Общество с ограниченной ответственностью «СКАЛА-Р»

(ООО «СКАЛА-Р»)

Машина хранения данных

СКАЛА-Р МХД.О

(РМБГ.466535.002-565)

Руководство администратора

РМБГ.466535.002-565РА

Страниц 49

Москва 2026 г.

Содержание

Аннотация

Настоящий документ представляет собой руководство администратора Машины хранения данных СКАЛА-Р МХД.О РМБГ.466535.002-565 (далее – МХД.О/ Изделие).

Термины и определения

Термин, сокращение	Определение
ACC	(англ. Access Control) Сервис контроля доступа
ACL	(англ. Access Control List) Список управления доступом
AD	(англ. Active Directory) Служба каталогов, разработанная компанией Microsoft
Amazon S3	(англ. Amazon Simple Storage Service) Облачная система хранения в составе Amazon Web Services, организованная по объектному принципу
API	(англ. Application Programming Interface) Интерфейс программирования приложений
Avanpost FAM	Система единой аутентификации сотрудников в корпоративных ресурсах организации
BBU	(англ. Battery Backup Unit) Модуль резервного питания для RAID-контроллера
BIOS	(англ. Basic input/output system) Набор микропрограмм, реализующих низкоуровневые API для работы с аппаратным обеспечением компьютера, а также создающих необходимую программную среду для запуска операционной системы
CLI	(англ. Command line interface) Способ взаимодействия между человеком и компьютером путём отправки компьютеру команд, представляющих собой последовательность символов
CPU	(англ. central processing unit) Центральное обрабатывающее устройство
CS	(англ. Chunk Server) Сервис фрагментов
DHCP	(англ. Dynamic Host Configuration Protocol) Сетевой протокол, который позволяет автоматически назначать подключаемым к сети устройствам IP-адреса и другие параметры конфигурации
DOCX	формат файла, который используется для создания и сохранения документов, созданных в программе обработки текстов Microsoft Word
DWPD	(англ. Drive Writes Per Day) Показатель надёжности SSD-накопителя, который указывает, сколько раз можно перезаписать весь SSD в день в течение гарантийного срока

Термин, сокращение	Определение
Ethernet	Семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей
FQDN	группа полных доменных имен
gRPC	(англ. Remote Procedure Call) Открытый протокол удалённого вызова процедур (RPC), предоставляющий механизм взаимодействия между клиентскими и серверными приложениями на разных платформах и в разных языках программирования
GW	(англ. Gateway) Сервис обрабатывающий S3 запросы на серверах хранения
HDD	(англ. Hard Disk Drive) Запоминающее устройство (устройство хранения информации, накопитель) произвольного доступа, основанное на принципе магнитной записи на жёсткие (алюминиевые или стеклянные) пластины, покрытые слоем ферромагнитного материала
HTTP	(англ. HyperText Transfer Protocol) Протокол передачи информации в интернете
HTTPS	(англ. HyperText Transfer Protocol Secure) Безопасный протокол передачи данных, который поддерживает шифрование посредством криптографических протоколов SSL и TLS и является расширенной версией протокола HTTP
IAM	(англ. Identity and Access Management) Управление идентификацией и контролем доступа — совокупность технологий, операций, методов и политик для управления доступом пользователей к инфраструктуре
IP-адрес	Уникальный адрес, который присваивается устройствам при подключении к интернету или локальной сети
JAM	(англ. Just-a-Minute) Метод анутентификации
JBOD	(англ. Just a bunch of disks) Режим работы RAID-контроллера, при котором физические диски объединяются в единый логический том, при этом процессор получает доступ к накопителям по отдельности
JSON	(англ.. JavaScript Object Notation) Текстовый формат обмена данными, который используется для хранения данных и их передачи между различными системами и приложениями
KeyCloak	Программный продукт с открытым исходным кодом для управления идентификацией и доступом
LDAP	(англ. Lightweight Directory Access Protocol) Протокол для работы с данными, чаще всего учетными записями пользователей, организованными в виде дерева (каталог)

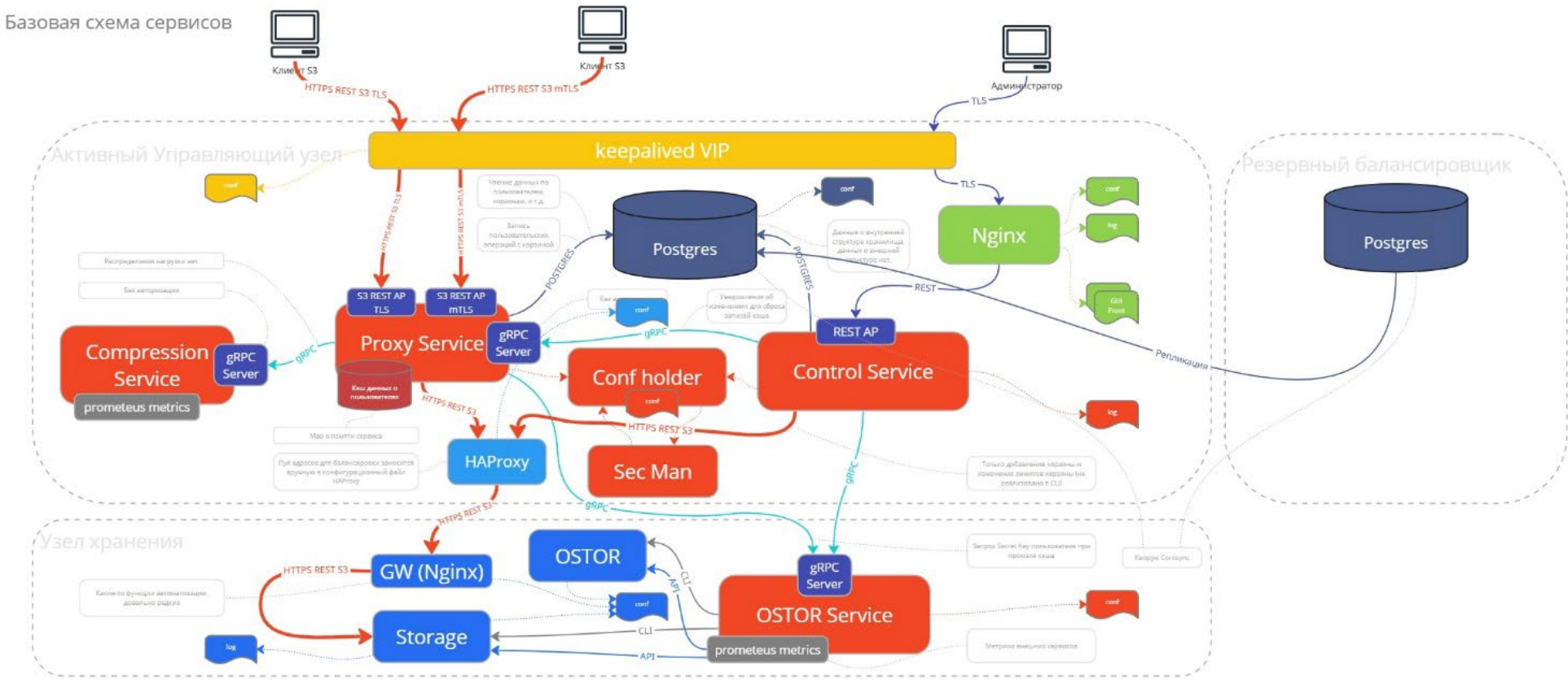
Термин, сокращение	Определение
Linux	Семейство операционных систем с открытым исходным кодом
MAC	(англ. Media Access Control) Уникальный идентификатор, который присваивается каждому устройству, подключённому к сети
MDS	Сервис хранения мета информации SDS
Microsoft Word	Текстовый процессор, предназначенный для создания, просмотра, редактирования и форматирования текстов статей, деловых бумаг, а также иных документов
MGMT	VLAN для управления сетевым оборудованием
MPU	(англ. Multi Part Upload) Метод загрузки больших файлов, при котором файл делится на части
mTLS	(англ. Mutual TLS) Протокол, основанный на TLS с усиленной безопасностью, включающий дополнительную аутентификацию клиента с помощью сертификата
NAS	(англ. Network Attached Storage) Устройство хранения данных, подключённое непосредственно к локальной сети предприятия
NS	Сервер имен
NVMe	(англ. NVM Express (NVMe, NVMHCI – Non-Volatile Memory Host Controller Interface Specification) – Интерфейс доступа к твердотельным накопителям, подключённым по шине PCI Express
OS	Сервер объектов
PostgreSQL	Свободная объектно-реляционная система управления базами данных
PDF	(англ. Portable Document Format) Формат файлов для надёжного представления и обмена документами, независимо от программного обеспечения, оборудования или операционной системы
RAID	(англ. Redundant Array of Independent Disks) Избыточный массив независимых дисков, технология виртуализации данных для объединения нескольких физических дисковых устройств в логический Модуль для повышения отказоустойчивости и/или производительности
REST API	Интерфейс HTTP для работы с сервисом Amazon S3
S3	(англ. Simple Storage Service) Сервис хранения цифровых данных большого объема. Работает по одноименному протоколу S3 и основан на API, разработанном в Amazon Web Services (AWS)
SAN	(англ. Storage Area Network) Высокоскоростная сеть, которая объединяет серверы и устройства хранения данных

Термин, сокращение	Определение
SAS	(от англ. Serial Attached SCSI) Последовательный компьютерный интерфейс, разработанный для подключения различных устройств хранения данных (например, жестких дисков, ленточных накопителей)
SATA	(от англ. Serial ATA) Последовательный интерфейс обмена данными с накопителями информации
SELinux	(англ. Security-Enhanced Linux) Модуль безопасности для операционных систем на базе Linux
SMR	(англ. Shingled Magnetic Recording) Технология черепичной магнитной записи в жёстких дисках, которая позволяет повысить плотность записи
SSD	(англ. Solid-State Drive) Компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти
SSL-сертификат	(англ. Secure Sockets Layer) Цифровой сертификат, который удостоверяет подлинность веб-сайта и позволяет использовать зашифрованное соединение
TCP	(англ. Transmission Control Protocol) Протокол транспортного уровня, который обеспечивает надёжный обмен данными в компьютерных сетях. Он позволяет передавать информацию между устройствами и серверами с максимальной точностью и минимальными потерями
TLS	(англ. Transport layer security) Безопасность транспортного уровня
UEFI	(англ. Unified Extensible Firmware Interface) интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования, позволяющий корректно инициализировать оборудование при включении системы и передать управление загрузчику или непосредственно ядру операционной системы
UDP	(англ.User Datagram Protocol) Протокол транспортного уровня, который не устанавливает постоянного соединения. Он отправляет данные в виде отдельных пакетов, называемых дейтаграммами
UI	(англ. User Interface) Интерфейс пользователя, который представляет собой комплекс визуальных элементов, через которые пользователь взаимодействует с программным продуктом
URL	(англ. Uniform Resource Locator) Единообразный указатель местонахождения ресурса — адрес ресурса в сети Интернет
VIP-адрес	(англ. Very Important Person) адрес, имеющий персональные

Термин, сокращение	Определение
	привилегии
VLAN	(англ. Virtual Local Area Network) Виртуальная локальная компьютерная сеть, представляющая собой группу хостов с общим набором требований, которые взаимодействуют как подключенные к широковещательному домену независимо от их физического местонахождения
XML	(англ. eXtensible Markup Language) Расширяемый язык разметки, который превращает документы в структурированные «деревья» данных
ZSTD	Алгоритм сжатия данных без потерь, основная функция которого - сжимать и распаковывать файлы и потоки данных
АС	Автоматизированная система
БД	База данных
ИБ	Информационная безопасность
Модуль	Функционально завершенный комплект сконфигурированного для выполнения заданных функций аппаратных и/или программных компонентов, аппаратных узлов и программного обеспечения (ПО), оформленный как самостоятельная единица продаж со своим кодом (part number) и стоимостью. Является единым и неделимым элементом спецификации. Зарегистрирован в ЕРРРП
Мультитенантность	Предоставление изолированного доступа к общим ресурсам разным арендаторам, то есть тенантам. Это свойство программного обеспечения, которое позволяет нескольким пользователям или организациям использовать одну и ту же программную систему или приложение. Это означает, что каждый пользователь имеет свой собственный набор данных и настроек, но все они работают на одной и той же программной платформе. Это позволяет экономить ресурсы и упрощает управление системой, так как администратор может управлять всеми пользователями и их данными в единой системе
МХД	Машина хранения данных
ОЗУ	Оперативное запоминающее устройство
ОКПД2	Общероссийский классификатор продукции по видам экономической деятельности
ООО	Общество с ограниченной ответственностью
ОС	Операционная система
ПО	Программное обеспечение

Термин, сокращение	Определение
РК	Резервное копирование
СУБД	Система управления базами данных
Узел	Вычислительный сервер в составе Модуля
ЦП	Центральный процессор

Базовая схема сервисов



1 ПО Скала^р Спектр.S3

Подключение к интерфейсу управления Скала^р Спектр.S3 выполняется по установленному в процессе настройке адресу по протоколу HTTPS. При обращении к Скала^р Спектр.S3 осуществляется перенаправление к интерфейсу аутентификации Keycloak или Avanpost FAM. В котором необходимо ввести логин и пароль пользователя, зарегистрированного в Keycloak или Avanpost FAM.

