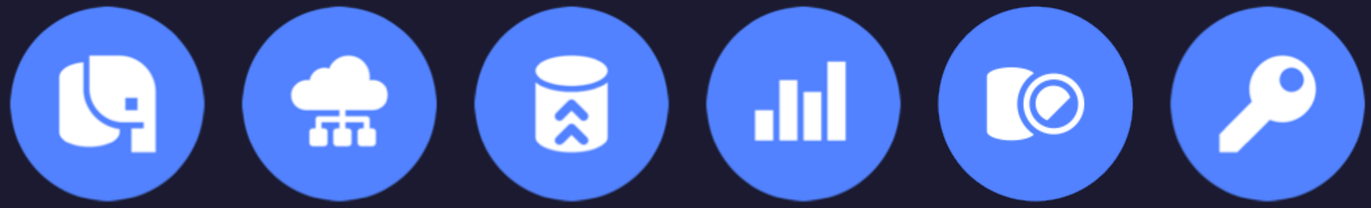
Yandex Cloud



Миграция в облако: технологии, люди и процессы

Всеволод Грабельников

Старший архитектор облачных решений, Yandex.Cloud

Программа

01 Коротко о причинах миграции

02 Информационная безопасность

03 Организация сетевой связности

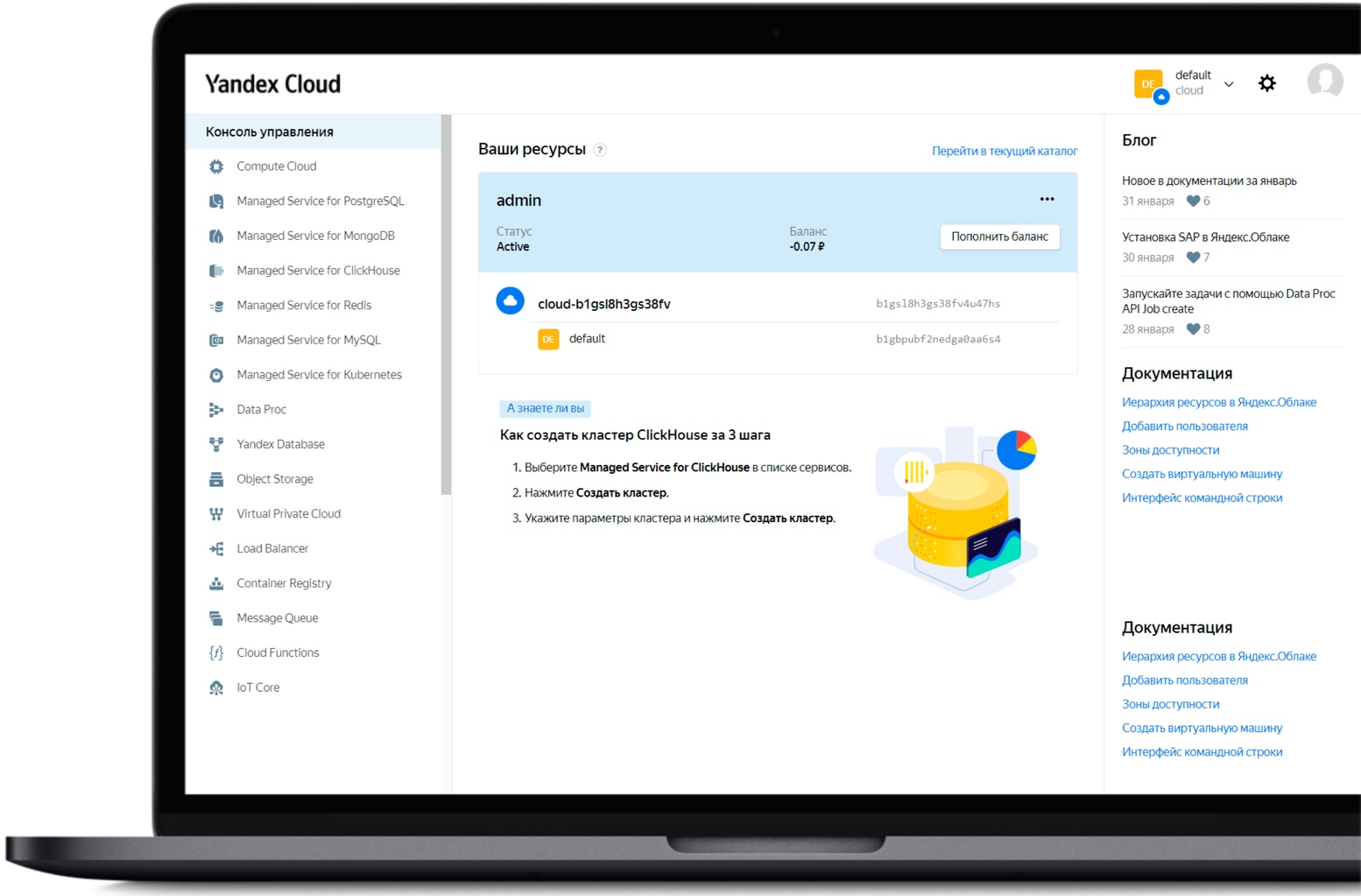
04 Миграция при помощи Data Transfer

05 Ограничения PostgreSQL as a Service и SLA

Коротко о причинах миграции

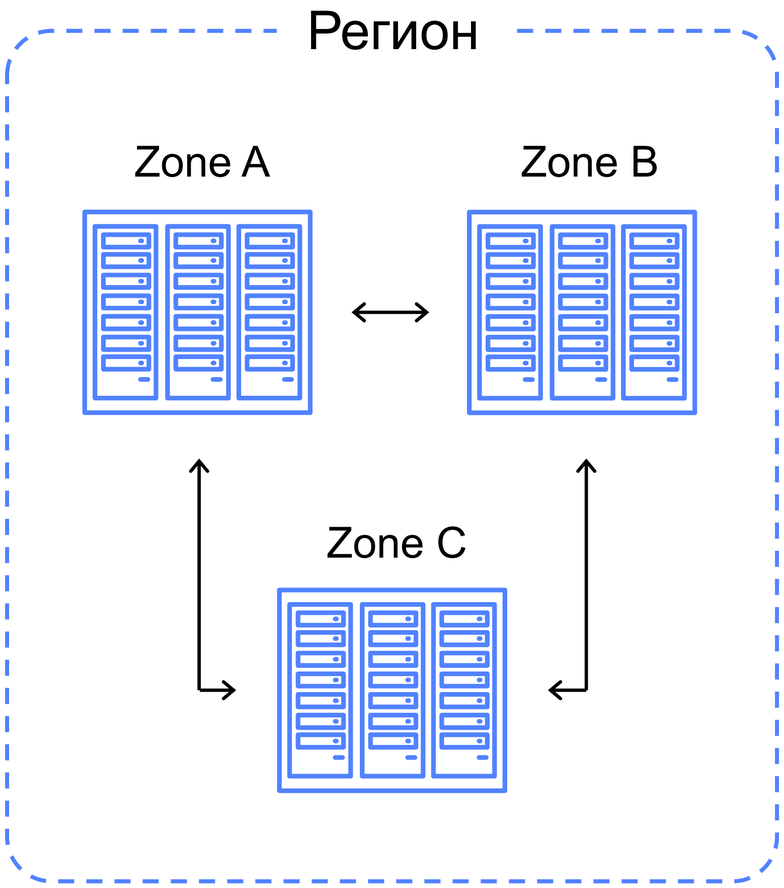
Удобный инструмент для разработчика

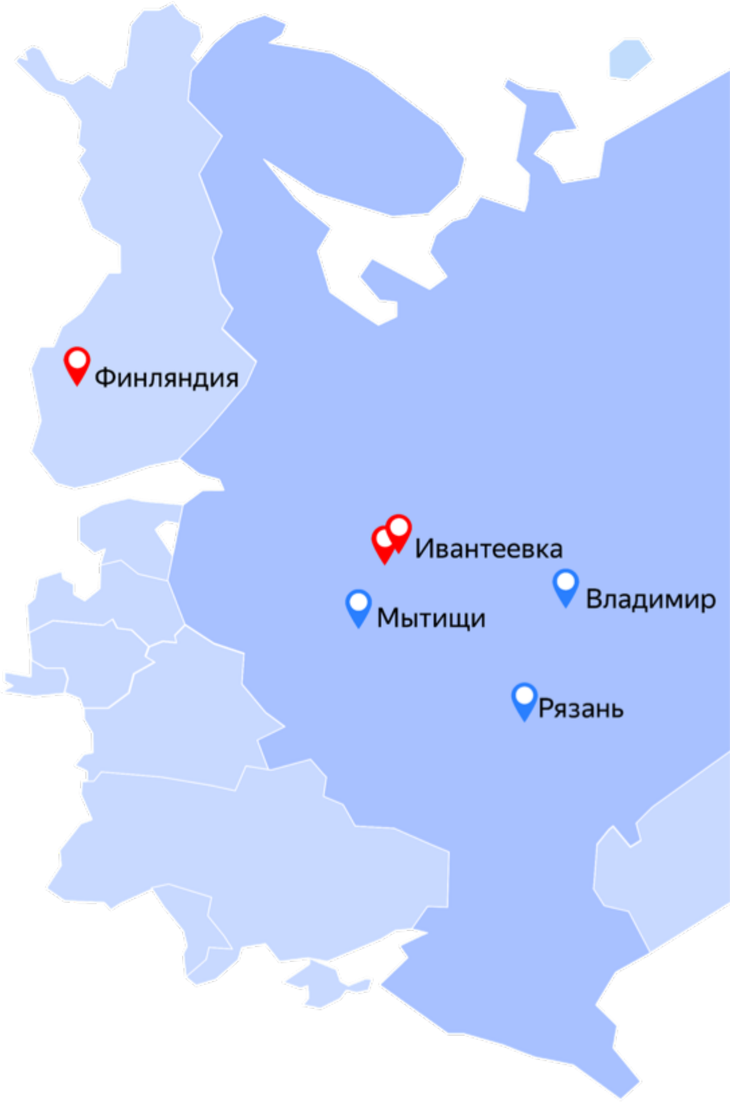
- Полнофункциональная консоль управления
- Доступ к сервисам через API, CLI, Terraform
- Русскоязычная документация
- Несколько уровней технической поддержки



