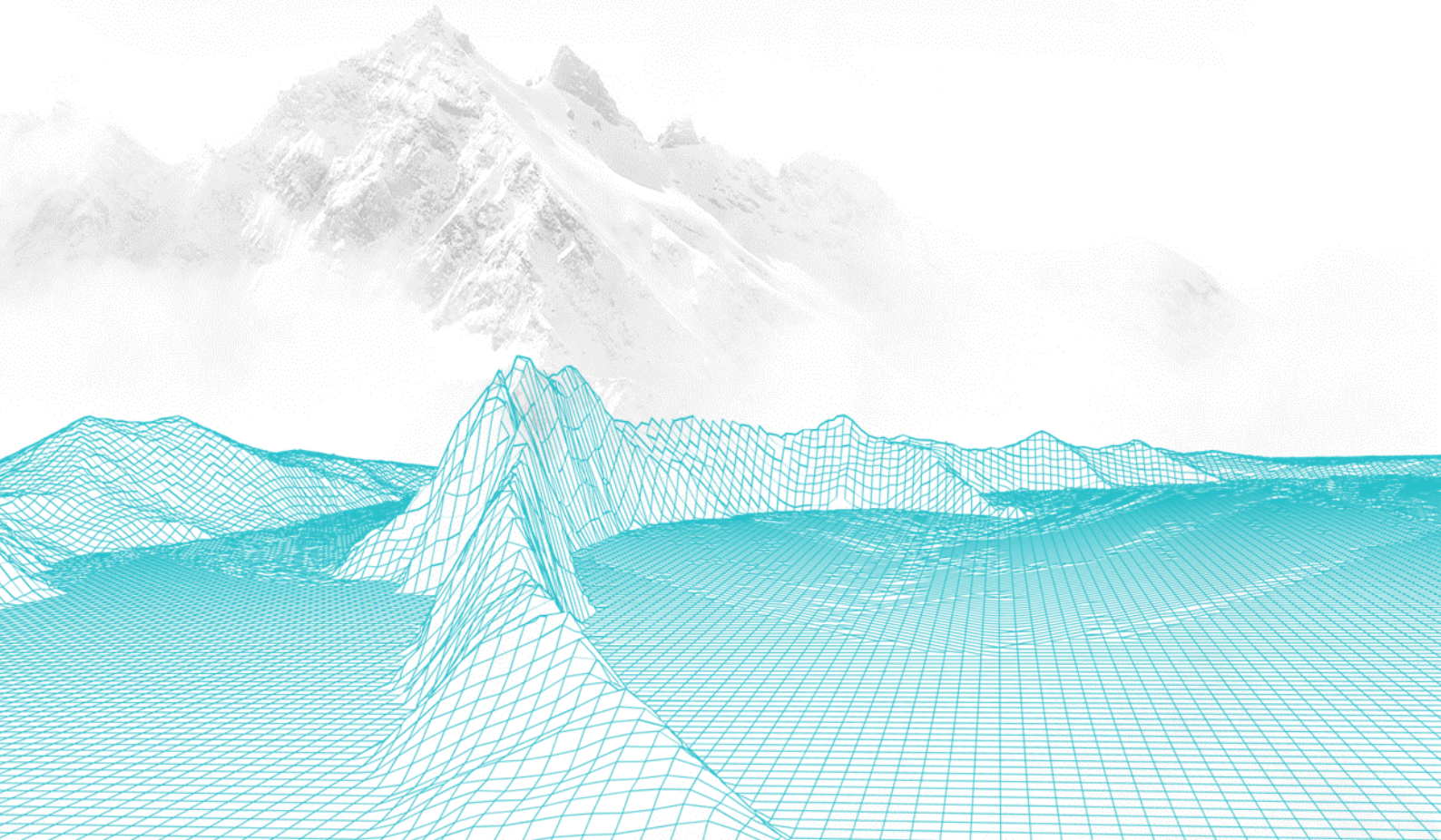
Программное обеспечение
FORTEIA

РУКОВОДСТВО АДМИНИСТРАТОРА

Москва 2026



СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ 5
   1.1. О документе 5
   1.2. Общие сведения о продукте 5
2. УСЛОВИЯ ПРИМЕНЕНИЯ 6
3. НАСТРОЙКА И ЗАПУСК ШЛЮЗА 7
   3.1. Управление контейнером при помощи скрипта 7
      3.1.1. Загрузка образа из удаленного репозитория 8
      3.1.2. Загрузка образа из файла 9
      3.1.3. Остановка контейнера при помощи скрипта 10
      3.1.4. Использование отдельных дисков для размещения данных и метаданных шлюза 11
      3.1.5. Очистка локального репозитория образов контейнеров 11
4. СТРУКТУРА ИНТЕРФЕЙСА УПРАВЛЕНИЯ 13
   4.1. Общая структура интерфейса 13
   4.2. Стартовая страница 15
   4.3. Модальные окна 16
   4.4. Уведомления 16
5. ТИПОВЫЕ ОПЕРАЦИИ 18
   5.1. Получение сведений о шлюзе 18
   5.2. Поиск, фильтрация и сортировка в таблицах 18
   5.3. Ввод и копирование данных 18
   5.4. Контекстное меню действий 19
6. ВХОД В СИСТЕМУ 20
7. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ ИНТЕРФЕЙСА УПРАВЛЕНИЯ 21
   7.1. Ролевая модель 21
   7.2. Встроенные пользователи 21
   7.3. Создание нового пользователя 21
   7.4. Редактирование свойств пользователя 22
   7.5. Удаление пользователя 23
8. УПРАВЛЕНИЕ РЕСУРСАМИ ХРАНЕНИЯ 25
   8.1. Добавление NFS-папки 25
   8.2. Редактирование NFS-папки 26
   8.3. Дренирование NFS-папки 26
   8.4. Удаление NFS-папки 27

9. РАБОТА С КЛИЕНТАМИ 28
9.1. Создание клиента 28
9.2. Получение ключей доступа клиента 29
9.3. Редактирование свойств клиента 29
9.4. Удаление клиента 30
9.5. Обновление Secret key 31
9.6. Блокировка клиента 31
9.7. Разблокирование клиента 32
10. РАБОТА С БАКЕТАМИ 34
10.1. Создание бакета 34
10.2. Удаление бакета 35
11. РАБОТА С ПОЛИТИКАМИ 36
11.1. Создание политики 37
11.2. Редактирование политики 40
11.3. Привязка политики к клиенту 41
11.4. Удаление политики 42
12. МОНИТОРИНГ И ЛОГИРОВАНИЕ 43
12.1. Мониторинг здоровья 43
12.2. Просмотр журнала событий 43
12.3. Просмотр журнала аудита 44
12.4. Выгрузка лога событий 45
12.5. Выгрузка лога аудита 46
12.6. Удаление созданных дампов журналов 47
12.7. Настройка логирования 48
13. НАСТРОЙКА ШЛЮЗА ДЛЯ ПОДКЛЮЧЕНИЯ КЛИЕНТОВ 50
14. ОБНОВЛЕНИЕ ПО ШЛЮЗА 51
15. РЕКОМЕНДАЦИИ ПО РЕЗЕРВНОМУ КОПИРОВАНИЮ 52
15.1. Метаданные (MongoDB) 52
15.2. Данные (объекты) 52
15.3. Логи и метрики 53
15.4. Общие рекомендации 53
16. REST-API 55
17. СПИСОК ПОДДЕРЖИВАЕМЫХ ОПЕРАЦИЙ S3 API 56