Общий вид меню Скала^р Спектр.S3 представлен на рисунке ниже (рисунок 1).

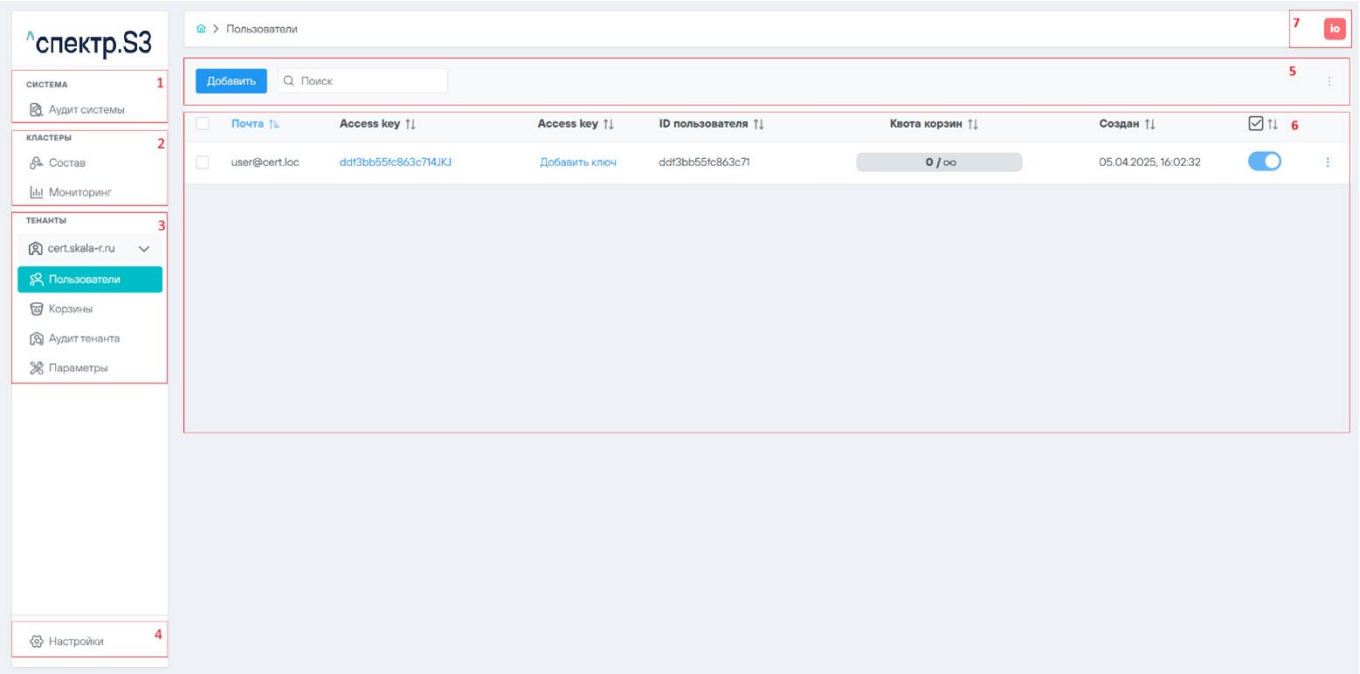


Рисунок 1 - Общий вид меню Скала^р Спектр.S3

Назначение областей:

– область 1 – меню аудита системы;

– область 2 – меню управления кластером;

– область 3 – меню выбора тенанта и управления текущим тенантом;

– область 4 – меню общих настроек Скала^р Спектр.S3;

– область 5 – меню рабочей области;

– область 6 – рабочая область;

– область 7 – информация о текущем пользователе и его ролях.

Скала^р Спектр.S3 обеспечивает возможность создание тенантов. Под тенантом подразумевается выделенное логическое пространство, реализующее сервис хранения данных с доступом по протоколу S3 со следующими уникальными параметрами:

– FQDN;

– уровень отказоустойчивости;

– уровень хранения;

– уровень избыточности;

– SSL ссертификат;

– состав администраторов;

– пространство имен пользователей;
– пространство имен корзин (bucket);
– пространство имен объектов.

Создание нового тенанта доступно только для роли администратора кластера. Для создания нового тенанта нажмите на поле отображения имени текущего тенанта. Внизу появившегося выпадающего списка нажмите кнопку «Создать». Появится меню создания нового тенанта как это показано на рисунке ниже (рисунок 2).

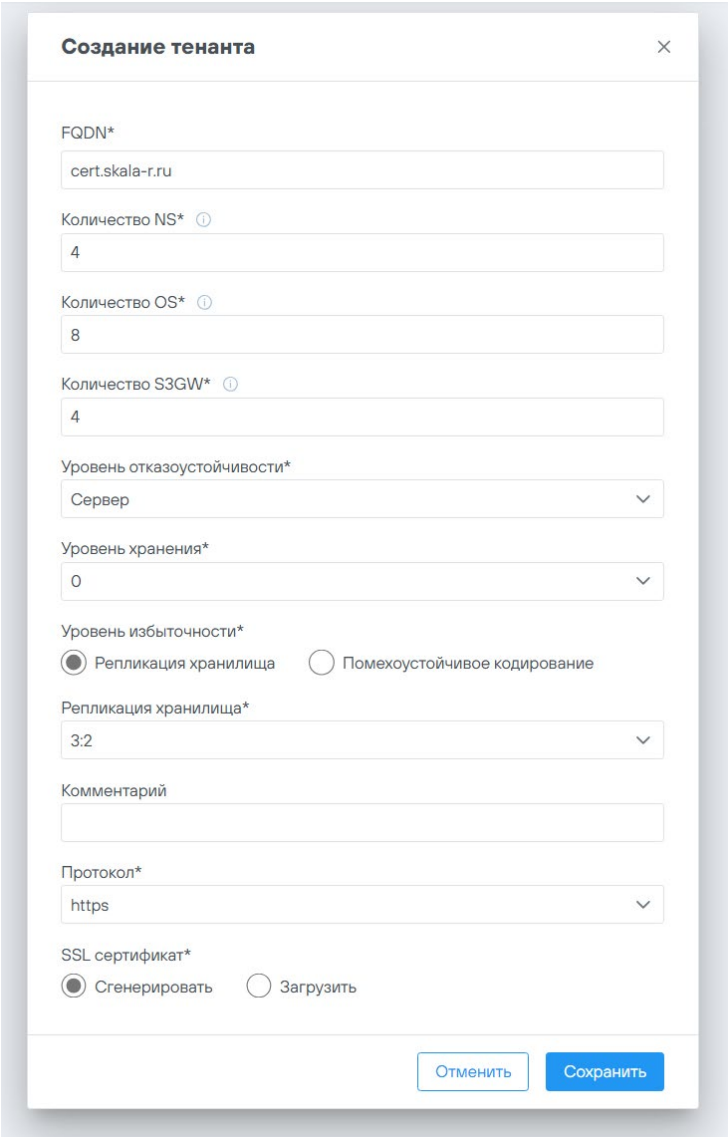


Рисунок 2 - Создание тенанта

Далее необходимо заполнить поля с параметрами настройки тенанта:
– FQDN;
– количество NS;
– количество OS;
– количество S3GW;
– уровень отказоустойчивости;
– уровень хранения;

– уровень избыточности;
– протокол доступа к тенанту;
– комментарии;
– SSL сертификат.

1.1 FQDN

В поле FQDN задается доменное имя сервиса S3, который будет размещаться в создаваемом тенанте. Задаваемое имя должно соответствовать правилам формирования доменного имени и правилам, определенным в документе "Правила регистрации доменных имен в доменах .RU и. РФ" (утв. решением Координационного центра национального домена сети Интернет от 05.10.2011 N 2011-18/81) (ред. от 07.11.2022).

Примеры корректных записей FQDN:

– example.company.com;
– cert.skala.ru.

Примеры не корректных записей FQDN:

– example@company-ru;
– cert_skala.ru.

1.2 Количество сервисов

При создании кластера тенанта S3 предлагается выбрать количество сервисов соответствующее начальному размеру тенанта. Можно выбрать наиболее подходящее кол-во сервисов в зависимости от предполагаемого профиля нагрузки и тем самым добиться наибольшей производительности, стабильности и отказоустойчивости. После создания кластера кол-во отдельных сервисов можно увеличивать сплитированием в ручном режиме.

1.3 Выбор количества OS

OS – сервер объектов. Хранит актуальные данные объектов, полученные от службы S3GW. Эти данные упаковываются в специальные контейнеры для достижения высокой производительности. Контейнеры хранятся в блочном хранилище со встроенной высокой доступностью.

Количество сервисов OS необходимо выбирать из расчета однин сервис на каждые 4 ТБ эффективного объема данных (без учета избыточности основного хранилища), чтобы кластер имел стабильную производительность вплоть до достижения установленного объема. Например, для объема хранилища 700 ТБ требуется выбрать 175 сервисов OS.

При последующей эксплуатации необходимо сплитировать сервисы OS при достижении размера 4 ТБ.

Максимальное количество служб OS для одного тенанта не ограничивается.

1.3.1 Сплитирование

Сервисы OS необходимо сплитировать при достижении размера 4 ТБ. Принудительно запустить процесс сплитирования сервиса можно командой:

```
ostor-ctl split -i SVCID
```

Сплитирование сервиса OS является продолжительной и затратной операцией, уменьшающей производительность кластера. Рекомендуется проводить сплитирование в дни обслуживания кластера.

Мониторить процесс сплитирования можно командой:

```
ostor-ctl get-config | grep OS
```

По результату работы команды старый сервис будет удален, а вместо него будет создано два новых сервиса, содержащих в совокупности все объекты старого сервиса. Кроме того, будет произведена дефрагментация и компактинг (возврат места, занимаемого ранее удаленными объектами, в основное хранилище).

Следует также учитывать, что увеличение количества сервисов увеличивает потребление ОЗУ на каждом сервере кластера.

1.4 Выбор количества NS

Служба NS – сервер имен. Хранит метаданные об объектах, полученные от службы S3GW. Метаданные включают имя объекта, его размер, список контроля доступа (ACL), расположение, владельца, теги и др. Сервер имен также хранит свои собственные данные на распределенном дисковом массиве со встроенной функцией высокой доступности.

Количество сервисов NS, при настройке тенанта, рекомендуется выбирать равным предполагаемому, в начале эксплуатации количеству корзин.

При последующей эксплуатации необходимо сплитировать сервисы NS при достижении размера 1 ТБ. В случае отсутствия окна обслуживания сервис следует сплитировать при достижении размера 500 ГБ, чтобы избежать уменьшения производительности кластера, а также сократить время, необходимое для завершения сплитирования.

Не следует выбирать максимальное количество служб во всех случаях, т.к. неиспользуемые службы будут расходовать ресурсы.

Необходимо учитывать, что распределение корзин между NS осуществляется по первому символу в названии корзины. Весь алфавит равномерно распределяется между созданными, при создании тенанта, службами NS. Вновь созданная корзина прикрепляется для обслуживания службе NS, «отвечающей» за соответствующую букву алфавита, с которой начинается название создаваемой корзины. В этой связи для обеспечения равномерной нагрузки на службы NS, желательно соблюдать следующие правила:

– создавать корзины с именами, начинающимися с разных букв алфавита;

– не записывать все объекты в единственную корзину, а распределять их по нескольком корзинам. В этом плане использование «папок» в корзине является менее предпочтительным, чем создание нескольких корзин.

1.4.1 Сплитирование

Чтобы увеличить производительность кластера в случае недостаточного количества сервисоа NS необходимо сплитировать сервисы NS командой:

```
ostor-ctl split -i SVCID
```

По результату работы команды старый сервис будет удален, а вместо него будет создано два новых сервиса, содержащих в совокупности все метаданные старого сервиса.

Сплитирование сервиса NS является продолжительной и затратной операцией, уменьшающей производительность записи и чтения в обслуживаемые корзины. Рекомендуется проводить сплитирование в дни обслуживания кластера.

Если сплитирование зависло в состоянии сервиса FROZEN, то это означает, что была произведена попытка сплитировать пустой сервис NS и он перешел в режим ожидания первых корзин. Сплитирование завершится автоматически, когда в этот сервис будет записана первая корзина. Однако, можно отменить такое сплитирование при помощи команды:

```
ostor-ctl split -i SVCID -c
```

1.5 Выбор количества шлюзов S3GW

S3GW – прокси-сервер между службами объектного хранилища и серверами шлюза Спектр.S3. Он получает и обрабатывает запросы протокола S3, выполняет аутентификацию пользователей S3 и проверку ACL, он не сохраняет данные о запросах. S3GW использует веб-сервер NGINX для внешних подключений и не имеет собственных данных (то есть работает без сохранения состояния). Количество сервисов может быть как увеличено, так и уменьшено в процессе эксплуатации.

Для нагруженных кластеров рекомендуется разворачивать по 6 шлюзов S3GW на каждую ноду хранения. В процессе эксплуатации, количество шлюзов можно уменьшить в случае низкой производительности дисковой подсистемы для экономии оперативной памяти. Также, количество шлюзов S3GW можно увеличить через меню Параметры в меню выбора тенанта до 10 в случае высокой производительности дисковой подсистемы, сети и процессоров сервера.

1.6 Сервис ACC

Сервер политики корзин (Account Control, или ACC). Он обеспечивает выполнение правил жизненного цикла и обеспечения безопасности, заданных в политиках корзин. В UI никак не настраивается и в типовом варианте развёртывания количество экземпляров сервиса всегда равно 1. Однако в случае необходимости для высоконагруженных кластеров, количество сервисов ACC также может быть увеличено.

