

Облака, их бенефиты и КАК К НИМ ГОТОВИТЬСЯ



Максим Чернухин

СТО клиентского сервиса
СберСтрахование Жизни

О себе:

- 10+ лет в IT
- Разрабатывал Back-end Front-end
- Люблю ТРИЗ и сложные задачи
- Нравится восходить на горы
- Есть 30 – 40-летний бонсай



Сегодня мы разберём:

- Что такое Cloud
- Варианты использования Cloud
- Требование к современным проектам
- Итоги

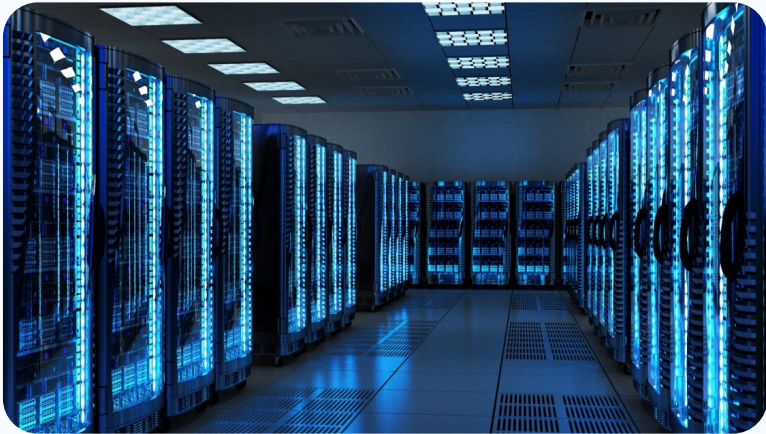


Сейчас мы тут

- Что такое Cloud
- Варианты использования Cloud
- Требование к современным проектам
- Итоги



Что такое Cloud?



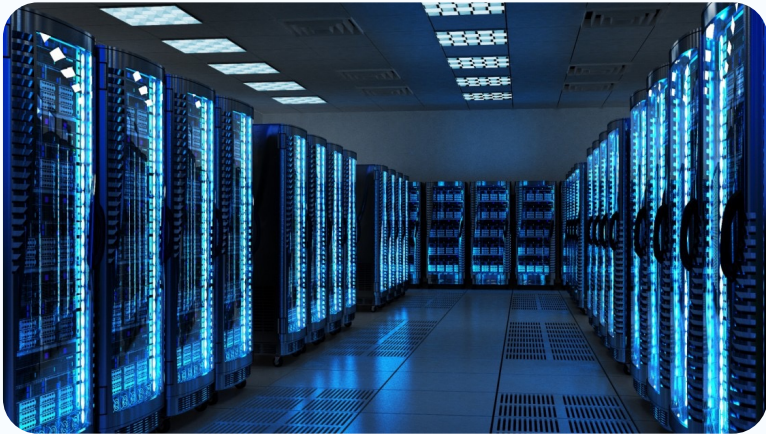
**Ваша
инфраструктура**



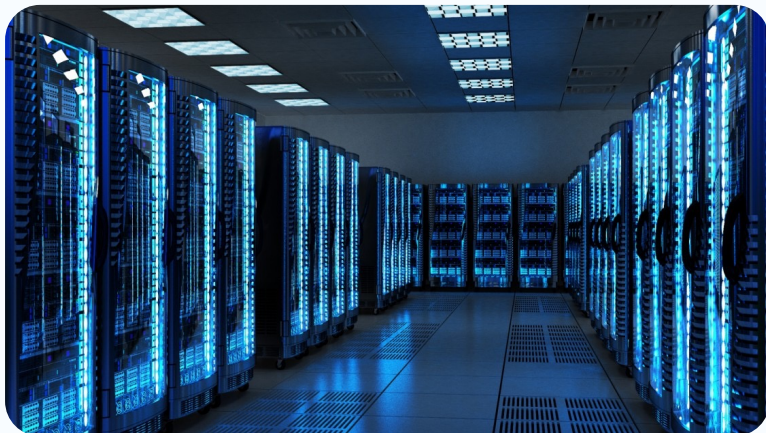
**Облачная
инфраструктура**



Что такое Cloud?



**Ваша
инфраструктура**



Облачная инфраструктура

- Специалисты
- Построенные ЦОДы
- Настроенное обслуживание серверов
- **Продукты в облаке Kubernetes, ML, DB**

Сейчас мы тут

- Что такое Cloud
- **Варианты использования Cloud**
- Требование к современным проектам
- Итоги



Варианты использования Cloud

Вам нужны ресурсы

Стойки целиком

Виртуальный ресурсы

Kubernetes и контейнеры

**Вам нужны
облачные продукты**

Технологии для создания
своих продуктов

Готовые продукты,
такие как SpeechKit

Варианты использования Cloud

Вам нужны ресурсы

Вам нужны
облачные продукты

Стойки целиком

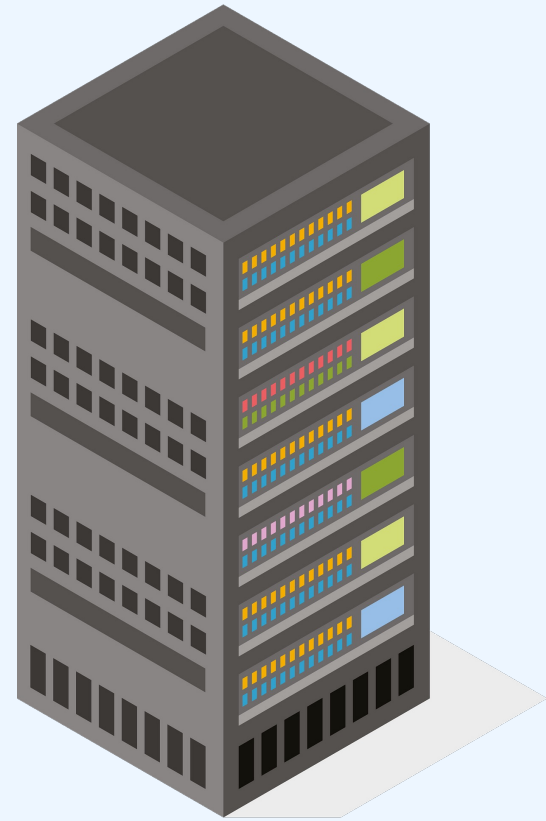
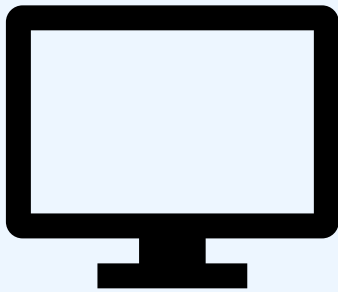
Технологии для создания
своих продуктов

Виртуальный ресурсы

Kubernetes и контейнеры

Готовые продукты,
такие как speechKit

Аренда стоек



Варианты использования Cloud

Вам нужны ресурсы

Стойки целиком

Виртуальный ресурсы

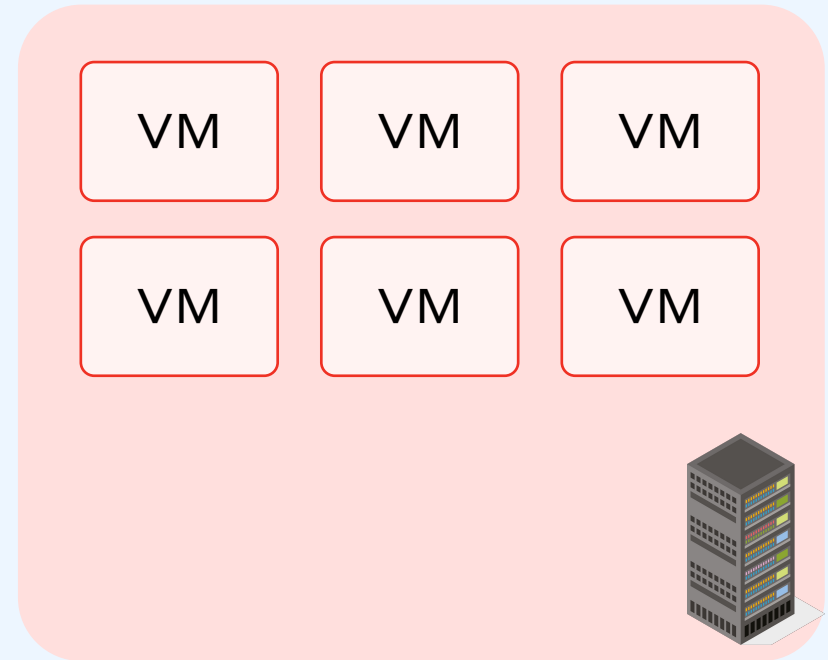
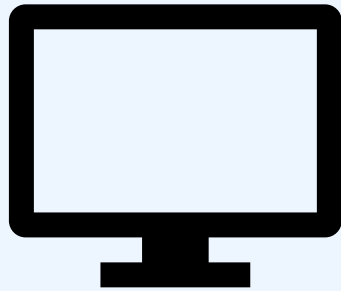
Kubernetes и контейнеры