Дата-центры

- Три ДЦ → три зоны доступности → регион
- Независимые системы энергоснабжения
- Собственная оптоволоконная сеть
- 300 км между ДЦ
- Пропускная способность в Тбит/с благодаря DWDM





Экскурсия 360˚ по владимирскому дата-центру Яндекса: youtube.com/watch?v=PN388y41X-k

Yandex.Cloud — это платформа

SaaS

Магазин партнёрских приложений и сервисов (Yandex Marketplace)

PaaS

Управление данными и аналитика

Инструменты управления и разработки

Сервисы машинного обучения

IaaS

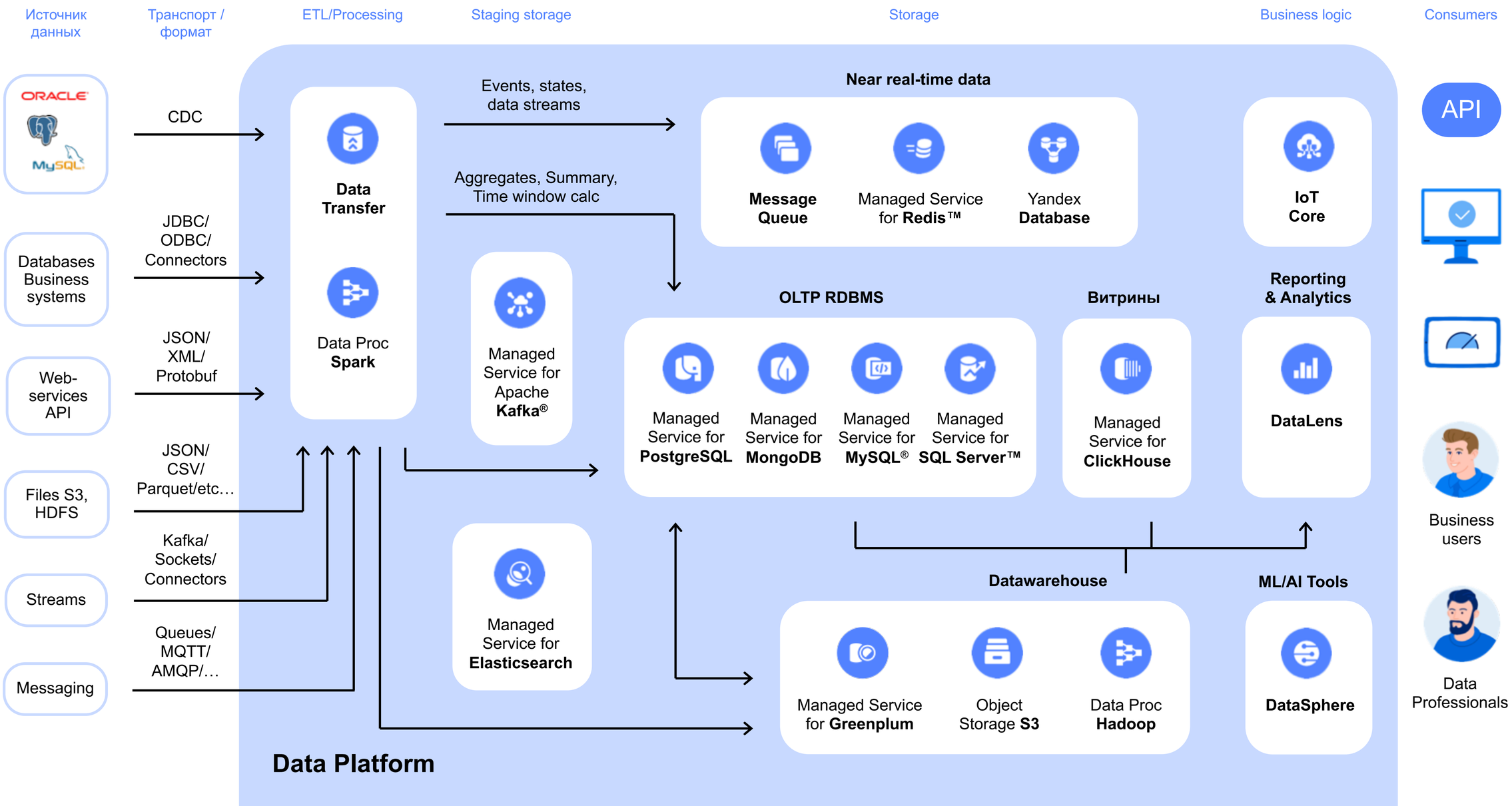
Идентификация и безопасность

Виртуальные машины и контейнеры

Объектное и блочное хранилища

Сеть и доставка контента

Платформа данных Yandex.Cloud



Yandex Managed Service for PostgreSQL

Команда MDB Яндекс.Облака

- Доступность и отказоустойчивость
- Резервное копирование
- Консоль мониторинга
- Обновления (как минорные, так и мажорные)
- Поддерживаемые клиенты
- Техническая поддержка

Пользователь

- Схема данных
- Запросы
- Мониторинг производительности
- Контроль занимаемого места

Информационная безопасность

Типичные вопросы ИБ

Можно ли использовать облачную платформу для обработки конфиденциальных данных, защищаемых законодательством?

Как организовать безопасный канал передачи данных в облако из локальных систем?

Как ограничить доступ в Интернет из облака?

Имеете ли вы доступ к нашим данным? Где хранятся ключи шифрования? Можем ли мы шифровать данные на своих ключах? У кого есть физический доступ к данным? Как изолированы друг от друга виртуальные машины? Может ли повлиять безалаберность одного заказчика на безопасность данных другого? Кто отвечает за безопасность наших данных? Можем ли мы прописать в договоре вашу ответственность за любые утечки информации, «расположенной» в облаке?

Compliance

Соответствие законодательным и индустриальным требованиям

152 ФЗ, УЗ-1. Аттестат соответствия по требованиям 21-го приказа ФСТЭК.

Соответствует для Евросоюза

Реестр отечественного ПО

Для ЦОД и облачных сервисов

ГОСТ 57580. Безопасность финансовых (банковских) операций

Защита данных в Yandex.Cloud

Мы заботимся о безопасности на всех этапах создания и эксплуатации Yandex.Cloud

Физическая безопасность

- Строгие регламенты обслуживания серверов
- Все стойки с Yandex.Cloud под видеонаблюдением
- Строгие регламенты уничтожения носителей информации

Безопасность разработки

- Своя команда инженеров ИБ
- Регулярный аудит безопасности кода приложений
- Регулярное обновление уязвимостей в сторонних компонентах
- Статический и динамический анализ кода

Шифрование данных

- Безопасность разработки
- Все сервисы облака хранят пользовательские данные в зашифрованном виде
- Протокол TLS обеспечивает защиту данных при передаче по интернет-каналам

Детали: youtube.com/watch?v=X62Z8-M4luM

Сервисы безопасности

Безопасность платформы

Сервисы

- IAM
- KMS NEW
- Certificate Manager NEW
- Lockbox PREVIEW
- Yandex DDoS

Смежная функциональность

- Выделенный хост PREVEW
- Interconnect

Партнёрские/Marketplace

- WAF NEW
- NGFW NEW
- Antivirus NEW
- Disaster Recovery

Функциональность

- Сервисные роли NEW
- Bucket Policy NEW
- Группы безопасности PREVIEW
- Шифрование Object Storage на ключах KMS PREVIEW
- Федерация с AD
- Автоматизированный backup в MDB

Compliance

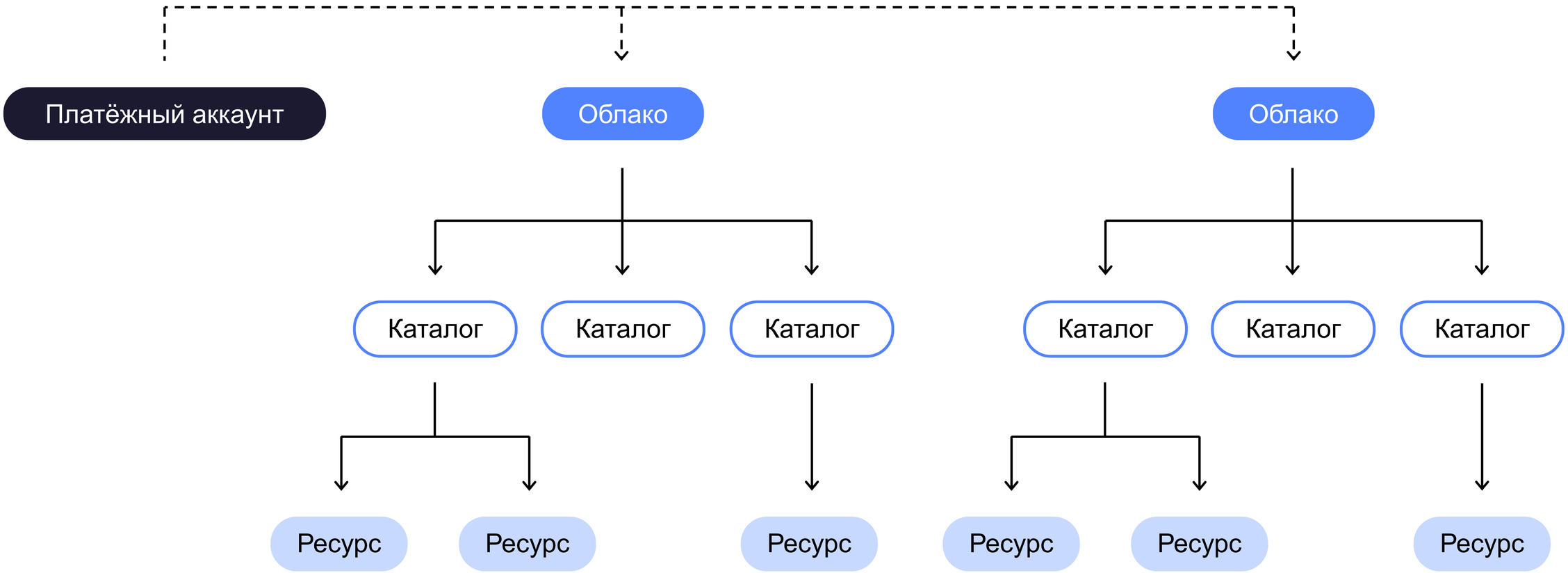
- ISO 27001, ISO 27017, ISO 27018
- ФЗ 152 УЗ-1 NEW
- PCI DSS для ЦОД
- PCI DSS для облачных сервисов NEW
- GDPR
- ГОСТ 57580 NEW