1.6.1 Сплитирование

Чтобы увеличить производительность кластера в таком случае необходимо сплитировать сервисы ACC командой:

```
ostor-ctl split -i SVCID
```

Мониторить процесс сплитирования можно командой:

```
ostor-ctl get-config | grep ACC
```

По результату работы команды старый сервис будет удален, а вместо него будет создано два новых идентичных сервиса (сервисы являются stateless).

1.7 Примеры расчёта количества сервисов

Допущение, принятое к данным в таблице ниже (таблица 12) - каждый 1 сервер даёт 30 Тб полезного пространства. Естественно, в реальных спецификациях эта цифра может отличаться как в большую, так и в меньшую сторону.

Второе допущение, в таблице приведены данные для случая, когда создаётся один тенант в кластере. Для случаев когда тенантов создаётся более одного, количество NS и OS расчитывается от объёма данных и количества бакетов, S3GW принимается равным трем сервисам на каждый сервер (для каждого тенанта), а ACC – 1.

Таблица 11 - Примеры расчёта количества сервисов

Количество серверов хранения	Полезный объём ТБ	Бакетов	NS	OS	S3GW	ACC
5	150	1	1	38	30	1
		5-20	5	38	30	1
		20-50	20	38	30	1
		50-100	50	38	30	1
10	500	1	1	125	60	1
		5-20	5	125	60	1
		20-50	20	125	60	1
		50-100	50	125	60	1
20	1000	1	1	250	120	1
		5-20	5	250	120	1
		20-50	20	250	120	1
		50-100	50	250	120	1
20+	2000+	1	1	500+	120+	1
		5-20	5	500+	120+	1
		20-50	20	500+	120+	1
		50-100	50	500+	120+	1

1.8 Уровень отказоустойчивости

Уровень отказоустойчивости определяет домен отказоустойчивости – область хранения, которая может содержать только одну копию данных. Потеря одного домена отказоустойчивости, например, из-за аппаратного сбоя, не приведет к потере данных. Доступно 4 варианта доменов отказоустойчивости:

- диск;
- сервер;
- стойка;
- ряд стоек.

1.9 Уровень хранения

В состав кластера могут входить узлы хранения с разными типами накопителей, отличающихся емкостью и производительностью. На базе каждого типа дисков реализуется независимая область хранения с показателями емкости и производительности, определяемой типами накопителей. При создании тенанта необходимо выбрать номер области хранения (Уровень хранения), на которую, по умолчанию, будут записываться объекты в создаваемом тенанте.

1.10 Уровень избыточности

Уровень избыточности определяет технологию хранения данных, которая будет использоваться для создаваемого тенанта.

Значения вариантов количества реплик, предлагаемых к выбору в окне «Репликация хранилища» зависят от количества узлов хранения в кластере.

1.11 Протокол

По умолчанию выбрать можно только защищенный протокол доступа HTTPS. Другие варианты в данный момент не поддерживаются.

1.12 Комментарий

В комментарии необходимо указать данные информационного характера, например о владельце/пользователе тенанта. Можно оставить пустым.

1.13 SSL сертификат

Необходимо выбрать какой тип сертификата будет использоваться для работы HTTPS протокола. При выборе «Загрузить» будет предложено загрузить сертификат и ключ, сформированные внешним удостоверяющим центром.

Необходимо отметить, что Скала^р Спектр.S3 позволяет использовать для каждого отдельного тенанта как один и тот же сертификат, так и уникальные.

В случае, если в дальнейшем предполагается использовать тенант в режиме гео-репликации, необходимо использовать вариант с загрузкой SSL сертификата. Георепликация не может быть настроена при использовании самоподписанных сертификатов.

1.14 Роли для доступа к тенанту

При создании тенанта формируется возможность доступа к Скала^р Спектр.S3 пользователей, являющихся администраторами созданного тенанта. Для этого необходимо создать роли со следующими названиями:

- TenantAdmin_<FQDN имя тенанта> – администратор тенанта;
- TenantAuditor_<FQDN имя тенанта> – аудитор тенанта.

Для использования этих ролей, они должны быть заведены в Keycloak или Avanpost FAM, после чего могут быть присвоены пользователю, зарегистрированному в Keycloak или Avanpost FAM.

1.15 Управление тенантом

Управление тенантом доступно только для пользователя с ролью TenantAdmin_<FQDN имя тенанта>, где <FQDN имя тенанта> имя тенанта, которым планируется управлять.

Функции управления тенантом расположены в боковом меню управления. К числу таких функций относятся:

– «Пользователи» - управление пользователями;

– «Корзины» - управление корзинами;

– «Аудит тенанта» - аудита операций администраторов тенанта;

– «Параметры» - изменение параметров тенанта.

1.16 Управление пользователями

В разделе управления пользователями (рисунок 3) выполняется управление непривилегированными пользователями. Управление привилегированными пользователями осуществляется через Avanpost FAM.

Для начала работы с данными по протоколу S3 необходимо создать пользователей S3. Для этого в главном меню «Скала^р Спектр.S3» выбрать пункт «Пользователи». При первом запуске на странице не будут отображаться пользователи, если «Скала^р Спектр.S3» используется впервые.

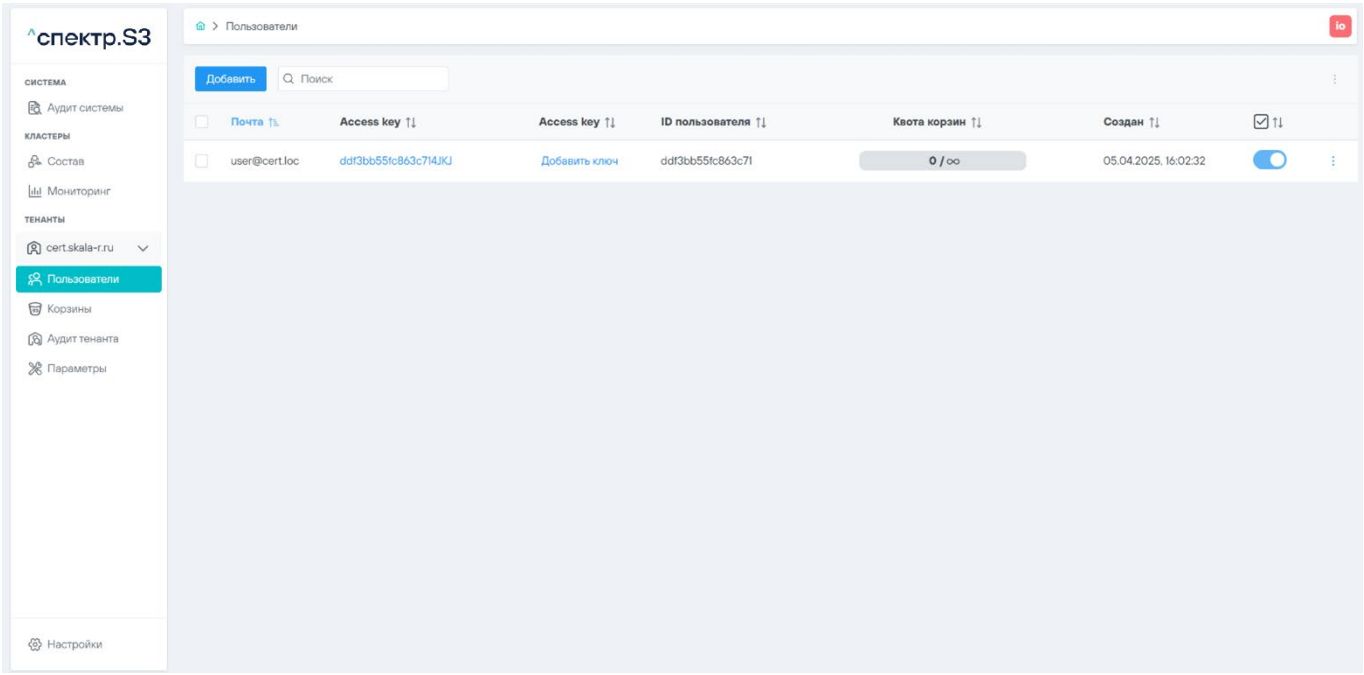


Рисунок 1 - Управление не привилегированными пользователями

При нажатии на кнопку «Добавить» откроется диалоговое окно для добавления обычных пользователей S3 (рисунок 4).

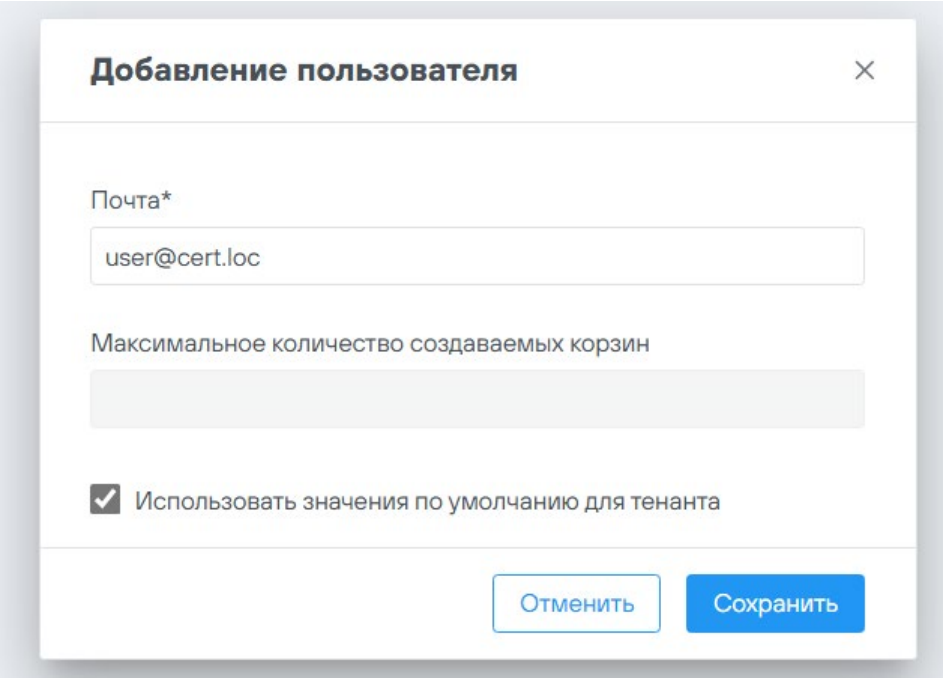


Рисунок 4 - Форма создания пользователя

Пользователь заводится в формате e-mail, так как показано на рисунке 8. При создании можно указать квоту на количество создаваемых корзин. Квота означает максимальное количество корзин, которые может создать этот пользователь для работы с ними по протоколу S3. В случае если количество не будет задано вручную, будет использовано значение, установленное по умолчанию для тенанта. Значение по умолчанию для тенанта определяет какое количество корзин будет иметь каждый создаваемый в рамках этого тенанта пользователь.

В случае успешного создания пользователя будет показано меню со значениями Access key и Secret key (рисунок 5), которые должны быть скопированы и переданы пользователю.

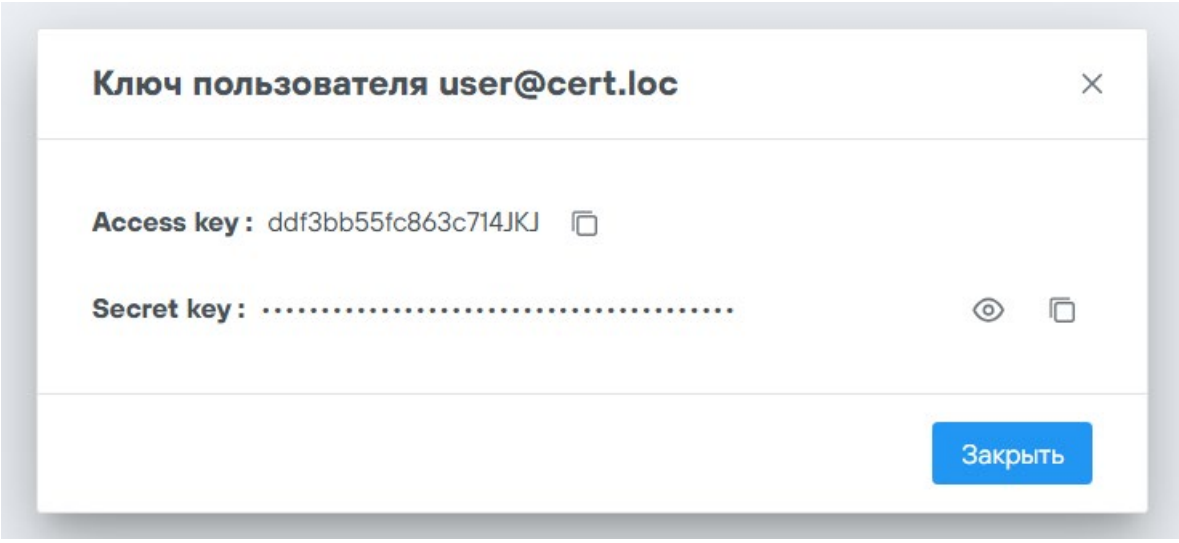


Рисунок 5 - Ключи пользователя при его создании

Данные из поля Secret key доступны только при создании пользователя или при повторной генерации Access key. В случае закрытия окна из рисунка выше увидеть этот Secret key будет невозможно.

