

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

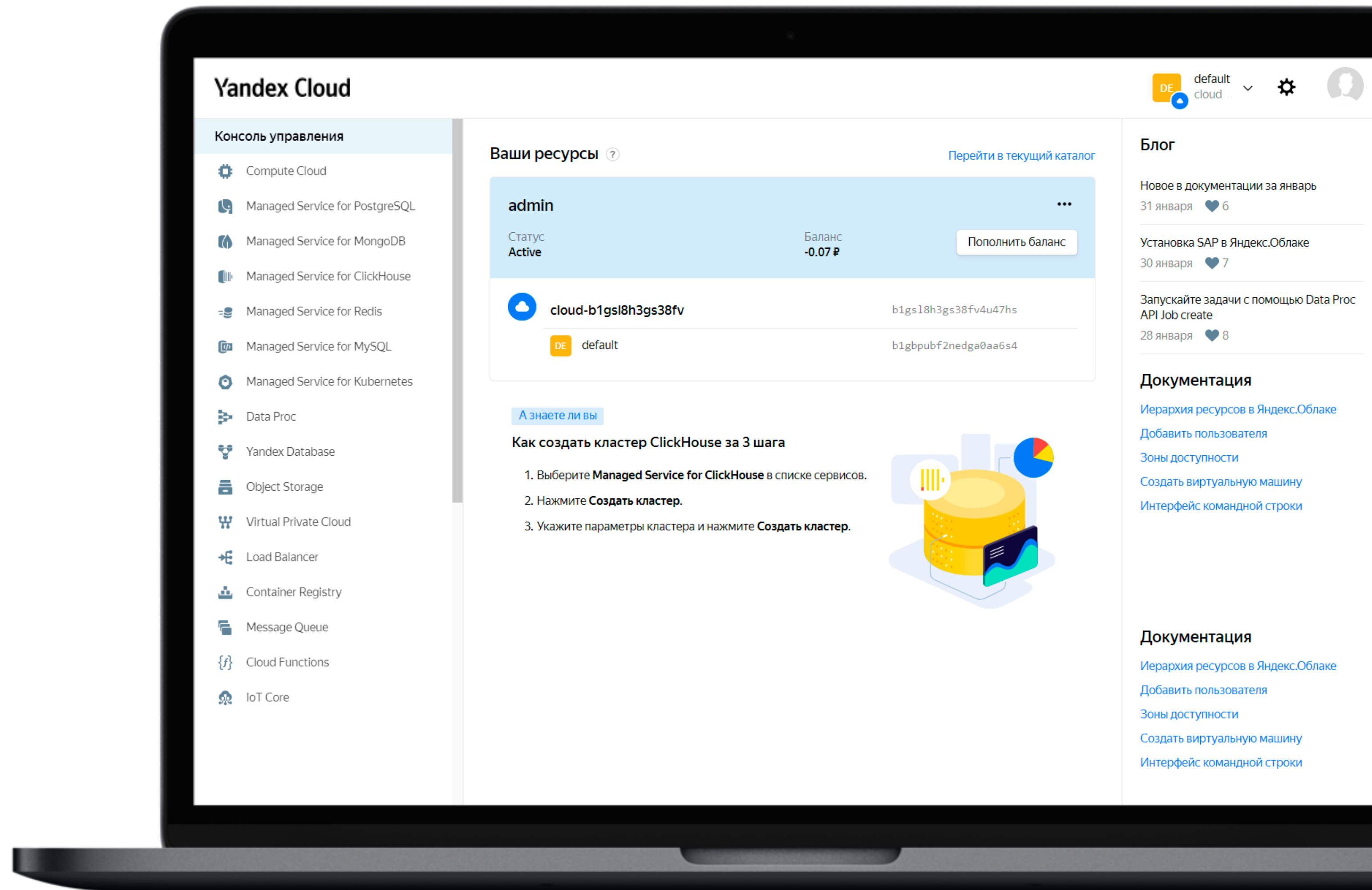
05

Ограничения PostgreSQL as a Service и SLA