ГЛОССАРИЙ

Термин	Определение
Авторизация	Предоставление полномочий на выполнение действий в системе
Журнал	Текстовый файл, куда автоматически записывается информация о событиях в системе
Клиент	Внешняя система, которой предоставляется доступ к шлюзу
Метаданные	Служебные данные об объекте в системе: дата создания, права доступа и т.п.
Протокол	Набор правил, определяющих способы взаимодействий различного типа между субъектами
ПО	Программное обеспечение
Ресурс хранения	Логическая или физическая единица емкости в СХД
Роль	Заранее определенный набор общесистемных разрешений и уровней доступа, выделяемых отдельным пользователям в зависимости от их должностных обязанностей или задач
Сервис	Программный модуль, реализующий тот или иной функционал шлюза
Сетевой интерфейс	Программно-аппаратное обеспечение, взаимодействующее с сетевым драйвером и с уровнем IP
СХД	Система хранения данных
Управляющий интерфейс	Сетевой интерфейс, через который пользователь получает доступ к веб-интерфейсу шлюза
Хост	Устройство, инициирующее операции чтения/записи данных шлюза
API	Application Programming Interface. Программный интерфейс приложений, набор правил, по которым разные программы взаимодействуют между собой и обмениваются данными
RAID	Redundant Array of Independent Disks. Технология объединения нескольких физических носителей в единый логический массив для повышения производительности и/или отказоустойчивости
SSD	Solid-State Drive. Твердотельный диск, энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти
SSL	Secure Sockets Layer. Протокол, обеспечивающий безопасное соединение в компьютерной сети
REST-API	Representational State Transfer Application Programming Interface. архитектурный стиль взаимодействия между клиентом и сервером через HTTP.

1. ВВЕДЕНИЕ

1.1. О документе

Руководство содержит инструкции по использованию программного обеспечения FORTEIA. В документе приводится описание основных элементов веб-интерфейса, типовых операций и настроек необходимых для эксплуатации системы.

Документ предназначен для администраторов и специалистов технической поддержки.

1.2.Общие сведения о продукте

FORTEIA — это кластерный программный шлюз, предоставляющий S3-совместимый интерфейс для доступа к данным, размещённым на внешних системах хранения данных (СХД) через протокол NFS.

Шлюз состоит из нескольких (обычно 4–6) равноправных узлов, каждый из которых не хранит данные локально (stateless).

Все узлы имеют доступ к общим NFS-папкам, где непосредственно хранятся файлы объектов, и к единой базе данных MongoDB, которая служит централизованным хранилищем метаданных (информация о бакетах, объектах, пользователях, политиках доступа, ACL и местоположении реплик).

Основная задача шлюза — преобразовывать S3-запросы клиентских приложений в операции с файлами в NFS-папках и управлять метаданными в MongoDB.

Для обеспечения отказоустойчивости данных объекты синхронно реплицируются на несколько NFS-папок (реплика-группа) в соответствии с настраиваемой политикой размещения. Метаданные защищены благодаря использованию реплика-сета MongoDB с автоматическим переключением при отказах.

Шлюз поддерживает широкий набор операций S3 API, включая управление бакетами, загрузку и скачивание объектов, multipart-загрузки, тегирование, CORS, логирование, а также IAM-авторизацию на основе политик и ACL.

Полный список поддерживаемых операций представлен в разделе 17 «Список поддерживаемых операций S3 API» настоящего руководства.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

ПО FORTEIA предназначено для эксплуатации на физических серверах либо виртуальных машинах, с процессором x86. Шлюз поставляется в виде OCI-совместимого контейнерного образа. Для работы ПО шлюза требуется ОС семейства Linux, например, Ubuntu версии 22.04 или выше с установленным ПО Podman.

Шлюз не отвечает за отказоустойчивое и надежное хранение самих данных. За это отвечает СХД, которая предоставляет шлюзу свой ресурс для хранения данных.

Для достижения лучшей производительности шлюза, требуется использовать для хранения данных и базы метаданных отдельные ресурсы. Производительность шлюза напрямую зависит от скорости работы ресурсов СХД обеспечивающих хранение данных. Рекомендуется использование высокопроизводительных ресурсов.

Для обеспечения сохранности данных, требуется проведение регулярного резервного копирования данных и метаданных шлюза, см. раздел 15 «Рекомендации по резервному копированию» настоящего руководства.

Управление шлюзом FORTEIA выполняется при помощи установленного на компьютере администратора ПО веб-браузера. Список совместимых веб-браузеров:

Chrome — версия 105 и выше;

Яндекс.Браузер — версия 105 и выше;

Firefox — версия 142 и выше

Edge — версия 139 и выше;

Opera — версия 120 и выше;

Safari iOS — версия 11 и выше.

3. НАСТРОЙКА И ЗАПУСК ШЛЮЗА

Для корректной работы шлюза требуется задать параметры его конфигурации: порт для подключения нагрузки, порт для управления, а также указать пути к ресурсам для хранения объектов и метаданных.

Для упрощения управления контейнером шлюза разработан скрипт-инсталлятор run_swarm.sh.

Вся настройка шлюза выполняется на этапе сборки и запуска контейнера, при помощи параметров скрипта-инсталлятора, которые будут рассмотрены ниже.

Порт 8080 служит для подключения нагрузки (S3 API).

Порт 8959 служит для управления работой шлюза и получения справочной информации по REST-API. Доступ к управлению выполняется через эндпоинты:

/ui/ - подключение к GUI;

/swagger/ - сваггер.

3.1. Управление контейнером при помощи скрипта

1. Скопируйте в систему скрипт run_swarm.sh
2. Установите утилиту skopeo командой: **sudo apt install skopeo**.