Вам нужны
облачные продукты

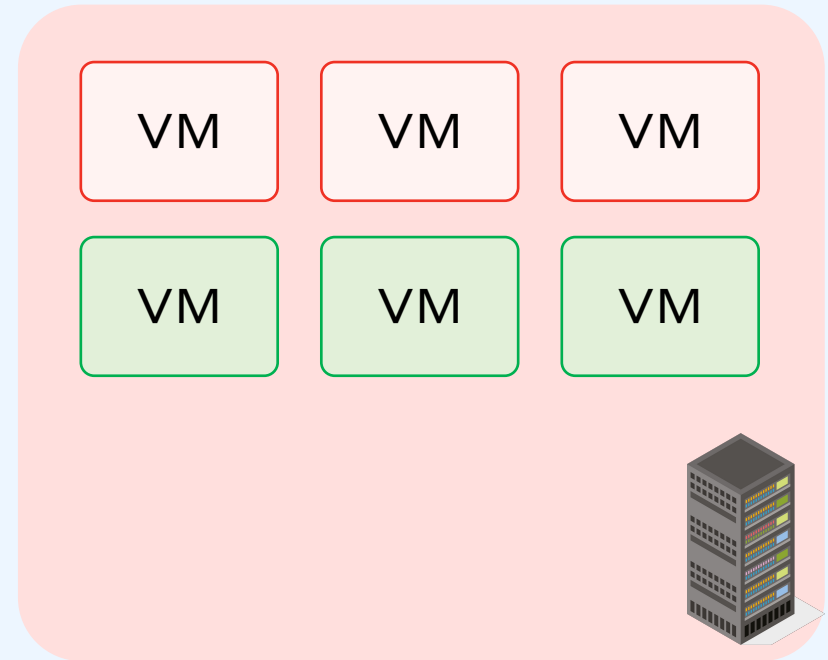
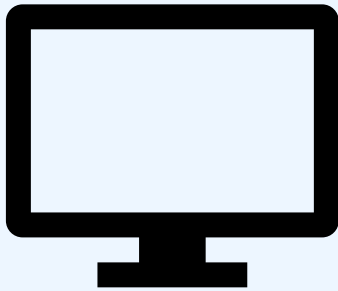
Технологии для создания
своих продуктов

Готовые продукты,
такие как speechKit

Аренда виртуальных ресурсов



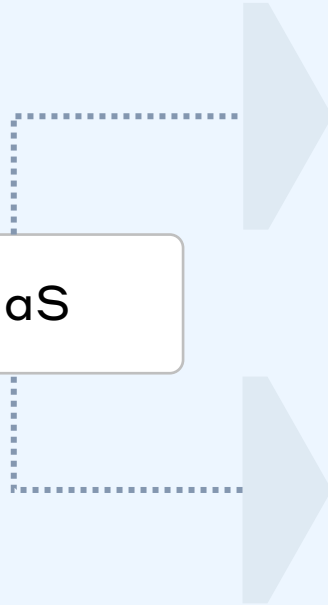
Аренда публичных ресурсов



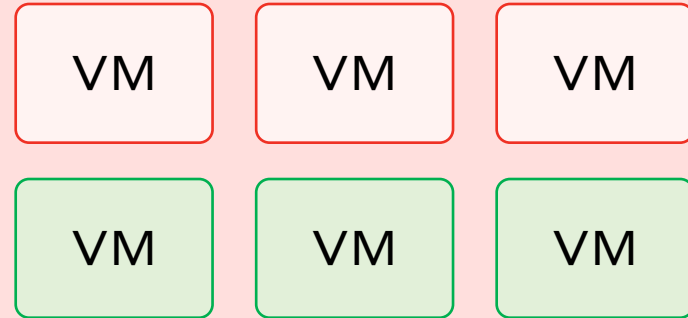
Аренда виртуальных ресурсов



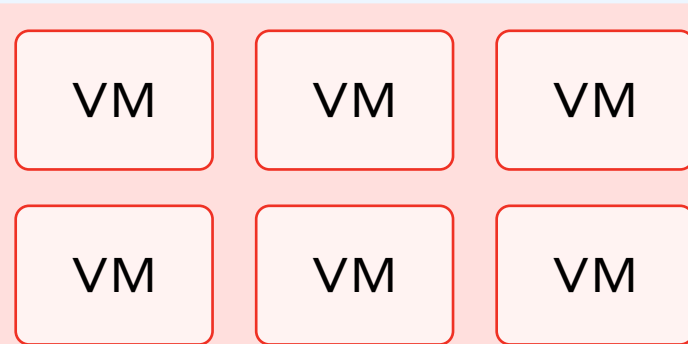
IaaS



Облачная инфраструктура



Внутренняя инфраструктура



Варианты использования Cloud

Вам нужны ресурсы

Стойки целиком

Виртуальный ресурсы

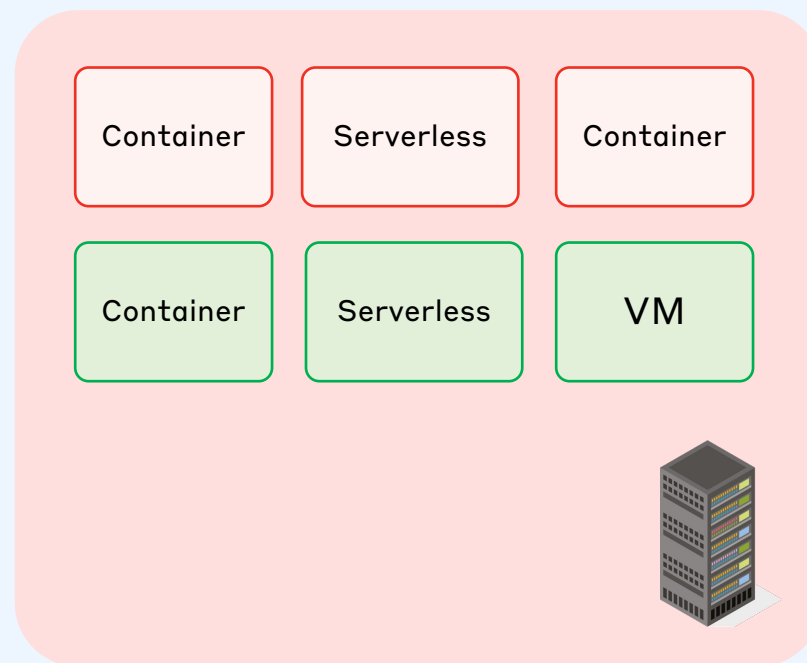
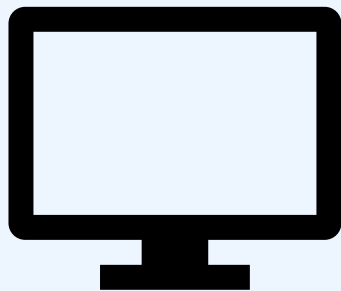
Kubernetes и контейнеры

