Наш путь: выбор и принятие APIM Gravitee

Спикер: Никита Михайлов,
Передовые Платёжные Решения

ППР

Никита Михайлов

- **Старший инженер интеграций** в департаменте разработки и продуктовых решений
- **Создаю интеграции** и внедряю инструменты
- **Хочу больше уметь** поэтому рассказываю что знаю
- **Вдохновлён идеей подключить что угодно к интернету**

ППР

Немного про нас

Чем занимаемся

ППР

Наш бизнес

- Процессинг платежей
- Топливные карты
- Предоставления широкого спектра услуг для бизнеса

ППР

Наши цели

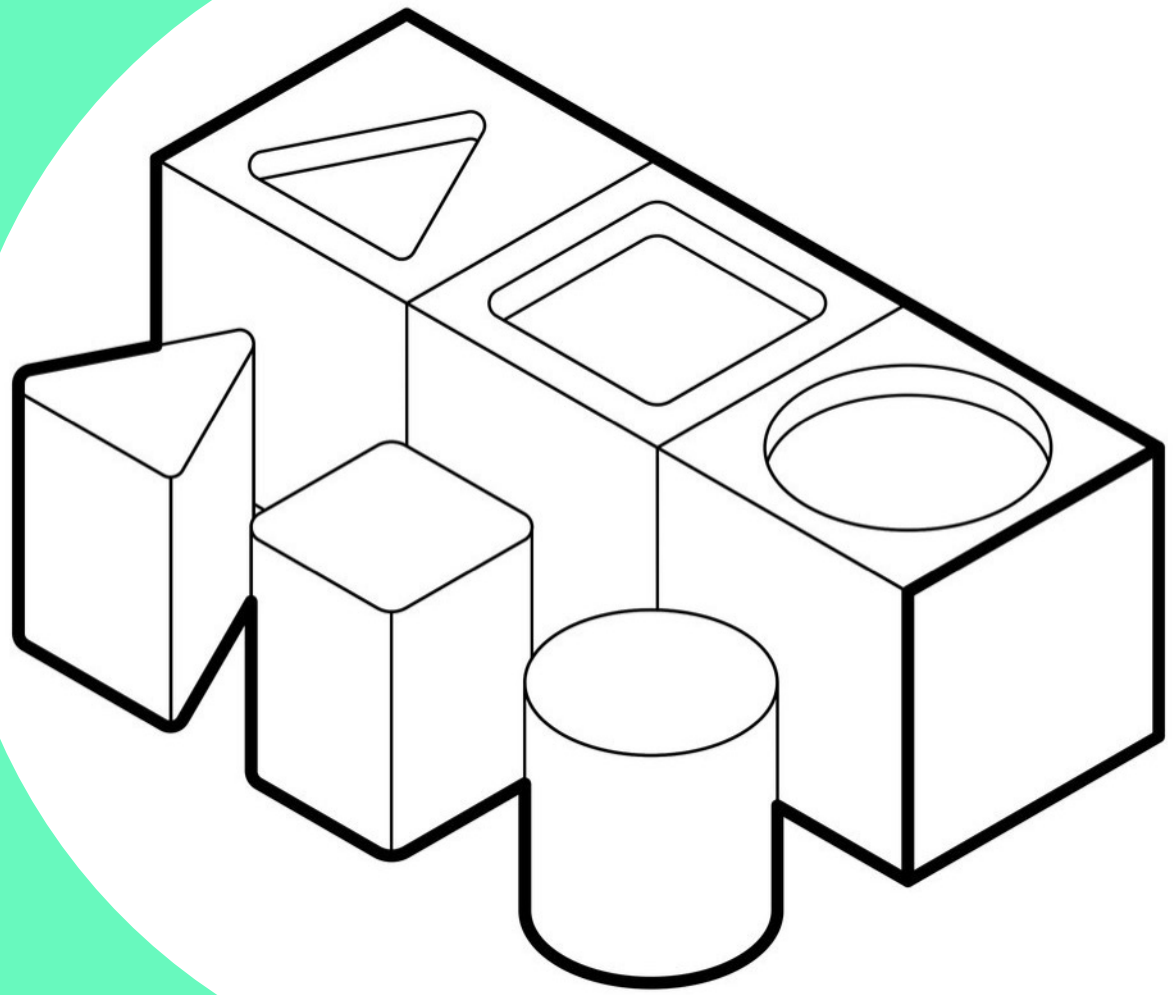
Экосистема решений для бизнеса

Лучший цифровой опыт для клиентов и партнёров

ППР

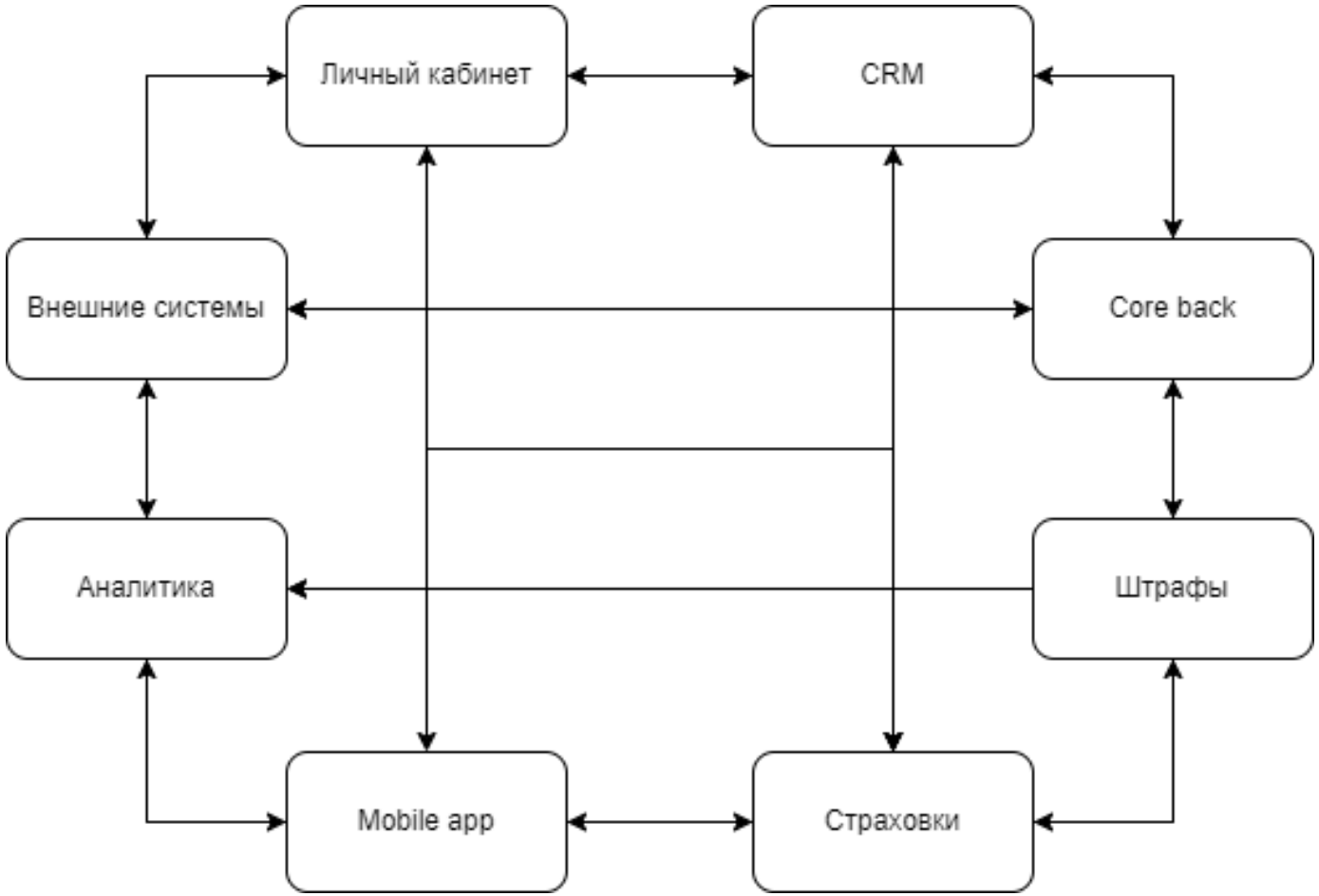
Решаемые задачи

Ключевые цели



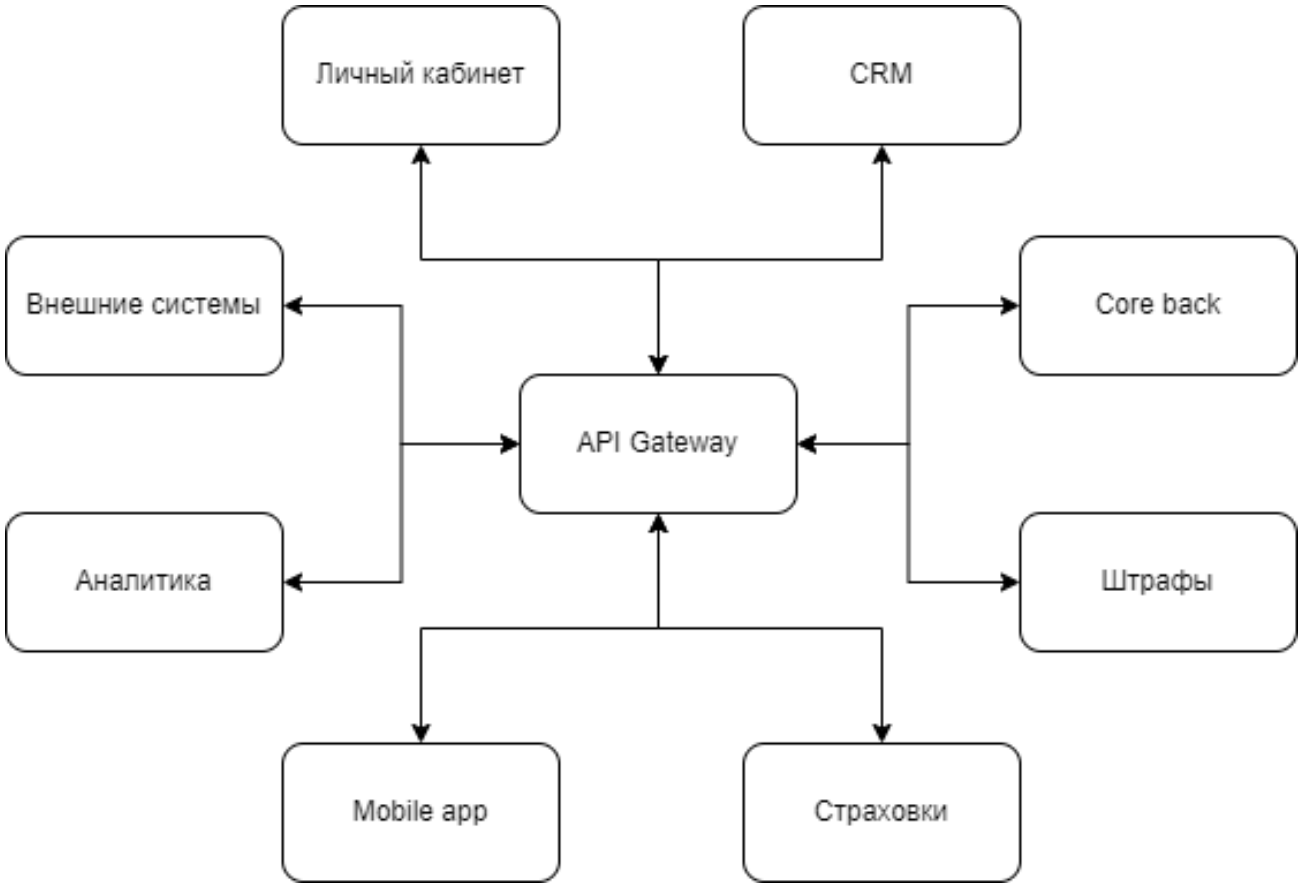
ППР

Очень больно



ППР

А как хочется



ППР

Ключевые цели

- Безопасность
- Маршрутизация
- Агрегация
- Кеширование

ППР

Ключевые цели – чего достигли

- Безопасность
- Маршрутизация
- Агрегация
- Кеширование

ППР

Анализ и альтернативы

Почему Gravitee?

ППР

Инструменты и требования

- 14 требований
- 21 инструмент
- 2 раунда
- 3 прототипа
- 1 выбор

Изыскания

Инструмент	Среда работы	Environment hub (UI консоль)	Политики доступа пользователей	Пользовательская саморегистрация	Политики доступа разработчиков	Саморегистрация разработчиков	CIAM	CI/CD (DevOps)	Стоимость	mTLS	Политики количества API запросов	Политики контроля ресурсов для API	Возможность интеграции с не API системами