# Коротко о причинах миграции

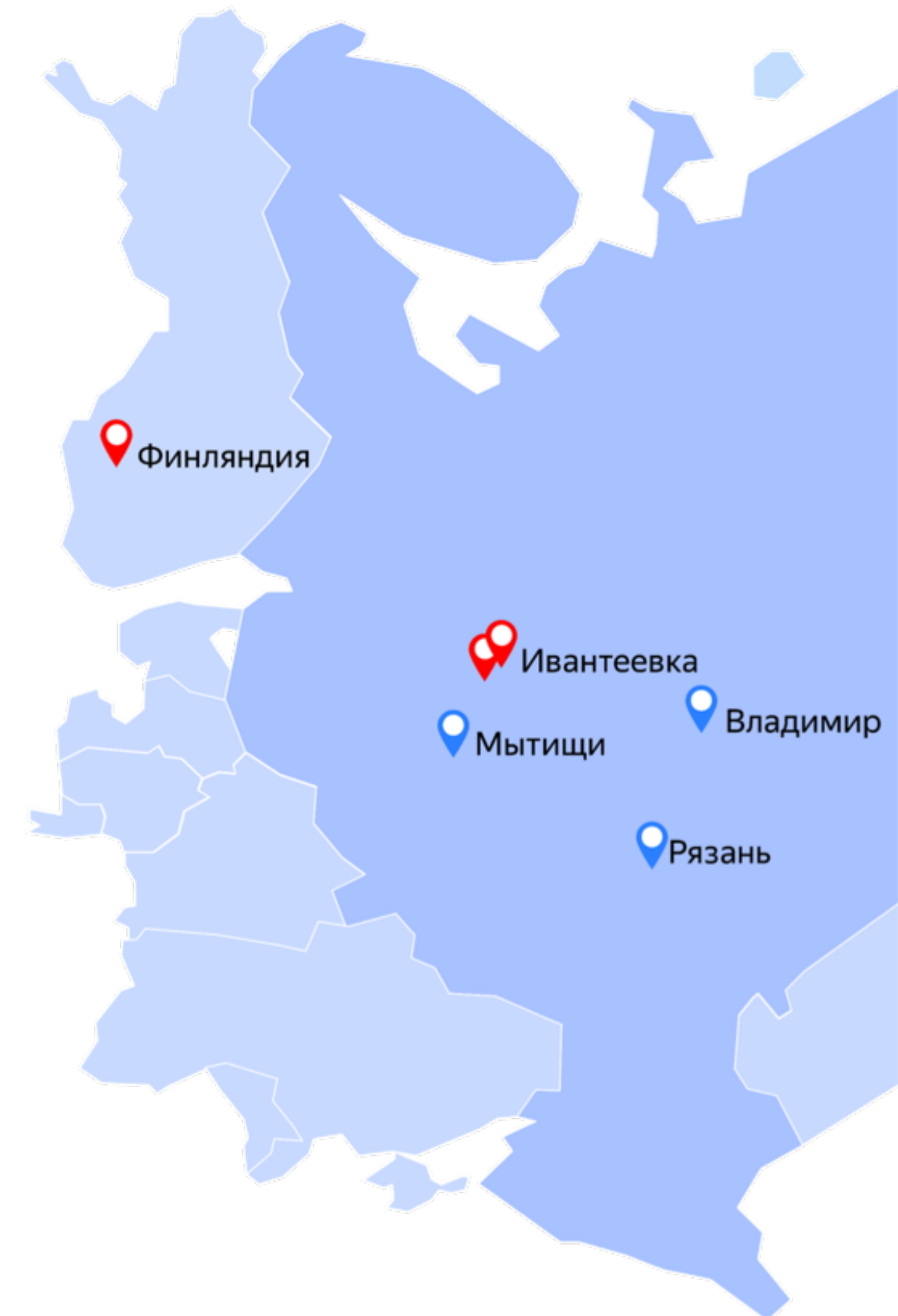
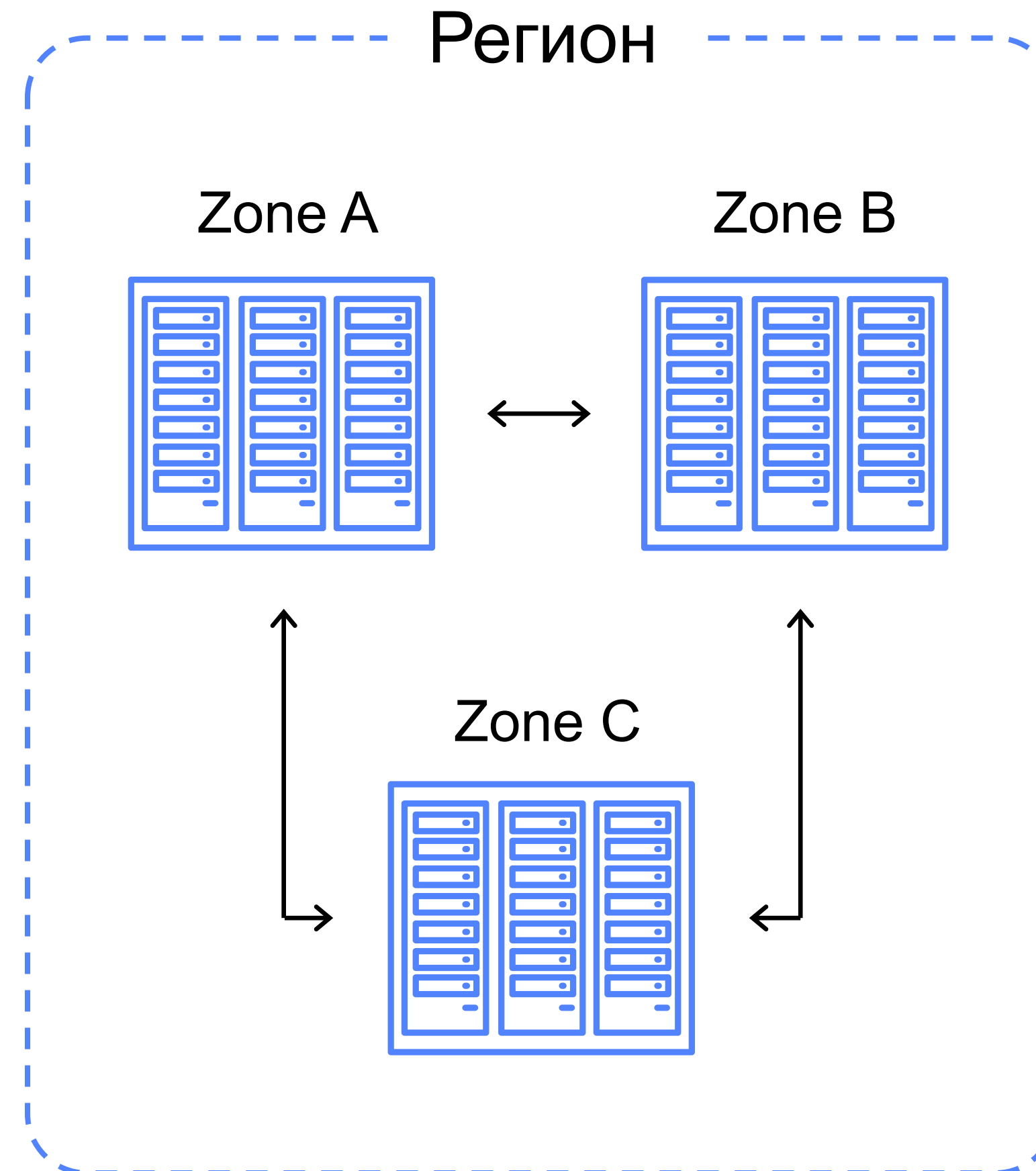
# Удобный инструмент для разработчика