IAM

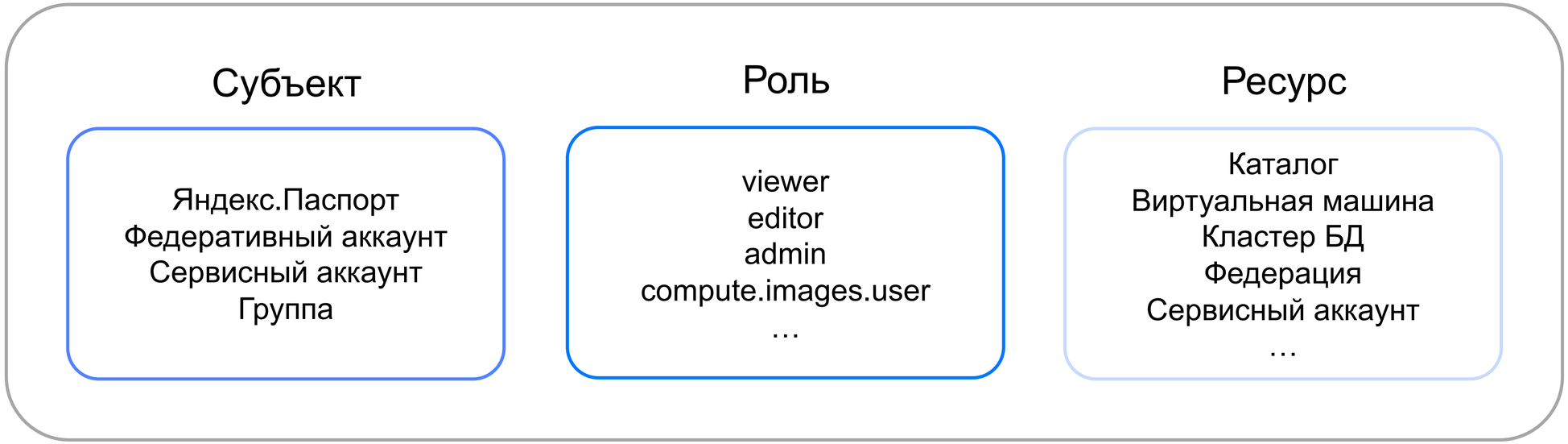
- Базовый сервис для разграничения прав доступа
- Простая RBAC модель
- Предустановленный набор ролей
- Каждая роль — набор разрешений

console.cloud.yandex.com/iam

Дерево ресурсов



Права доступа



Права доступа определяют, кто (субъект) что (роль) и где (ресурс) может делать

Роли

- Примитивные
- Сервисные
- Специальные

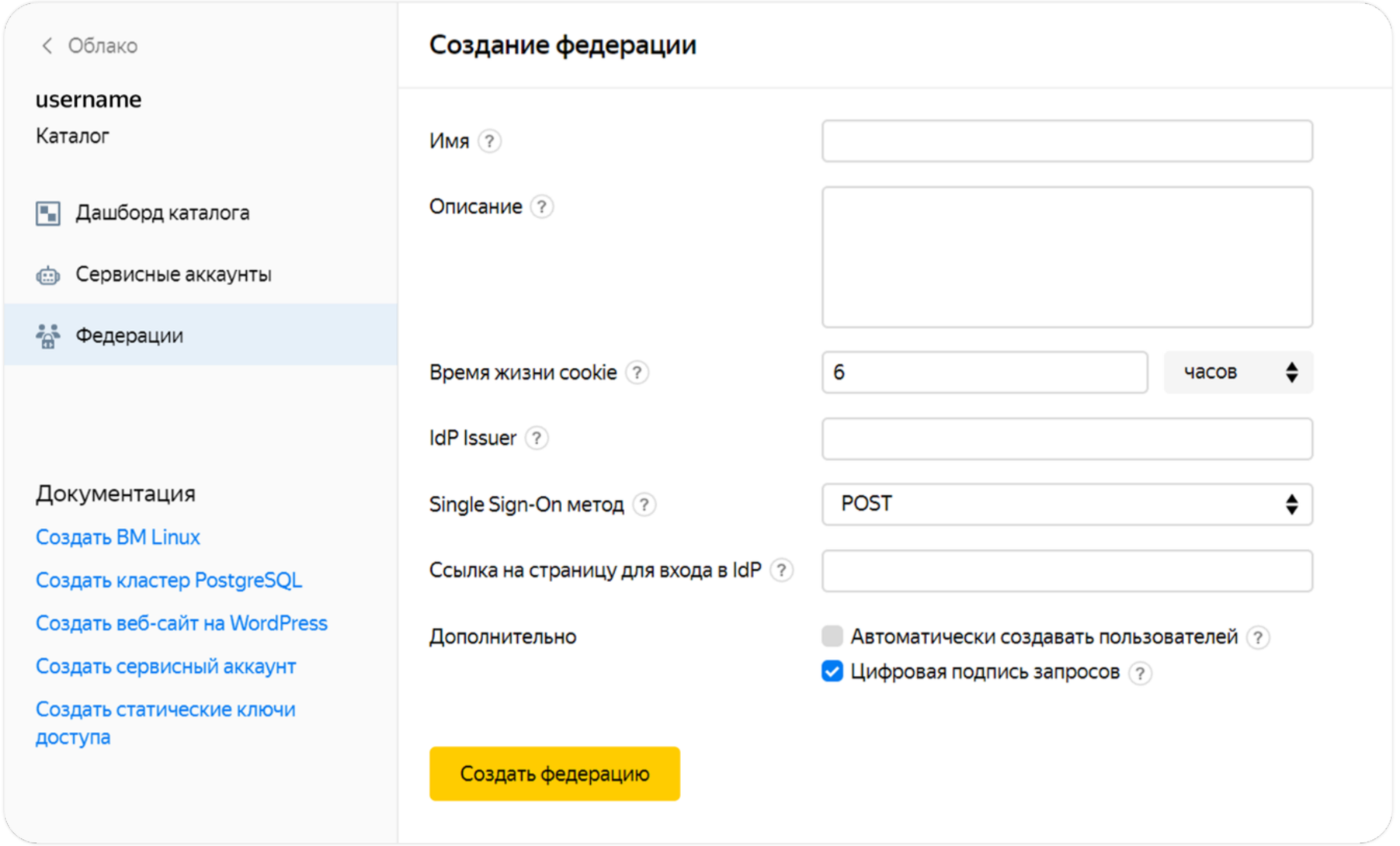
Сервисные роли

- YMQ, Container Registry, YDB, Serverless, DataLens
  - ServiceName.Admin
- Object Storage
  - Storage.admin
  - Storage.configurer
  - Storage.editor
  - Storage.uploader
  - Storage.viewer
- Key Management Service
  - KMS.admin
  - KMS.key.EncrypterDecrypter
- Managed Database
  - Mdb.admin
  - MDB.viewer
- IAM
  - IAM.ServiceAccounts.admin
- VPC
  - VPC.admin
  - VPC.PublicAdmin
  - VPC.PrivateAdmin
  - VPC.user
  - VPC.viewer
- Load Balancer
  - Load-balancer.admin
  - Load-balancer.PrivateAdmin
  - Load-balancer.viewer
- Compute
  - Compute.admin
  - IAM.ServiceAccounts.admin

Identity Federation

- Контроль аутентификации на стороне клиента
- Базовый сценарий — ADFS
- SAML может работать с чем угодно
- G Suite, Bitrix24 и т.д., все с поддержкой SAML