У каждого пользователя может быть по две пары Access key и Secret key. Для создания второй пары необходимо нажать на надпись «Добавить ключ». При нажатии на отображаемый Access key будет предложено выполнить операции обновления Secret Key или удаления пары ключей, как это показано на рисунке ниже (рисунок 6).

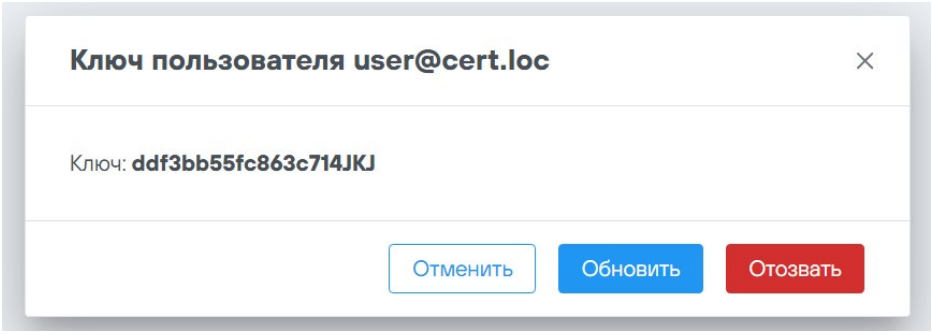


Рисунок 6 - Ключи пользователя при его создании

При нажатии кнопки «Отозвать» выполняется удаление Access key, для которого было запрошено это действие.

Выполнение операции удаления пары ключей пользователя закончится ошибкой, если в момент удаления пользователь является владельцем корзины (корзина создана пользователем). При нажатии кнопки «Обновить» выполняется генерация нового Secret key.

На форме списка пользователей ползунок служит для изменения статуса зарегистрированного пользователя: Активен / Не активен. В случае если пользователь не активен, действие его Access key и Secret key временно приостанавливается, и он теряет возможность использовать сервисы S3. Это позволяет временно прекратить доступ пользователя без его удаления.

Значок служит для удаления пользователя, при этом выполняется удаление учетной записи пользователя, включая адрес электронной почты, и пары Access key и Secret key, сформированные ранее для этого пользователя.

Выполнение операции удаления пользователя закончится ошибкой, если в момент удаления пользователь является владельцем корзины (корзина создана пользователем). Для успешного удаления пользователя необходимо предварительно удалить корзины, созданные пользователем или назначить им другого владельца.

1.17 Управление корзинами

В меню «Корзины» отображаются все созданные в хранилище S3 корзины (рисунок 7).

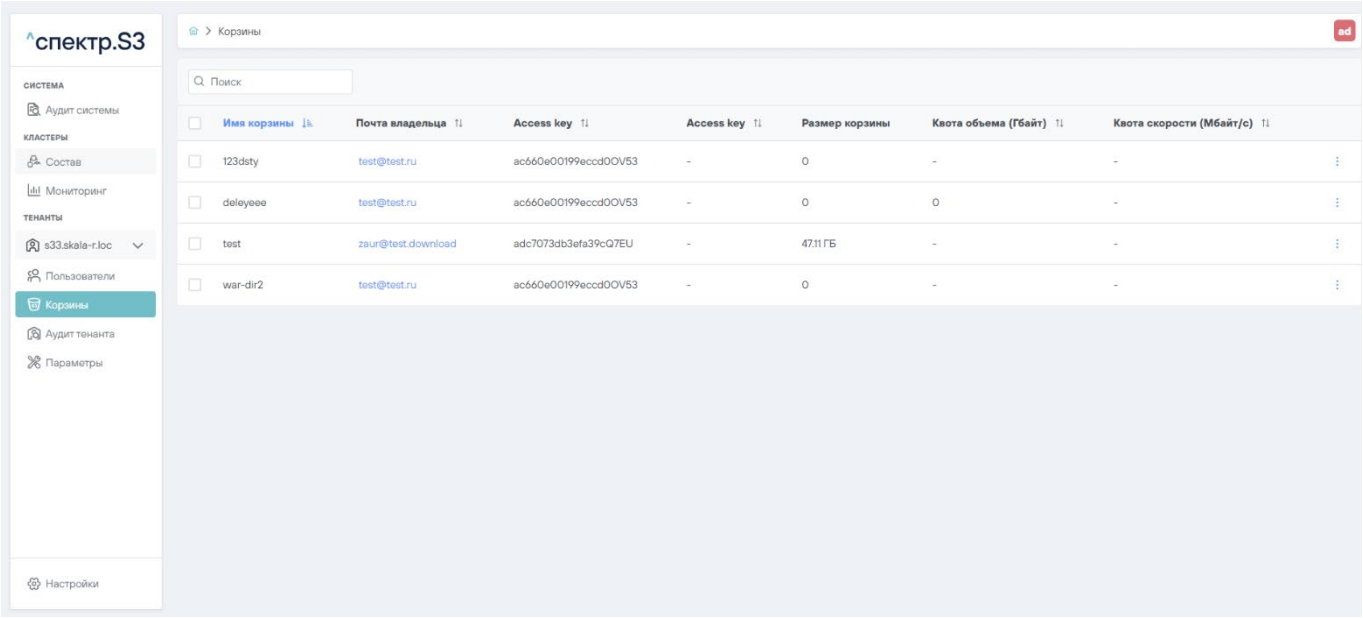


Рисунок 7 - Форма списка бакетов

1.17.1 Создание новой корзины

При использовании кнопки «Добавить» появляется меню создания новой корзины (рисунок 8).

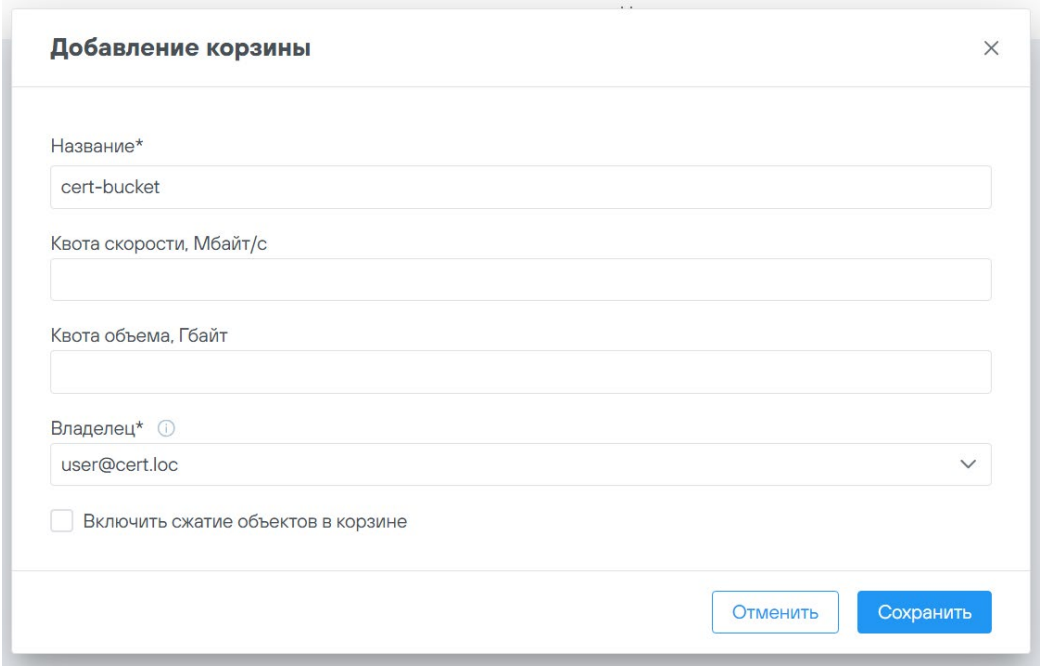


Рисунок 8 - Создание бакета

В поле «Название» надо ввести имя новой корзины, удовлетворяющее следующим требованиям:

– должно содержать от 3 (минимум) до 63 (максимум) символов;
– состоит только из строчных букв латинского алфавита, цифр, точек (.) и дефисов (-);
– начинается и заканчивается буквой или цифрой;
– не содержать две смежные точки;
– не отформатирован как IP-адрес (например, 192.168.5.4);

– не начинается с префикса xn--;

– не заканчивается суффиксом -s3alias;

– не заканчивается суффиксом --ol-s3;

– является уникальным для выбранного тенанта.

В поле «Квота скорости, Мбайт/с» может быть введено значение, ограничивающее скорость информационного обмена при обращении пользователей к корзине.

В поле «Квота объема, Гбайт» может быть введено значение, ограничивающее максимальный суммарный объем дискового пространства, который может быть занят корзиной.

Значение квот может быть отредактировано в дальнейшем.

В поле «Владелец» должен быть указан непривилегированный пользователь, заведенный в тенанте, где создается корзина. Привилегированный пользователь, имеющий права администратора, не может быть владельцем корзины.

Чекбокс «Включить сжатие объектов», активирует функцию сжатия объектов на лету для всех объектов, записываемых в корзину. Эту функцию целесообразно использовать при хранении объектов типа XML или JSON, которые могут сжиматься до 20 раз. Сжатие файлов PDF, DOCX и т.п. как правило не превышает 15%. Использовать сжатие для объектов, включающих графические и видео материалы – не целесообразно.

Для редактирования параметров корзины используется контекстное меню, которое вызывается по нажатию значка ⋮ и содержит следующие пункты (рисунок 9):

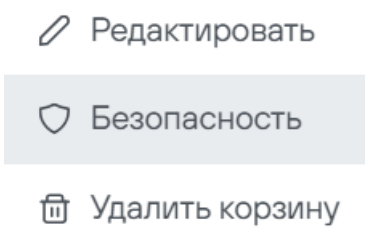


Рисунок 9 - Список параметров редактирования корзины

1.17.2 Редактировать

При выборе пункта меню «Редактировать» появляется меню, в котором приведены заданные для корзины параметры настроек и владелец (рисунок 10). Если ранее квоты не устанавливались – поля пустые.

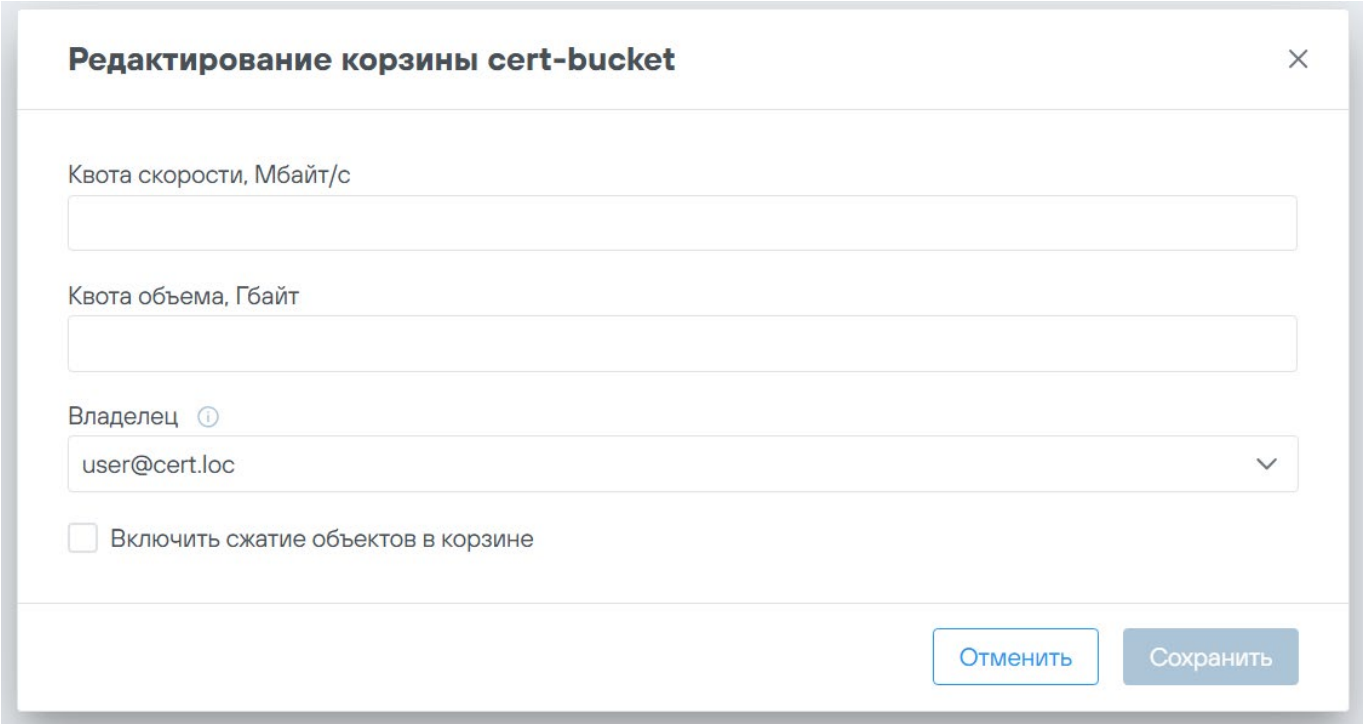


Рисунок 2 - Редактирование корзины

Необходимо ввести требуемые значения квот и применить их.

Уменьшение квот по объему хранимых объектов необходимо выполнять с осторожностью, т.к. если объем хранимых данных превысит заданную квоту, пользователи потеряют возможность записывать в корзину новые объекты.