Для просмотра справки по использованию скрипта, запустите скрипт run_swarm.sh с ключом **–h**.

```
oleg@oleg-VirtualBox:~$ ./run_swarm.sh -h
Скрипт управления контейнером swarm.

Использование:
  -l, --local-list                Показать список локальных MR-образов
  -L, --remote-list               Показать список удалённых MR-образов
  -r, --run-master                Запустить master
  -m <MR>, --run-mr <MR>          Запустить MR
  -d, --delete                    Остановить контейнер
  -c, --clean                     Очистить систему (overlay + dangling images)
  -s <MR>, --save <MR>            Экспорт локального контейнера в файл
  -S <MR>, --download <MR>        Сохранение контейнера из репозитория в файл
  -f <file>, --file <file>        Файл для сохранения контейнера
                                  (если параметра нет, то будет создано имя s3_gateway_<MR>.tar)
  -i <file>, --import <file>      Имя файла контейнера
  --logs-dir <dir>                Директория логов
  --meta-dir <dir>                Директория метаданных
  --data-dir <dir>                Директория данных
  --vmstore-dir <dir>             Директория для VM storage
  -h, --help                      Показать справку

Примеры:
  run_swarm.sh -l
  run_swarm.sh -r
  run_swarm.sh -m mr-1078
  run_swarm.sh -d
  run_swarm.sh -c
  run_swarm.sh -s mr-1078 -f file.tar
  run_swarm.sh -S mr-1078 -f file.tar
  run_swarm.sh -i file.tar
  run_swarm.sh --logs-dir ./tmp/logs
  run_swarm.sh --data-dir ./tmp/data
```

Рисунок 1. Окно терминала с выводом справки по командам скрипта

Скрипт может загрузить образ контейнера с удаленного репозитория либо работать с локальным файлом образа, предварительно импортировав его в систему.

В скрипте заданы следующие номера портов для работы с шлюзом: 8080 – для подключения нагрузки, 8959 – для управления.

Внимание! Без явного указания каталогов требующихся для хранения данных (для этого используются ключи --logs-dir, --meta-dir, --data-dir и --vmstore-dir), скрипт самостоятельно создаст нужные каталоги в каталоге /tmp, который будет создан в том же каталоге откуда был запущен скрипт.

3.1.1. Загрузка образа из удаленного репозитория

1. Запустите скрипт run_swarm.sh с ключом **–L**, чтобы просмотреть образы в удаленном репозитории, доступные к загрузке.

```
oleg@oleg-VirtualBox:~$ ./run_swarm.sh -L
Получение списка удалённых MR...
172.16.22.219:5000/swarm/swarm  master
172.16.22.219:5000/swarm/swarm  mr-1067
172.16.22.219:5000/swarm/swarm  mr-1074
172.16.22.219:5000/swarm/swarm  mr-1085
172.16.22.219:5000/swarm/swarm  mr-1091
172.16.22.219:5000/swarm/swarm  mr-1092
172.16.22.219:5000/swarm/swarm  mr-1094
172.16.22.219:5000/swarm/swarm  mr-1097
172.16.22.219:5000/swarm/swarm  mr-1098
172.16.22.219:5000/swarm/swarm  mr-1099
172.16.22.219:5000/swarm/swarm  mr-1100
172.16.22.219:5000/swarm/swarm  mr-1101
```

Рисунок 2. Вывод списка образов в удаленном репозитории

2. Загрузите и запустите выбранный образ контейнера, указав его имя, например, **run_swarm.sh -m mr-1101**.

При необходимости загрузить образ мастера, используйте ключ –r.

```
oleg@oleg-VirtualBox:~$ ./run_swarm.sh -m mr-1101
 Попытка получить список удалённых MR...
remote hash image: sha256:5d3f6d1249829db96b3df036af2dd1b81a79a5e94bbc35dc7750a8d58831f1bd
local hash image:
 Выкачиваю 172.16.22.219:5000/swarm/swarm:mr-1101...
Trying to pull 172.16.22.219:5000/swarm/swarm:mr-1101...
Getting image source signatures
Copying blob a478f5198ace skipped: already exists
Copying blob ff13a453bc91 skipped: already exists
Copying blob 909b3d94524f skipped: already exists
Copying blob 7f34f89e7ab6 skipped: already exists
Copying blob 79df80c24add skipped: already exists
Copying blob 847f9aa2702e skipped: already exists
Copying blob b13b1dddfabc skipped: already exists
Copying blob 400365fce19a skipped: already exists
Copying blob 0771ddcbd585 skipped: already exists
Copying blob 175f1365d773 skipped: already exists
Copying blob 087b137edacf done   |
Copying blob 36ff513acc67 done   |
Copying blob 547bacc52932 done   |
Copying blob 7ef6783e507b done   |
Copying config 5b51a0d4cd done   |
Writing manifest to image destination
5b51a0d4cd1863cdb5b57dd3ef93834efb25812bb85e875e30ca79b72552bc90
 Образ 172.16.22.219:5000/swarm/swarm:mr-1101 успешно получен.
 Запускаю контейнер swarm из образа 172.16.22.219:5000/swarm/swarm:mr-1101...
474ff78db92d7d303454b3572a9b837960ec3f1ffda9096416f7120d010c5494
 Контейнер успешно запущен.
```

Рисунок 3. Пример окна терминала после загрузки и запуска контейнера

3. Подключитесь к IP адресу шлюза используя веб браузер. По умолчанию, для подключения к GUI назначен порт 8950.

Должна открыться страница входа в систему, как показано на рисунке ниже:

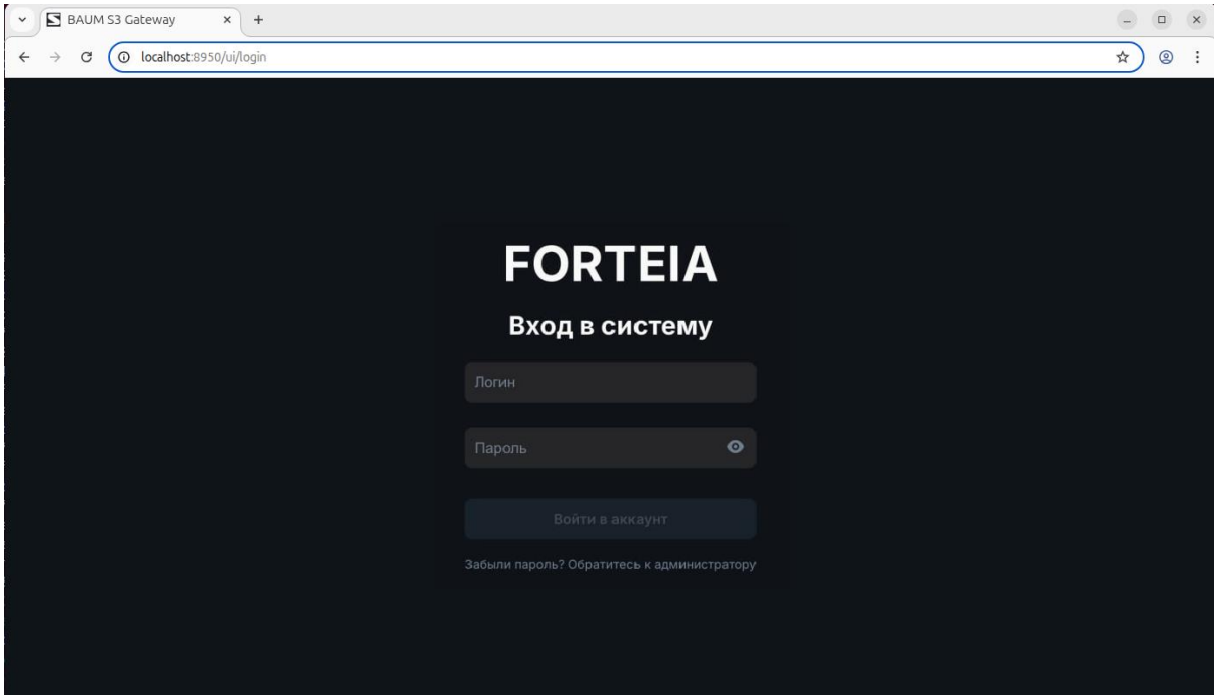


Рисунок 4. Страница входа в систему

3.1.2. Загрузка образа из файла

Предполагается, что файл образа контейнера, с именем rc_0.0.1.0.tar, был скопирован в домашний каталог.