Вам нужны
облачные продукты

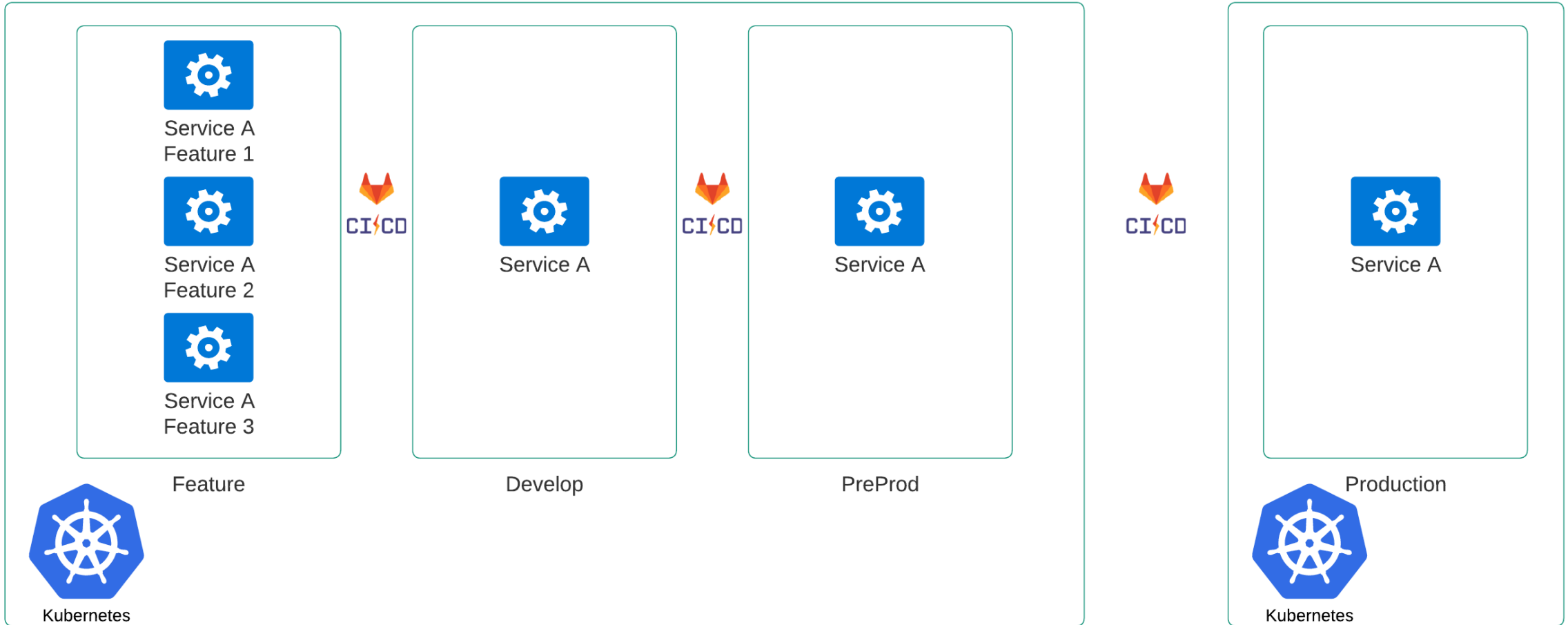
Технологии для создания
своих продуктов

Готовые продукты,
такие как speechKit

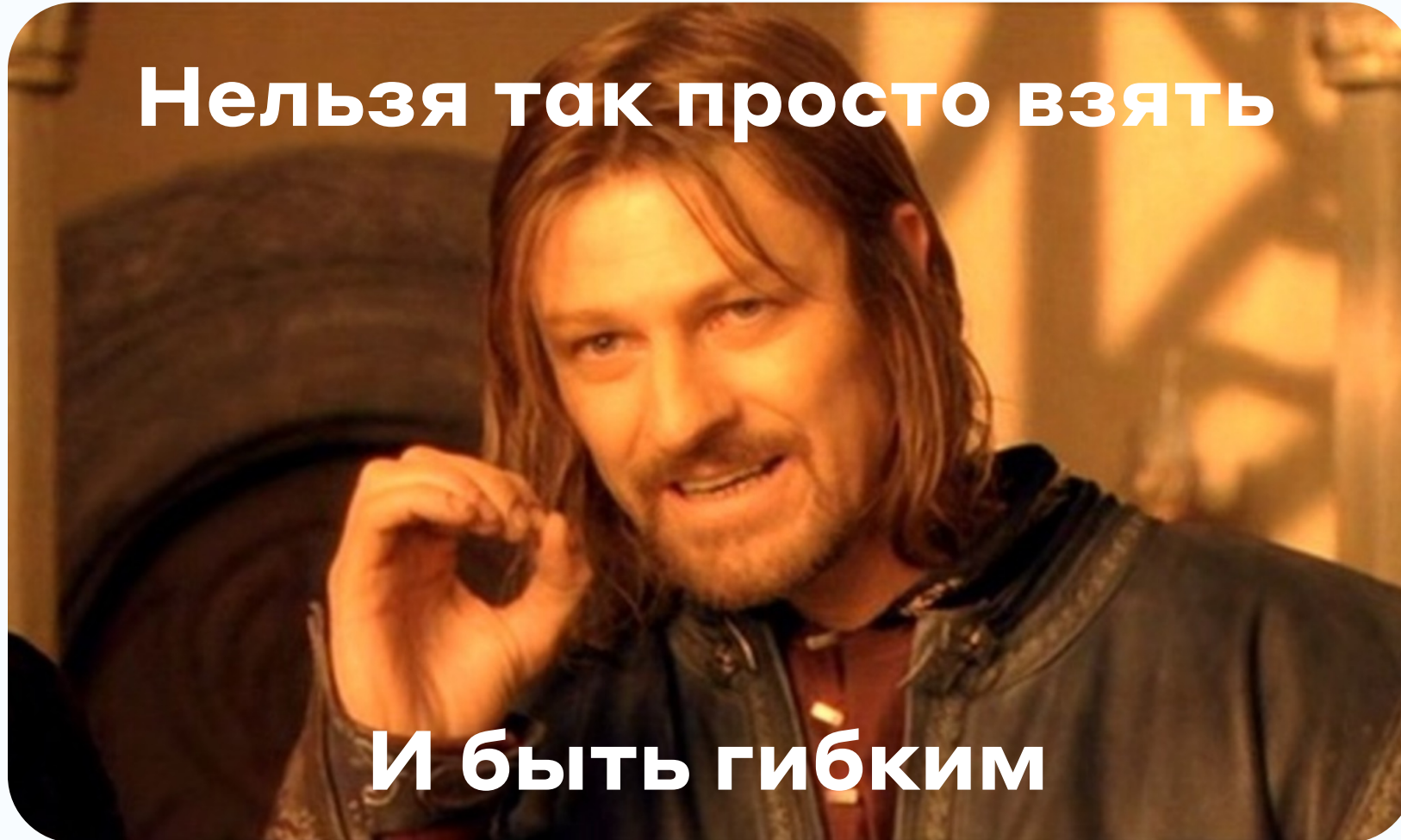
Аренда мощностей (containers, serverless)



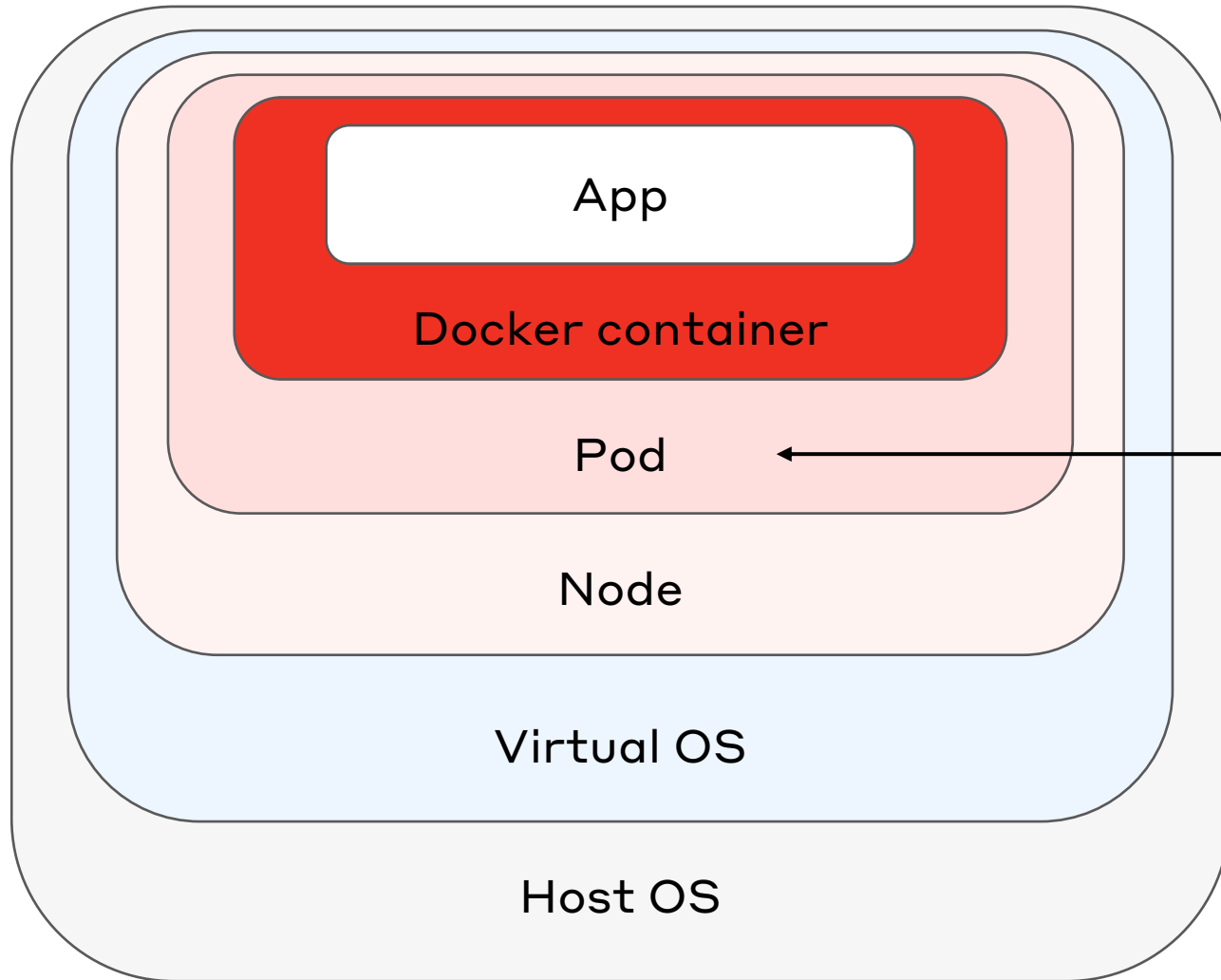
Гибкость, Kubernetes



Гибкость, Kubernetes

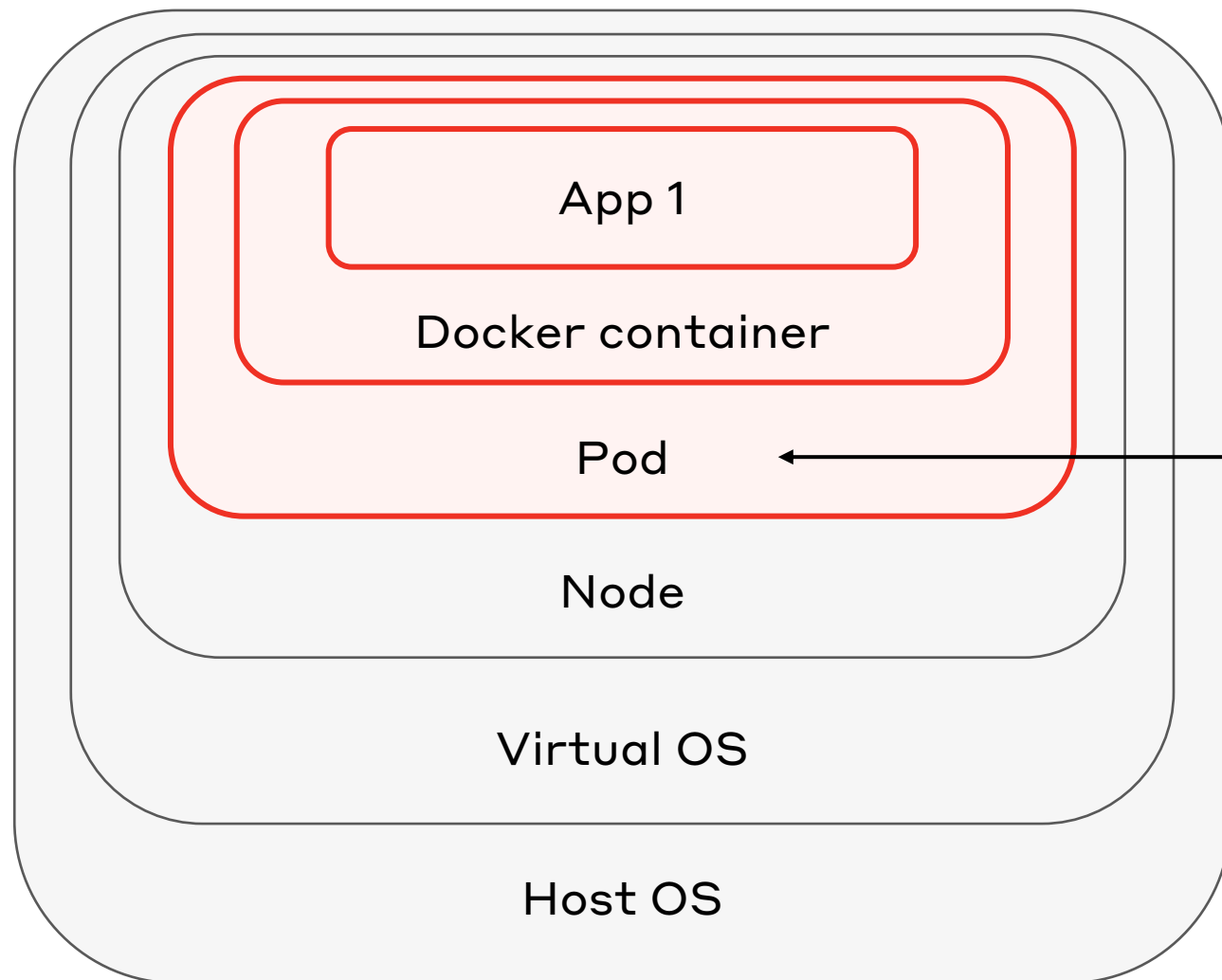


Безопасность в облаках



Тут может быть
больше одного
контейнера

Безопасность в облаках



Тут может быть
больше одного
контейнера



Безопасность в облаках

Должен быть выставлен параметр
"readonlyRootFilesystem — true"