IBM API GateWay	Облако, локально (только micro gw)	Можно иметь несколько каталогов в рамках одной среды (сервиса)	Доступ определяется на уровне API (когда происходит деплой можно определить кто имеет доступ)	Доступно. Кастом или встроенное решение.	Поддержка функциональности ролей	Нет	Open Authorization (OAuth)/OpenID Connect (OIDC)	apic cli	Бесплатно + подписк + лицензии	Да	Определяется для каждого API, достаточно гибко	Нет	Нет
Сбер API GateWay	Облако	Одно облако с разделением API на группы	Нет	Нет	Поддержка функциональности ролей на облаке	Нет	OpenID/SAML на уровне облака с нюансами	Manual	Платное	Нет	Определяется на уровне API	Нет	Нет
Yandex API Gateway	Облако, Terraform, Yandex.Cloud Toolkit	Нет	Только yandex.cloud пользователи	Нет	Поддержка функциональности ролей на облаке	Нет	Нет	CLI, API Methods, Terraform, Yandex.Cloud toolkit	Подписка	Нет	Нет	Нет	Только те что развёрнуты на Yandex.cloud
Mulesoft	Локально, Консоль - несколько сред	Да. Функционал RTF (возможно создание сред мануально, но управление через hub)	Управляется с помощью communities	может быть создан процесс саморегистрации и через salesforce	Поддержка функциональности ролей	SSO (OpenID, SAML)	Да, на уровне API	maven	Нужно связаться для получения прайса (можно уточнить у наших US, EU коллег)	Да с нюансами	Определяется на уровне API Manager	для API	Да
NGINX API GateWay (payed)	Локально, любая среда (контейнер)	Нет, но косвенно может быть реализовано через просмотр конфигураций	Нет	Нет	-	Нет	Да через имплементацию на js	Через `.conf` файлы		Да	Определяется на уровне API	для среды	Нет

ППР

Раунд 2


krakenD
Прототип WSO2
GRAVITEE.IO
неделя
неделя
Прототип KrakenD
неделя
Прототип Gravitee
WSO2