Внимание! При загрузке образа контейнера из файла, доступ к удаленному репозиторию не требуется.

1. Импортируйте файл образа в локальный репозиторий.

./run_swarm.sh -i rc_0.0.1.0.tar

```
oleg@oleg-VirtualBox:~$ ./run_swarm.sh -i rc_0.0.1.0.tar
Getting image source signatures
Copying blob 0771ddcbd585 skipped: already exists
Copying blob 7f34f89e7ab6 skipped: already exists
Copying blob ff13a453bc91 skipped: already exists
Copying blob a478f5198ace skipped: already exists
Copying blob 79df80c24add skipped: already exists
Copying blob 909b3d94524f skipped: already exists
Copying blob 847f9aa2702e skipped: already exists
Copying blob b13b1dddfabc skipped: already exists
Copying blob 400365fce19a skipped: already exists
Copying blob 175f1365d773 skipped: already exists
Copying blob f25a4524602a skipped: already exists
Copying blob 695b2e4c55c7 skipped: already exists
Copying blob b32fdeae8bdf skipped: already exists
Copying blob e630ce7efdb7 skipped: already exists
Copying config 56314b94e9 done   |
Writing manifest to image destination
Loaded image: 172.16.22.219:5000/swarm/swarm:rc_0.0.1.0
```

Рисунок 5. Результат выполнения команды импорта файла образа контейнера

2. Убедитесь в том, что импортированный образ находится в репозитории:

./run_swarm.sh -l

```
oleg@oleg-VirtualBox:~$ ./run_swarm.sh -l
 Локальные MR-образы:
172.16.22.219:5000/swarm/swarm  rc_0.0.1.0
172.16.22.219:5000/swarm/swarm  master
172.16.22.219:5000/swarm/swarm  mr-1101
172.16.22.219:5000/swarm/swarm  mr-1097
172.16.22.219:5000/swarm/swarm  mr-1098
```

Рисунок 6. Вывод содержимого локального репозитория

3. Запустите импортированный образ контейнера, указав его имя:

./run_swarm.sh -m mr-1098.

```
oleg@oleg-VirtualBox:~$ ./run_swarm.sh -m rc_0.0.1.0
 Попытка получить список удалённых MR...
remote hash image: sha256:864665098ae8ba23b144a41417aeb0f7e17649747729e76864c214
ddd44e8232
local hash image: sha256:864665098ae8ba23b144a41417aeb0f7e17649747729e76864c214d
dd44e8232
 Запускаю контейнер swarm из образа 172.16.22.219:5000/swarm/swarm:rc_0.0.1.0...
571033c09912f5b0a2e25438af69dfc5d8829bde6bba99e8127277921ee0d05e
 Контейнер успешно запущен.
```

Рисунок 7. Вывод результата запуска образа из локального репозитория

4. Подключитесь к IP адресу шлюза используя веб браузер. По умолчанию, для подключения к GUI назначен порт 8950.

Должна открыться страница входа в систему.

3.1.3. Остановка контейнера при помощи скрипта

Внимание! После запуска команды остановки контейнера, все процессы записи и чтения объектов будут прерваны.

Остановка контейнера шлюза выполняется командой:

run_swarm.sh –d.

```
oleg@oleg-VirtualBox:~$ ./run_swarm.sh -d
 Контейнер останавливается.
WARN[0010] StopSignal (37) failed to stop container swarm in 10 seconds, resorti
ng to SIGKILL
swarm
 Контейнер остановлен.
```

Рисунок 8. Вывод результата остановки контейнера

3.1.4. Использование отдельных дисков для размещения данных и метаданных шлюза

При запуске контейнера имеется возможность указать отдельные диски для размещения данных и метаданных. Диски предварительно должны быть отформатированы в файловой системе XFS или EXT4. Для этого предназначены ключи: --meta-dir и --data-dir. Пример команды запуска контейнера для работы с отдельными дисками, смонтированными в каталоги /mnt/meta и /mnt/data:

sudo ./run_swarm.sh -m swarm_1.0.0 --meta-dir=/mnt/meta --data-dir=/mnt/data

Внимание! При изменении параметров запуска контейнера, которые были указаны ключами --meta-dir и --data-dir, потребуется выполнить очистку локального репозитория перед повторным запуском контейнера (run_swarm.sh –c). В противном случае контейнер будет использовать прежние значения.

3.1.5. Очистка локального репозитория образов контейнеров

Для того, чтобы очистить локальный репозиторий образов контейнеров и освободить место на системном диске выполните команду:

./run_swarm.sh –c

Рисунок 9. Вывод результата очистки локального репозитория образов

После выполнения очистки репозитория, потребуется повторно импортировать в репозиторий образ контейнера или загрузить образ из удаленного репозитория, если к нему имеется доступ.

4.СТРУКТУРА ИНТЕРФЕЙСА УПРАВЛЕНИЯ

4.1. Общая структура интерфейса

Окно интерфейса управления состоит из двух основных компонентов:

- панель основного меню (слева);
- страница меню, содержащая блок информации и инструментов просматриваемого раздела (справа).