Поле «Владелец» работает в режиме поиска и/или выбора из списка, зарегистрированных в тенанте пользователей.

В случае включения функции сжатия после того как в корзину были помещены объекты, сжиматься будут только вновь записываемые объекты. Уже сохраненные объекты останутся без изменения. Реализация сжатия уже сохраненных объектов планируется в следующих версиях.

При отмене сжатия, все вновь сохраняемые объекты сжиматься не будут. Ранее сохраненные объекты останутся сжатыми.

1.17.3 Безопасность

При выборе пункта меню «Безопасность» появляется меню, в котором отображены все установленные на корзину правила доступа (рисунок 11).

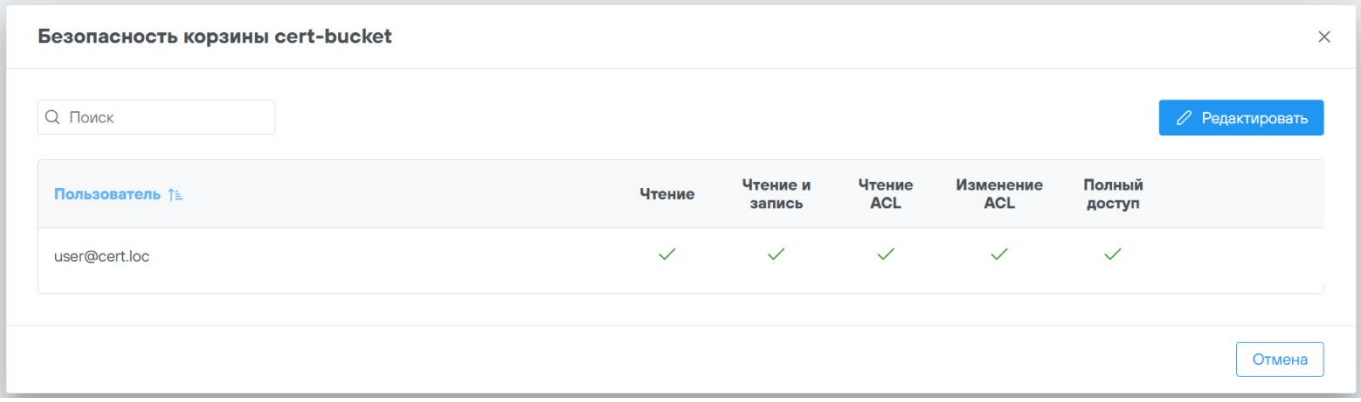


Рисунок 3 - Редактирование параметров безопасности корзины

По умолчанию, в первой строке отображается владелец корзины.

Можно удалить существующие правила доступа, либо создать новое правило, нажав на кнопку «Редактировать».

Для каждой корзины может быть создано не более 100 правил, при этом обращаем внимание, что правило, определенной каждым чек-боксом (если он выбран) сохраняется как отдельное правило.

1.17.4 Удаление корзин

При выборе пункта меню «Удалить корзину» (рисунок 12) безвозвратно удаляется корзина со всем ее содержимым.

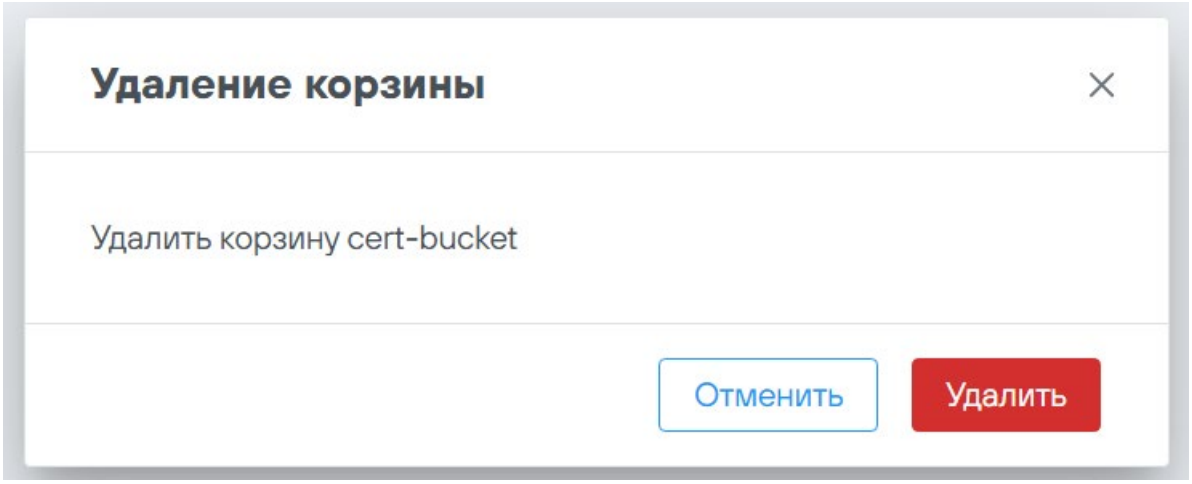


Рисунок 12 - Удаление корзины

Важно помнить, что при удалении корзины, процесс вызывается через системную утилиту, что позволяет удалять не пустые корзины. Через API S3 корзину с объектами удалить нельзя без указания специальных ключей.

1.17.5 Аудит действий тенанта

В меню «Аудит тенанта» (рисунок 13) отображаются действия, выполняемые администратором выбранного тенанта.

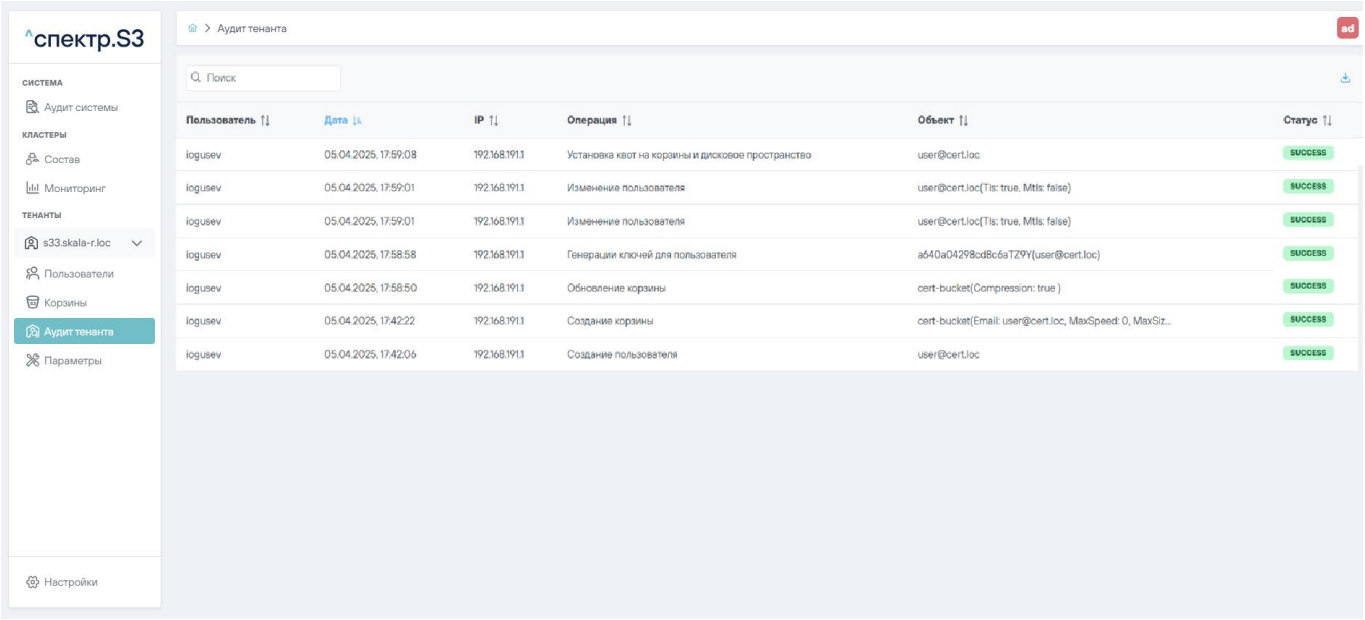


Рисунок 13 - Аудит тенанта

Регистрируемые события для тенанта приведены в таблице ниже (таблица 2).

Таблица 2 - Регистрируемые события для тенанта

Объект	Действие	Включение дебаг режима
Корзина	Получение списка корзин	+
	Создание корзины	
	Удаление корзины	
	Обновление корзины	
Пользователь	Получение списка пользователей	+
	Получение пользователя	+
	Создание пользователя	
	Удаление пользователя	
	Изменение пользователя	
ACL	Получение списка ACL	+
	Изменение безопасности корзины	
Ключи	Генерация ключей для пользователя	
	Отзыв ключа пользователя	
	Обновление ключа пользователя	
Логи	Запрос логов	+

1.17.6 Аудит действий системы

В меню «Аудит системы» (рисунок 14) отображаются действия, выполняемые пользователями с системой.

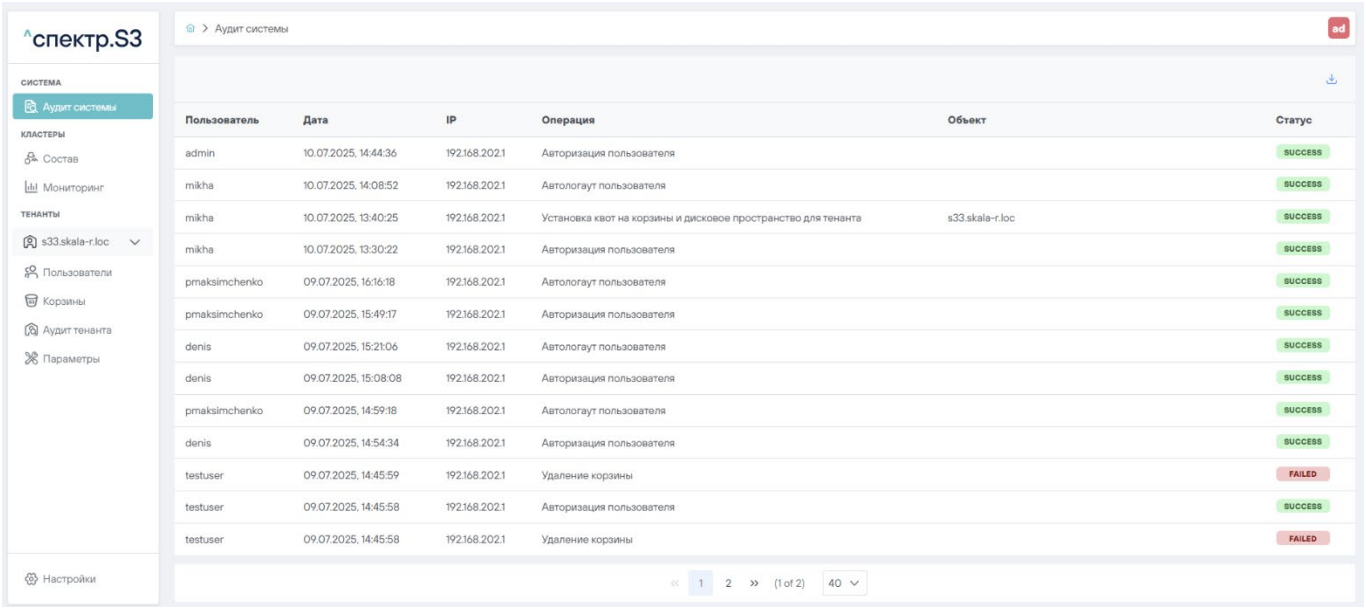


Рисунок 14 - Аудит системы

Регистрируемые события для системы приведены в таблице ниже (таблица 3).

Таблица 3 - Регистрируемые события для системы

Объект	Действие	Включение дебаг режима
Кластер	Получение списка доступных уровней тенанта	+
	Получение списка серверов	+
	Получение списка сетевых интерфейсов	+
	Изменение сервера	
	Получение списка дисков	+
	Добавление роли диска	
	Изменение диска	
	Удаление роли диска	
	Удаление журнала записей	
Пользователь	Авторизация пользователя	
	Логаут пользователя	
Лицензия	Установка лицензии	
Логи	Запрос логов	+

Объект	Действие	Включение дебаг режима
Тенант	Получение списка тенантов	+
	Создание тенанта	
	Получение тенанта	+
	Изменение тенанта	
	Удаление тенанта	
	Изменение режима работы с Mtls	

Кроме веб-интерфейса «Скала^р Спектр.S3», также просмотр лог-файлов сервисов «Скала^р Спектр.S3» доступен через консоль управления ОС.

Настройка параметров логирования осуществляется в конфиг файле /opt/skala-r/s3gateway/s3gateway.config.json.

`"proxy_log_path": "/var/log/skala-s3gw-proxy/proxy.log "`, – Путь куда будут записываться логи прокси.

`"control_log_path": "/var/log/skala-s3gw-control/control.log "`, – Путь куда будут записываться логи модуля управления.

`"rsyslog_url": "127.0.0.1:514"`, – URl rsyslog сервера (ip:port).

`"log_period_sec": 5` – Периодичность, с которой записываются логи прокси сервера.

1.18 Настройка ротации логирования

В файле конфигурации "/etc/logrotate.d/skala-s3gw" возможно изменение параметров ротации событий в журналах.