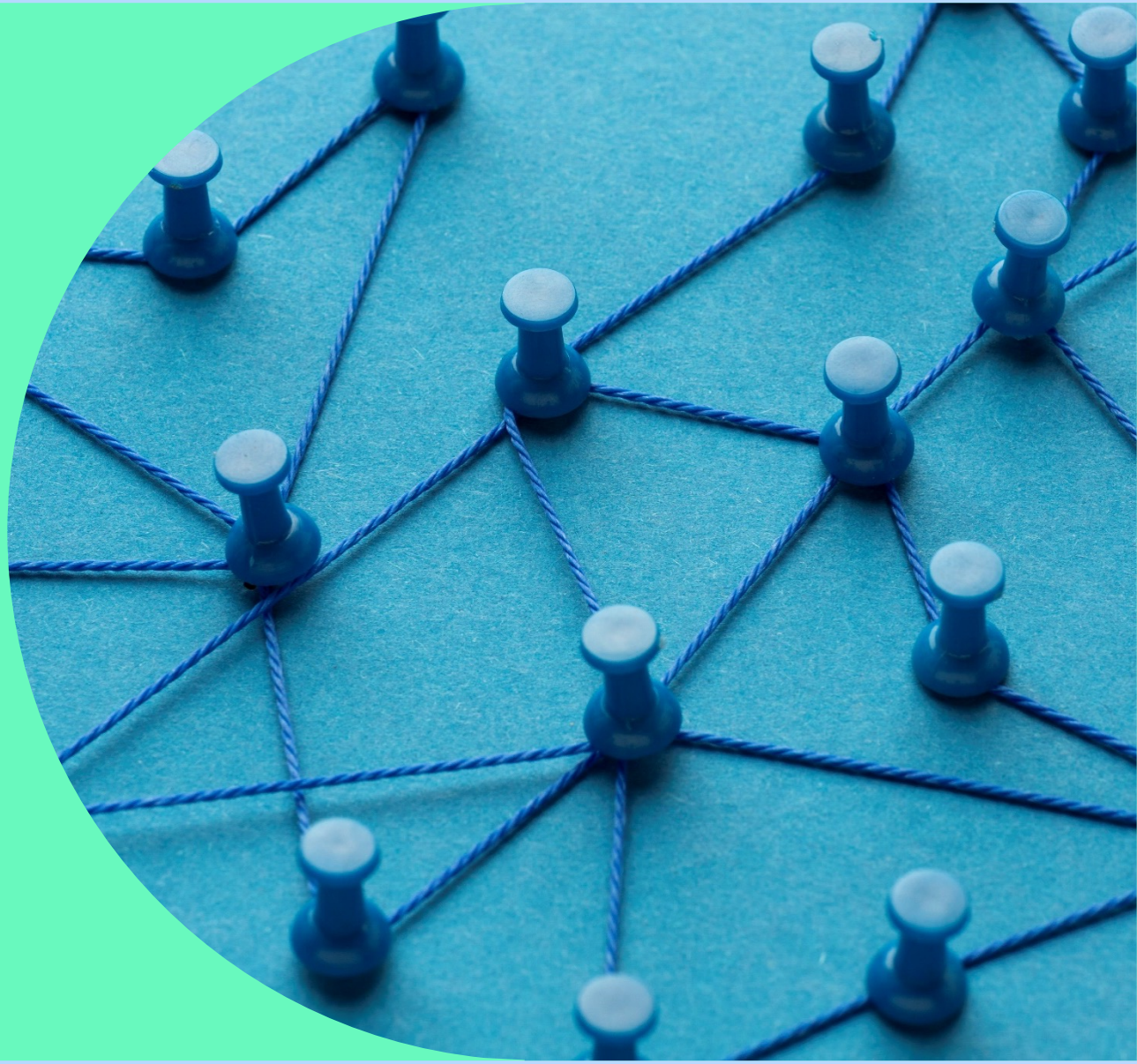
ППР

Выбор


krakenD
GRAVITEE.IO
WSO2
неделя
неделя
неделя
Прототип KrakenD
Прототип WSO2
Прототип Gravitee