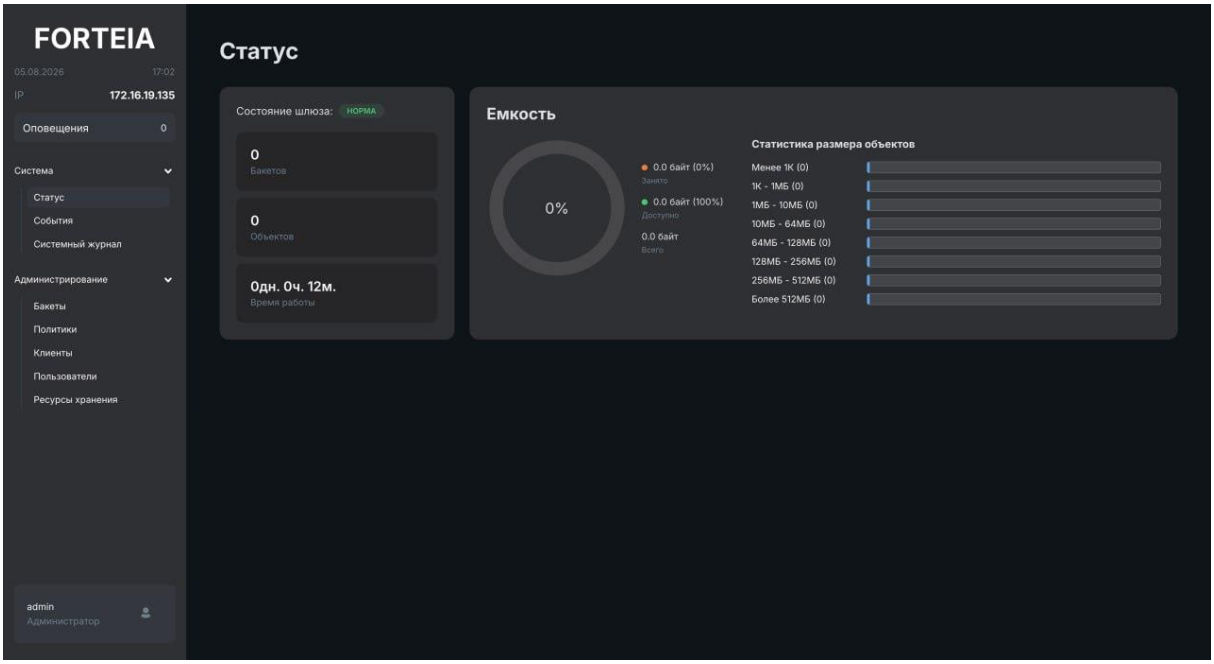


Рисунок 10. Внешний вид интерфейса управления

Основное меню содержит два раздела: Система и Администрирование, в которых сгруппированы подразделы, содержащие инструментарий управления соответствующим функционалом шлюза. При нажатии на стрелку справа от наименования раздела, раскрывается или скрывается список доступных для перехода подразделов. При нажатии на название раздела происходит переход на его страницу меню.

Блок информации и инструментов содержит:

- панели управления функционалом;
- блок фильтров (опционально);
- перечень данных просматриваемого раздела в виде списка, разворачиваемых блоков или нескольких областей.

В верхней части панели основного меню, под названием продукта, выводится информация о хосте, на котором работает шлюз: IP адрес, а также текущая дата и время.

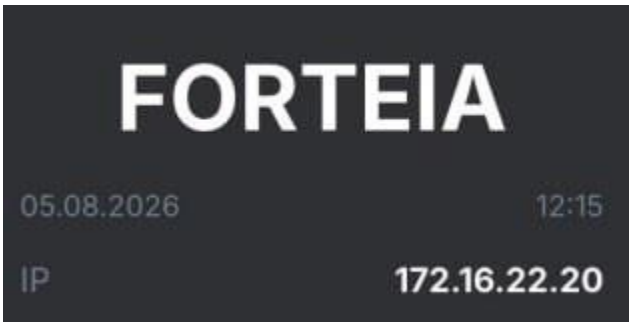


Рисунок 11. Информация о хосте

В нижней части панели основного меню, находится область информации о текущем пользователе, где выводится имя текущего пользователя и его роль в системе.

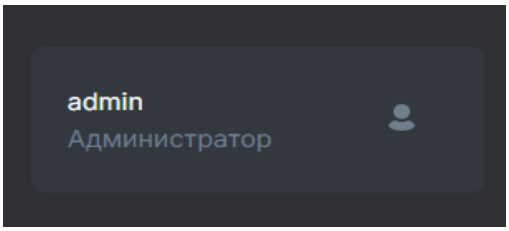


Рисунок 12. Панель информации о текущем пользователе

При нажатии левой кнопкой мыши в области информации о текущем пользователе, открывается модальное окно «Профиль пользователя», содержащее информацию о пользователе, версию ПО шлюза и язык интерфейса (русский/английский), который выбирается из списка.

Переключение языка интерфейса происходит сразу после его выбора в списке.

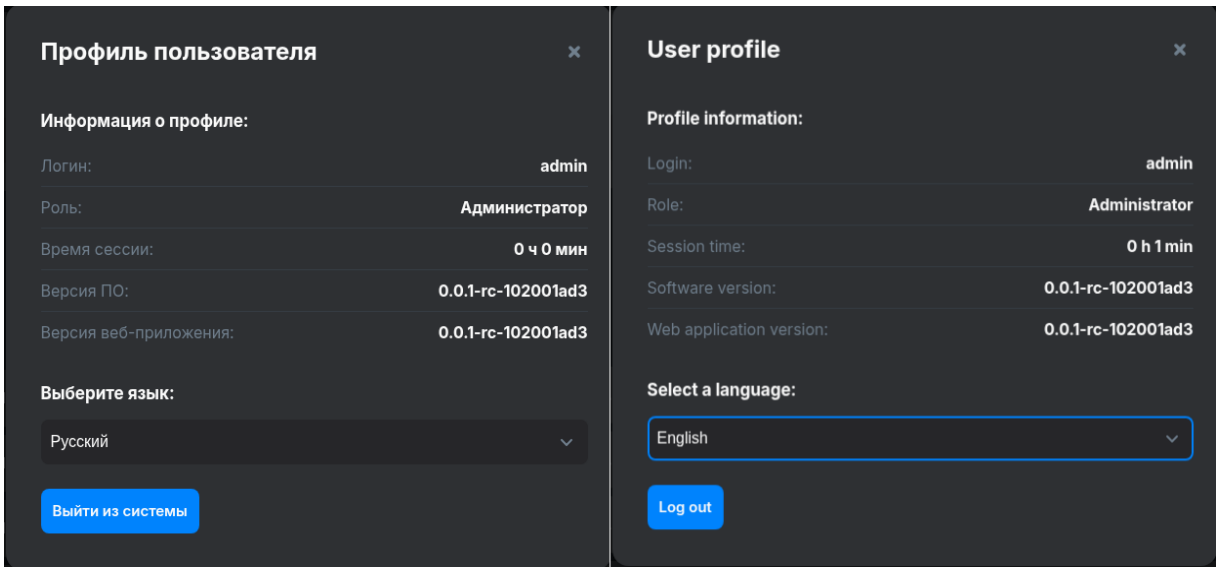


Рисунок 13. Модальное окно "Профиль пользователя" на русском и английском языке.

В окне профиля пользователя также расположена кнопка [**Выйти из системы**] предназначенная для завершения сеанса пользователя.

4.2. Стартовая страница

После успешного входа в систему, открывается раздел меню **Система > Статус**.