Запрещено использование
небезопасных системных вызовов
(sysctl):

Параметры hostPID и hostIPC
должны быть выставлены в
значении "false"

kernel.shm*,

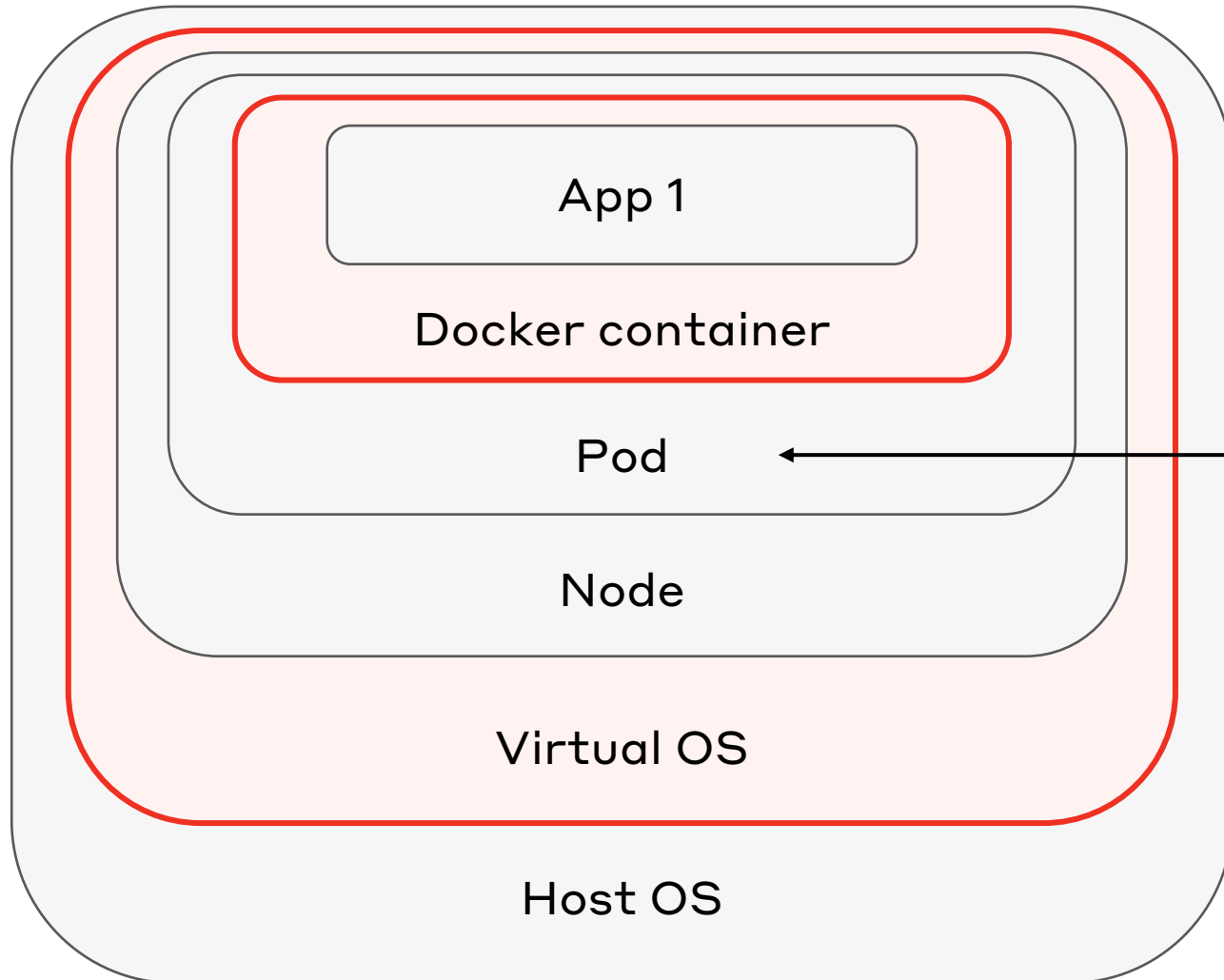
kernel.sem,

Параметр hostNetwork должен
быть выставлен в значении "false"

kernel.msg*,

fs.mqueue.*,"

Безопасность в облаках



Тут может быть больше одного контейнера



Безопасность в облаках

Все смонтированные volume должны быть только на чтение (readonly).

Capabilities выдаются по принципу наименьших привилегий drop 'ALL', после чего необходимые capabilities для работы.