В примере ниже продемонстрирована настройка ротации через 93 дня для proxy.log.

```
/var/log/skala-s3gw/proxy.log {
    create 0640 s3gw_endpoint s3gw
    daily
    rotate 93
    missingok
    notifempty
}
```

Параметр «daily» указывает на ежедневную архивацию файла лога.

1.18.1 Отправка логов во внешние SIEM системы

Логи прокси сервера и модуля управления имеют возможность отправляться во внешние системы.

Настройка осуществляется в файле /opt/skala-r/s3gateway/s3gateway.config.json

```
"rsyslog": {
    "control_rsyslog_url": "127.0.0.1:514/tcp",
    "proxy_rsyslog_url": "127.0.0.1:514/udp"
  },
```

Имеется возможность соединения по TCP/UDP.

Для применения изменений, необходимо перезапустить соответствующие компоненты.

– при успешном соединении с proxy_rsyslog_url во время перезапуска прокси сервера будет выведено "connection to rsyslog is established".

– соединение с control_rsyslog_url для модуля управления проверяется при каждом логируемом действии. В случае ошибки выводится "failed connect to rsyslog"

1.18.2 Изменение параметров тенанта

Изменение параметров тенанта возможно от имени пользователя с ролью Администратор инфраструктуры (рисунок 15). Для удаления тенанта надо выбрать его имя и войти в меню «Параметры».

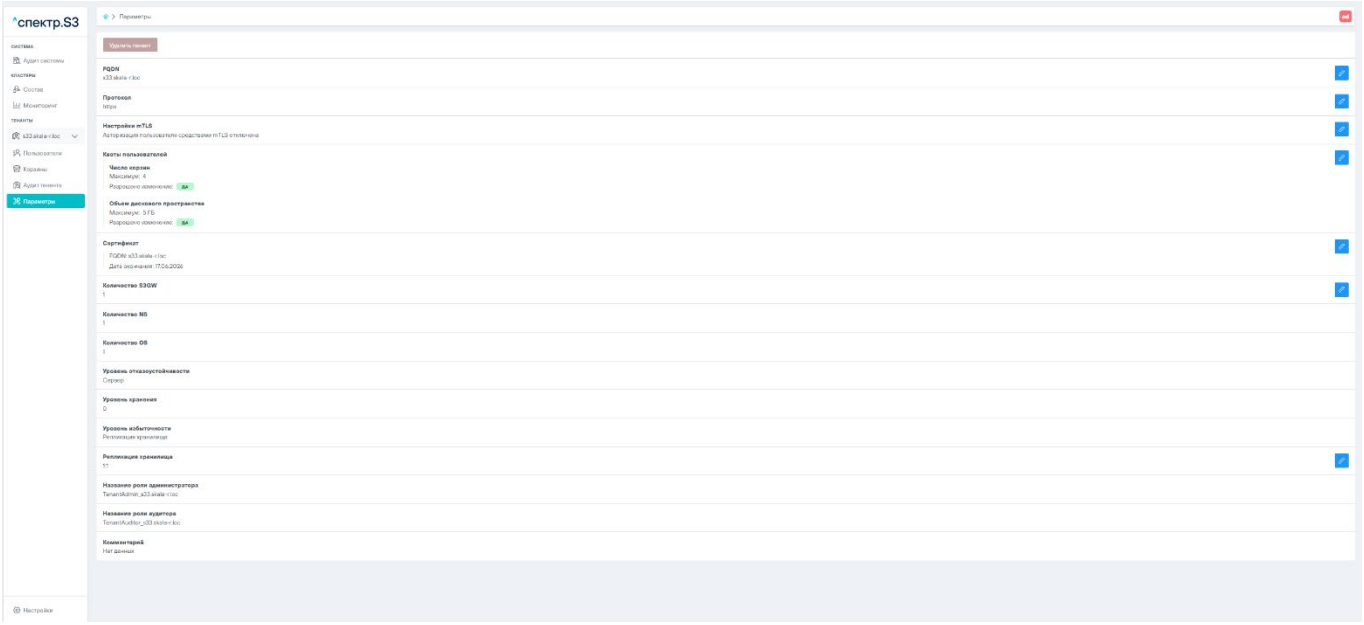


Рисунок 15 - Параметры тенанта

Параметры, значение которых можно изменить отмечены значком  :

– FQDN – меняется доменное имя сервиса S3, реализуемого в рамках тенанта;

– настройка mTLS – позволяет управлять авторизацией пользователя средствами mTLS;

– квоты пользователей – позволяет установить значение по умолчанию для всех пользователей тенанта и разрешить/запретить пользователям изменять значение самостоятельно;

– сертификат – позволяет загрузить сертификат для FQDN имени тенанта

– количество S3GW – меняет количество сервисов GW, отвечающих за производительность сервиса S3 тената при большом количестве одновременных операций. Обратите внимание, что здесь общее кол-во служб S3GW, которые создаются для текущего тенанта на всех узлах хранения кластера.

– репликация хранилища – меняет количественный состав реплик. Необходимо использовать с осторожностью, т.к., например, при увеличении количества требуемых реплик с 2-х до 3-х потребует дополнительного дискового пространства и может привести к недоступности тенанта.

2 Удаление тенанта

Удаление тенанта возможно от имени пользователя с ролью Администратор инфраструктуры и только после того, как пользователь с ролью Администратор тенанта удалил все корзины и пользователей.

Для удаления тенанта надо выбрать его имя и войти в меню «Параметры» (рисунок 16).

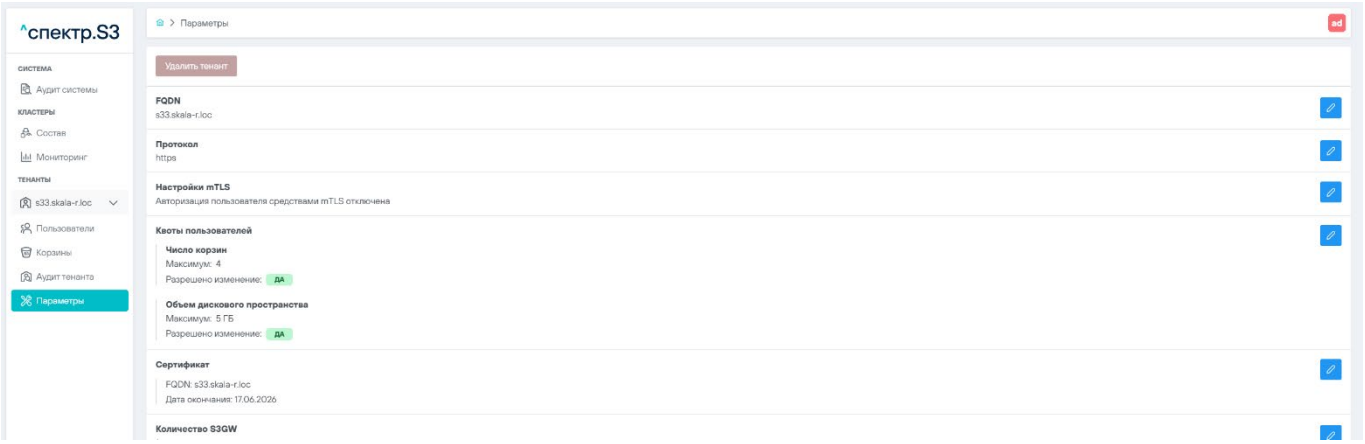


Рисунок 16 - Удаление тенанта

3 Параметры

Меню «Параметры» служит для настройки глобальных параметров Скала^р Спектр.S3.

3.1 Интеграция с KeyCloak

3.1.1 Настройка подключения к KeyCloak

Конфигурация интеграции с IAM на базе KeyCloak выполняется с использованием конфигурационного файла /opt/skala-r/s3gateway/s3gateway.config.json.

Для настройки интеграции с IAM используются следующие параметры:

– auth-server-url - путь до сервиса KeyCloak

– realm – имя проекта, для которого создано пользовательское пространство в KeyCloak

– resource – имя приложения, оно же client_id в KeyCloak

– use-resource-role-mappings – флаг, указывающий что надо учитывать роли, находящиеся в секции ресурсного уровня JWT-токена.

3.1.2 Ролевая модель Скала^р Спектр.S3

В Скала^р Спектр.S3 реализованы следующие роли:

– администратор инфраструктуры;

– аудитор инфраструктуры;

– администратор тенанта;

– аудитор тенанта.

Разделение полномочий между этими ролями приведены в таблице ниже (таблица 15).

Таблица 2 - Разделение полномочий между ролями

Операция/действие	Администратор инфр-ры	Аудитор инфр-ры	Администратор тенанта	Аудитор тенанта
Выполнять общие настройки системы	R/W	R		
Настройка параметров тенанта	R/W	R		
Просматривать статистику по тенантам	R/W	R		
Просматривать общесистемные логи (прикладной лог ПО)	R	R/W		
Чистить общесистемные логи		R/W		
Лог действия администраторов и аудиторов в административном интерфейсе	R	R/W		
Создавать тенант	R/W			
Удалять тенанты	R/W			

Операция/действие	Администратор инфр-ры	Аудитор инфр-ры	Администратор тенанта	Аудитор тенанта
Создавать бакеты			R/W	R
Настройка параметров бакеты			R/W	R
Удалять бакеты			R/W	
Создавать/блокировать/удалять пользователей			R/W	
Просматривать логи тенанта			R	R/W
Просматривать статистику по тенанту, администратором которого он является			R/W	R
Просматривать системные логи, относящиеся к тенанту			R	R/W
Лог действия администратора тенантов по тенанту, администратором которого он является			R	R/W
Просматривать логи пользователей тенанта			R	R/W
Чистить системные логи и пользовательские логи тенанта				R/W

Роли Администратор инфраструктуры и Аудитор инфраструктуры существуют по умолчанию и создаются при инсталляции. Их служебные названия задаются в конфигурационном файле opt/skala-r/s3gateway/s3gateway.config.json и по умолчанию это:

- S3_admin – Администратор инфраструктуры;
- S3_auditor - Аудитор инфраструктуры.

Название этих ролей может быть изменено правой конфигурационного файла.

Роли Администратора тенанта и Аудитора тенанта создаются автоматически и имеют названия:

- TenantAdmin_<FQDN имя тенанта> – администратор тенанта;
- TenantAuditor_<FQDN имя тенанта> – аудитор тенанта.

4 Описание конфигурационных файлов

С помощью конфигурационных файлов настраиваются параметры функционирования программного модуля компрессии / декомпрессии объектов.

В состав параметров, настраиваемых с использование конфигурационных файлов входит:

- Вкл/Выкл компрессию;
- максимальный размер сжимаемого файла;
- период обновления кэша с данными пользователей;
- адрес сервера (значение по умолчанию - ":8000")
- адрес control-server (значение по умолчанию – "localhost:50052");
- адрес сервера сжатия/декомпрессии (значение по умолчанию – "localhost:50051");
- адрес S3 хранилища (значение по умолчанию – http://s3.skala-r.loc);
- путь к конфигурационному файлу.

5 Использование логов

Для диагностики проблем может использоваться просмотр информации о ходе выполнения задач штатными средствами веб-интерфейса «Скала^р Спектр.S3», а также просмотр лог-файлов сервисов «Скала^р Спектр.S3».

5.1 Логирование событий

Настройка параметров логгирования осуществляется в конфиг файле /opt/skala-r/s3gateway/s3gateway.config.json.

`"proxy_log_path": "/var/log/skala-s3gw/proxy.log",` – Путь куда будут записываться логи прокси

`"control_log_path": "/var/log/skala-s3gw/control.log",` – Путь куда будут записываться логи модуля управления

`"rsyslog_url": "127.0.0.1:514",` – URl rsyslog сервера (ip:port). Настройка отпраки логов во внешние системы описана в п. 5.3

`"log_period_sec": 5` – Периодичность с которой записываются логи прокси сервера.