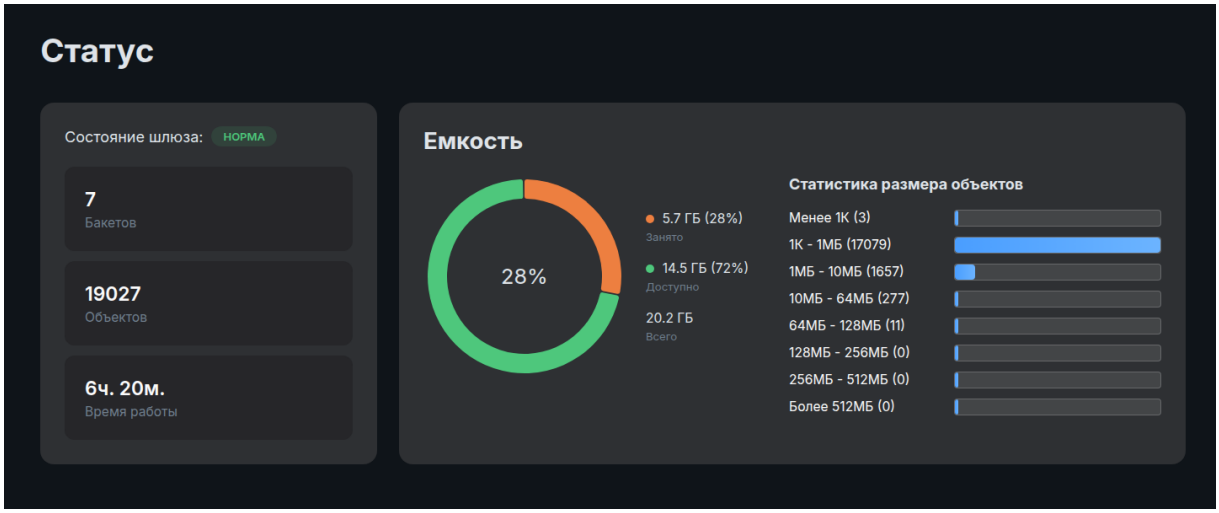


Рисунок 14. Страница меню Система-Статус.

Блок информации страницы меню **Система > Статус** содержит две панели. Левая панель отображает статистику шлюза, правая панель отображает статистику хранилища.

Панель статистики шлюза содержит:

- индикатор состояния шлюза, который показывает результат проверки работоспособности компонентов шлюза;
- счетчики количества бакетов и объектов;
- время беспрерывной работы системы (uptime).

Панель статистики хранилища содержит:

- статистику заполнения емкости хранилища;
- статистику размера объектов находящихся в хранилище.

Возможны следующие статусы проверки работоспособности:

- **Норма** (зеленый цвет) – система работает нормально;
- **Ошибка** (красный цвет) – обнаружена ошибка в работе системы.

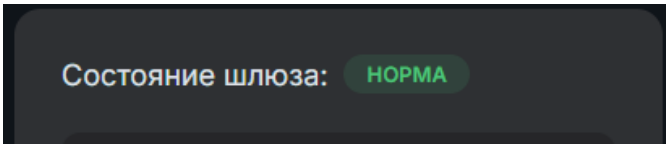


Рисунок 15. Отображение текущего состояния шлюза

4.3. Модальные окна

Некоторые операции в системе выполняются при помощи ввода параметров или подтверждения/отмены действий в модальных окнах.

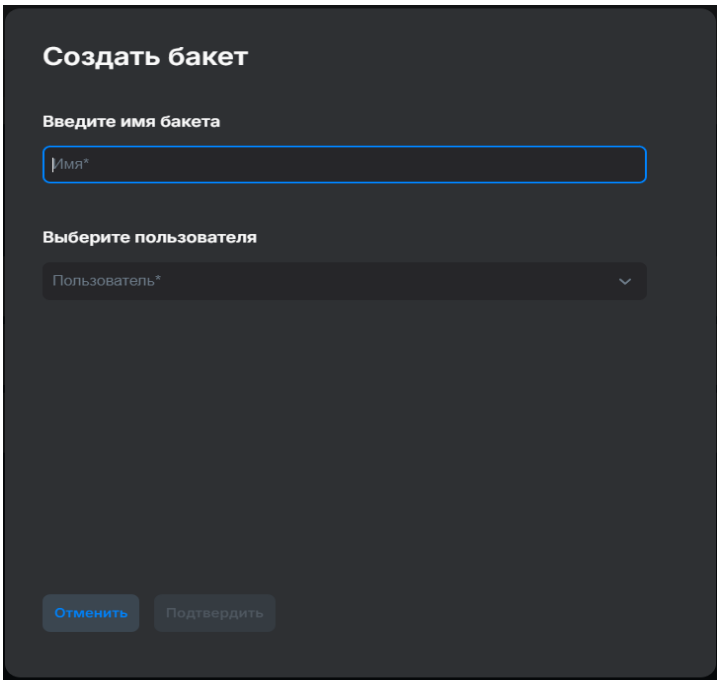


Рисунок 16. Пример модального окна

Закрытие модального окна выполняется нажатием на клавишу [**Esc**] на клавиатуре или нажатием на область за пределами окна. После этого требуется подтвердить закрытие окна.

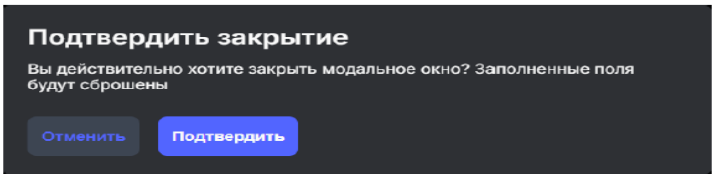


Рисунок 17. Окно подтверждения закрытия окон

4.4. Уведомления

В результате выполнения операций в правой нижней части экрана отображаются всплывающие уведомления. Сообщения об успешно выполненном действии имеют зеленую плашку, уведомления об ошибках — красную.

Рисунок 18. Пример всплывающего уведомления об успешном выполнении

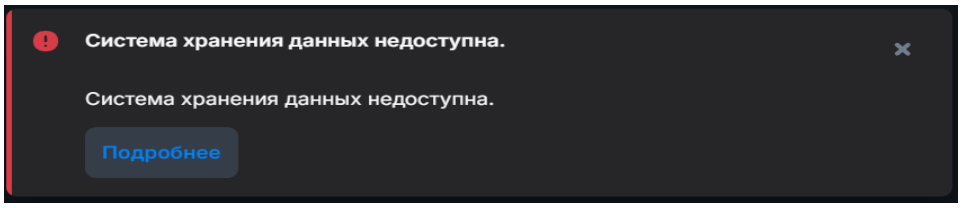


Рисунок 19. Пример всплывающего уведомления об ошибке

При нажатии на кнопку [Подробнее], расположенную в уведомлении об ошибке, откроется модальное окно с подробной информацией об ошибке и рекомендацией по её устранению.

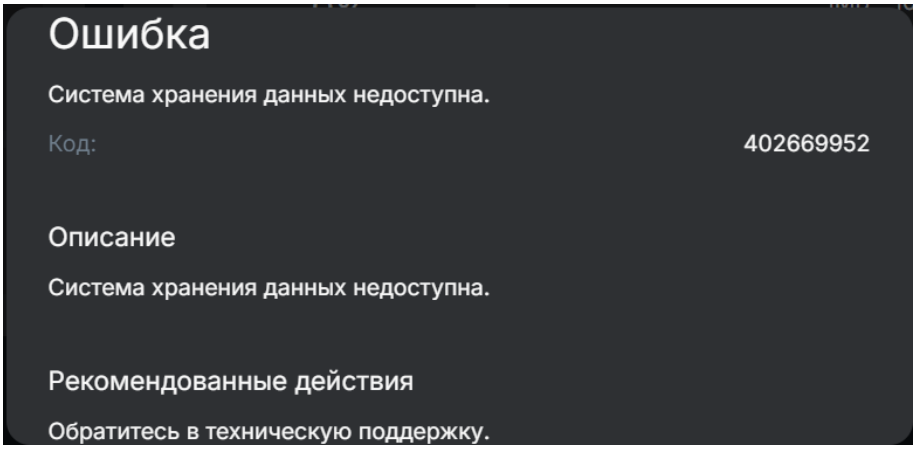


Рисунок 20. Окно с информацией об ошибке

В верхней части панели основного меню расположена область оповещений об ошибках, в которой выводится счетчик не просмотренных событий об ошибках, при нажатии на который выполняется переход на страницу меню Системный журнал.