Варианты использования Cloud

Вам нужны ресурсы

Стойки целиком

Виртуальный ресурсы

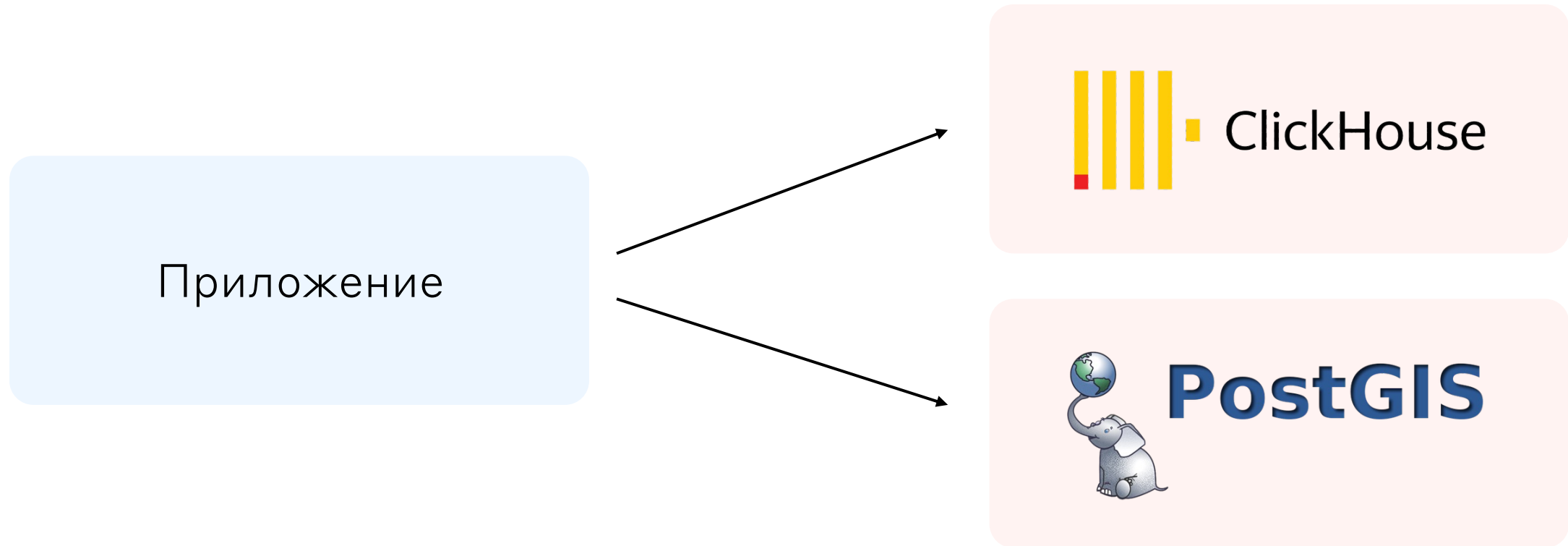
Kubernetes и контейнеры

**Вам нужны
облачные продукты**

Технологии
для создания
своих продуктов

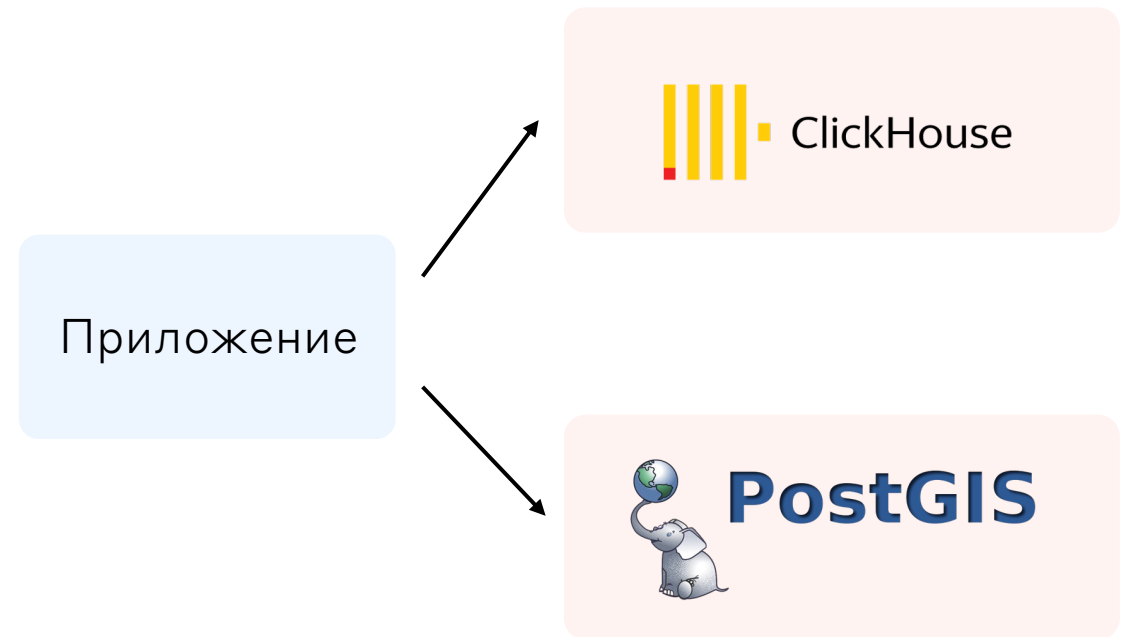
Готовые продукты,
такие как speechKit

Прототипирование и тест технологии



Прототипирование и тест технологии

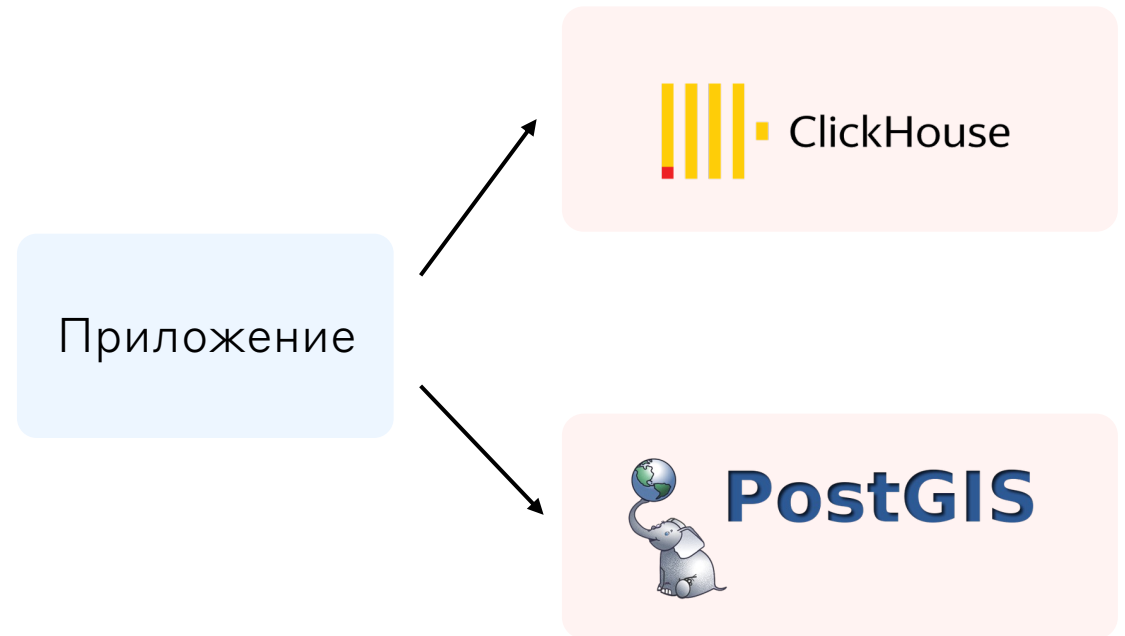
Выбрать технологию



Прототипирование и тест технологии

Выбрать технологию

Настроить инстанс



Прототипирование и тест технологии

Выбрать технологию

Настроить инстанс

Провести интеграцию

Приложение



ClickHouse



PostGIS

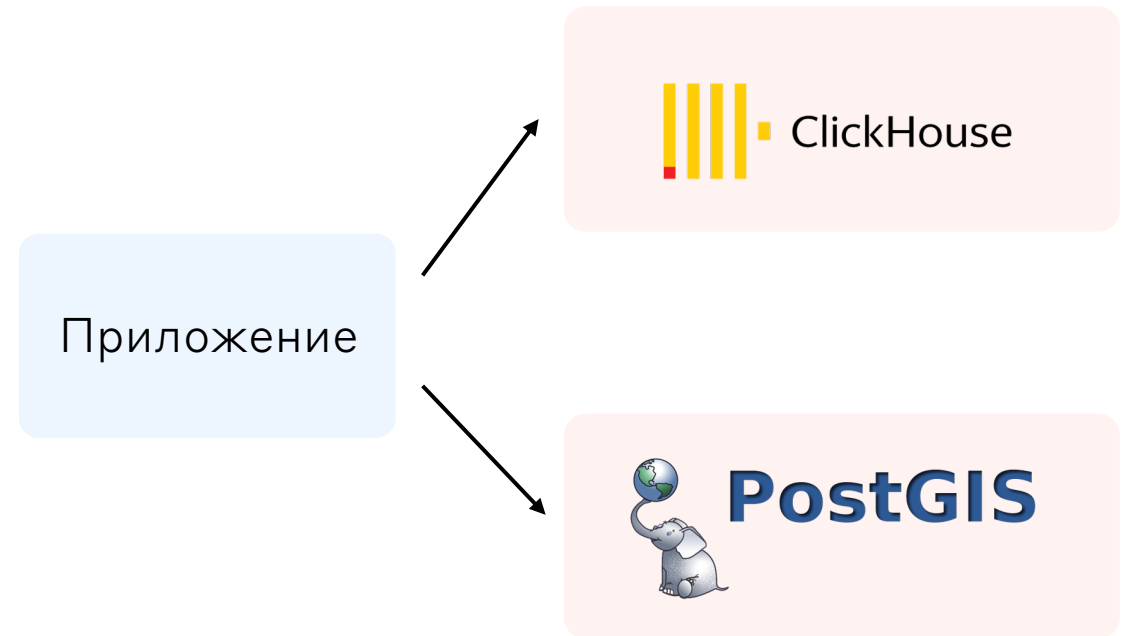
Прототипирование и тест технологии

Выбрать технологию

Настроить инстанс

Провести интеграцию

Убедиться, что всё хорошо



Прототипирование и тест технологии

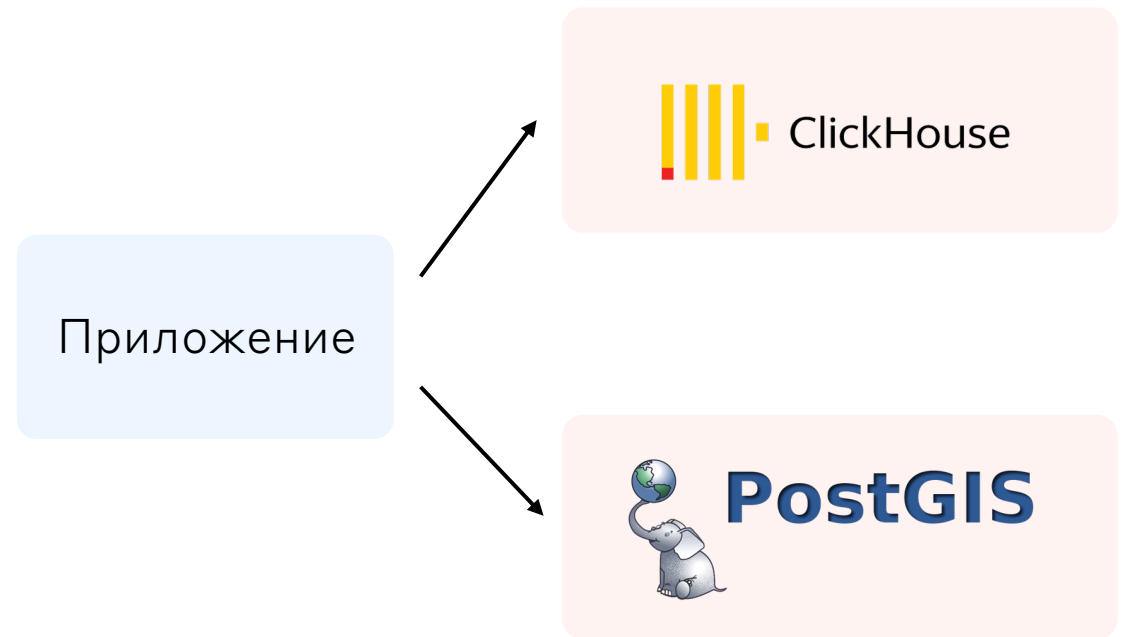
Выбрать технологию

Настроить инстанс

Провести интеграцию

Убедиться, что всё хорошо

Поднять кластер



Прототипирование и тест технологии

Выбрать технологию

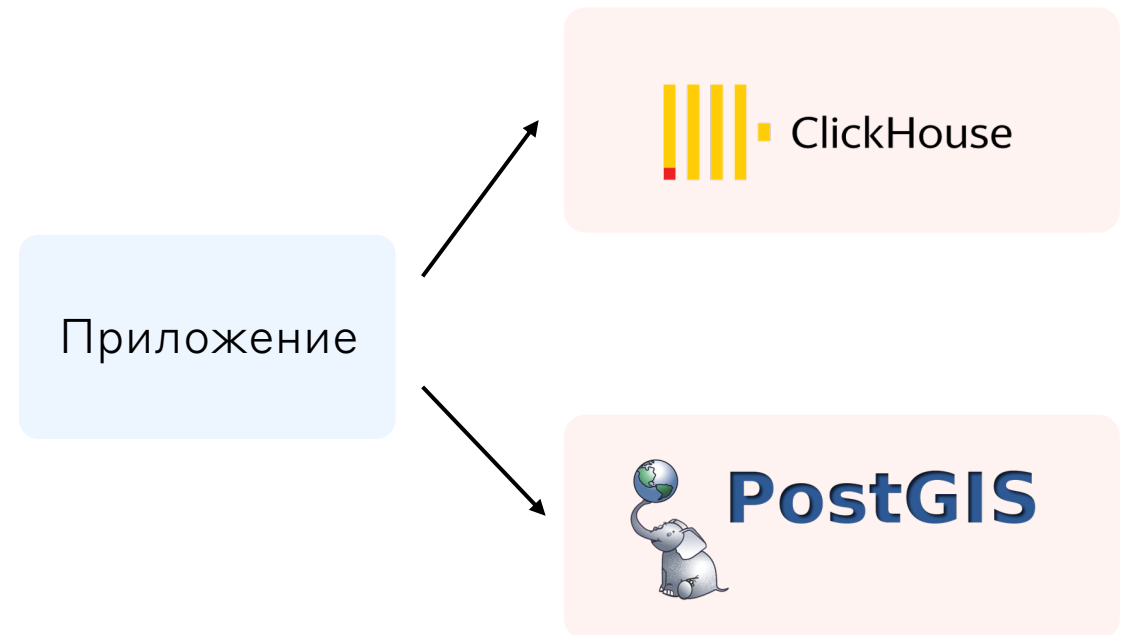