5.2 Настройка ротации логирования

Файл конфигурации "/etc/logrotate.d/skala-s3gw" и содержимым

```
/var/log/skala-s3gw/proxy.log {
    create 0640 s3gw_endpoint s3gw
    daily
    rotate 93
    missingok
    notifempty
}
```

5.3 Отправка логов во внешние источники

Для серверов шлюза Спектр.S3:

а) создать конфигурационный файл /etc/rsyslog.d/proxy.conf для логов прокси сервера:

```
$ModLoad imfile
$InputFileName /tmp/proxy.log
$InputFileTag proxy:
$InputFileStateFile proxy_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
```

. @@192.168.191.232:514 (url куда отправлять логи)

б) создать конфигурационный файл /etc/rsyslog.d/proxy.conf для логов модуля управления:

```
$ModLoad imfile
$InputFileName /tmp/control.log (путь к локальным логам)
$InputFileTag proxy:
$InputFileStateFile control_log
$InputFileSeverity info
```

```
$InputFileFacility local6
$InputRunFileMonitor
```

. @@192.168.191.232:514 (url куда отправлять логи)

в) перезагрузить rsyslog:

```
systemctl restart rsyslog
```

5.4 Выполнение резервного копирования на нодах Скала^р Спектр.S3

5.4.1 haproxy

Резервирование:

```
echo ${nowstamp}
cp -v /etc/haproxy/haproxy.cfg /backup_skala-mhdo/s3gateway/<nowstamp>/haproxy/
cp -rva /etc/haproxy/conf.d/ /backup_skala-mhdo/s3gateway/<nowstamp>/haproxy/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/haproxy/haproxy.cfg /etc/haproxy/
cp -rva /backup_skala-mhdo/s3gateway/<some_stamp>/haproxy/conf.d/ /etc/haproxy/
systemctl restart haproxy
```

5.4.2 keepalived

Резервирование:

```
echo ${nowstamp}
cp -v /etc/keepalived/keepalived.conf /backup_skala-
mhdo/s3gateway/<nowstamp>/keepalived/
cp -rva /etc/keepalived/scripts-skala-r/ /backup_skala-
mhdo/s3gateway/<nowstamp>/keepalived/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/keepalived/keepalived.conf
/etc/keepalived/
cp -rva /backup_skala-mhdo/s3gateway/<some_stamp>/keepalived/scripts-skala-r/
/etc/keepalived/
systemctl restart keepalived
```

5.4.3 s3gw

Резервирование:

```
echo ${nowstamp}
cp -rva /opt/skala-r/s3gateway/conf_holder/ /backup_skala-
mhdo/s3gateway/<nowstamp>/s3gateway/
cp -v /opt/skala-r/s3gateway/*.pem /backup_skala-mhdo/s3gateway/<nowstamp>/s3gateway/
cp -v /opt/skala-r/s3gateway/s3gateway.config.json /backup_skala-
mhdo/s3gateway/<nowstamp>/s3gateway/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -rva /backup_skala-mhdo/s3gateway/<some_stamp>/s3gateway/conf_holder/ /opt/skala-
r/s3gateway/
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/s3gateway/*.pem /opt/skala-
r/s3gateway/
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/s3gateway/s3gateway.config.json
/opt/skala-r/s3gateway/
systemctl start s3gateway-control-server.service s3gateway-proxy-server.service
```

5.4.4 sysctl.d

Резервирование:

```
echo ${nowstamp}
cp -v /etc/sysctl.d/85-mhd.o.conf /backup_skala-mhdo/s3gateway/<nowstamp>/sysctl.d/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/sysctl.d/85-mhd.o.conf /etc/sysctl.d/
sysctl –system
```

5.4.5 ssh

Резервирование:

```
echo ${nowstamp}
mkdir /backup_skala-mhdo/s3gateway/<nowstamp>/ssh/sshd_config.d/
cp -rva /etc/ssh/sshd_config.d/45-skala^r.conf /backup_skala-
mhdo/s3gateway/<nowstamp>/ssh/sshd_config.d/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/ssh/sshd_config.d/45-skala^r.conf
/etc/ssh/sshd_config.d/
systemctl restart sshd
```

5.4.6 chrony

Резервирование:

```
echo ${nowstamp}
```

```
cp -v /etc/chrony.conf /backup_skala-mhdo/s3gateway/<nowstamp>/chrony/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/chrony/chrony.conf /etc/
systemctl restart chronyd
```

5.4.7 nginx + ssl

Резервирование:

```
echo ${nowstamp}
cp -v /etc/nginx/nginx.conf /backup_skala-mhdo/s3gateway/<nowstamp>/nginx+ssl/
cp -rva /etc/nginx/conf.d/ /backup_skala-mhdo/s3gateway/<nowstamp>/nginx+ssl/
cp -rva /etc/nginx/ssl/ /backup_skala-mhdo/s3gateway/<nowstamp>/nginx+ssl/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/nginx+ssl/nginx.conf /etc/nginx/
cp -rva /backup_skala-mhdo/s3gateway/<some_stamp>/nginx+ssl/conf.d/ /etc/nginx/
cp -rva /backup_skala-mhdo/s3gateway/<some_stamp>/nginx+ssl/ssl/ /etc/nginx/
systemctl restart nginx
```

5.4.8 database

Резервирование:

раскомментировать/добавить если отсутствуют в конфигурационный файл СУБД pg_hba.conf строки, касающиеся replication connections

```
vim /var/lib/pgsql/15/data/pg_hba.conf
```

(пример ниже, выделено жирным)

Put your actual configuration here

#
If you want to allow non-local connections, you need to add more
"host" records. In that case you will also need to make PostgreSQL
listen on a non-local interface via the listen_addresses
configuration parameter, or via the -i or -h command line switches.

TYPE DATABASE USER ADDRESS METHOD
"local" is for Unix domain socket connections only
#local all all peer
local s3gw s3gwuser md5
local all postgres trust
IPv4 local connections:
#host all all 127.0.0.1/32 scram-sha-256

host s3gw s3gwuser 127.0.0.1/32 md5

 # Allow replication connections from localhost, by a user with the

 # replication privilege.

local replication postgres peer

host replication postgres 127.0.0.1/32 trust

#host replication all ::1/128 md5

перезагрузить конфигурацию СУБД

```
systemctl reload postgresql-15.service
```

запустить резервное копирование СУБД шлюза командой

```
echo ${nowstamp}
pg_basebackup -h 127.0.0.1 -p 5432 -U postgres -D /backup_skala-
mhdo/s3gateway/<nowstamp>/database -Ft -z -Xs -P
проверить наличие РК можно командой
ls -lah /backup_skala-mhdo/s3gateway/<nowstamp>/database/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

`systemctl stop s3gateway-control-server.service s3gateway-proxy-server.service`

(если работают сервисы S3GW)

```
systemctl stop postgresql-15.service
rm -rfv /var/lib/pgsql/15/data/*
tar -xvf /backup_skala-mhdo/s3gateway/<some_stamp>/database/base.tar.gz -C
/var/lib/pgsql/15/data
tar -xvf /backup_skala-mhdo/s3gateway/<some_stamp>/database/pg_wal.tar.gz -C
/var/lib/pgsql/15/data/pg_wal
chown -R postgres:postgres /var/lib/pgsql/15/
chmod -R go-rwx /var/lib/pgsql/15/
systemctl start postgresql-15.service
systemctl start s3gateway-control-server.service s3gateway-proxy-server.service
```

5.4.9 logrotate

Резервирование:

```
echo ${nowstamp}
cp -v /etc/logrotate.conf /backup_skala-mhdo/s3gateway/<nowstamp>/logrotate/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/logrotate/logrotate.conf /etc/
systemctl restart logrotate.service
```

5.4.10 logs

Резервирование:

```
echo ${nowstamp}
cp -v /var/log/skala-s3gw-proxy/proxy* /backup_skala-mhdo/s3gateway/<nowstamp>/logs/
```

```
cp -v /var/log/skala-s3gw-control/control* /backup_skala-
mhdo/s3gateway/<nowstamp>/logs/
cp -v /var/log/nginx/error* /backup_skala-mhdo/s3gateway/<nowstamp>/logs/
cp -v /var/log/nginx/access* /backup_skala-mhdo/s3gateway/<nowstamp>/logs/
cp -v /var/log/keepalived-skala-r/keepalived.log /backup_skala-
mhdo/s3gateway/<nowstamp>/logs/
cp -v /var/log/messages* /backup_skala-mhdo/s3gateway/<nowstamp>/logs/
```

Восстановление:

```
ls /backup_skala-mhdo/s3gateway/
```

выбрать папку с датой РК (some_stamp)

```
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/logs/proxy* /var/log/skala-s3gw-
proxy/
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/logs/control* /var/log/skala-s3gw-
control/
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/logs/error* /var/log/nginx/
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/logs/access* /var/log/nginx/
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/logs/keepalived.log
/var/log/keepalived-skala-r/
cp -v /backup_skala-mhdo/s3gateway/<some_stamp>/logs/messages* /var/log/
```

6 Описание кластера служебной СУБД и пример его конфигурации

6.1 Описание конфигурации кластера

Кластер собирается из 5-ти узлов. Состоит из 2х серверов с ролью «Балансировщик» и 3х серверов с ролью «Сервер хранения». Ресурс системная база данных доступен к запуску только на двух серверах балансировщиках, оставшиеся сервера используются в кворуме кластера высокой доступности.

Инструкция будет содержать пример построения кластера на серверах:

192.168.191.66 s3gw-01 - сервер с ролью «Балансировщик»"

192.168.191.67 s3gw-02 - сервер с ролью «Балансировщик»

192.168.191.16 mhdo-01 - сервер с ролью «Сервер хранения»

192.168.191.17 mhdo-02 - сервер с ролью «Сервер хранения»

192.168.191.18 mhdo-03 - сервер с ролью «Сервер хранения»

и VIP адрес 192.168.191.65

6.2 Требования по настройке дисковой подсистемы

Для уменьшения вероятности переполнения, необходимо предусмотреть отдельный том для системного каталога /var/lib размером не менее 20 Гб.

Подготовка серверов:

```
dnf update -y
dnf install redos-kernels6-release -y
dnf makecache
dnf update -y
```

Обновление ОС и компонентов:

```
cat /etc/hosts
```

Добавление настроек в файл hosts:

```
192.168.191.66  s3gw-01
192.168.191.67  s3gw-02
192.168.191.16  mhdo-01
192.168.191.17  mhdo-02
192.168.191.18  mhdo-03
```

Настройка SELinux и сетевого экрана:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
setenforce 0
tuned-adm profile throughput-performance
systemctl disable --now firewalld
reboot
```

Установка компонентов:

```
dnf install pcs pacemaker corosync postgresql15-server -y
```

Установка ПО кластера для серверов с ролью «Балансировщик»:

```
dnf install pcs pacemaker corosync -y
```

Установка ПО кластера для серверов с ролью «Сервер хранения»:

```
chmod 1700 /var/lib/pgsql
chown postgres:postgres /var/lib/pgsql
```

Настройка системного каталога postgresql для серверов с ролью «Балансировщик»

Настройка компонентов:

```
passwd hacluster
# потребует ввода пароля и его подтверждения
systemctl start pcsd.service
```

Настройка системного пользователя для серверов с ролью «Балансировщик»

Инициализация кластера выполняется на первом хосте из серверов с ролью «Балансировщик»:

```
pcs host auth s3gw-01 s3gw-02 mhdo-01 mhdo-02 mhdo-03 -u hacluster -p <пароль
пользователя hacluster>
pcs cluster setup mhdo s3gw-01 s3gw-02 mhdo-01 mhdo-02 mhdo-03 --force
pcs cluster setup mhdo s3gw-01 addr=192.168.191.66 s3gw-02 addr=192.168.191.67 mhdo-
01 addr=192.168.191.16 mhdo-02 addr=192.168.191.17 mhdo-03 addr=192.168.191.18 --
force
pcs cluster enable --all && pcs cluster start --all
pcs property set stonith-enabled=false
```

Инициализация кластера высокой доступности

Инициализация базы данных

Выполняется на первом хосте из серверов с ролью «Балансировщик»:

```
/usr/pgsql-15/bin/postgresql-15-setup initdb
mkdir /var/lib/pgsql/skala/
chmod 750 /var/lib/pgsql/skala/
chown postgres:postgres /var/lib/pgsql/skala/
sudo -u postgres mkdir /var/log/postgres-15/
```

Подготовка базы данных

Редактируем файл postgresql.conf:

```
listen_addresses = '*'wal_keep_size = 128
log_directory = '/var/log/postgres-15/'
```

Редактируем файл pg_hba.conf:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD
# "local" is for Unix domain socket connections only
 local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            scram-sha-256
host    s3gw            s3gwuser        <IP 1-вого сервера
балансировщика>/32            md5
host    s3gw            s3gwuser        <IP 2-го сервера
балансировщика>/32            md5
host    s3gw            s3gwuser        < VIP
Адрес>/32                                               md5
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
```

```
host    replication     all             127.0.0.1/32            scram-sha-256
host    replication     all             ::1/128                 scram-sha-256
host    replication     postgres         <IP 1-вого сервера
балансировщика>/32       trust
host    replication     postgres         <IP 2-го сервера
балансировщика>/32       trust
```

```
systemctl start postgresql-15.service
sudo -u postgres psql -c "CREATE USER s3gwuser WITH PASSWORD 's3gwuser';"
sudo -u postgres psql -c "CREATE DATABASE s3gw OWNER s3gwuser;"
```

Запускаем PostgreSQL и создаем пользователя и базу для Спектр.S3:

```
sudo -u postgres mkdir /var/log/postgres-15/
sudo -u postgres /usr/bin/pg_basebackup -h <ip адрес первой ноды шлюза> -U postgres -
D /var/lib/pgsql/15/data/ -X stream -P
systemctl stop postgresql-15.service
pcs node standby #!!!!!!!!выполнить команду на обоих нодах шлюза
systemctl enable pcsd.service
systemctl enable corosync
systemctl enable pacemaker
mkdir /var/lib/pgsql/skala/
chmod 750 /var/lib/pgsql/skala/
chown postgres:postgres /var/lib/pgsql/skala/
```

Выполняется на втором узле шлюза синхронизируем второй сервер с ролью «Балансировщик»:

```
cat > /var/lib/pgsql/skala/sync-db.sh
```

Копируем файл скрипта востановления ручного нод на обе ноды Спектр.S3:

```
#!/bin/bash
cmd="sudo -u postgres"
vip='<VIP мастера postgresql>'
if [ $(pcs resource status | grep Masters | grep $(pcs quorum status | grep local |
awk '{print $4}') | wc -l) -eq 1 ];then
    echo 'Операция отменена, сервер является мастером базы данных'
    exit 0
else
      echo "Старт удаления каталога данных PostgreSQL"
      $cmd rm -rf /var/lib/pgsql/15/data/
      echo "Старт синхронизации данных"
      $cmd /usr/bin/pg_basebackup -h $vip -U postgres -D /var/lib/pgsql/15/data/ -X
stream -P
      rm -f /var/lib/pgsql/tmp/PGSQL.lock
      pcs resource cleanup
exit 0
fi
```

Назначаем права на скрипт:

```
chown postgres:root /var/lib/pgsql/skala/sync-db.sh
chmod 750 /var/lib/pgsql/skala/sync-db.sh
```

Включить и запустить службу corosync на нодах кворума (ноды хранения).