- › 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



# 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

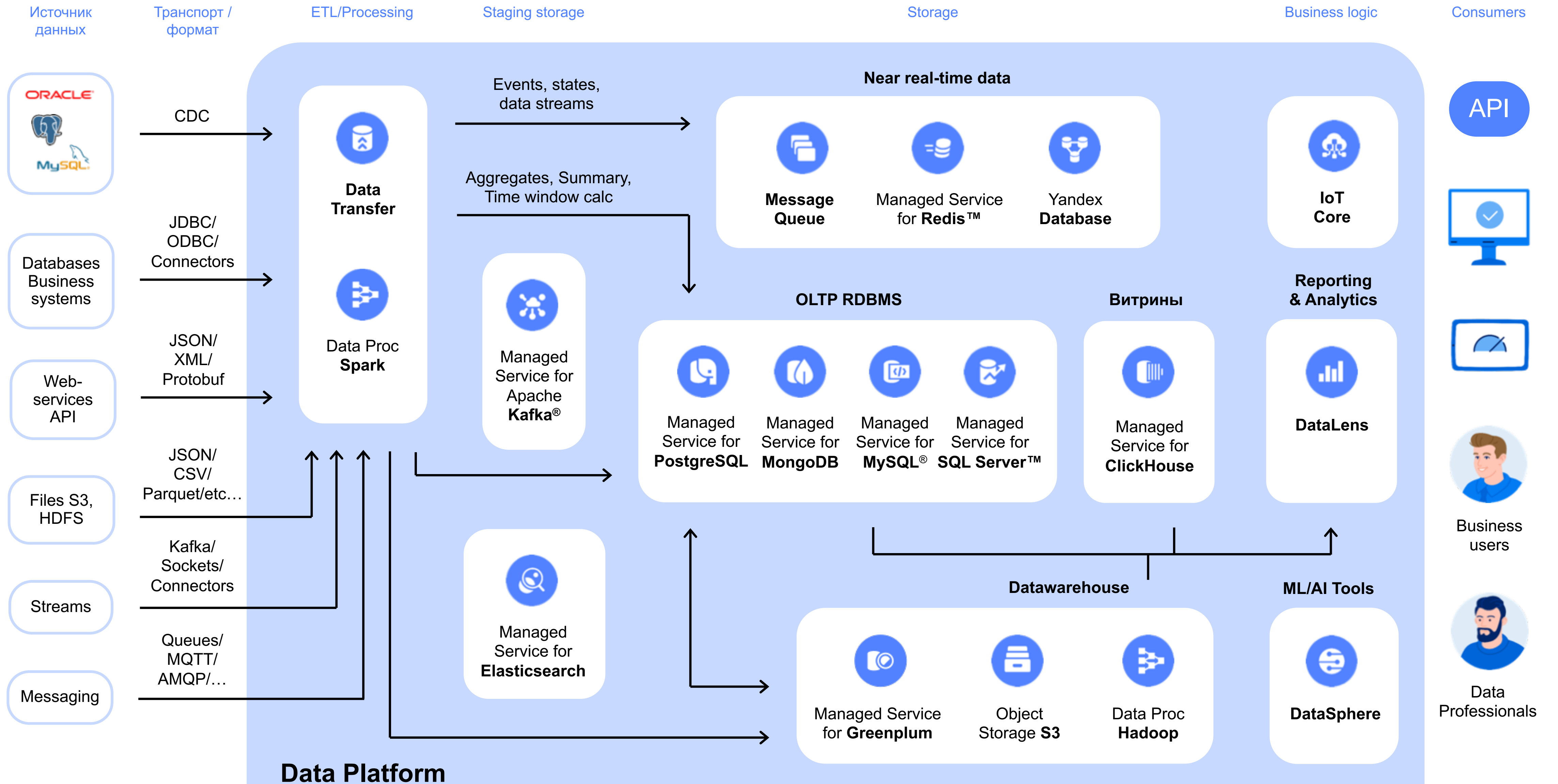
Идентификация  
и безопасность

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

Сервисы безопасности

# Безопасность платформы

## Сервисы

IAM

KMS **NEW**

Certificate Manager **NEW**

Lockbox **PREVIEW**

Yandex DDoS

## Смежная функциональность

Выделенный хост **PREVIEW**

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

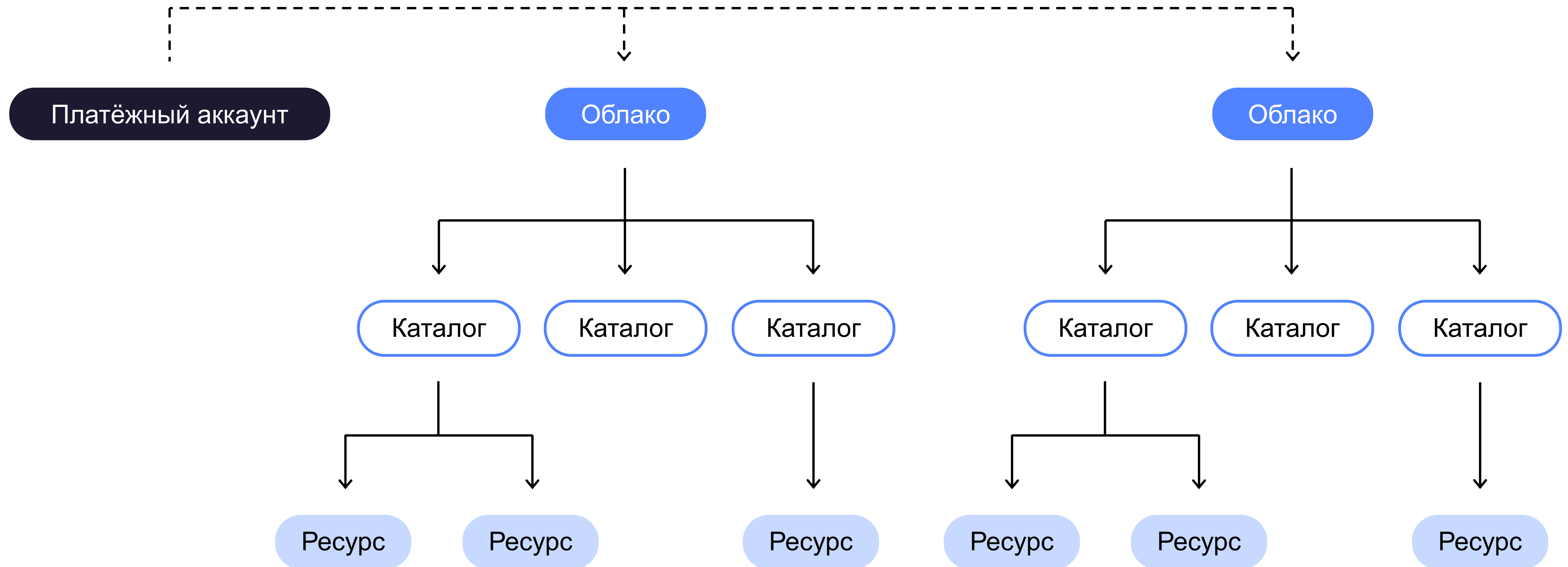


- › Базовый сервис для разграничения прав доступа
- › Простая RBAC модель
- › Предусмотренный набор ролей
- › Каждая роль — набор разрешений

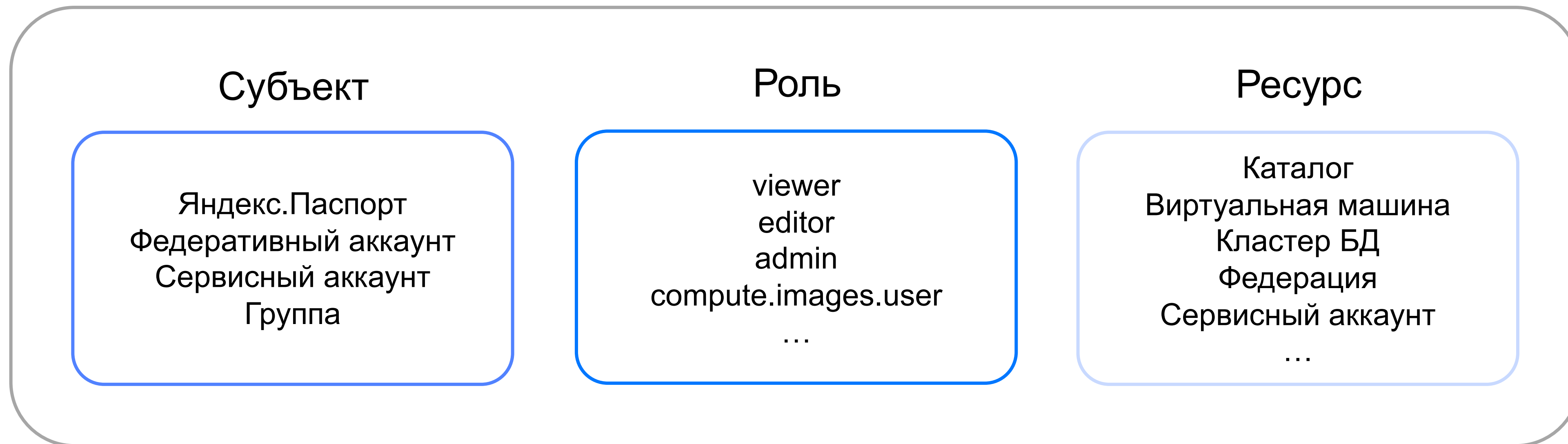
[console.cloud.yandex.com/iam](https://console.cloud.yandex.com/iam)



# Дерево ресурсов



# Права доступа



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

# Роли



- › Прimitives
- › Service
- › Special

# 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

< Облако

username  
Каталог

Дашборд каталога

Сервисные аккаунты

**Федерации**

Документация

[Создать VM Linux](#)

[Создать кластер PostgreSQL](#)

[Создать веб-сайт на WordPress](#)

[Создать сервисный аккаунт](#)

[Создать статические ключи доступа](#)