Настроить инстанс

Провести интеграцию

Убедиться, что всё хорошо

Поднять кластер

Провести нагрузочное тестирование



Прототипирование и тест технологии

Выбрать технологию

Настроить инстанс

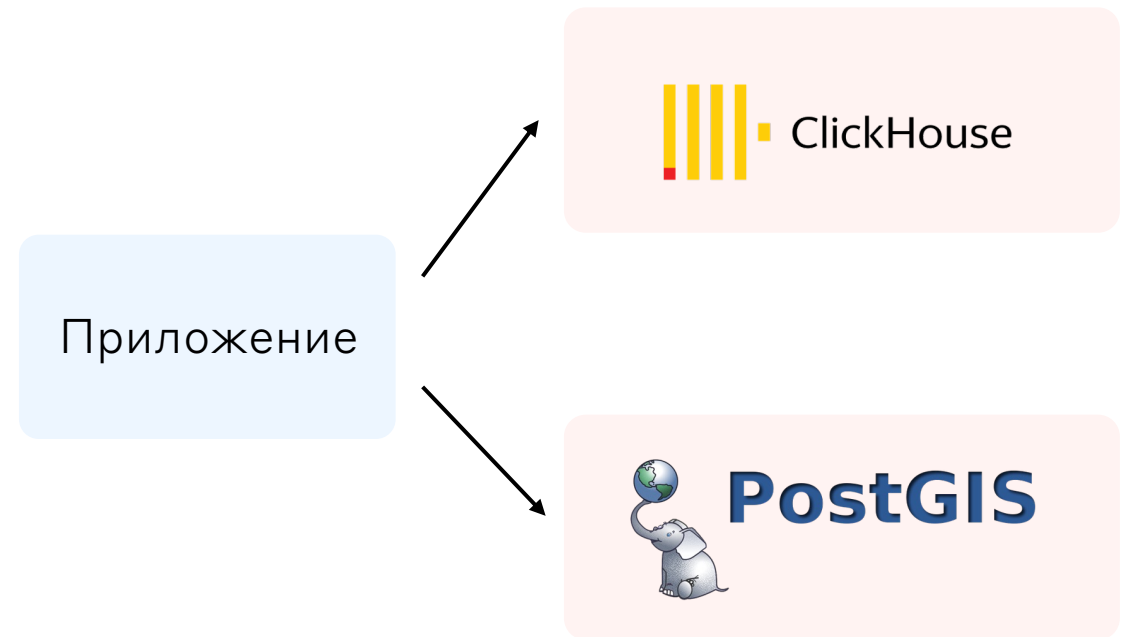
Провести интеграцию

Убедиться, что всё хорошо

Поднять кластер

Провести нагрузочное тестирование

Установить в PROD



Прототипирование и тест технологии

Выбрать технологию

Настроить инстанс

Провести интеграцию

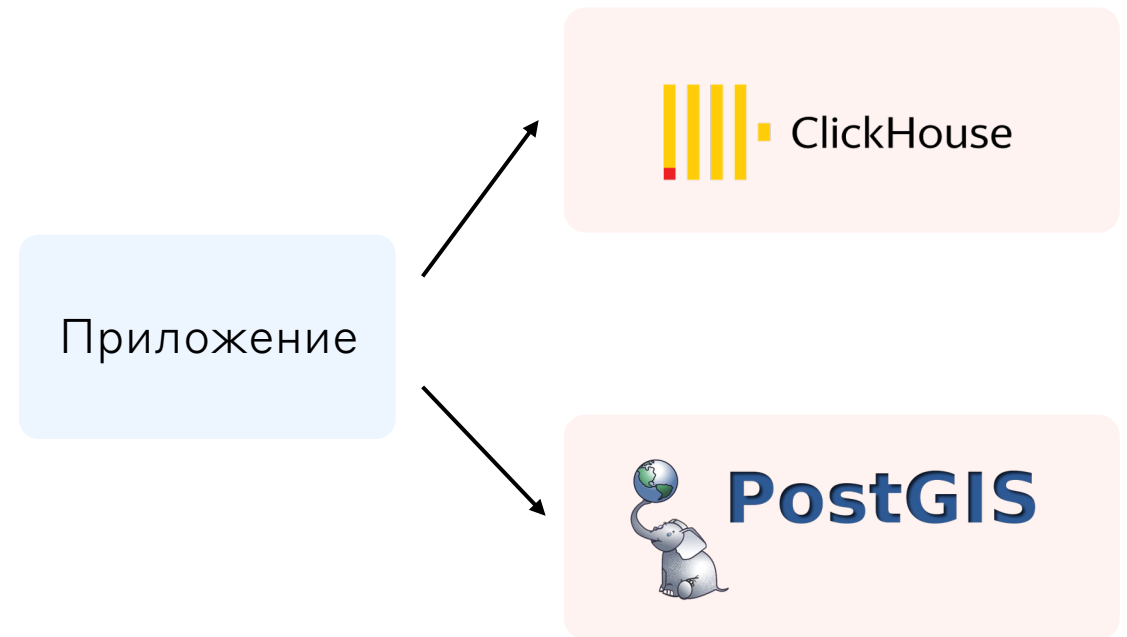
Убедиться, что всё хорошо

Поднять кластер

Провести нагрузочное тестирование

Установить в PROD

Profit



Прототипирование и тест технологии

Выбрать технологию

Настроить инстанс

Провести интеграцию

Убедиться, что всё хорошо

Поднять кластер

Провести нагрузочное тестирование

Установить в PROD (SLA !!!)

Profit



Прототипирование и тест технологии

Выбрать технологию

Настроить инстанс

Провести интеграцию

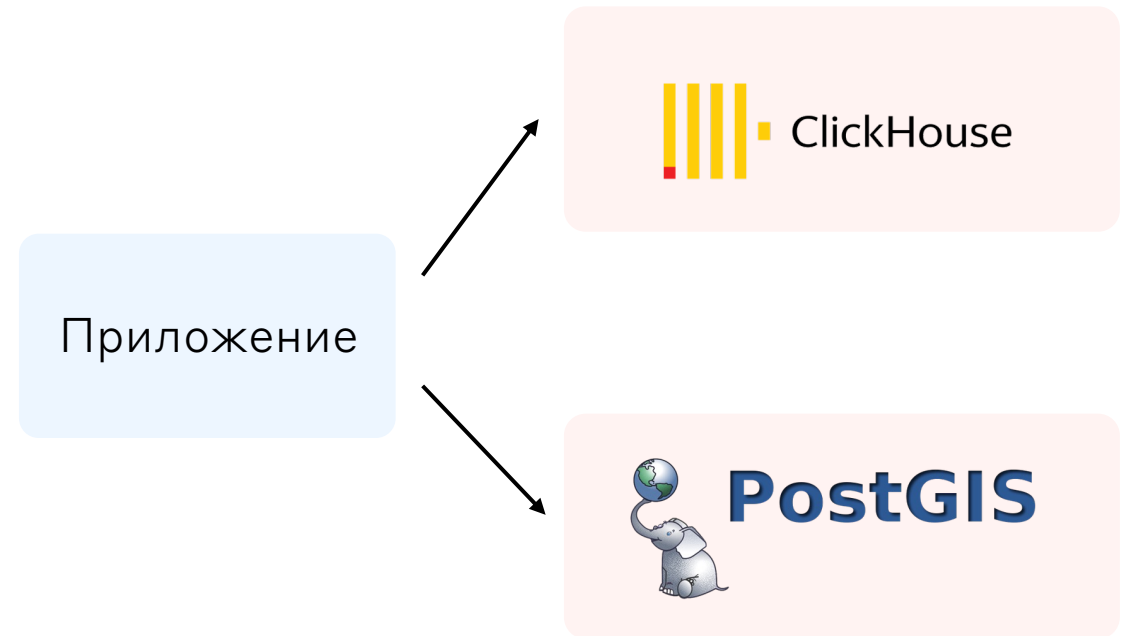
Убедиться, что всё хорошо

Поднять кластер

Провести нагрузочное тестирование

Установить в PROD (SLA !!!)