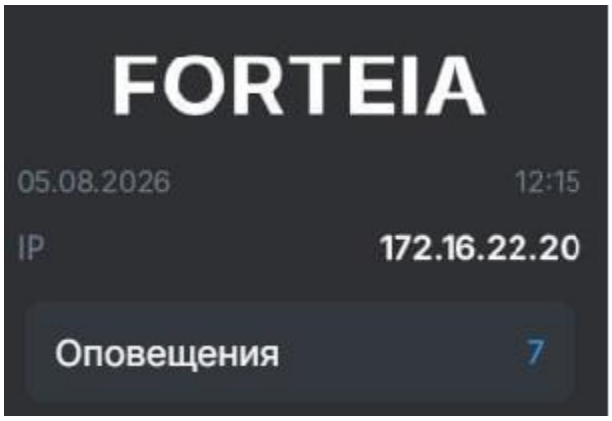


Рисунок 21. Область оповещений на панели основного меню

5. ТИПОВЫЕ ОПЕРАЦИИ

5.1. Получение сведений о шлюзе

Для получения версии шлюза нажмите левой кнопкой мыши в области информации о текущем пользователе, расположенной в нижней части панели главного меню. В открывшемся окне профиля пользователя представлена информация о версии ПО шлюза и версии его веб-приложения (GUI).

5.2. Поиск, фильтрация и сортировка в таблицах

Для поиска и фильтрации данных выводимых в табличном виде, например, списке клиентов, предназначена область **Поиск и фильтры**, расположенная в верхней части страницы меню.

Поиск выполняется после ввода критерия поиска в текстовое поле и нажатия на кнопку [**Найти**]. В списке отобразится результат поиска. Сброс фильтров и отображение всех данных выполняется нажатием на кнопку [**Сбросить**].

Сортировка данных выполняется после нажатия на значок  расположенный перед заголовком столбца таблицы. Повторное нажатие запустит обратную сортировку. Не все столбцы таблицы поддерживают возможность сортировки.

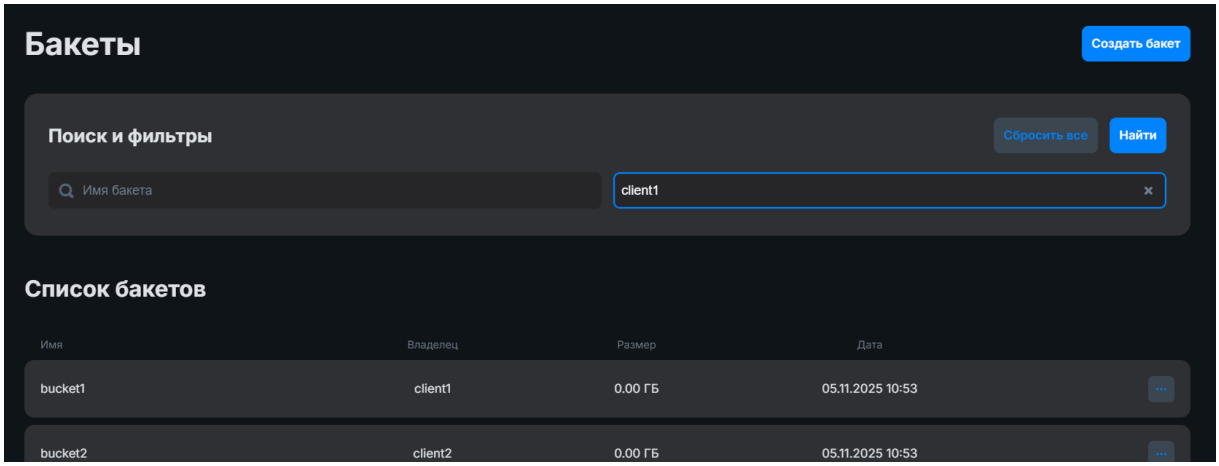


Рисунок 22. Пример области поиска и фильтров

5.3. Ввод и копирование данных

Заполнение текстовых полей выполняется путем ввода текста с клавиатуры или вставки ранее скопированного текста из буфера обмена.

Как правило, при вводе значений в текстовое поле должны использоваться буквы латинского алфавита, при необходимости - в сочетании с цифрами. Исключение составляют поля описаний, которые допускают ввод русских букв.

При выполнении некоторых действий от пользователя требуется скопировать данные выводимые в интерфейсе управления. Для этого предусмотрены специальные кнопки копирования .