## Создание федерации

Имя <sup>?</sup>

Описание <sup>?</sup>

Время жизни cookie <sup>?</sup>  часов

IdP Issuer <sup>?</sup>

Single Sign-On метод <sup>?</sup>

Ссылка на страницу для входа в IdP <sup>?</sup>

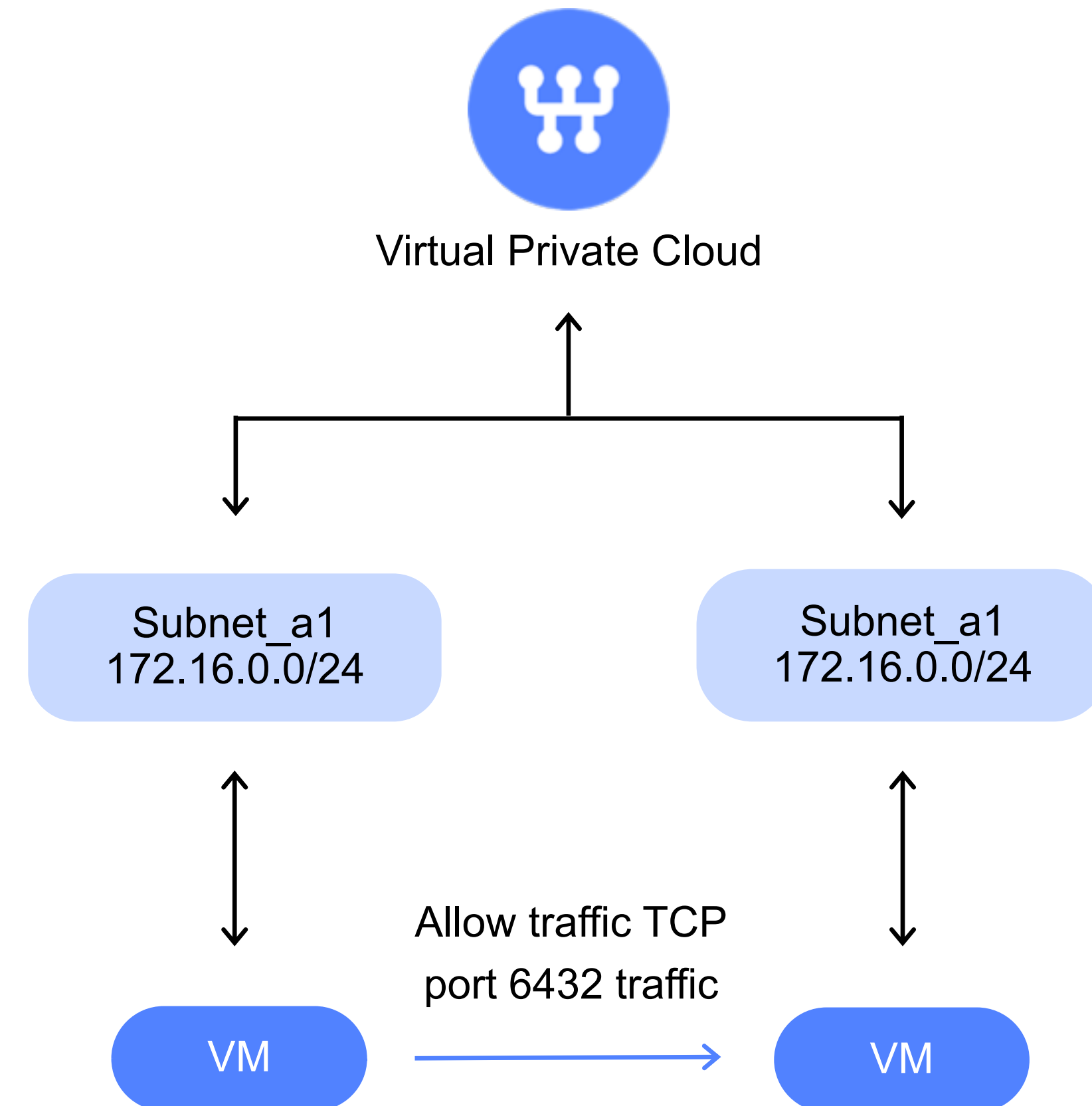
Дополнительно

Автоматически создавать пользователей <sup>?</sup>

Цифровая подпись запросов <sup>?</sup>

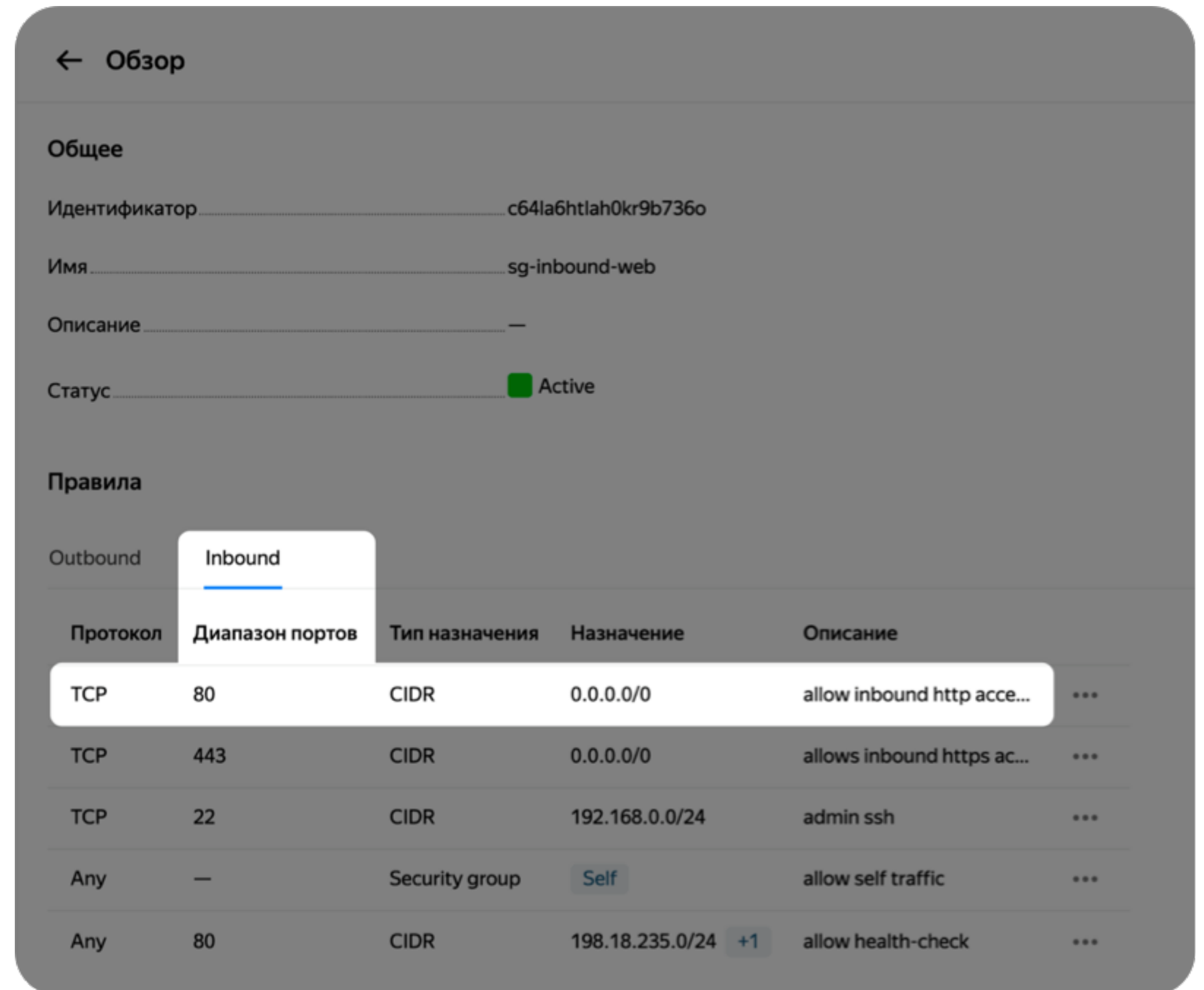
# Security Groups

- 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



← Обзор

Общее

Идентификатор c64la6htlah0kr9b736o

Имя sg-inbound-web

Описание —

Статус ■ Active

Правила

Outbound **Inbound**

Протокол	Диапазон портов	Тип назначения	Назначение	Описание	
TCP	80	CIDR	0.0.0.0/0	allow inbound http acce...	...
TCP	443	CIDR	0.0.0.0/0	allows inbound https ac...	...
TCP	22	CIDR	192.168.0.0/24	admin ssh	...
Any	—	Security group	Self	allow self traffic	...
Any	80	CIDR	198.18.235.0/24 +1	allow health-check	...