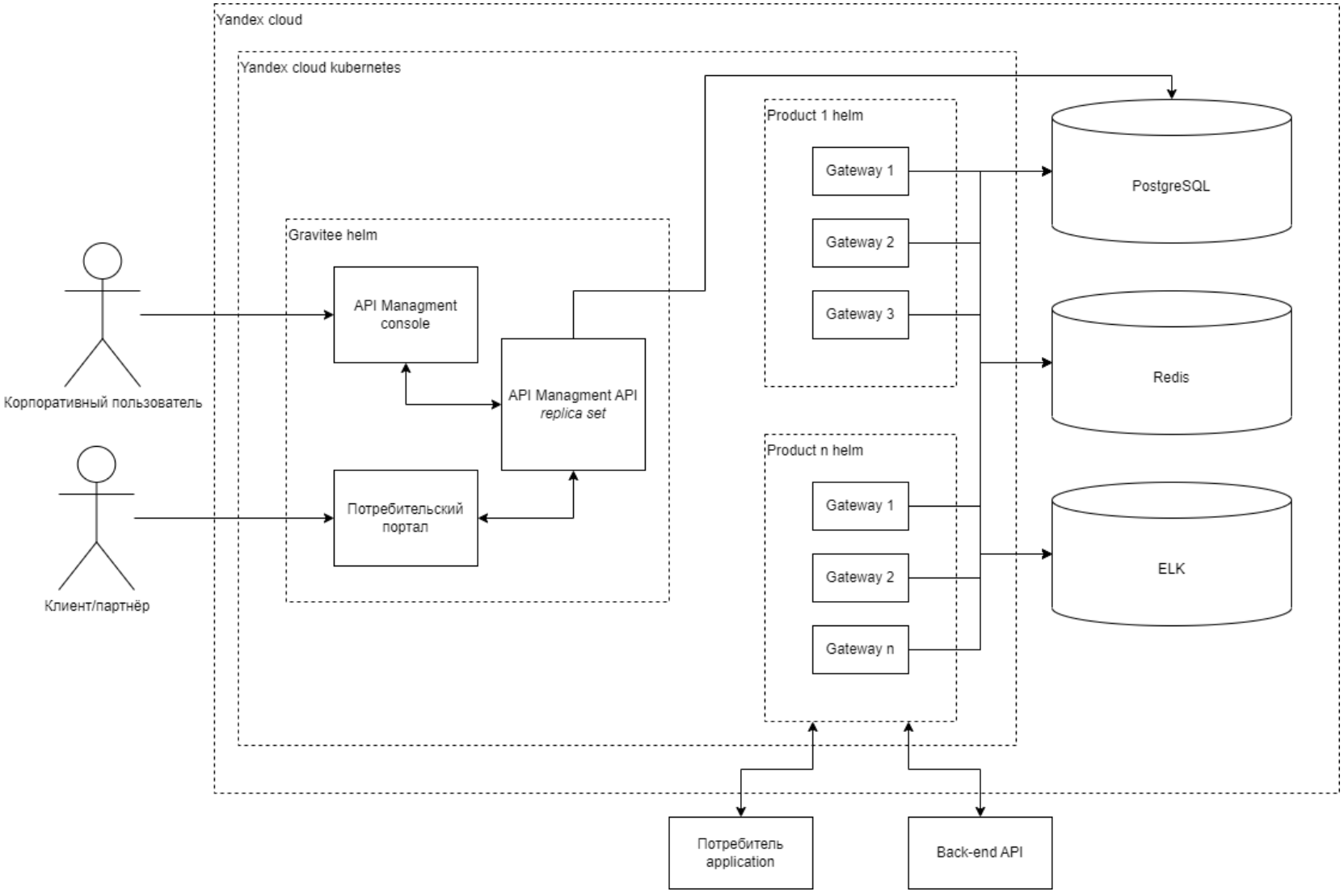
ППР

Архитектура решения



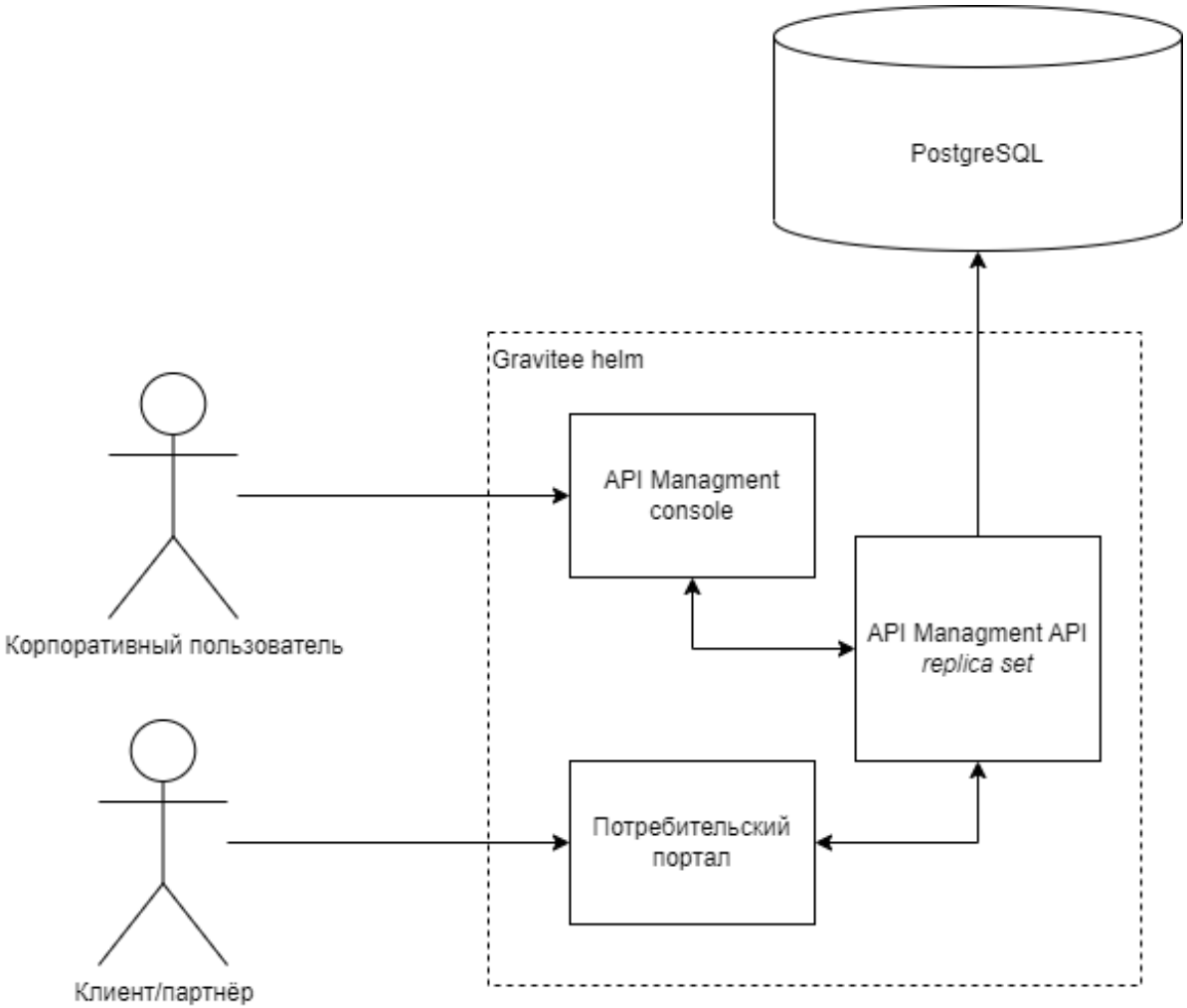
ППР

Архитектура решения



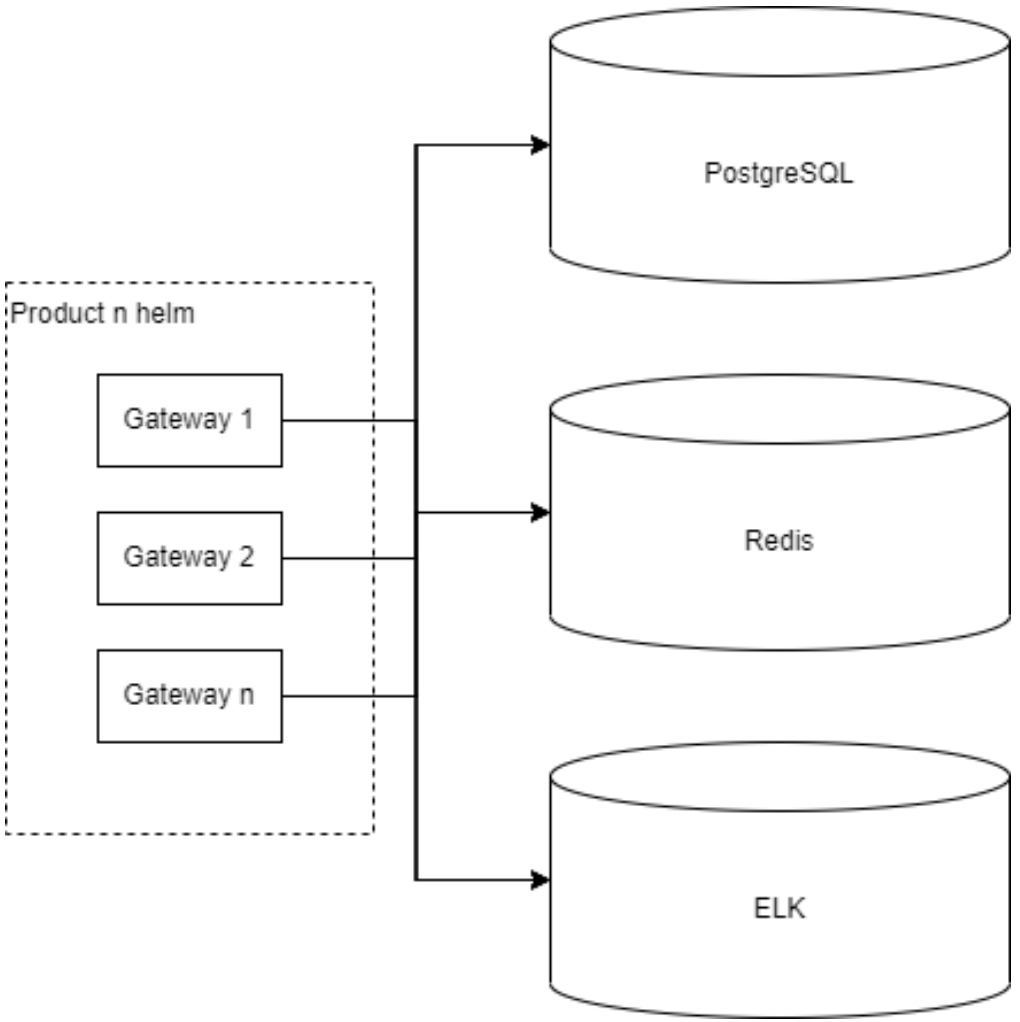
ППР

Архитектура решения



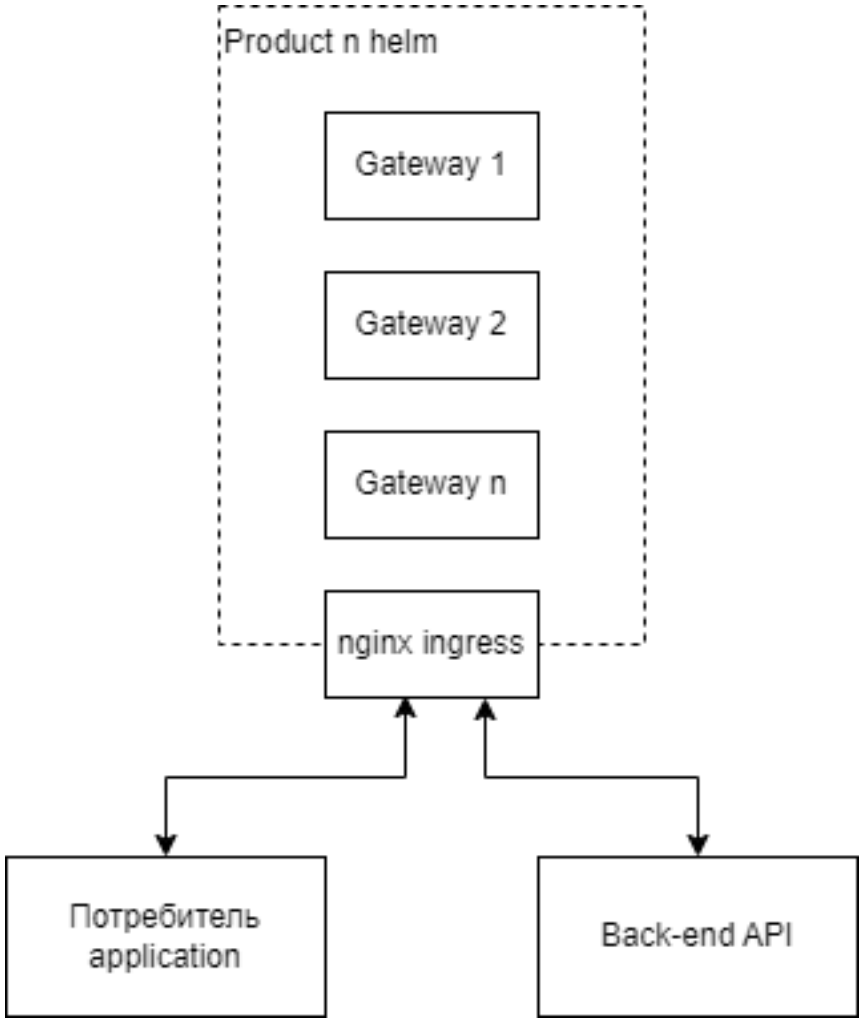
ППР

Архитектура решения



ППР

Архитектура решения



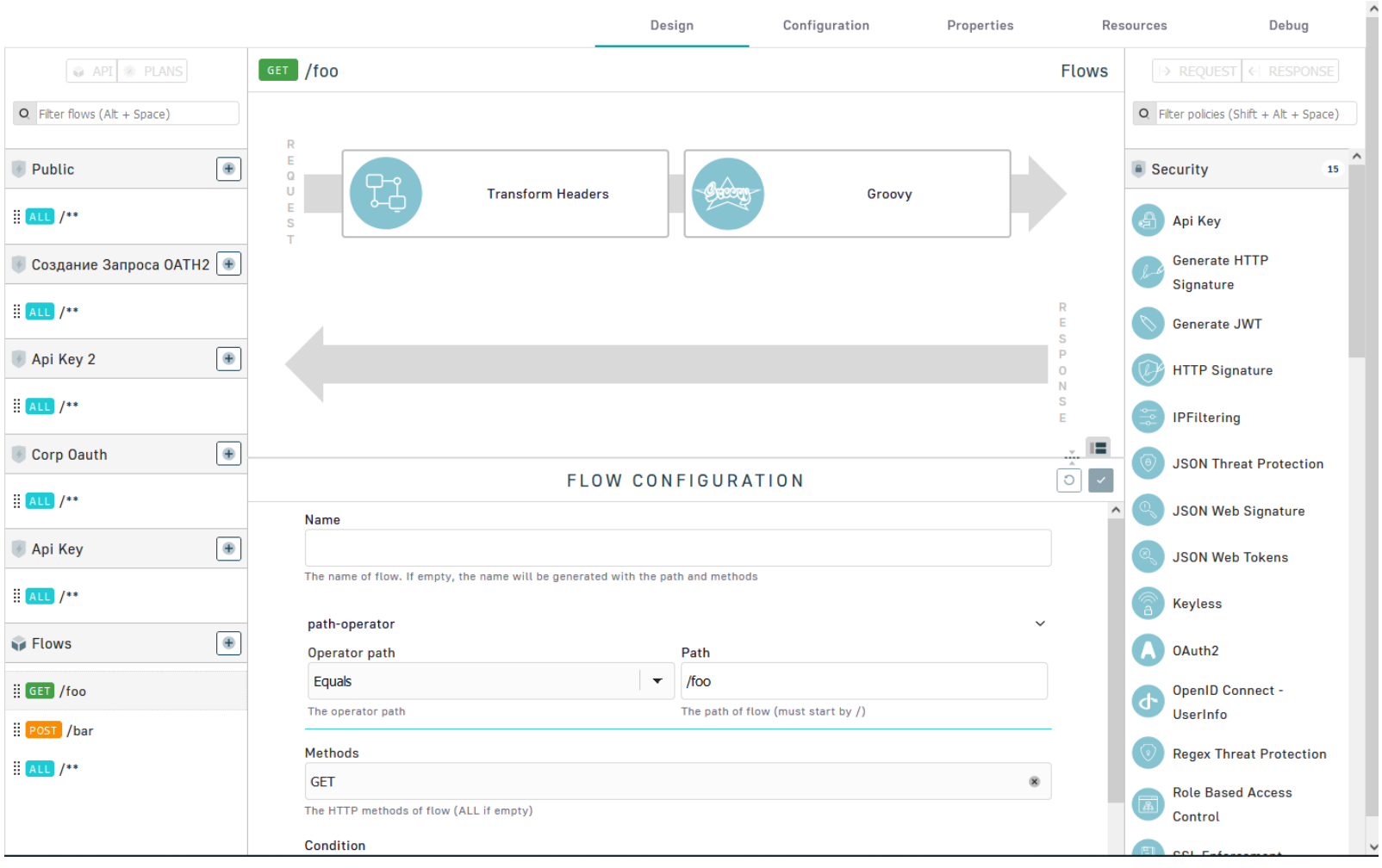