Profit



Варианты использования Cloud

Вам нужны ресурсы

Стойки целиком

Виртуальный ресурсы

Kubernetes и контейнеры

**Вам нужны
облачные продукты**

Технологии для создания
своих продуктов

Готовые продукты,
такие как speechKit

Использование облачных продуктов

Оставляйте время на то,
чтобы улучшать то, что является
вашим бизнесом



SpeechKit

Комплекс технологий
распознавания и синтеза речи



Vision

Анализ изображений
с помощью моделей машинного
обучения



Translate

Машинный перевод
с поддержкой более 90 языков

Использование облачных продуктов

Оставляйте время на то,
чтобы улучшать то, что является
вашим бизнесом

Надёжнее интегрируетесь,
ваши сервисы могут быть
в той же инфраструктуре



SpeechKit

Комплекс технологий
распознавания и синтеза речи



Vision

Анализ изображений
с помощью моделей машинного
обучения



Translate

Машинный перевод
с поддержкой более 90 языков

Сейчас мы тут

- Что такое Cloud
- Варианты использования Cloud
- **Требование к современным проектам**
- Итоги



The Twelve-Factor App

III. CONFIG

**Окружение хранит конфигурацию и передаёт
приложению**



The Twelve-Factor App

III. CONFIG

Окружение хранит конфигурацию и передаёт приложению

1. Идентификаторы подключения к ресурсам типа базы данных, кэш-памяти и другим сторонним службам



The Twelve-Factor App

III. CONFIG

Окружение хранит конфигурацию и передаёт приложению


1. Идентификаторы подключения к ресурсам типа базы данных, кэш-памяти и другим сторонним службам
2. Регистрационные данные для подключения к внешним сервисам



The Twelve-Factor App

III. CONFIG

Окружение хранит конфигурацию и передаёт приложению

1. Идентификаторы подключения к ресурсам типа базы данных, кэш-памяти и другим сторонним службам
 2. Регистрационные данные для подключения к внешним сервисам
 3. Значения зависящие от среды развёртывания такие, как имя хоста
- 

Kubernetes ConfigMaps

Место для хранения env переменных



Kubernetes ConfigMaps

Место для хранения env переменных

В каждом контейнере можно получить к ним доступ



Kubernetes ConfigMaps

Место для хранения env переменных

В каждом контейнере можно получить к ним доступ

Два подхода:

- Хранить много ConfigMaps под каждый сервис
- Хранить одну ConfigMaps под все сервисы



Kubernetes ConfigMaps

```
nameOverride: ""
fullnameOverride: "common-config-preprod"

imageCredentials:
- registry: alfab[REDACTED]
  username: tech-abru-ci
  password: AKCp5bt[REDACTED]
  # email:

configMaps:
  common-node:
    NODE_HOST: "0.0.0.0"
  common-keycloak:
    KEYCLOAK_REALM_URL: "https://keyclo[REDACTED]"
    KEYCLOAK_CLIENT_SSL_ALLOW_ANY_HOSTNAME: "false"
    KEYCLOAK_CLIENT_SSL_DISABLE_TRUST_MANAGER: "true"
    KEYCLOAK_BASE_PATH: "https://key[REDACTED]"
    KEYCLOAK_URL: "http://ke[REDACTED]"
    KEYCLOAK_REALM: "local_users"
    KEYCLOAK_INSECURE: "true"
  common-logging:
    LOGGING_LEVEL_ROOT: "INFO"
  common-postgres:
    PGHOST: "c-c9q4j[REDACTED]"
    PGPORT: "6432"
    PGPORT12: "6432"
    PGADDITIONALPARAMS: "?prepareThreshold=0"
    PGMAXCONNECTIONS: "5"
    SPRING_PG_URL: "jdbc:postgresql://c-c9q4[REDACTED]"

  YC_MANAGED_DB: "yes"
```

Kubernetes ConfigMaps

```
apiVersion: v1
kind: Pod
metadata:
  name: configmap-demo-pod
spec:
  containers:
    - name: demo
      image: alpine
      command: ["sleep", "3600"]
      env:
        # Define the environment variable
        - name: TEST_PARAMS # Notice that the case is different here
          # from the key name in the ConfigMap.
```


Kubernetes Secrets

Разграничение прав RBAC



Kubernetes Secrets

Разграничение прав RBAC

Доступ к ним можно получить через env



Kubernetes Secrets

Разграничение прав RBAC

Доступ к ним можно получить через env

Хранятся в базе Kubernetes в зашифрованном виде



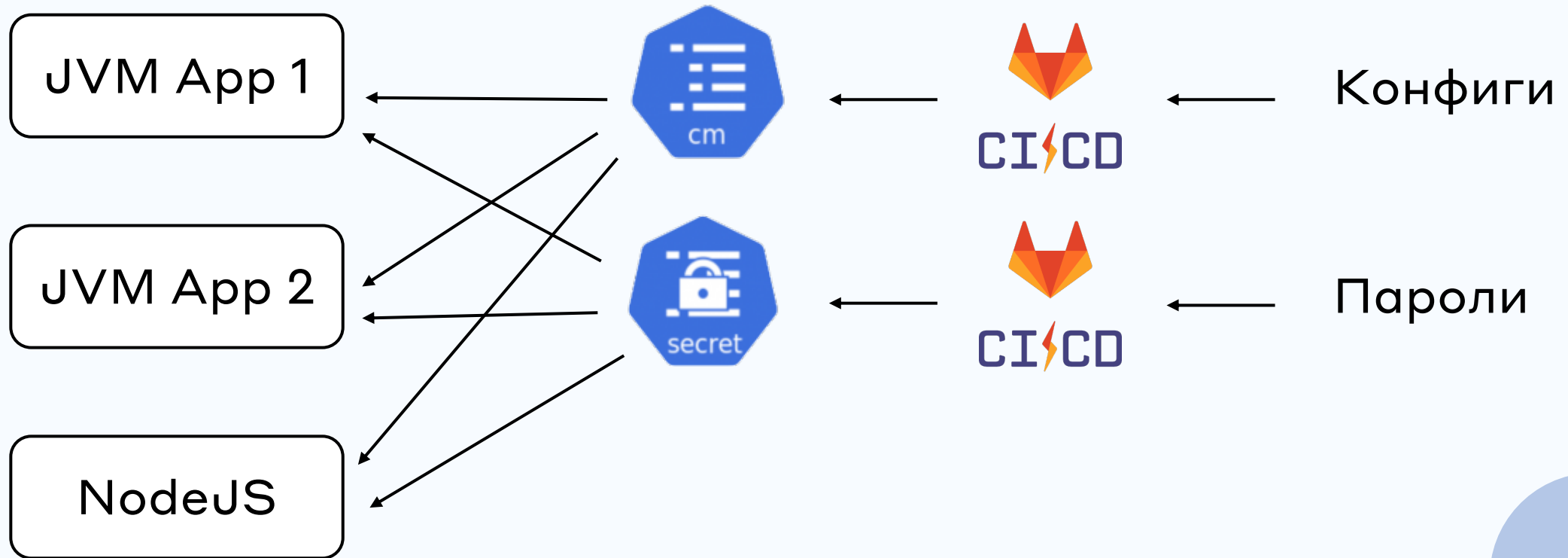
Kubernetes ConfigMaps & Secrets

Конфиги стали находится в ENV переменных

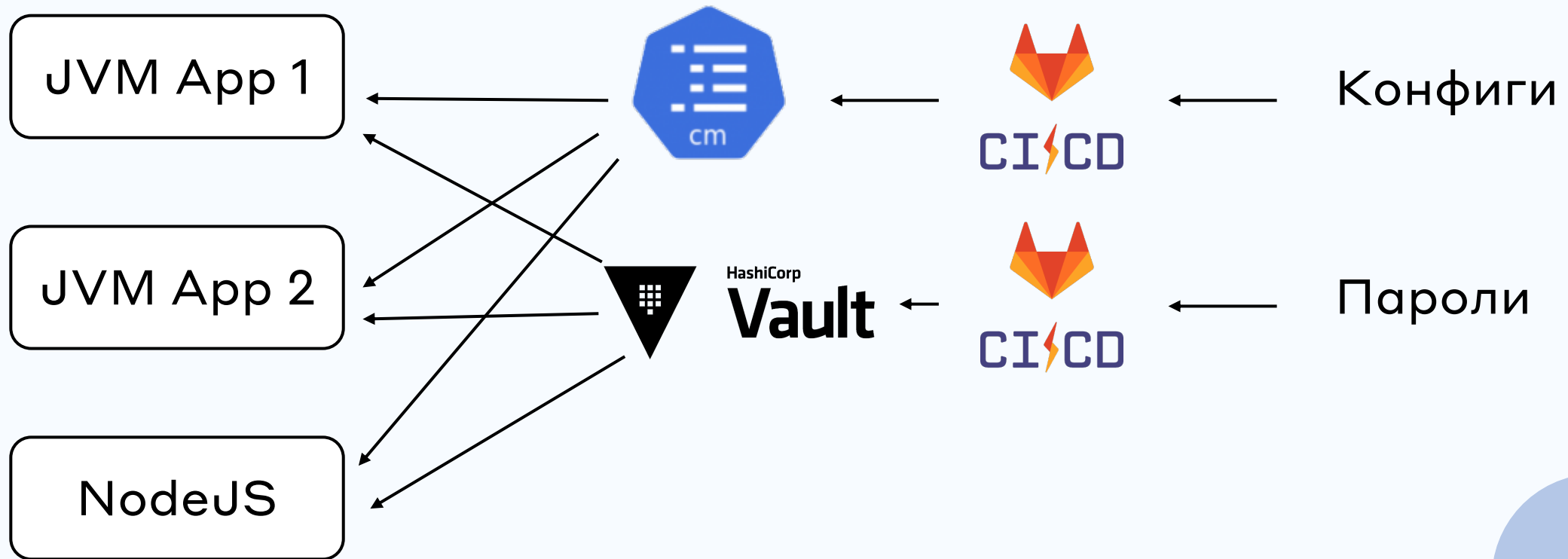
А где автоматизация?