\* 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

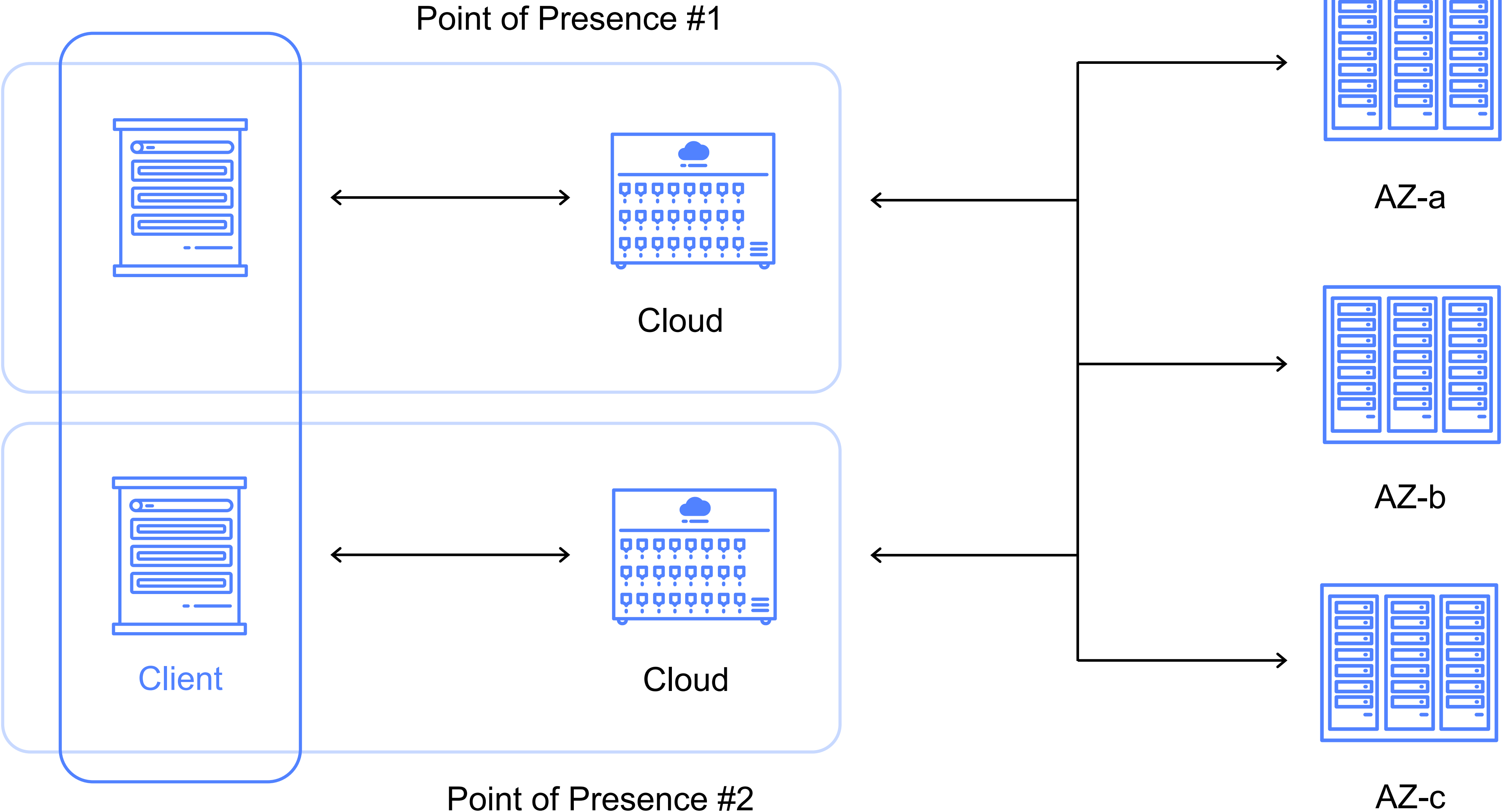
# Выделенные каналы



- Есть гарантии\***
- › Задержки — предсказуемы
- › Потери — нет
- › Скорость — стабильная