ППР

Конфигурация и backup

Жизненный цикл конфигураций API и их восстановление

ППР

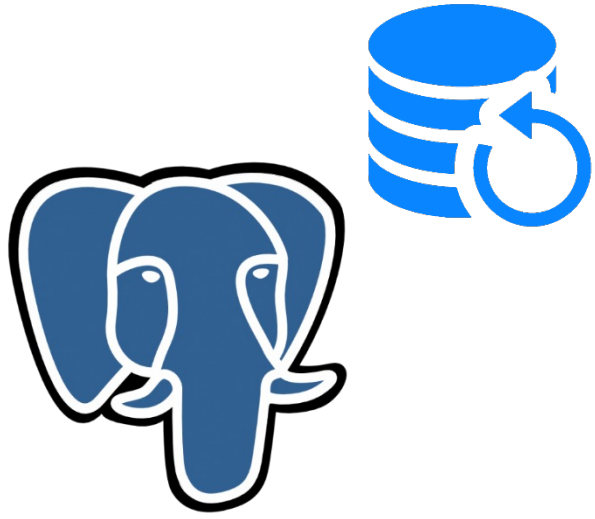
Конфигурация API



ППР

Конфигурация в базе данных

- Разработка через UI
- Test/stage API
- Эксперименты
- Переменные среды
- Жизненный цикл API
- Доступ к API администрами
- Мониторинг
- Аналитика