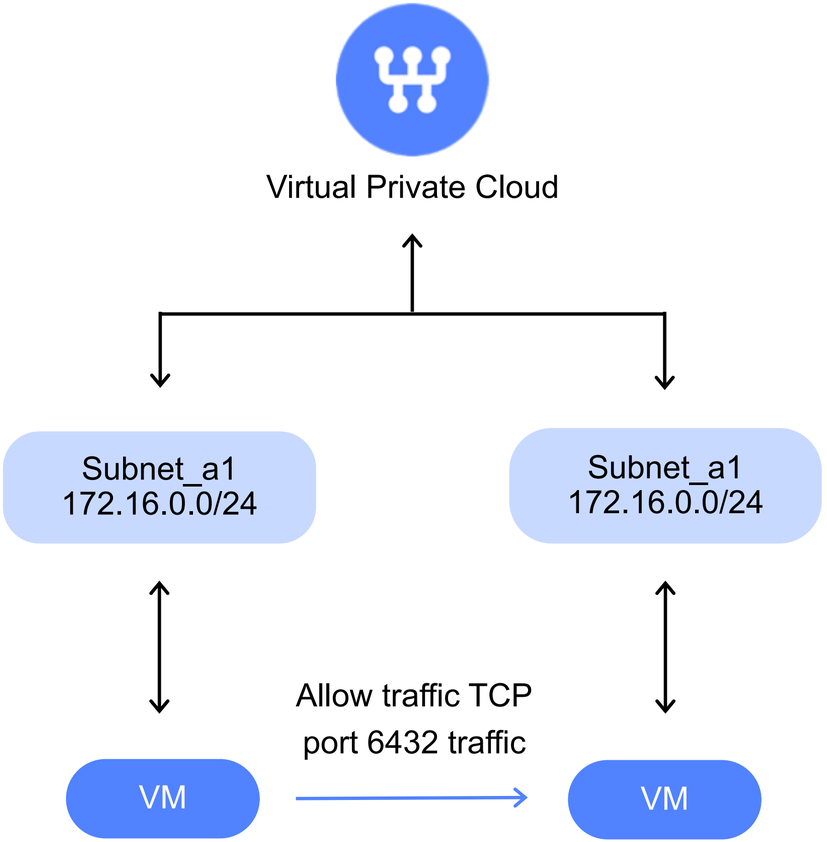
Создание федерации



Security Groups

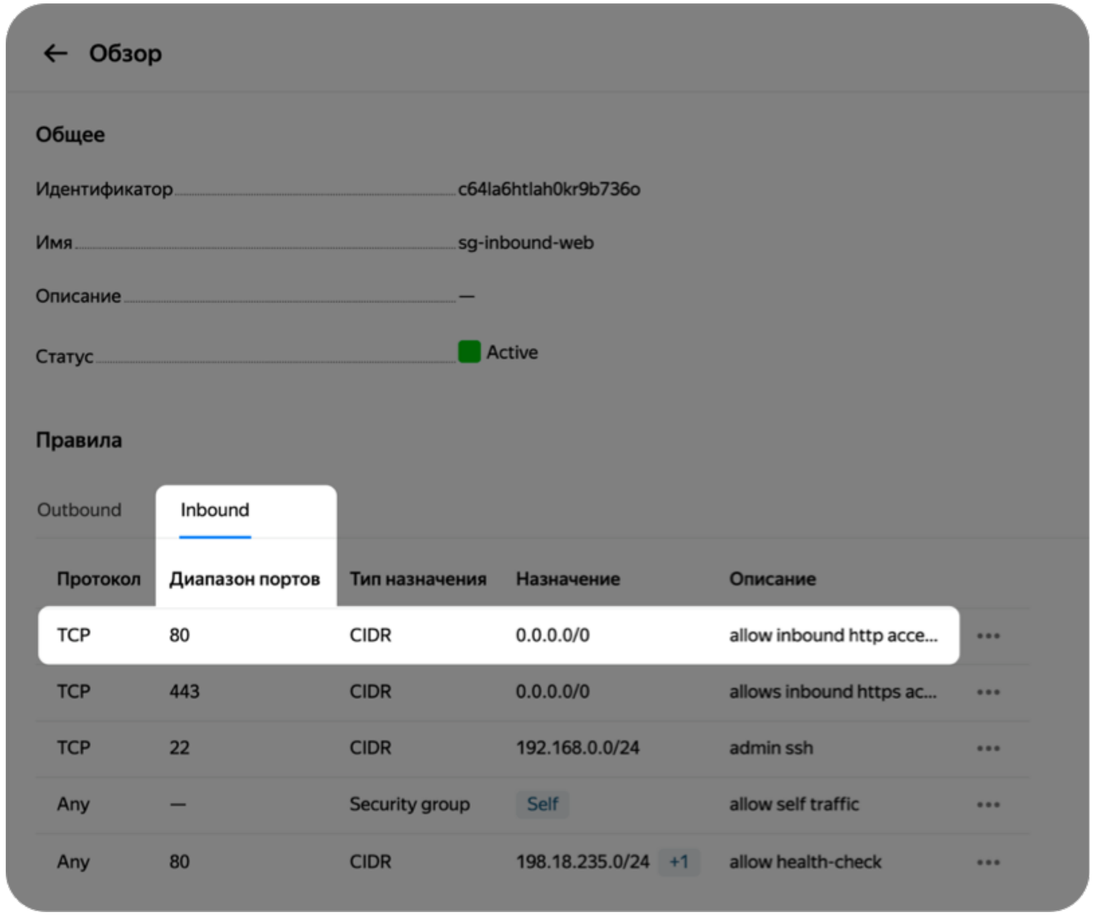
Группы безопасности позволяют ограничивать доступ VM к другим ресурсам и группам безопасности Yandex.Cloud или ресурсам в интернете

- Группа безопасности назначается сетевому интерфейсу VM и должна содержать правила для получения и отправки трафика
- Каждой VM можно назначить несколько групп безопасности



Security Groups

- Правила для входящего трафика. Определяют диапазоны адресов и портов или другие группы безопасности, откуда VM смогут принимать трафик
- Правила для исходящего трафика. Определяют диапазоны адресов и портов или другие группы безопасности, куда VM смогут отправлять трафик
- Если в группе безопасности существует правило для исходящего трафика, ответный трафик всё равно сможет поступать на VM



* Выделенная строка разрешает входящие подключения по 80-му порту TCP с любого адреса

