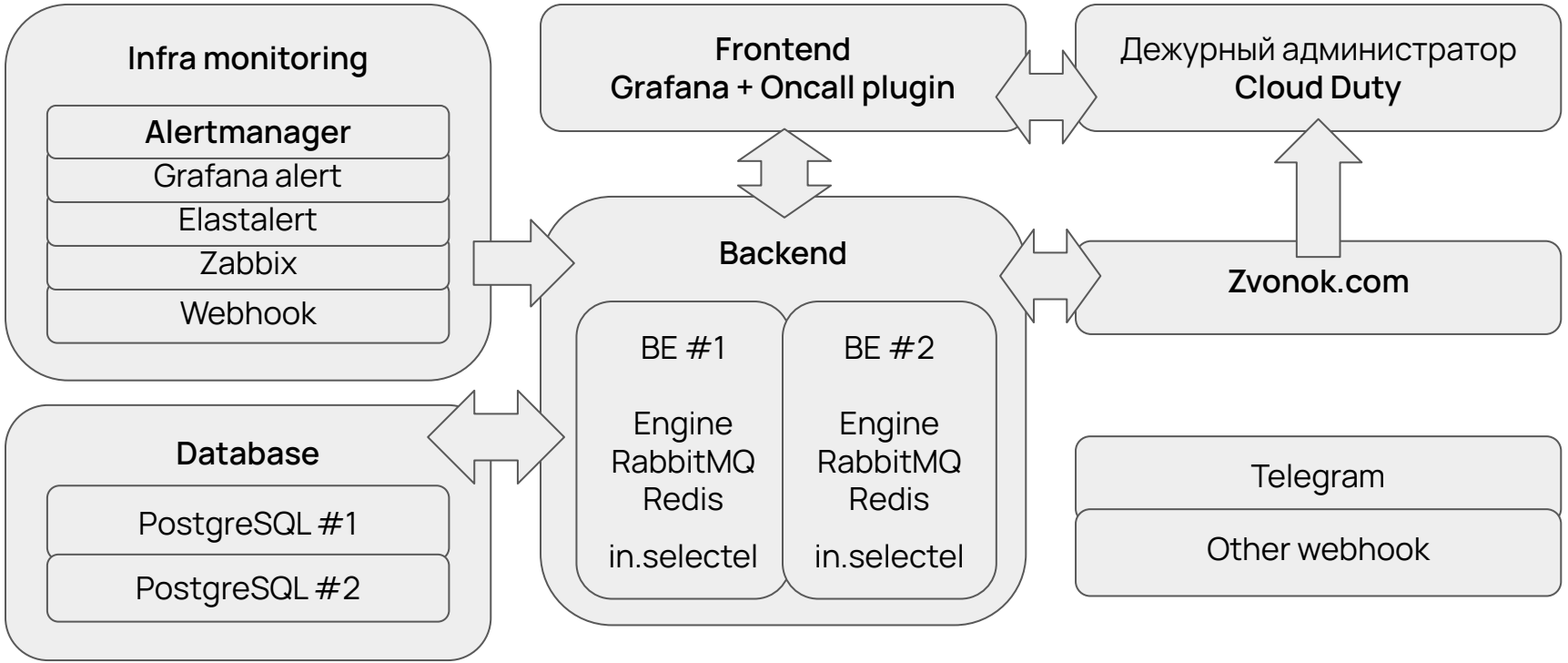
Как перешли на Oncall

- Осенью 2022 состоялся релиз Oncall
- Развернули версию Oncall для тестов
- Переписали интеграцию в API сервиса телефонии
- Добавили синхронизацию контактов сотрудников
- В январе 2023 переключили на него весь мониторинг облака

Мониторинг Облака



Grafana OnCall. Архитектура. Отказоустойчивость



Grafana Oncall. Наш идеальный вариант

✅ Open Source решение с коммерческой версией в Grafana Cloud

✅ Готовый механизм для надежного развертывания в Kubernetes

✅ Интеграция «из коробки» с Prometheus Alertmanager, Zabbix и Grafana Alerts

✅ Отечественные основатели и разработчики, RU-сообщество

❌ По умолчанию используется зарубежный сервис телефонии Twilio

Grafana Oncall. Наш идеальный вариант

✅ Open Source решение с коммерческой версией в Grafana Cloud

✅ Готовый механизм для надежного развертывания в Kubernetes

✅ Интеграция «из коробки» с Prometheus Alertmanager, Zabbix и Grafana Alerts

✅ Отечественные основатели и разработчики, RU-сообщество

❌ По умолчанию используется зарубежный сервис телефонии Twilio

Доделали сами:

✅ Расширили Incident API — PR #1037 https://github.com/grafana/oncall/pull/1037

✅ Добавили User webhook — PR #1038 https://github.com/grafana/oncall/pull/1038

✅ Интегрировали Oncall с внутренним порталом для синхронизации контактов дежурного

✅ Вместо Twilio «прикрутили» сервис телефонии zvonok.com

Grafana Oncall. Итоги на сегодня

✅ 2 минуты — максимальное время оповещения о critical alert

✅ Сняли нагрузку с саппорта — звонок дежурному работает автоматически

✅ Единое окно с упорядоченными в очередь алертами

✅ Меньше шума — схожие алерты группируются между собой

✅ Исполнитель алерта, понятный текущий статус, история работы с алертом

✅ Расписание дежурств с возможностью замен между сотрудниками

✅ Сбор данных об алертах в БД — материал для последующей аналитики

Backlog › ToDo

- Реализовать взаимосвязи между сервисами и их алертами
- Визуализировать данные об инцидентах: показатели, графики, тренды
- Добавить озвучку текста алерта во время звонка дежурному
- Полноценный chat-OPS в Telegram

Коротко о важном

- **Регламент работы** с алертами, аварийный регламент
- Простые и **понятные сообщения** от мониторинга
- **Инструкции** для сотрудников в тексте алерта
- **Автоматический звонок** на мобильный
- Очередь алертов, **единое окно**
- **Взаимосвязи между сервисами** – алерты-причины, алерты-следствия
- **Сбор данных**, их анализ и прогноз

Selectel. Мнения

Мы стремимся делать лучший продукт на рынке, а ваш голос может помочь нам в этом. Приходите к нам на исследования, делитесь опытом и получайте подарки →

Selectel

selectel.ru
selectel
selectel

Остались вопросы? Обращайтесь!

Александр Барсков
tg: @Barsman