\* По сравнению со связностью через интернет

# Cloud Interconnect



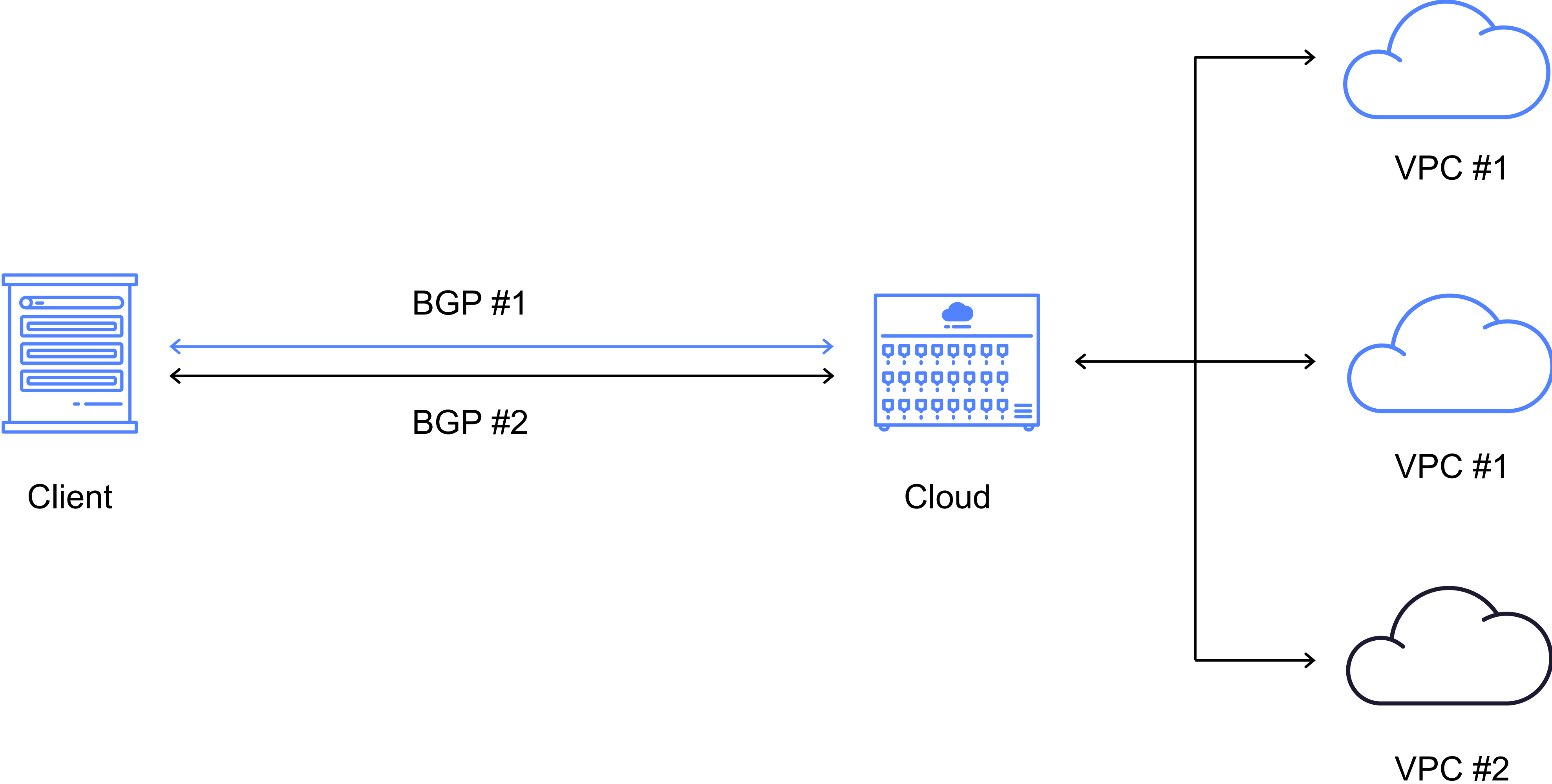
# Точки присутствия и партнёры

## Точки присутствия:

- › ММТС-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



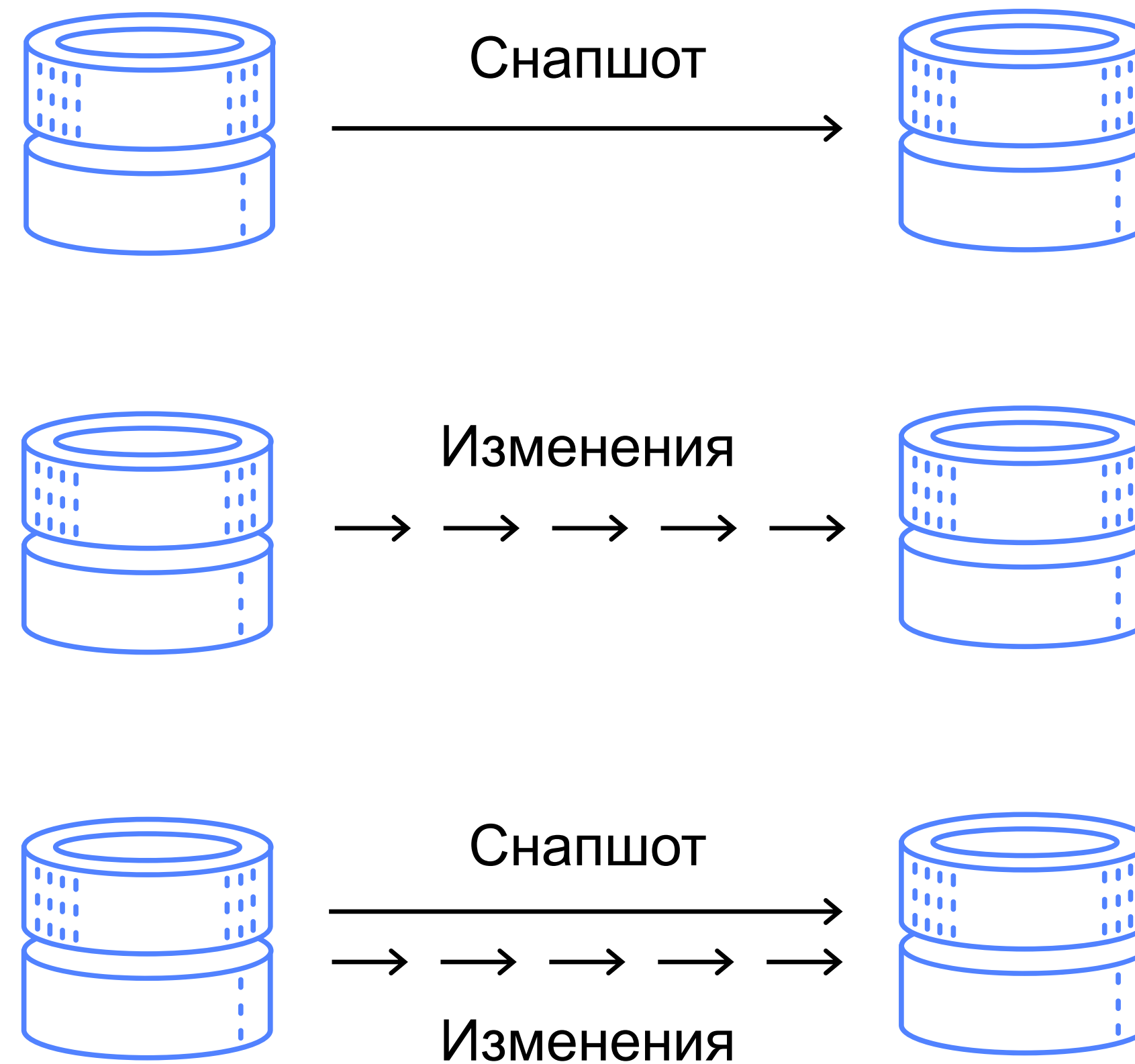
# Что такое Yandex Data Transfer?



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

The screenshot displays the Yandex Cloud console interface. The top left corner shows the 'Yandex Cloud' logo and a hamburger menu icon. Below it, a navigation sidebar contains the following items: 'Список трансферов' (Transfer list), 'pg-pg-demo Трансфер' (pg-pg-demo Transfer) with a blue circular icon, 'Обзор' (Overview) (highlighted), 'Логи' (Logs), 'Операции' (Operations), and 'Мониторинг' (Monitoring). The main content area is titled 'Обзор' (Overview) and is divided into three sections: 'Общая информация' (General information), 'Источник' (Source), and 'Приёмник' (Destination). Each section lists key attributes of the transfer operation.

Section	Attribute	Value
Общая информация	Идентификатор	dttg7sf8o4kupqbpk59
	Имя	pg-pg-demo
	Статус	Копируется
	Тип	Копировать и реплицировать
	Владелец	ajetv9d6edrg7igkoqc1
Источник	Идентификатор	dtegrgij7e6l9q6fk9vl
	Имя	test-pg-source
	База данных	Managed Service for PostgreSQL
Приёмник	Идентификатор	dte2v6v2vravpm2i8bct
	Имя	pg-dst-closed
	База данных	Managed Service for PostgreSQL

# Пример работы. Страница источника

The screenshot displays the Yandex Cloud console interface. The top navigation bar includes the Yandex Cloud logo, a user profile icon, and several utility icons (help, notifications, settings). The left sidebar shows a breadcrumb trail: 'Список эндпоинтов' > 'test-pg-source' > 'Эндпоинт' > 'Обзор'. The main content area is titled 'Общая информация' and lists various configuration parameters for the endpoint.