Сетевая связность

Через интернет

Нет гарантий

- Задержки — вариативные
- Потери — обычное дело
- Скорость — нестабильная

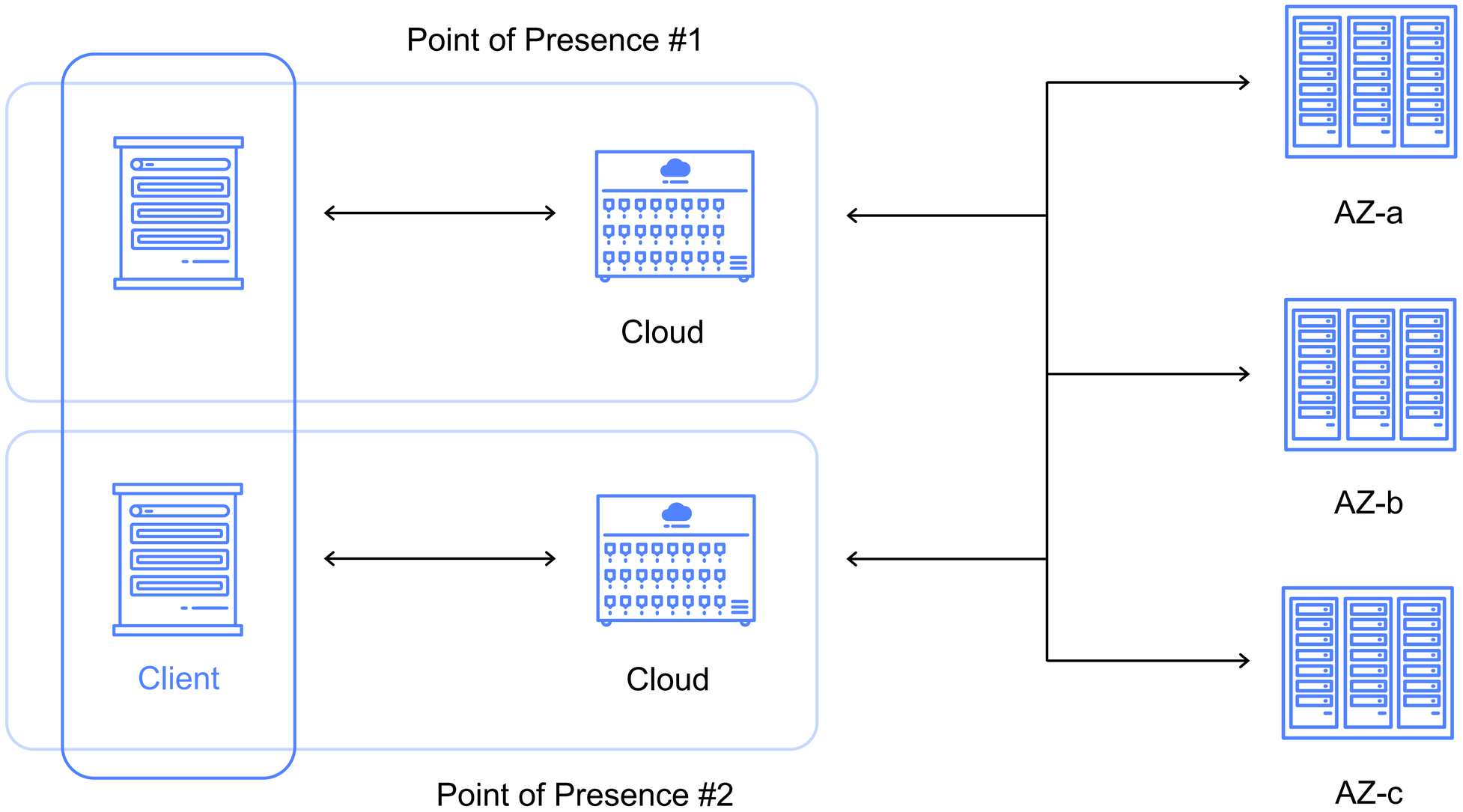
Выделенные каналы

Есть гарантии*

- Задержки — предсказуемы
- Потери — нет
- Скорость — стабильная

* По сравнению со связностью через интернет

Cloud Interconnect

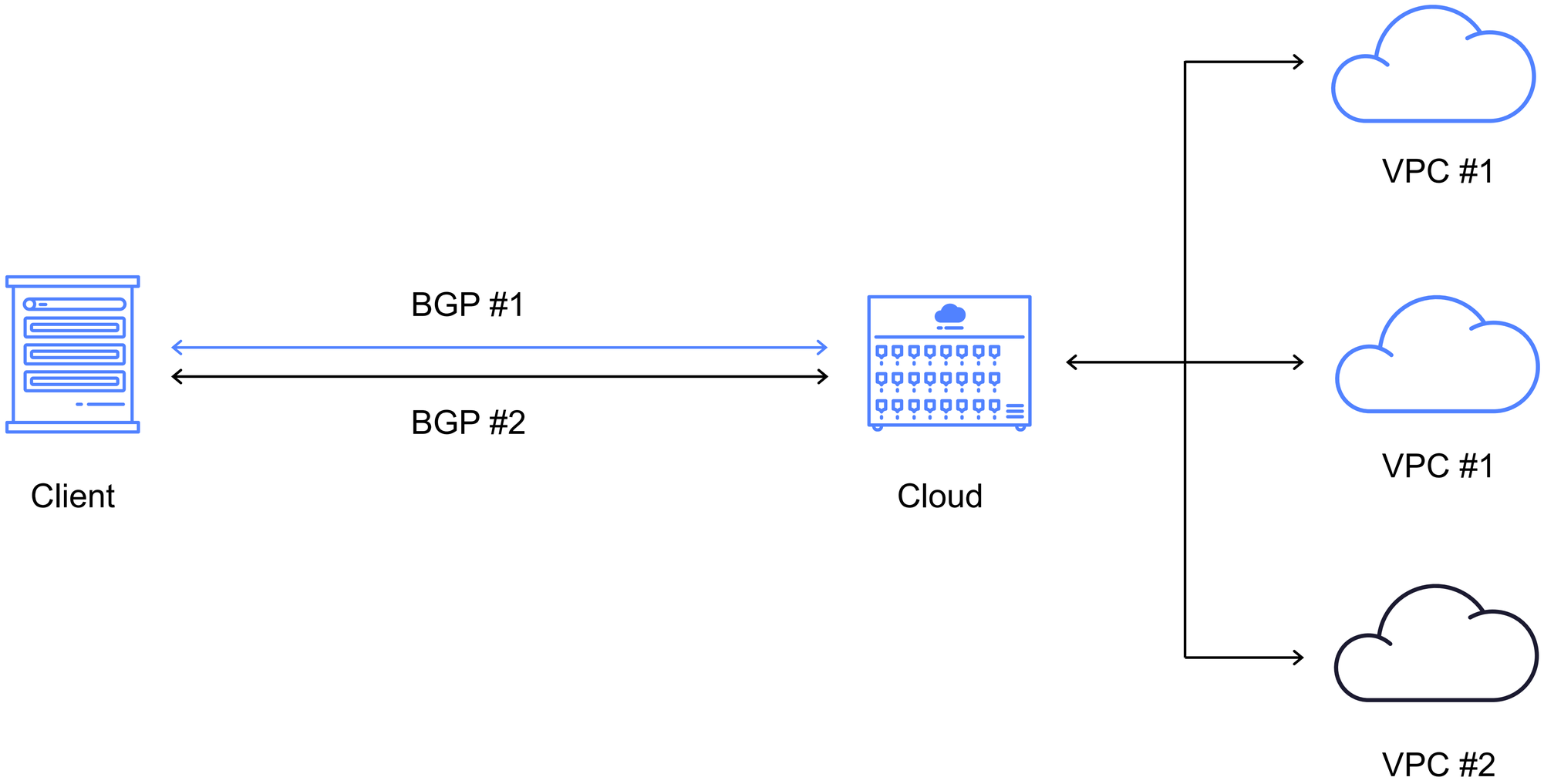


Точки присутствия и партнёры

Точки присутствия:

- MMTC-9
- StoreData
- DataLine Норд
- DataLine OST

Технические особенности



Cloud Interconnect

Этапы подключения услуги

- Заявка на подключение
  через партнера
  или самостоятельно
- Согласование параметров канала
  (точка подключения, скорость) и кроссировка линии
- Настройка BGP пиринга для каждой VPC
- Выбор префиксов для анонса (можно
  анонсировать только часть подсетей в VPC)

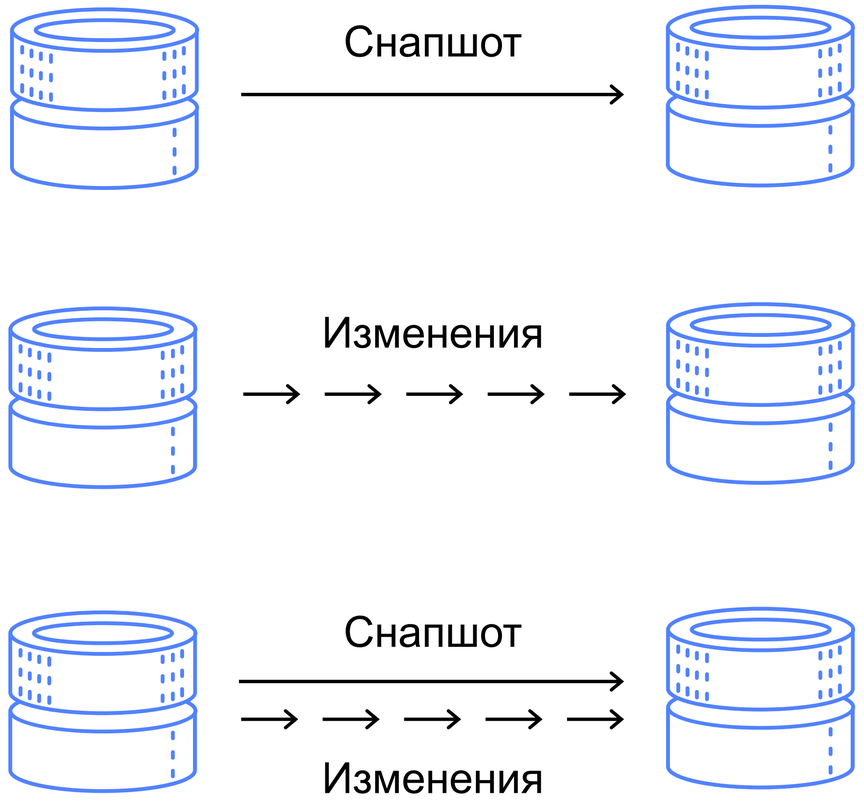
Data Transfer

Что такое Yandex Data Transfer?

Yandex Data Transfer помогает быстро и безопасно выполнить миграцию баз данных из других облачных платформ или локальных баз данных в сервисы управляемых баз данных Yandex.Cloud

Типы трансферов

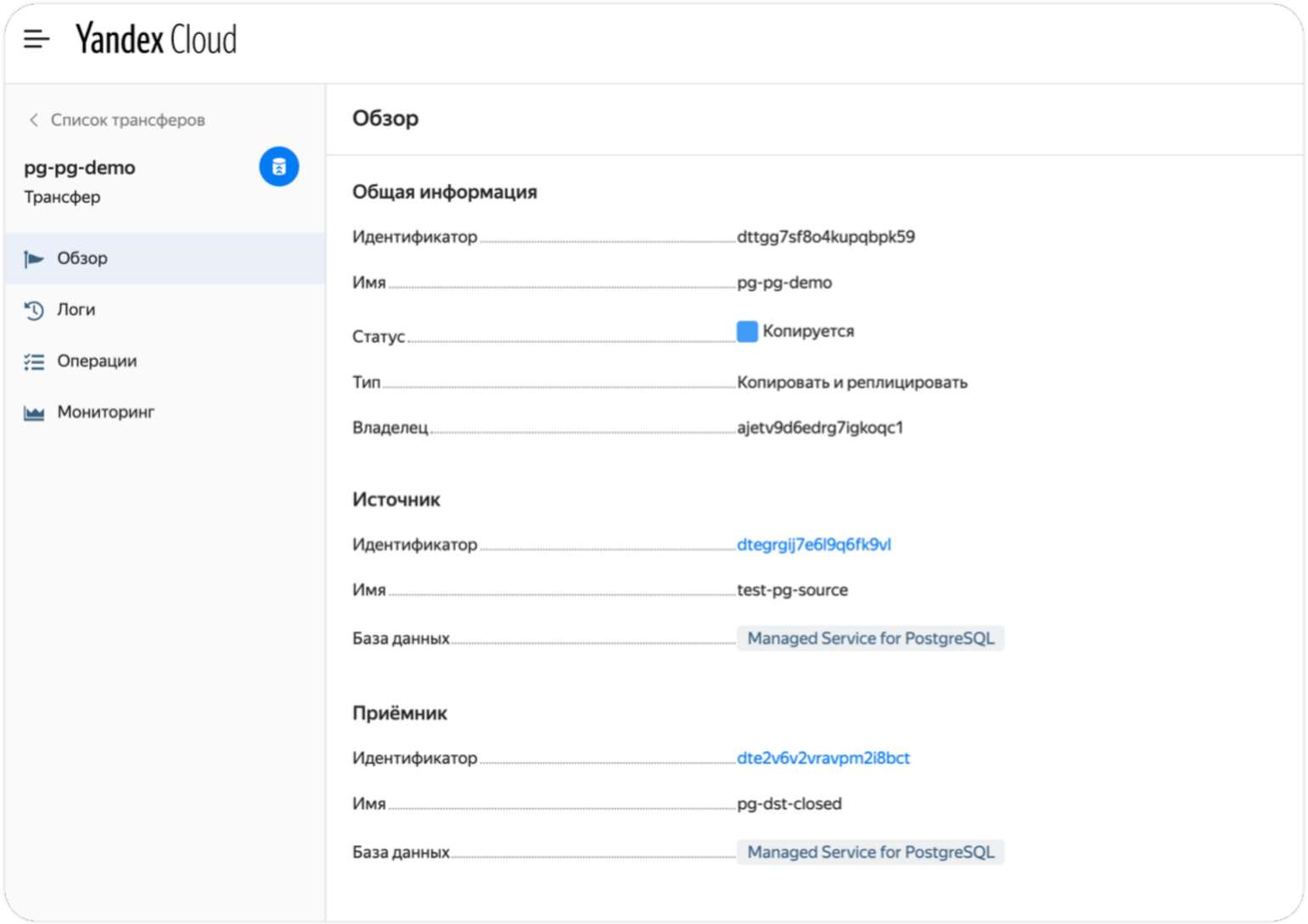
Трансфер — процесс переноса данных между источником и приёмником