```
systemctl enable corosync
```

```
systemctl start corosync
```

Включить и запустить службу corosync на нодах кворума (ноды хранения).

Настройка ресурсов кластера высокой доступности:

```
pcs resource create ClusterIP ocf:heartbeat:IPaddr2 nic=<Сетевой интерфейс куда
прикрутим VIP> ip=<VIP адрес> cidr_netmask=<Маска сети> op monitor interval=3s --
group system-db

pcs resource create pgsql pgsql \
    pgctl="/usr/pgsql-15/bin/pg_ctl" \
    psql="/usr/pgsql-15/bin/psql" \
    pgdata="/var/lib/pgsql/15/data" \
    rep_mode="sync" \
    repuser="postgres" \
    master_ip="192.168.191.65" \  # VIP адрес
    node_list="s3gw-01 s3gw-02" \ # Ноды шлюза где живет БД
    check_wal_receiver="true" \
    primary_conninfo_opt="keepalives_idle=60 keepalives_interval=5
keepalives_count=5" \
    op start timeout="60s" interval="0s" on-fail="restart" \
    op monitor timeout="60s" interval="3s" role="Promoted" \
    op monitor timeout="60s" interval="4s" on-fail="restart" \
    op promote timeout="60s" interval="0s" on-fail="restart" \
    op demote timeout="60s" interval="0s" on-fail="stop" \
    op stop timeout="60s" interval="0s" on-fail="block" \
    op notify timeout="60s" interval="0s" \
    --group system-db

pcs resource promotable pgsql master-max=1 master-node-max=1 clone-max=2 clone-node-
max=1 notify=true
pcs constraint colocation add ClusterIP with master pgsql-clone INFINITY
pcs constraint order promote pgsql-clone then start ClusterIP symmetrical=false
score=INFINITY
pcs constraint order demote pgsql-clone then stop ClusterIP symmetrical=false
pcs constraint location pgsql-clone avoids mhdo-01=INFINITY
pcs constraint location pgsql-clone avoids mhdo-02=INFINITY
pcs constraint location pgsql-clone avoids mhdo-03=INFINITY
pcs node unstandby
```

Выполняем на первом сервере с ролью «Балансировщик»:

```
после того как выполнили команду pcs node unstandby на первой ноде
ждем около 30 секунд
pcs node unstandby # Выполняем на второй ноде шлюза
```

Выполняем на второй ноде Спектр.S3:

```
pcs resource cleanup
```

Выполняем на первой ноде Спектр.S3:

```
pcs status -full


[root@s6-s3gw-01 ~]# pcs status --full
Cluster name: s6-mhdo
```

```
Cluster Summary:
* Stack: corosync (Pacemaker is running)
* Current DC: s6-s3gw-02 (2) (version 2.1.6-1.el7-6fdc9deea29) - partition with
quorum
* Last updated: Thu Apr 3 10:25:19 2025 on s6-s3gw-01
* Last change: Wed Apr 2 15:28:06 2025 by root via crm_attribute on s6-s3gw-01
* 5 nodes configured
* 3 resource instances configured

Node List:
* Node s6-mhdo-01 (3): online, feature set 3.17.4
* Node s6-mhdo-02 (4): online, feature set 3.17.4
* Node s6-mhdo-03 (5): online, feature set 3.17.4
* Node s6-s3gw-01 (1): online, feature set 3.17.4
* Node s6-s3gw-02 (2): online, feature set 3.17.4

Full List of Resources:
* Resource Group: system-db:
* ClusterIP (ocf::heartbeat:IPaddr2): Started s6-s3gw-01
* Clone Set: pgsql-clone [pgsql] (promotable):
* pgsql (ocf::heartbeat:pgsql): Slave s6-s3gw-02
* pgsql (ocf::heartbeat:pgsql): Master s6-s3gw-01
* pgsql (ocf::heartbeat:pgsql): ORPHANED Stopped

Node Attributes:
* Node: s6-s3gw-01 (1):
* master-pgsql : 1000
* pgsql-data-status : LATEST
* pgsql-master-baseline : 00000000030000A0
* pgsql-receiver-status : normal (master)
* pgsql-status : PRI
* Node: s6-s3gw-02 (2):
* master-pgsql : 100
* pgsql-data-status : STREAMING|SYNC
* pgsql-receiver-status : normal
* pgsql-status : HS:sync

Migration Summary:

Tickets:

PCSD Status:
s6-mhdo-01: Online
s6-mhdo-02: Online
s6-mhdo-03: Online
s6-s3gw-01: Online
s6-s3gw-02: Online

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

Смотрим статус кластера БД:

```
[root@s6-s3gw-01 ~]# pcs  status quorum
```

```
Quorum information
------------------
Date:             Thu Apr  3 10:26:32 2025
Quorum provider:  corosync_votequorum
Nodes:            5
Node ID:          1
Ring ID:          1.d
Quorate:          Yes

Votequorum information
----------------------
Expected votes:   5
Highest expected: 5
Total votes:      5
Quorum:           3
Flags:            Quorate

Membership information
----------------------
    Nodeid      Votes    Qdevice Name
         1          1         NR s6-s3gw-01 (local)
         2          1         NR s6-s3gw-02
         3          1         NR s6-mhdo-01
         4          1         NR s6-mhdo-02
         5          1         NR s6-mhdo-03
```

Проверяем статус кворума:

```
[root@s6-s3gw-01 ~]# pcs config show
Cluster Name: s6-mhdo
Corosync Nodes:
 s6-s3gw-01 s6-s3gw-02 s6-mhdo-01 s6-mhdo-02 s6-mhdo-03
Pacemaker Nodes:
 s6-mhdo-01 s6-mhdo-02 s6-mhdo-03 s6-s3gw-01 s6-s3gw-02

Resources:
  Group: system-db
    Resource: ClusterIP (class=ocf provider=heartbeat type=IPaddr2)
      Attributes: ClusterIP-instance_attributes
        cidr_netmask=24
        ip=192.168.100.171
        nic=ens3
      Operations:
        monitor: ClusterIP-monitor-interval-3s
          interval=3s
        start: ClusterIP-start-interval-0s
          interval=0s
          timeout=20s
        stop: ClusterIP-stop-interval-0s
          interval=0s
          timeout=20s
  Clone: pgsql-clone
    Meta Attributes: pgsql-clone-meta_attributes
      clone-max=2
      clone-node-max=1
      master-max=1
```

```
      master-node-max=1
      notify=true
      promotable=true
    Resource: pgsql (class=ocf provider=heartbeat type=pgsql)
      Attributes: pgsql-instance_attributes
        check_wal_receiver=true
        master_ip=192.168.100.171
        node_list="s6-s3gw-01 s6-s3gw-02"
        pgctl=/usr/pgsql-15/bin/pg_ctl
        pgdata=/var/lib/pgsql/15/data
        primary_conninfo_opt="keepalives_idle=60 keepalives_interval=5
keepalives_count=5"
        psql=/usr/pgsql-15/bin/psql
        rep_mode=sync
        repuser=postgres
      Operations:
        demote: pgsql-demote-interval-0s
          interval=0s
          timeout=60s
          on-fail=stop
        methods: pgsql-methods-interval-0s
          interval=0s
          timeout=5s
        monitor: pgsql-monitor-interval-3s
          interval=3s
          timeout=60s
          role=Master
        monitor: pgsql-monitor-interval-4s
          interval=4s
          timeout=60s
          on-fail=restart
        notify: pgsql-notify-interval-0s
          interval=0s
          timeout=60s
        promote: pgsql-promote-interval-0s
          interval=0s
          timeout=60s
          on-fail=restart
        start: pgsql-start-interval-0s
          interval=0s
          timeout=60s
          on-fail=restart
        stop: pgsql-stop-interval-0s
          interval=0s
          timeout=60s
          on-fail=block

Stonith Devices:
Fencing Levels:

Location Constraints:
  Resource: pgsql-clone
    Disabled on:
      Node: s6-mhdo-01 (score:-INFINITY) (id:location-pgsql-clone-s6-mhdo-01--
INFINITY)
```

```
      Node: s6-mhdo-02 (score:-INFINITY) (id:location-pgsql-clone-s6-mhdo-02--
INFINITY)
      Node: s6-mhdo-03 (score:-INFINITY) (id:location-pgsql-clone-s6-mhdo-03--
INFINITY)
Ordering Constraints:
  promote pgsql-clone then start ClusterIP (score:INFINITY) (non-symmetrical)
(id:order-pgsql-clone-ClusterIP-INFINITY)
  demote pgsql-clone then stop ClusterIP (kind:Mandatory) (non-symmetrical)
(id:order-pgsql-clone-ClusterIP-mandatory)
Colocation Constraints:
  ClusterIP with pgsql-clone (score:INFINITY) (rsc-role:Started) (with-rsc-
role:Master) (id:colocation-ClusterIP-pgsql-clone-INFINITY)
Ticket Constraints:

Alerts:
 No alerts defined

Resources Defaults:
  Meta Attrs: build-resource-defaults
    resource-stickiness=1
Operations Defaults:
  No defaults set

Cluster Properties:
 cluster-infrastructure: corosync
 cluster-name: s6-mhdo
 dc-version: 2.1.6-1.el7-6fdc9deea29
 have-watchdog: false
 last-lrm-refresh: 1743596862
 stonith-enabled: false

Tags:
 No tags defined

Quorum:
  Options:
```

Смотрим конфигурацию кластера БД

Восстановление сервера после падения:

```
/var/lib/pgsql/skala/sync-db.sh
```

Запуск скрипта синхронизации.

7 Модуль лицензии

Модуль лицензии используется в модуле управления и в модуле парсинга.

У модуля лицензии есть состояние.

Состояние может быть true(лицензия активна, разрешается доступ к функциям, закрытым лицензией) или false(лицензия не активна, доступ запрещен).

Состояние устанавливается по результату проверки ключей, хранящихся в БД.

Если хотя бы один ключ активен - то лицензия активна.

Если хотя бы у одного ключа есть компрессия, то компрессия разрешается.

Состояние модуля лицензии меняется в следующих случаях:

– при старте сервиса;

– после старта раз в заданный временной период (24 часа);

– при добавлении нового ключа через модуль управления. В этом случае модуль управления уведомляет модуль парсинга о добавлении ключа;

– TODO: обновлять состояние модуля лицензии при запросе списка ключей.

7.1 Лицензионный ключ

Состоит из комбинации лицензионного ключа S3 и ключа шлюза.

Ключ шлюза состоит из:

– список hw_id;

– дата окончания (нулевое значение, если список hw_id не пустой);

– компрессия (да/нет);

– hw_id - поле осталось для совместимости со старой версией ключей, где мог быть только одни hw_id.

Ключ шлюза активен если:

– если список hw_id не пустой и hw_id сервера, на котором работает модуль, есть в списке hw_id ключа;

– если список hw_id пустой и дата окончания позже времени проверки ключа.

Добавление нового лицензионного ключа

При загрузке лицензионного ключа на сервер через модуль управления, ключ валидируется и разделяется на S3 ключ и ключ шлюза.

Нельзя загрузить два одинаковых ключа.

Нельзя загрузить два разных ключа, содержащих одинаковые S3 ключи.

Если S3 ключ не активен или ключ шлюза не активен, тогда лицензионный ключ не загрузится.

8 Модуль компрессии

Модуль компрессии используется Модулем парсинга при операциях с объектами.

В настоящее время на лету сжимаются файлы размером до 50Мб. При использовании механизма Multi Part Upload (MPU) ограничение в 50 Мб относится к размеру каждой отдельной части.

8.1 Аргументы командной строки при запуске модуля:

Порт сервера модуля парсинга: --port=50051 (значение по умолчанию)

Путь к конфиг --cfg=/opt/skala-r/s3gateway/s3gateway.env (значение по умолчанию)

Содержимое конфигурационного файла:

CPU=3

Указывается количество доступных сервису ядер процессора.

8.2 Метрики

Сервер собирает метрики о своей работе. Метрики можно получить в формате prometheus и через методы GRPC.

8.2.1 Формат Prometheus

`s3_compressor_compress_operations` - общее количество операций компресии с момента запуска сервера.

`s3_compressor_decompress_operations` - общее количество операций декомпресии с момента запуска сервера.

`s3_compressor_before_compression_bytes` - количество байт переданных на компрессию.

`s3_compressor_after_compression_bytes` - количество байт после завершения операции компресии.

`s3_compressor_before_decompression_bytes` - количество байт переданных на декомпрессию.

`s3_compressor_after_decompression_bytes` - количество байт после завершения операции декомпресии.

Запрос метрик в формате promethus

```
GET <адрес_хоста>:8088/metrics.
```

8.2.2 Формат GRPC

Метрики запрашиваются за период. допутимое значение периода - 1, 5 или 15 минут.

- CmpSize: compressed MB per period(MB/sec);
- DcmpSize: decompressed MB per period(MB/sec);
- CmpVelocity: average compress velocity per period(MB/sec);
- DcmpVelocity: average decompress velocity per period(MB/sec).