**Общая информация**

- Идентификатор: dtegrgij7e6l9q6fk9vl
- Имя: test-pg-source
- База данных: Managed Service for PostgreSQL

**Параметры эндпоинта**

- Идентификатор кластера: c9qu4fr94df1crecv55b
- Имя базы данных: db
- Имя пользователя: db\_user

**Белый список таблиц**

- Белый список таблиц 0: public.pgbench\_accounts
- Белый список таблиц 1: public.pgbench\_branches
- Белый список таблиц 2: public.pgbench\_tellers

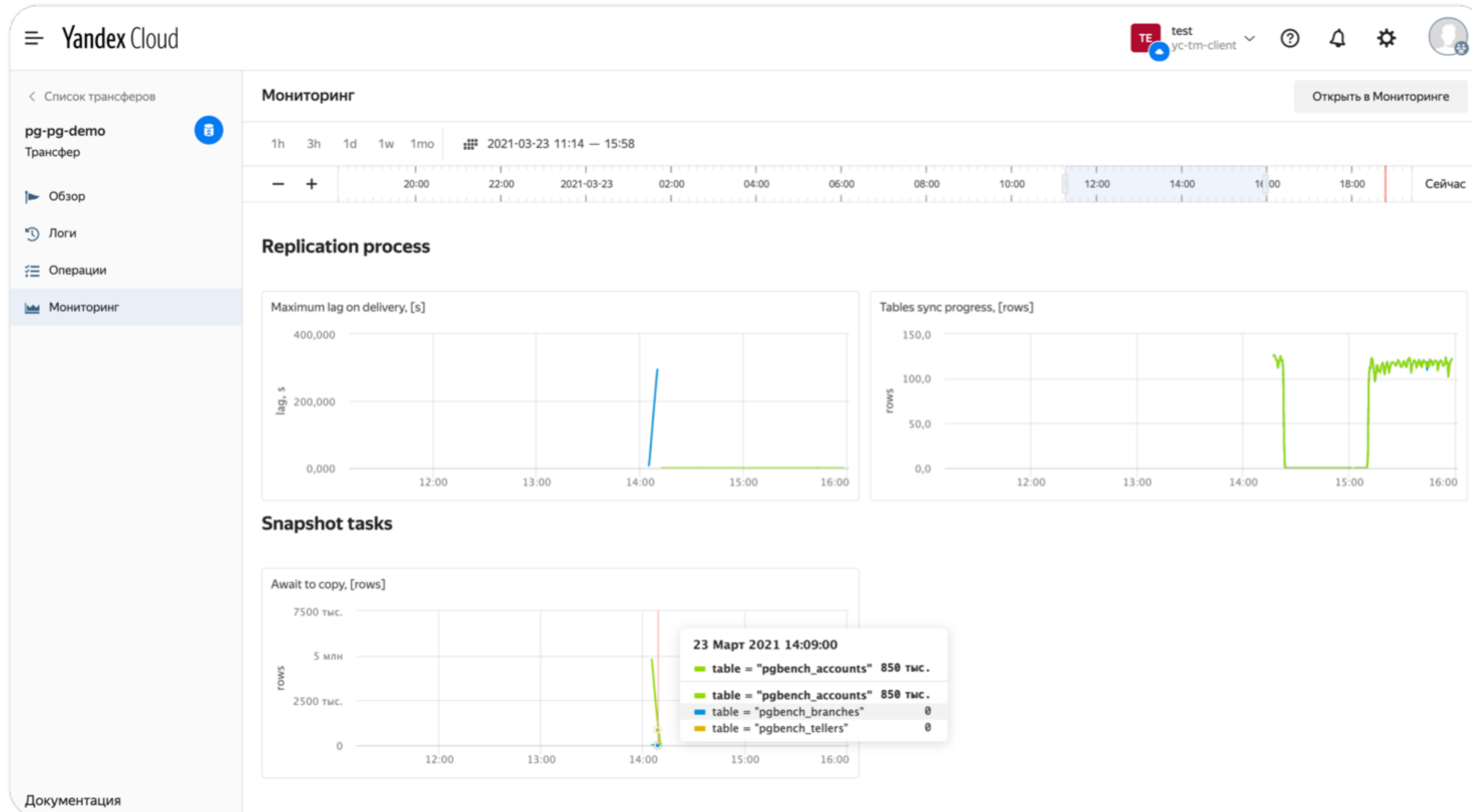
**Черный список таблиц**

- Максимальный размер WAL для слота р...: 9223372036854775807
- Схема БД приёмника, в которой будет с...: public
- Объединить наследуемые таблицы: false

**Первичная конфигурация переноса схемы**

- Table: true
- View: true
- Sequence: true
- Sequence\_owned\_by: true

# 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 `Isn`



# Roadmap



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

# SLA и ограничения PostgreSQL as a Service

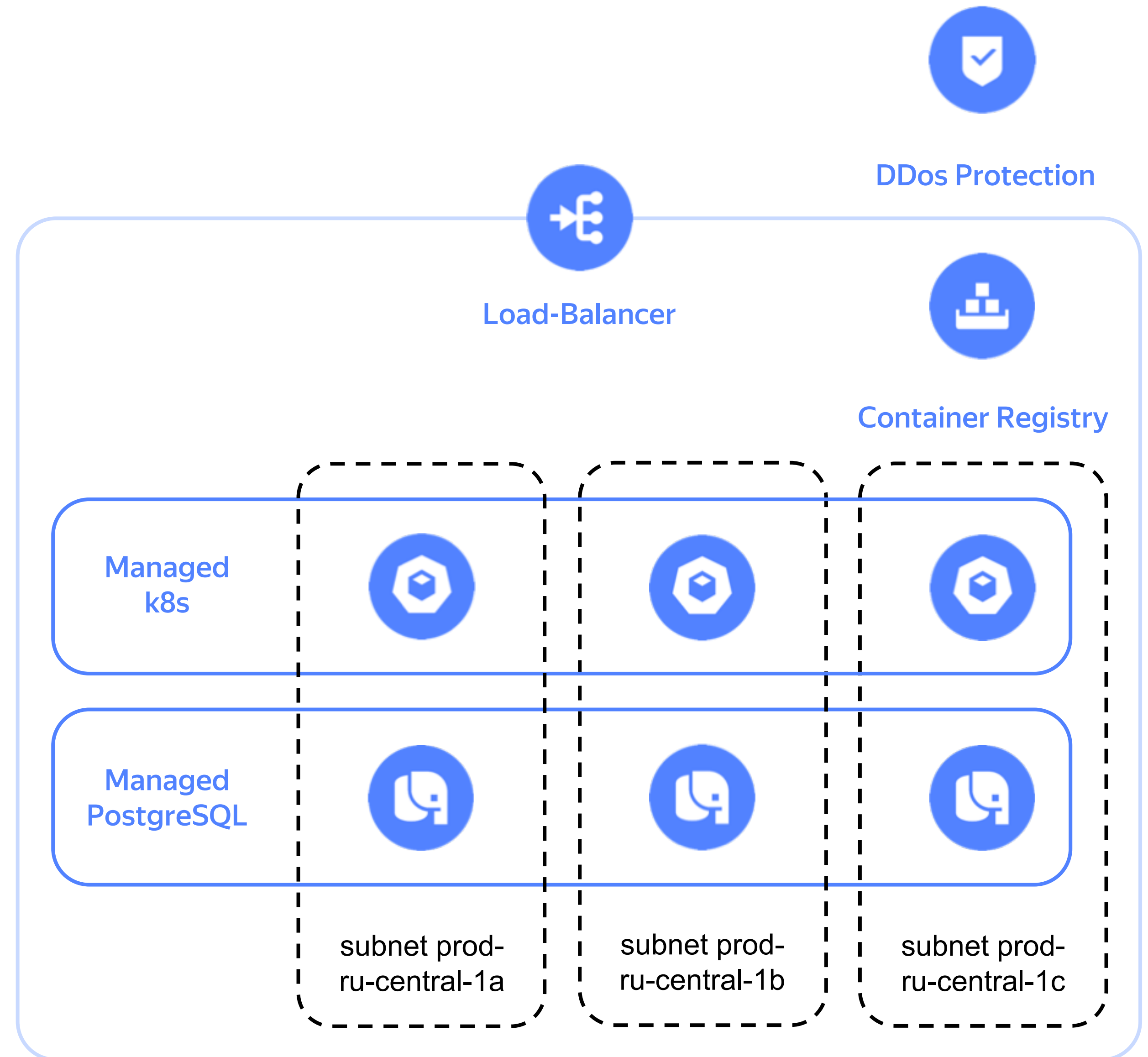
# SLA PostgreSQL

## › Uptime

- 99,99% на чтение
- 99,95% на запись

## › Распространяется на конфигурацию

- С минимум **двумя** хостами в разных зонах доступности
- При использовании поддерживаемых клиентов



# 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

The screenshot shows a configuration window titled "Настройка пользователя testrole" with a close button (X) in the top right corner. Below the title, it indicates the database "База данных db1" with a menu icon, a close button (X), and a plus sign (+). A dropdown menu labeled "Настройки СУБД" is expanded, showing several settings:

- Conn limit: 0
- Default transaction isolation: — (dropdown)
- Synchronous commit: — (dropdown)
- Lock timeout: (empty text input)
- Log statement: — (dropdown)
- Log min duration statement: (empty text input)
- Temp file limit: (empty text input)

At the bottom right, there are two buttons: "Отменить" (Cancel) and "Сохранить" (Save).