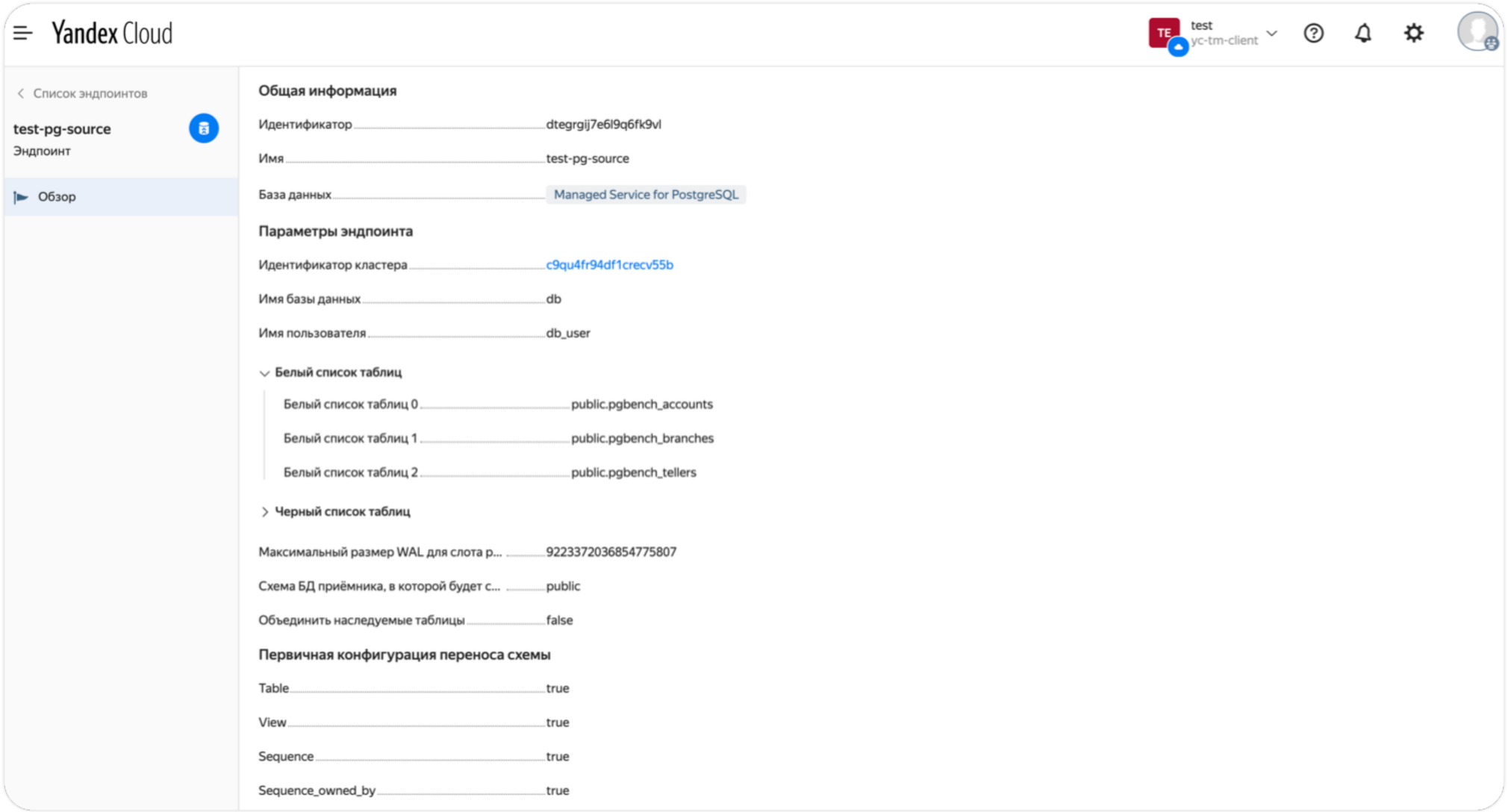
Сценарии использования

1. Миграция в Yandex.Cloud
2. Разделение и объединение баз данных
3. Разделение аналитической и продуктовой нагрузки
4. Разворачивание инфраструктуры разработки
5. Способ попробовать Yandex.Cloud на реальных данных
6. Disaster recovery

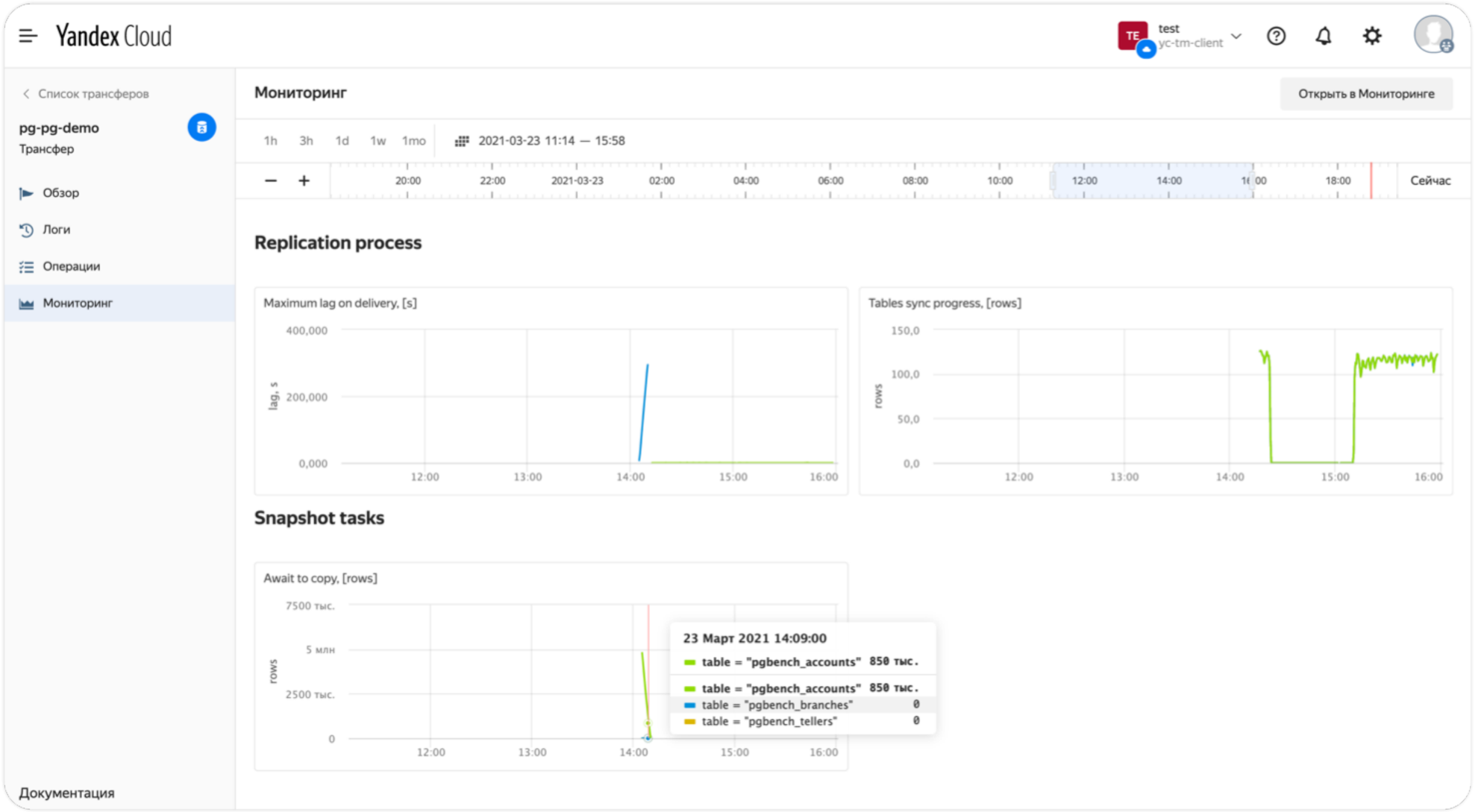
Пример работы. Страница трансфера



Пример работы. Страница источника



Пример работы. Мониторинг



Перенос элементов схемы. PostgreSQL

Умеем переносить элементы схемы отдельно от данных

- На активации: TABLE, VIEW, PRIMARY KEY, SEQUENCE, SEQUENCE OWNED BY, RULE, TYPE, FUNCTION, DEFAULT
- На деактивации: CONSTRAINT/FK_CONSTRAINT/INDEX/TRIGGER
- Запрещён перенос таблиц без PRIMARY KEY в режиме репликации. Требуется настроить REPLICA IDENTITY

Как пережить переезд мастера источника? PostgreSQL

Плагин PostgreSQL pg_tm_aux

Чтобы активировать этот режим, нужно выполнить два действия:

- Включить на источнике плагин pg_tm_aux
- Перезапустить трансфер, чтобы запустился трекер lsn

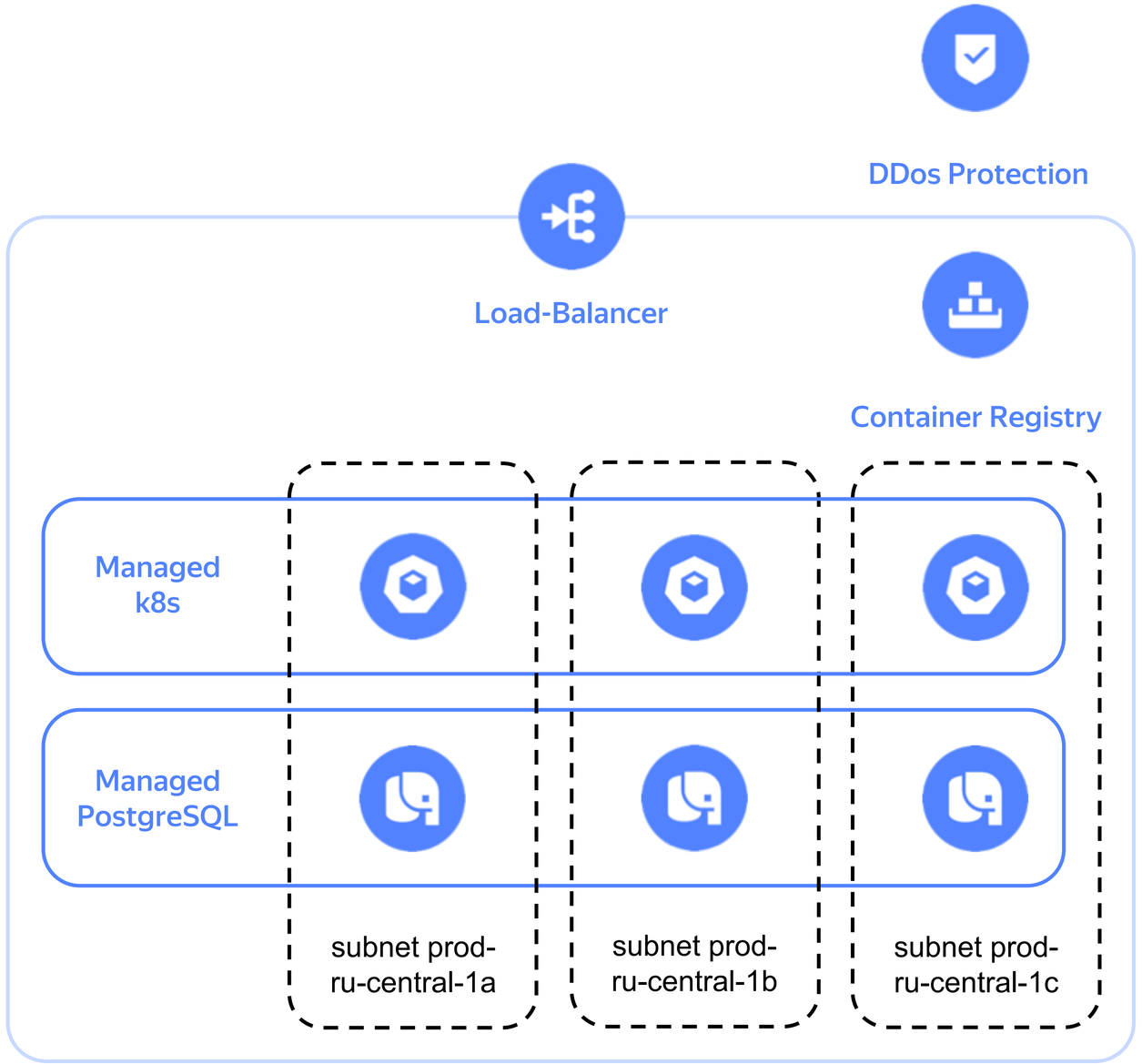
Roadmap

- PostgreSQL → PostgreSQL доступно
- PostgreSQL → ClickHouse (снапшот) по запросу
- PostgreSQL → S3 (снапшот) Q4 2021