Конфигурация в git

- CI/CD
- Доступ к prod версии для команд
- Prod релиз процесс

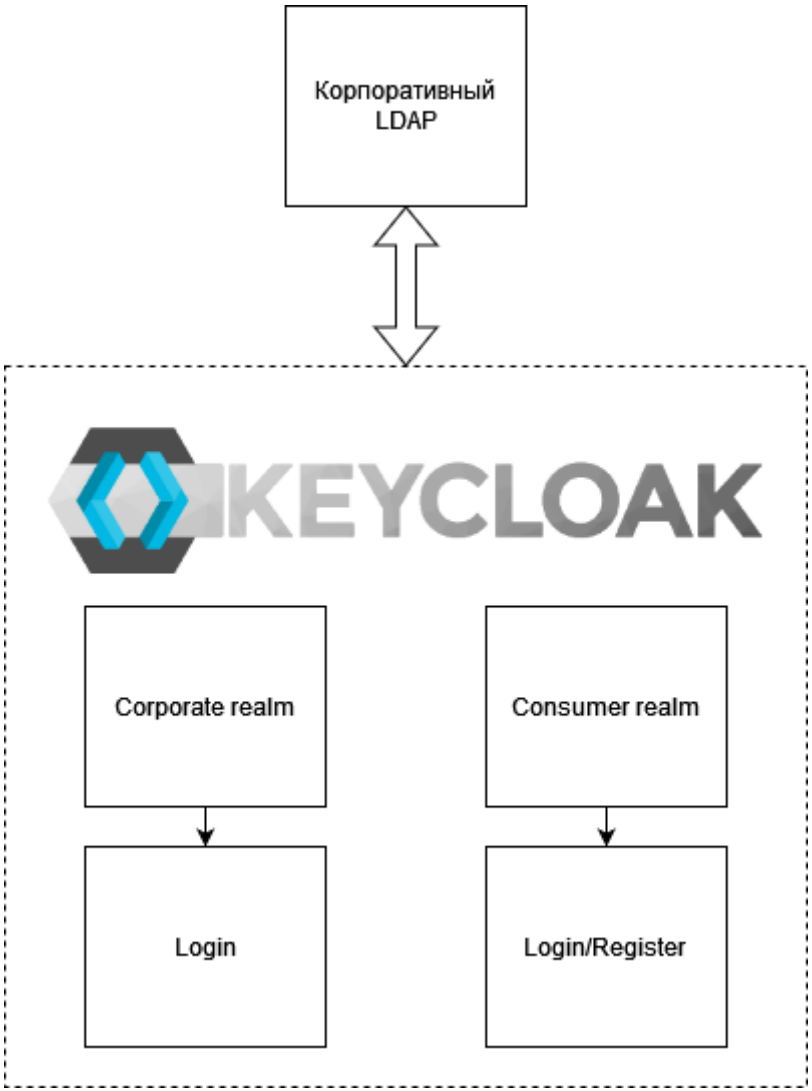
GitLab

Аутентификация и авторизация

ППР

Аутентификация

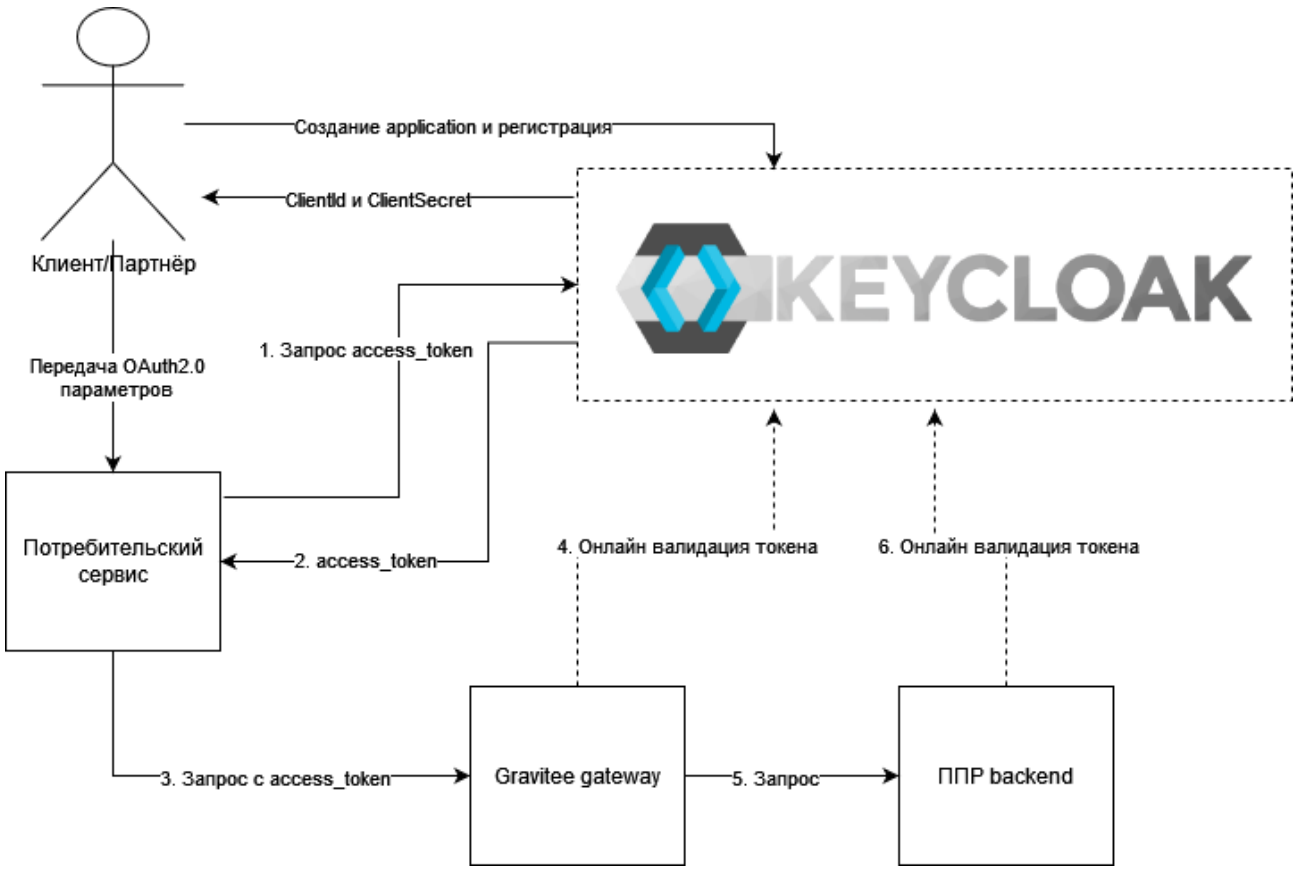
- Доступ для корпоративных пользователей
- Доступ для внешних пользователей
- Разделение на роли
- Контроль доступа