# 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

Настройки СУБД

Row security	<input checked="" type="checkbox"/>
Search path	<input type="text" value="*\$user*, public"/>
Seq page cost	<input type="text" value="1"/>
Shared buffers	<input type="text" value="4294967296"/>
Shared preload libraries	<input type="text" value="—"/>
Standard conforming strings	<input checked="" type="checkbox"/>
Statement timeout	<input type="text" value="0"/>
Synchronize seqscans	<input checked="" type="checkbox"/>
Synchronous commit	<input type="text" value="on"/>
Temp buffers	<input type="text" value="8388608"/>
Temp file limit	<input type="text" value="-1"/>
Timezone	<input type="text" value="Europe/Moscow"/>

Отмена

# 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

Настройки СУБД	
Log temp files	-1
Log transaction sample rate	
Maintenance work mem	67108864
Max connections	800
Max locks per transaction	64
Max parallel maintenance workers	2
Max parallel workers	8
Max parallel workers per gather	2
Max pred locks per transaction	64
Max prepared transactions	0
Max standby streaming delay	30000

# 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

### Изменить PostgreSQL-кластер

**Базовые параметры**

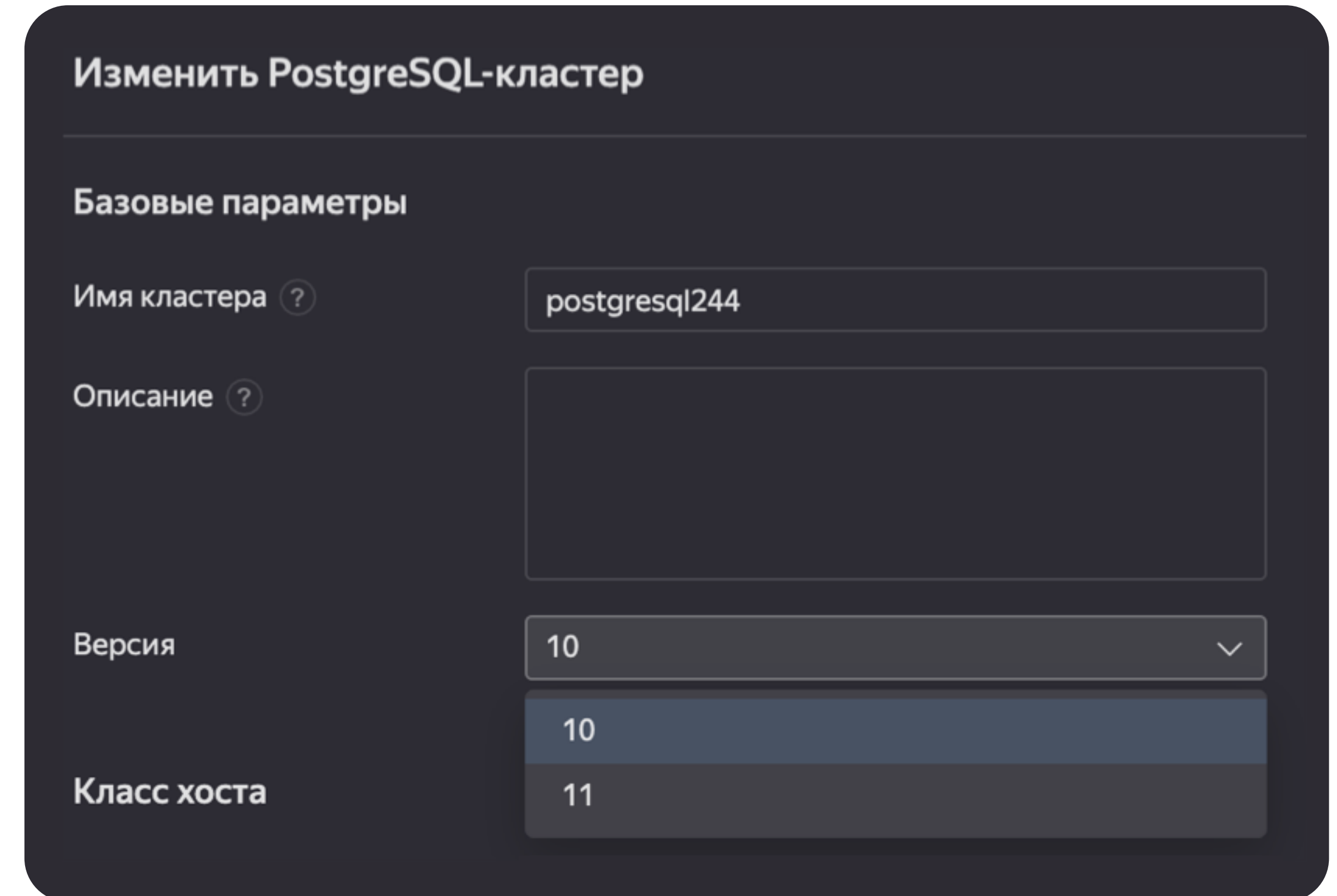
Имя кластера ? postgresql244

Описание ?

Версия 10

Класс хоста

- 10
- 11



# Расширения PostgreSQL

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

### Дополнения PostgreSQL

<input type="checkbox"/> lo	<input type="checkbox"/> ltree
<input type="checkbox"/> moddatetime	<input type="checkbox"/> pg_buffercache
<input type="checkbox"/> pg_hint_plan	<input type="checkbox"/> pg_partman
<input type="checkbox"/> pg_repack	<input type="checkbox"/> pg_stat_kcache
<input type="checkbox"/> pg_stat_statements	<input type="checkbox"/> pg_tm_aux
<input type="checkbox"/> pg_trgm	<input type="checkbox"/> pgcrypto
<input type="checkbox"/> pgrouting	<input type="checkbox"/> pgrowlocks
<input type="checkbox"/> pgstattuple	<input type="checkbox"/> postgis
<input type="checkbox"/> postgis_tiger_geocoder	<input type="checkbox"/> postgis_topology
<input type="checkbox"/> postgres_fdw	<input type="checkbox"/> seg
<input type="checkbox"/> smlar	<input type="checkbox"/> tablefunc
<input type="checkbox"/> unaccent	<input type="checkbox"/> uuid-ossdp

Отмена Изменить



Yandex Cloud



# Спасибо! Вопросы?

**Всеволод Грабельников**

Старший архитектор облачных решений Yandex.Cloud

[vsgrab@yandex-team.ru](mailto:vsgrab@yandex-team.ru)