SLA и ограничения PostgreSQL as a Service

SLA PostgreSQL

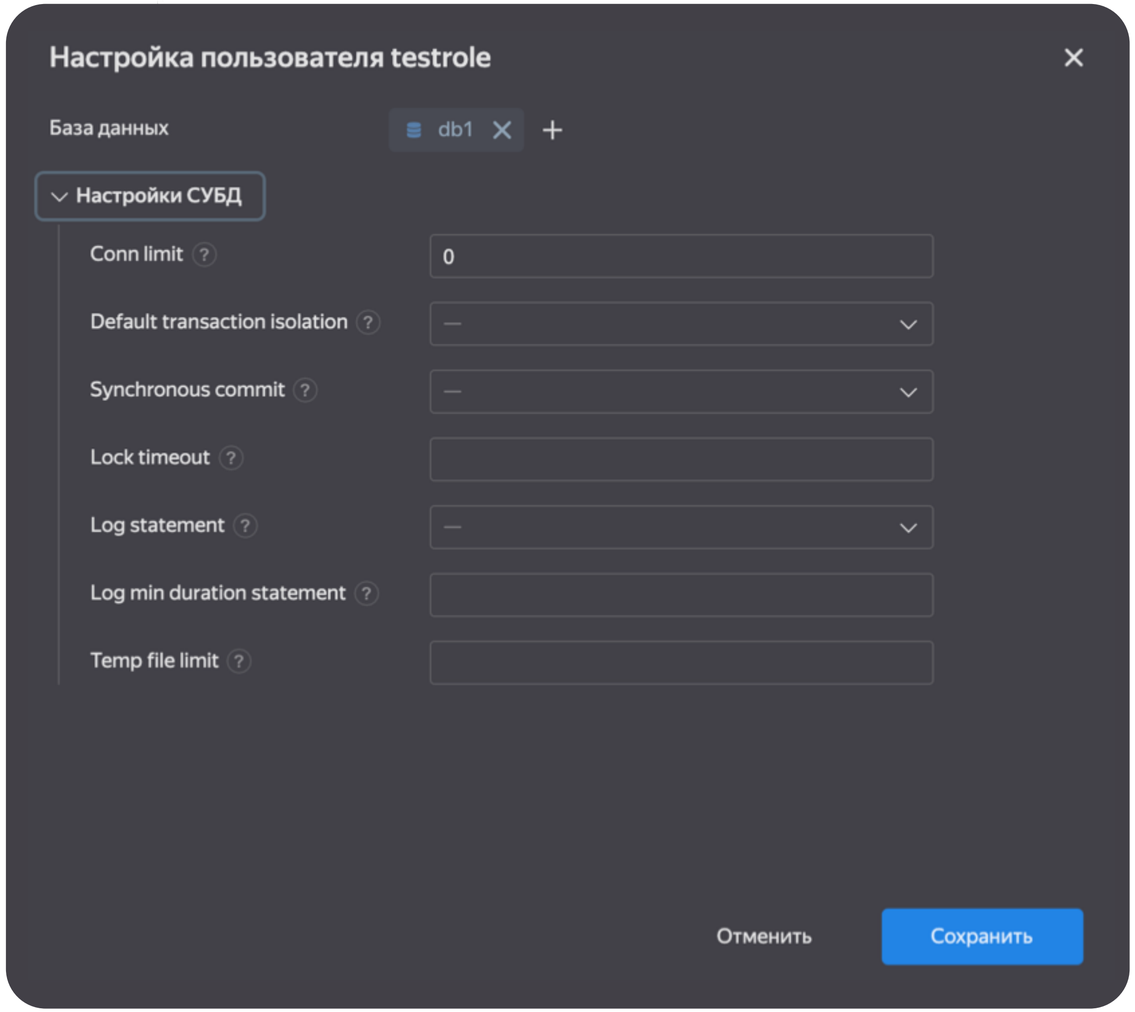
- Uptime
  - 99,99% на чтение
  - 99,95% на запись
- Распространяется на конфигурацию
  - С минимум **двумя** хостами в разных зонах доступности
  - При использовании поддерживаемых клиентов



yandex.ru/legal/cloud_sla_mdb/

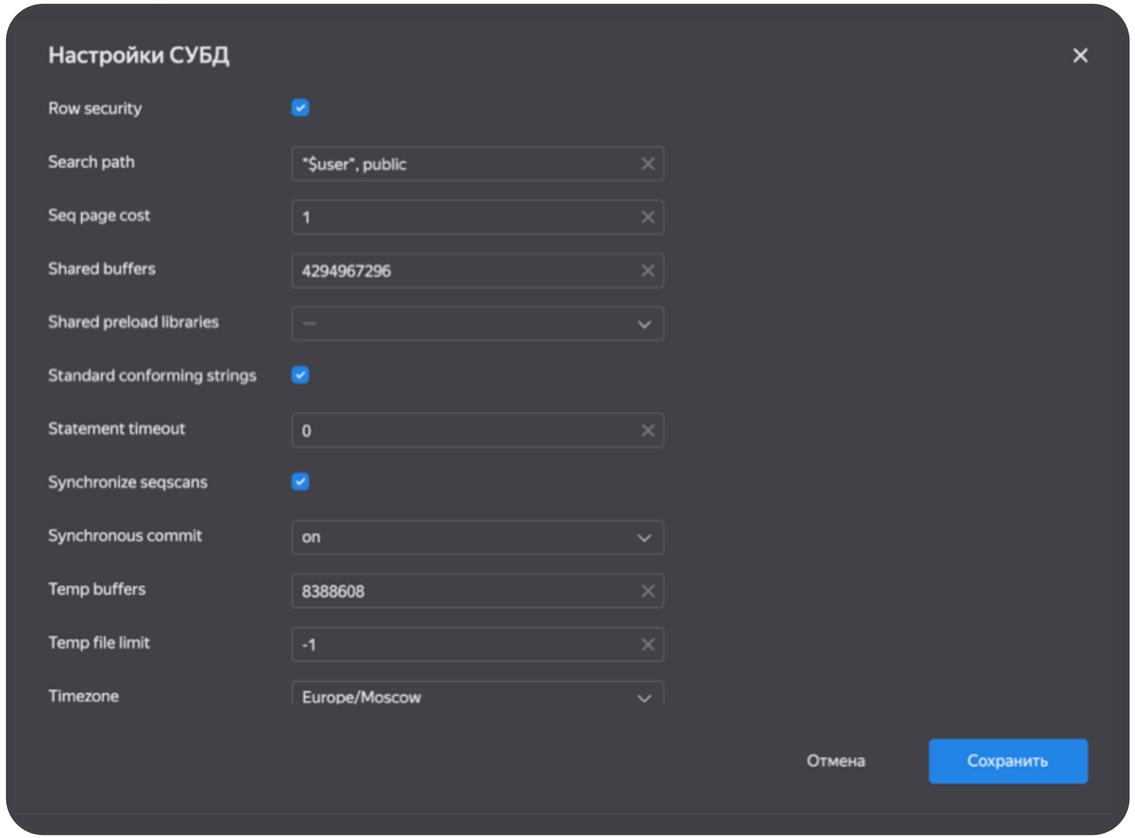
Базы данных и пользователи

- В управляемом сервисе у вас **нет** прав **суперпользователя** и доступа по SSH на узлы
- Базы данных и пользователи создаются и удаляются **только** через API
- Выдача ролей через API
- При создании базы надо указать пользователя-владельца
- Остальным пользователям надо выдать привилегии в базе, используя SQL



Настройки кластера

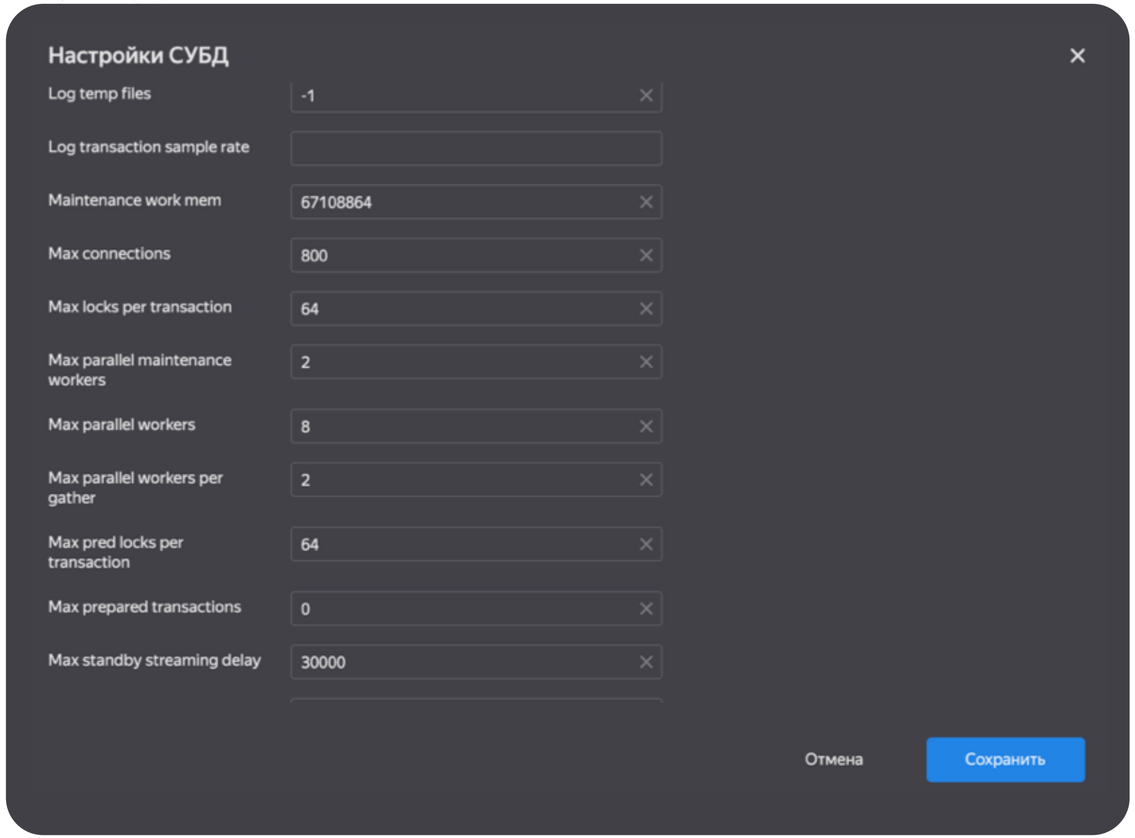
- Кластер автоматически настраивает значения для базы по умолчанию
- Часто значения по умолчанию зависят от количества ядер или RAM
- Значения можно изменить (не выходя за рамки лимитов)
- Измененные значения останутся такими же при изменении количества vCPU кластера
- Некоторые изменения могут потребовать каскадного перезапуска баз в кластере