Kubernetes ConfigMaps & Secrets



Kubernetes ConfigMaps & Secrets



Kubernetes Load Balancing Networking

В Kubernetes есть встроенная возможность
балансирования запросов



Kubernetes Load Balancing Networking

В Kubernetes есть встроенная возможность балансирования запросов

```
apiVersion: v1
kind: Service
metadata:
  name: my-service
spec:
  selector:
    app.kubernetes.io/name: MyApp
  ports:
    - protocol: TCP
      port: 80
      targetPort: 9376
```


Kubernetes Load Balancing Networking

В Kubernetes есть встроенная возможность балансирования запросов

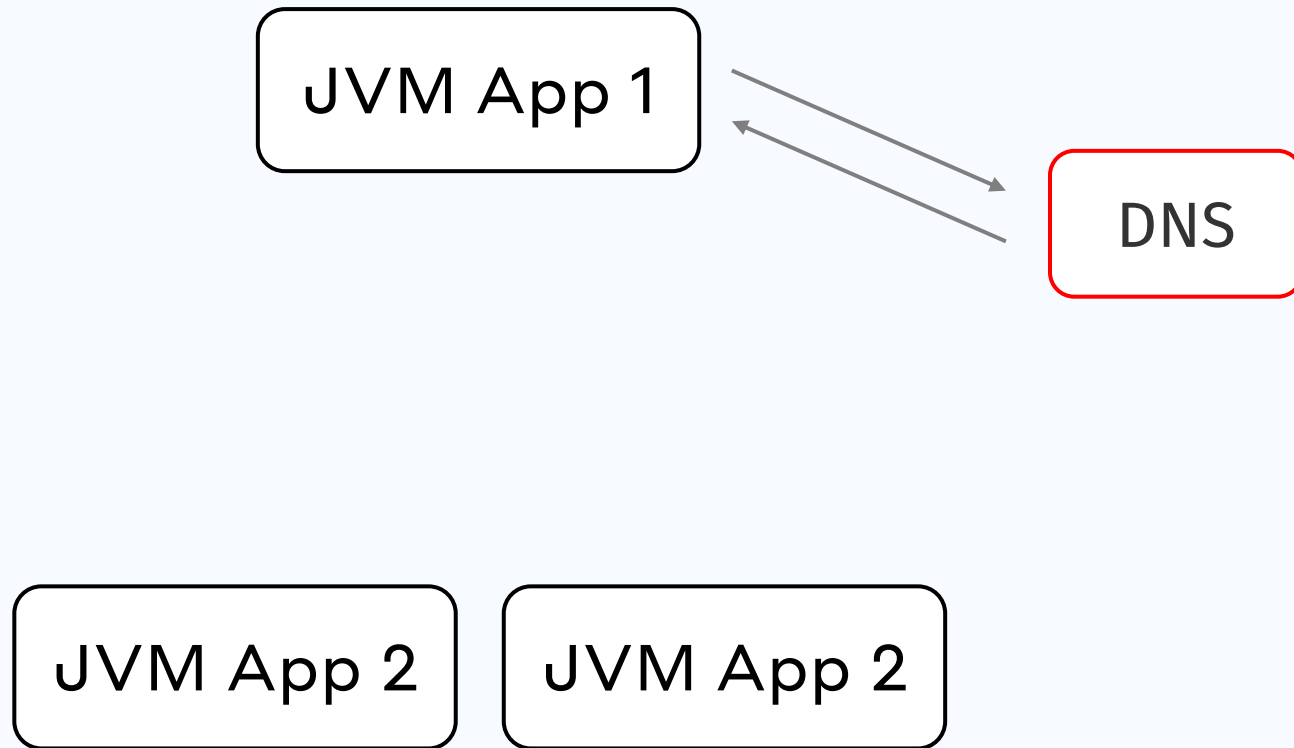
```
apiVersion: v1
kind: Service
metadata:
  name: my-service
spec:
  selector:
    app.kubernetes.io/name: MyApp
  ports:
    - protocol: TCP
      port: 80
      targetPort: 9376
```

Kubernetes Load Balancing Networking

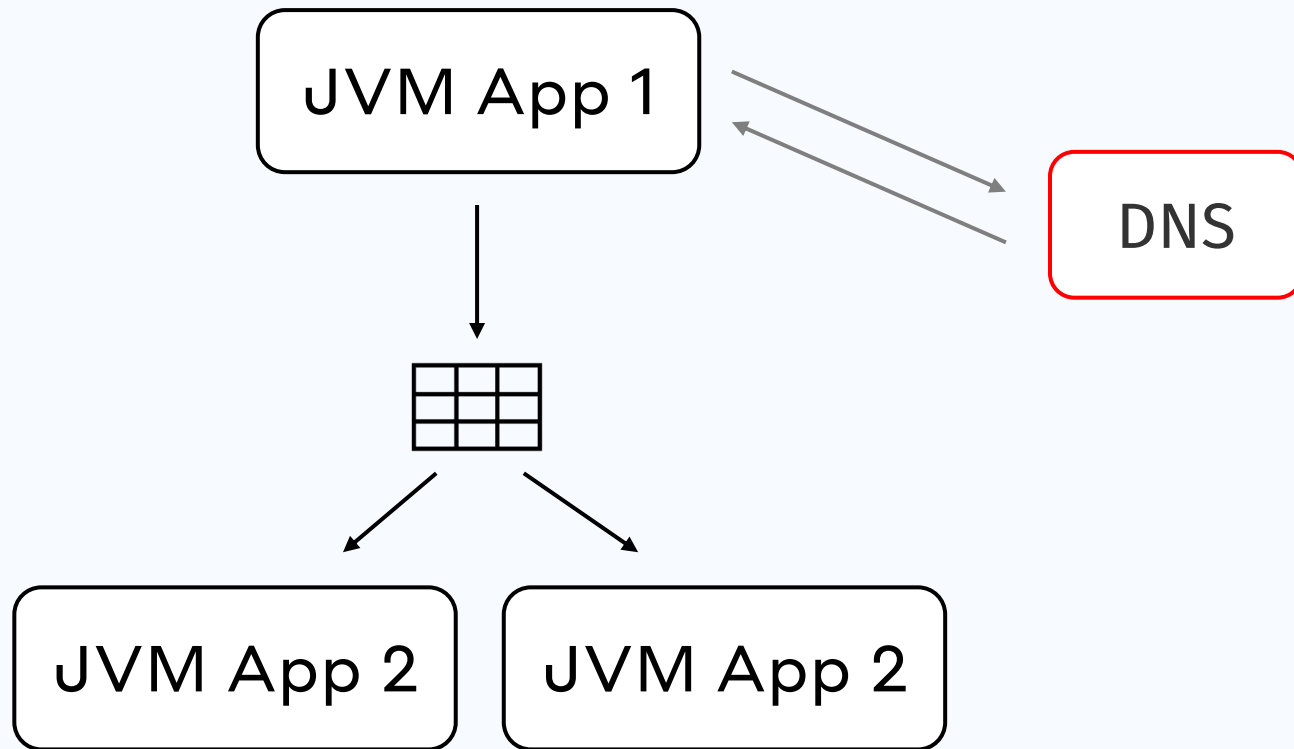
В Kubernetes есть встроенная возможность балансирования запросов

```
apiVersion: v1
kind: Service
metadata:
  name: my-service
spec:
  selector:
    app.kubernetes.io/name: MyApp
  ports:
    - protocol: TCP
      port: 80
      targetPort: 9376
```

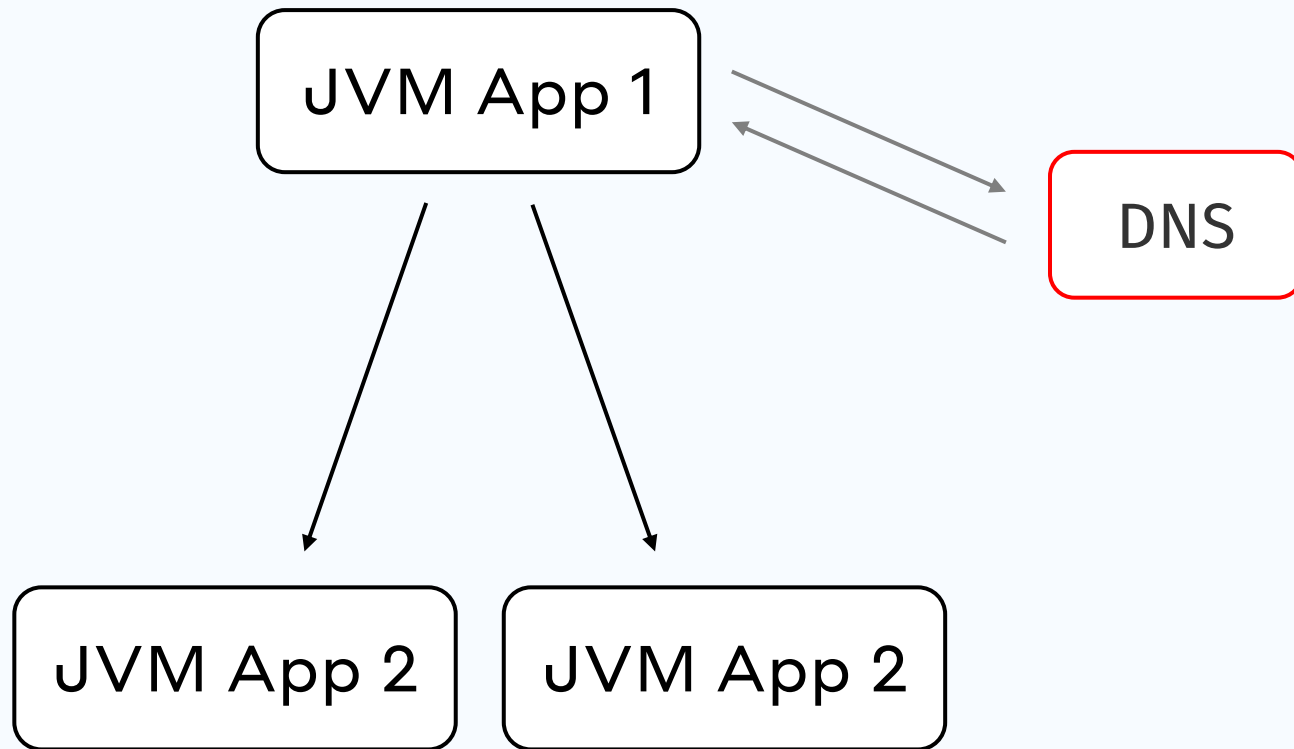
Kubernetes Load Balancing Networking



Kubernetes Load Balancing Networking



Kubernetes Load Balancing Networking



Сейчас мы тут

- Что такое Cloud
- Варианты использования Cloud
- Требование к современным проектам
- **Итоги**



Итоги

- Комбинирование подходов



Итоги

- Комбинирование подходов
- Окружение хранит конфигурацию



Итоги

- Комбинирование подходов
- Окружение хранит конфигурацию
- Облако отличный способ проверить ваше проект на best practice



Вопросы

Чернухин Максим

 <https://www.facebook.com/chernukhin.maksim>

 @MaksCher