ППР

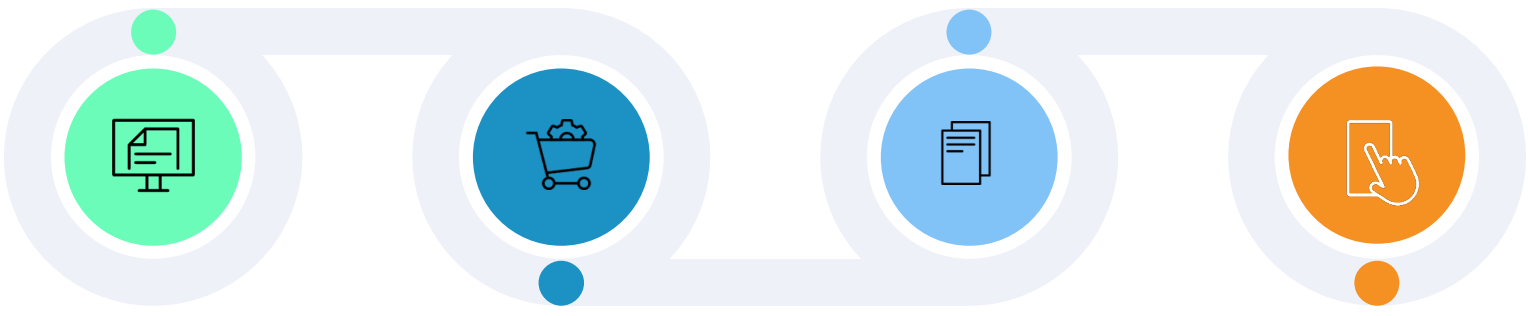
Авторизация

- Доступ для систем делающих API запросы
- OAuth2.0 как стандарт
- Контроль доступа
- Dynamic client registration



ППР

Процесс предоставления безопасного доступа



Правило
Команда создаёт правило проверки роли

Application
Потребитель получает clientId и clientSecret

Выдача роли
Команда запрашивает выдачу нужной роли для clientId

Подписка
Потребитель подписывается на API и получает данные через процесс OAuth2.0

ППР

Собирать самому или брать готовое?

ППР

Образы

- Требования ИБ
- Дополнительный функционал и фикс багов

graviteeio/apim-portal-ui
graviteeio/apim-portal-ui-ee

graviteeio/apim-management-ui
graviteeio/apim-management-ui-ee

graviteeio/apim-management-api
graviteeio/apim-management-api-ee

graviteeio/apim-gateway
graviteeio/apim-gateway-ee

ППР

Свой потребительский портал

- Локализация
- Отсутствие нужной гибкости в дизайне
- Критичные баги
- План по единой поддержке контента

gravitee/ppr-apim-portal-webui

Подводные камни

Но есть нюанс

ППР

Баги

Группа пользователей для application

Нельзя выдать доступ группе пользователей на application

- Добавляем каждого пользователя отдельно
- Ждём фикс

ППР

Моментальное заполнение пула PostgreSQL

Моментальное заполнение пула PostgreSQL

- Во время работы и обновлений 200+ активных подключений к базе
- Новые конфигурации не обновляются на Gateway

- Для каждого сервиса Gravitee установили минимальные и максимальные размеры пула подключений

Регенерация clientSecret

ППР

Регенерация clientSecret

- Процесс не нативен для keycloak, хотя работает из коробки с Gravitee AM
- Потребители не могут сами создать себе новый clientSecret

- Создано API для работы с keycloak admin API
- Пользователи могут сами создавать новые clientSecret

ППР

Среды

Отсутствие сред в community версии

- Нельзя бесплатно создать dev, test и другие среды
- Заблокирован механизм миграции из среды в среду

- Создали процесс работы в одной среде
- Разделили среды на уровне инфраструктуры
- Доступ к продуктивной среде через CI/CD

Алертинг

Отсутствие алертинга в community версии

- Нельзя нативно создать уведомления на события связанные с запросами

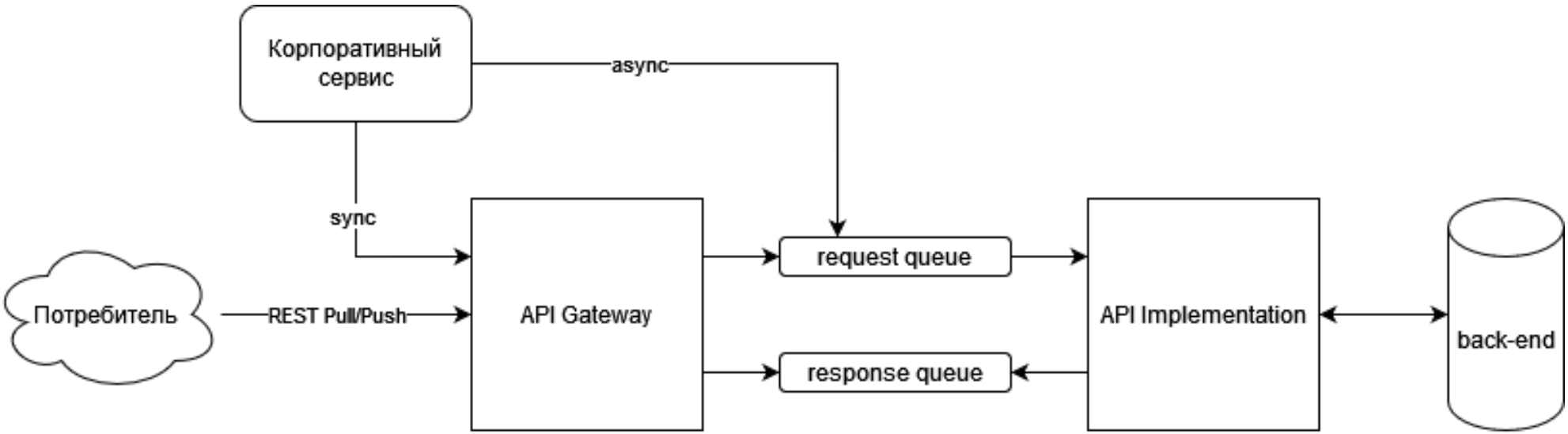
- Используем плагины ELK для отправки уведомлений