Настройка max_connections

На всю СУБД

- Зависит от:
  - числа ядер (200 за 1 vCPU)
  - типа CPU (частичное использование ядра или нет)
  - 15 служебных соединений резервируется для служебных нужд
- Для повышения значения надо увеличивать число ядер

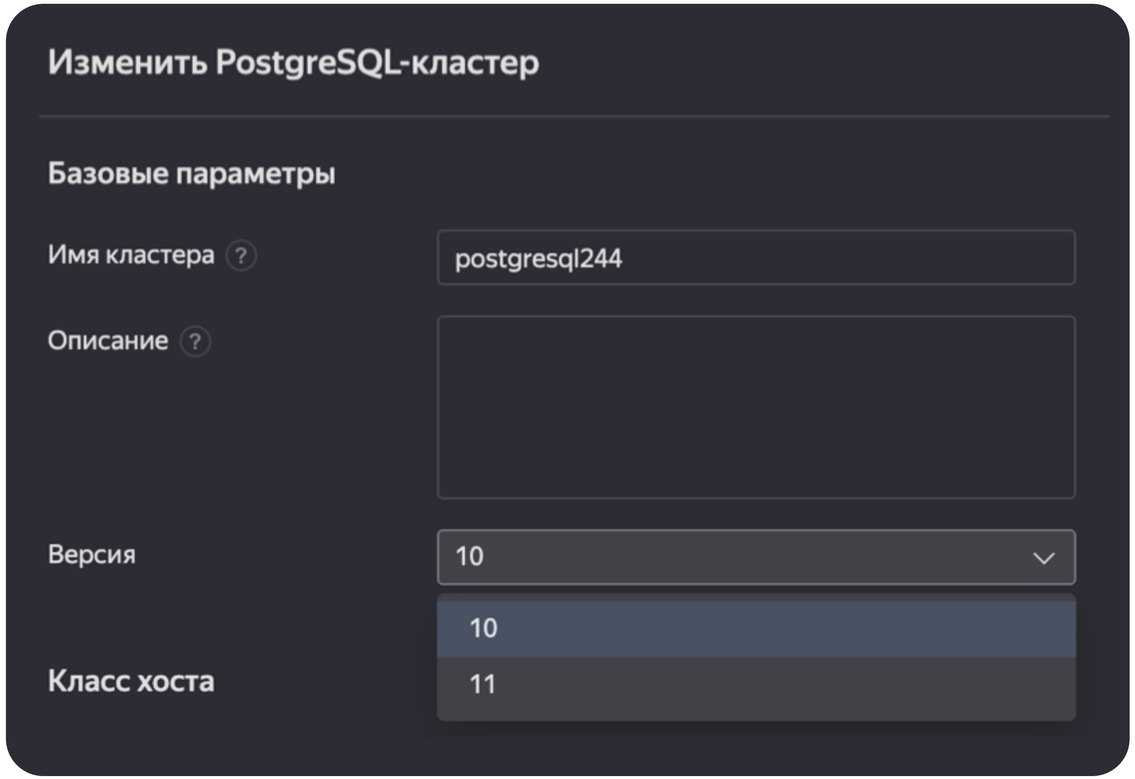


На пользователя

- В сумме число соединений всех пользователей не должно превышать число на кластер

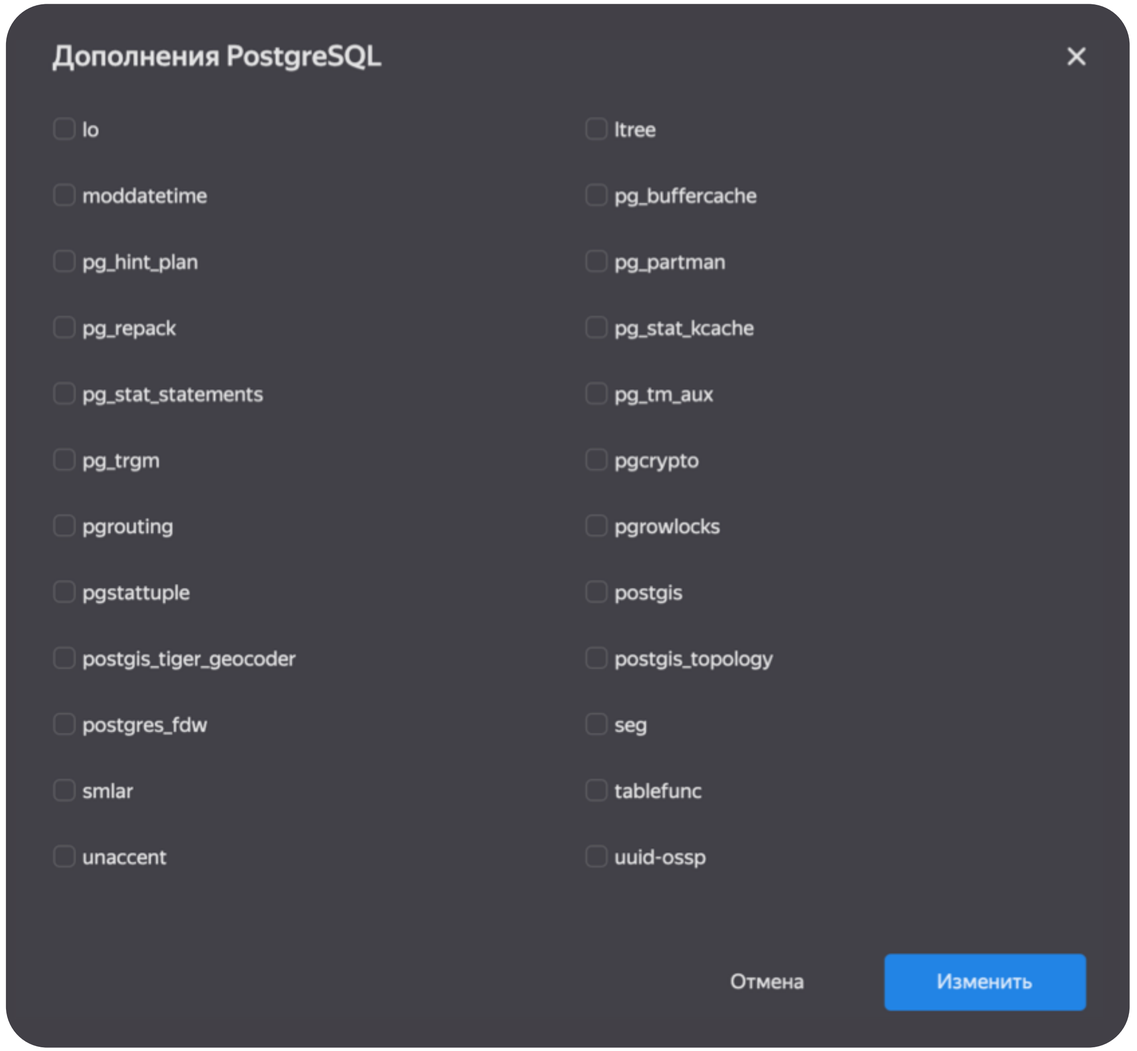
Обновления

- Минорные: рассылка письма и перезапуск базы
- Мажорные:
  - pg_upgrade
- Недоступность записи во время обновления
  - Минуты
- Обновление можно делать только на одну версию выше
- Для более неподдерживаемых версий уведомляем пользователя об обновлении за 1 месяц для мажорных или 7 дней для минорных. Затем производится автоматическое обновление до следующей поддерживаемой версии

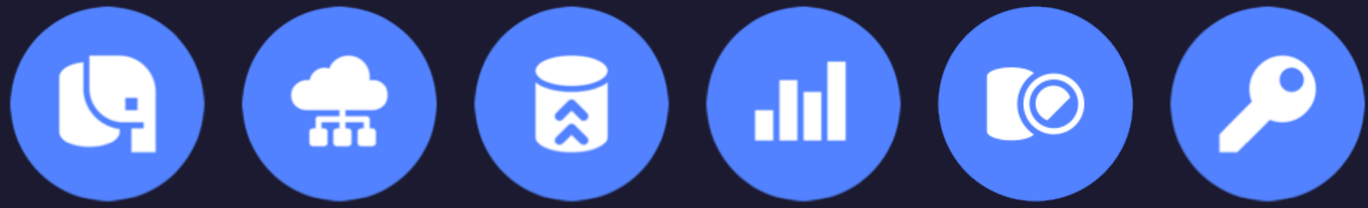


Расширения PostgreSQL

- Выставляются через API
- Версии расширения меняются в зависимости от версии PostgreSQL



Yandex Cloud



Спасибо! Вопросы?

Всеволод Грабельников

Старший архитектор облачных решений Yandex.Cloud

vsgrab@yandex-team.ru