ППР

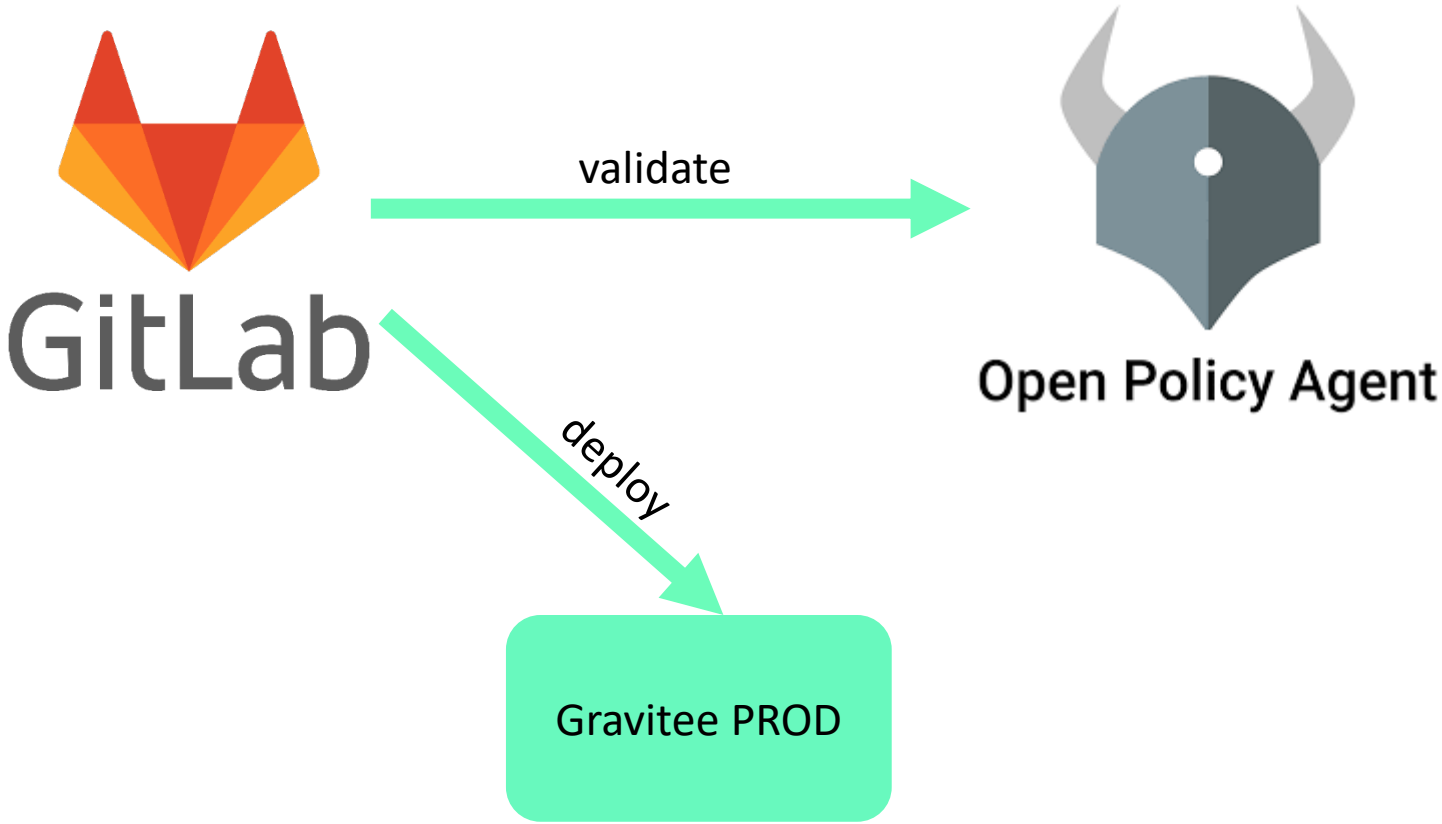
Дальнейшие планы

ППР

Асинхронные API



Валидация конфигураций



Метрики

ППР

Метрики

С начала 2023 года по данный момент

6 Активных API

39618 Созданных лидов

514 Каско полисов

319 Полисов страхования грузов

3 Запроса в секунду

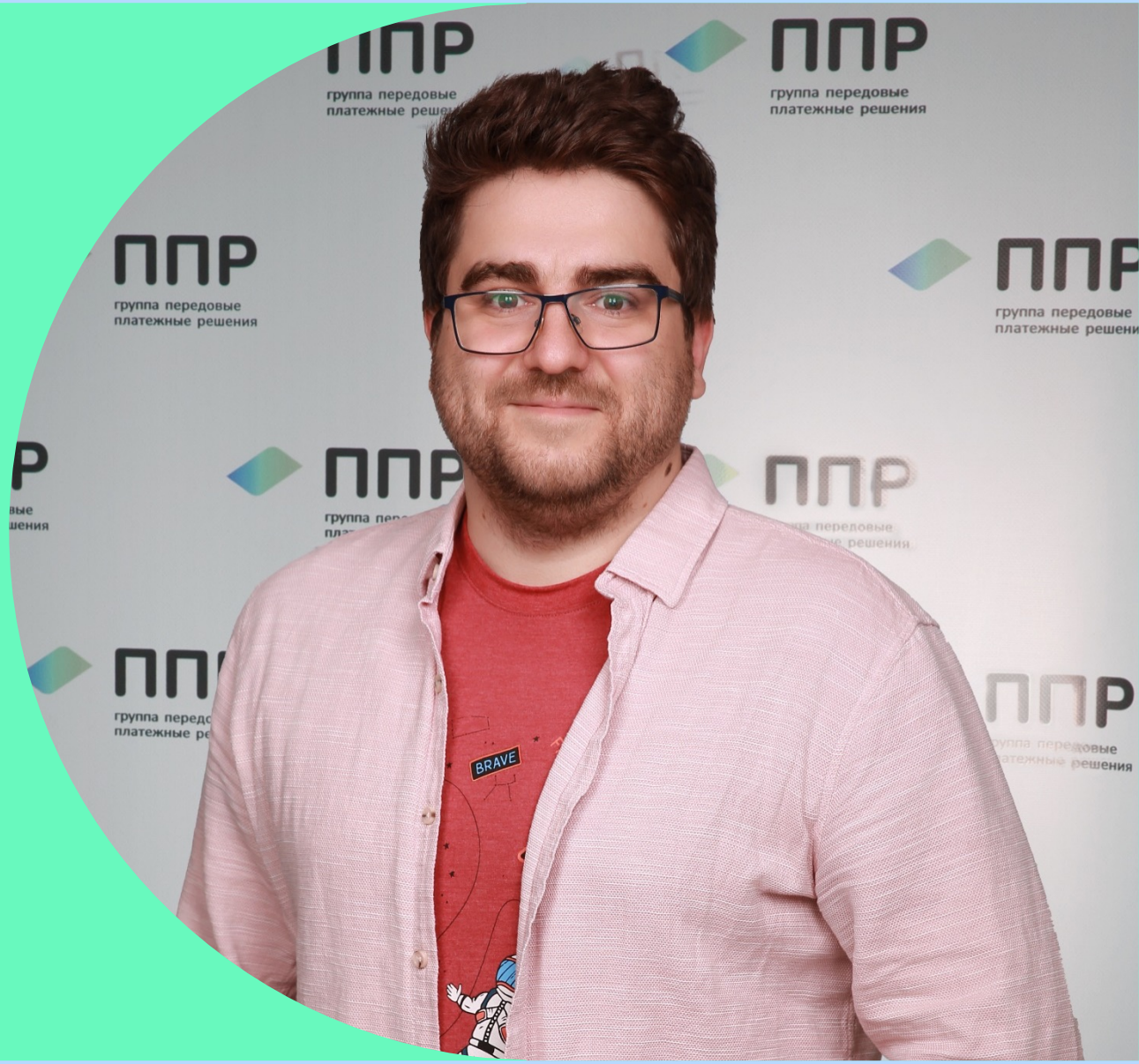
160 ms Среднее медианное время обработки запроса (включая работу back-end)

ППР

Русскоязычное Gravitee сообщество

ППР

Время для вопросов



Никита Михайлов

Nikita.Mikhailov@pprcard.ru

ППР

Наш путь: выбор и принятие APIM Gravitee

Спикер: Никита Михайлов,
Передовые Платёжные Решения

ППР