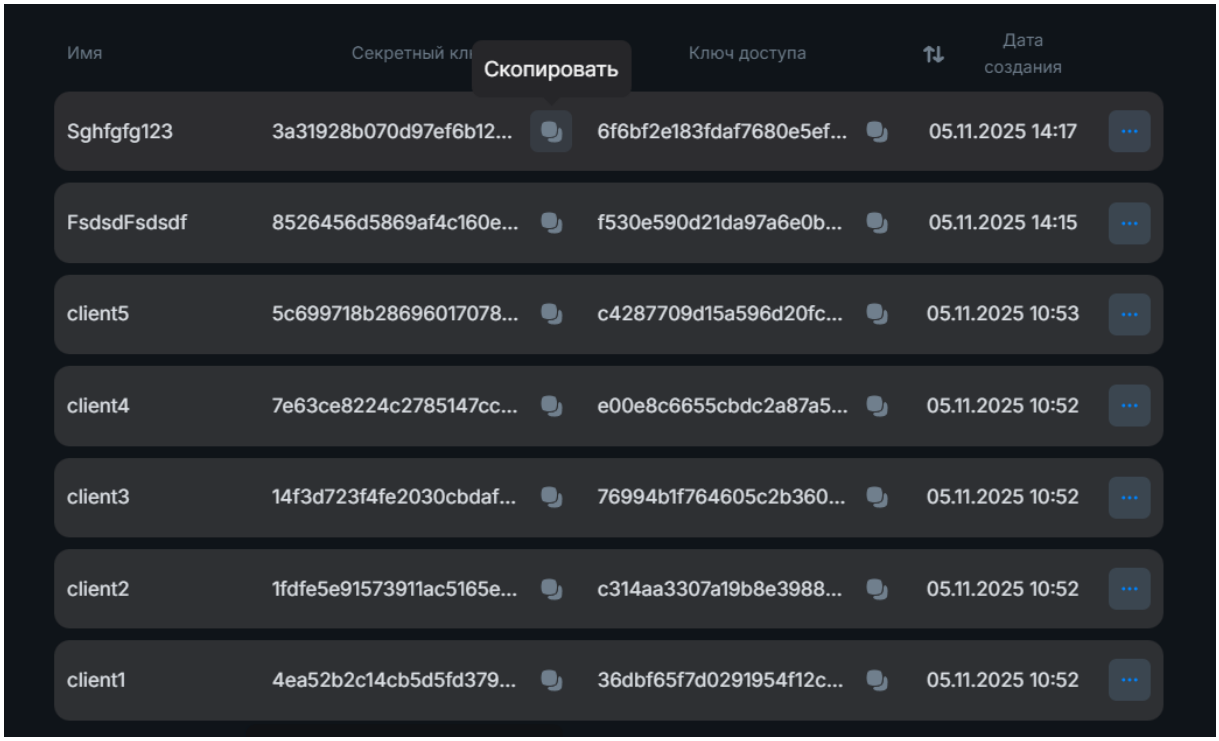


Рисунок 23. Кнопки копирования ключей доступа в списке клиентов

5.4. Контекстное меню действий

Управление объектами в веб-интерфейсе выполняется при помощи контекстного меню действий, которое расположено в правой части каждой строки таблицы. При нажатии на кнопку открывается окно контекстного меню с доступными для данного объекта действиями.

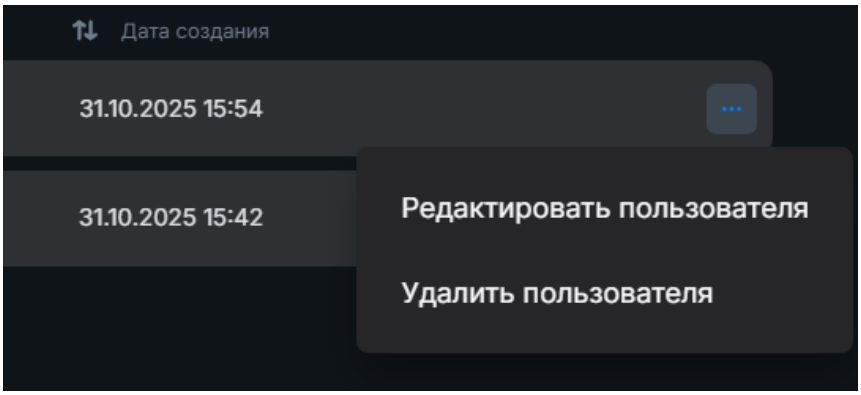


Рисунок 24. Пример контекстного меню действий

6. ВХОД В СИСТЕМУ

Для подключения к веб-интерфейсу шлюза, на компьютере пользователя должен быть установлен веб-браузер. Компьютер пользователя должен быть в одной подсети с сетевым портом шлюза, настроенным для управления через веб-интерфейс.

В адресной строке веб-браузера введите ip адрес и порт интерфейса управления шлюза, например, http://172.16.19.181:8950/.

При успешном соединении, на экране появится окно входа в систему, в которое требуется ввести логин и пароль пользователя веб-интерфейса.

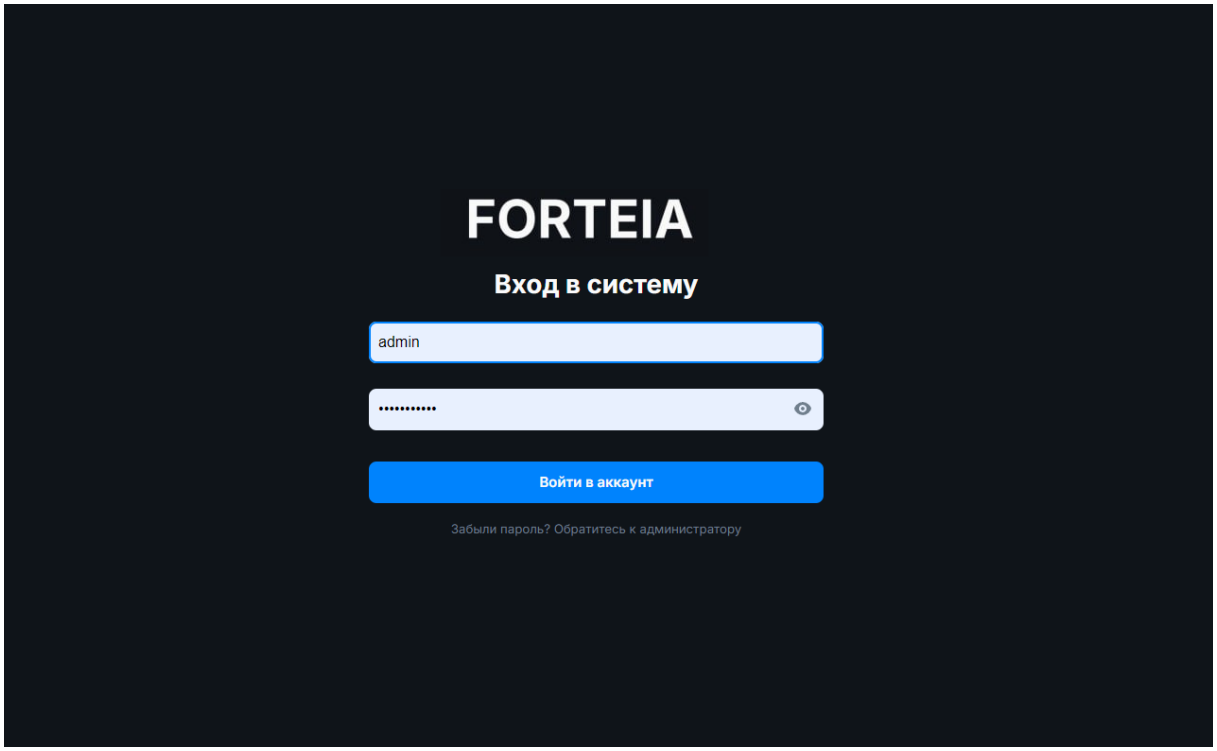


Рисунок 25. Окно входа в систему

При первом запуске шлюза, в системе присутствует только один пользователь – admin.

Введите в окне входа:

логин: **admin**

пароль: **Sd5vok7cls!**

Нажмите на кнопку [**Войти в аккаунт**].

На экране должна появиться стартовая страница интерфейса управления, раздел меню **Система > Статус**.

7. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ ИНТЕРФЕЙСА УПРАВЛЕНИЯ

7.1. Ролевая модель

Ролевая модель доступа к интерфейсу управления включат в себя две роли:

- Администратор – обладает всеми правами доступа к UI;
- Наблюдатель – обладает только правом просмотра настроек системы и выгрузки логов.

Роли назначаются при создании новых пользователей и могут быть переназначены при редактировании свойств пользователя.

7.2. Встроенные пользователи

После установки системы, в ней существует только один пользователь – admin, с ролью администратор системы. Этого пользователя невозможно удалить.

Настоятельно рекомендуется, перед началом эксплуатации шлюза, задать пользователю admin новый пароль.

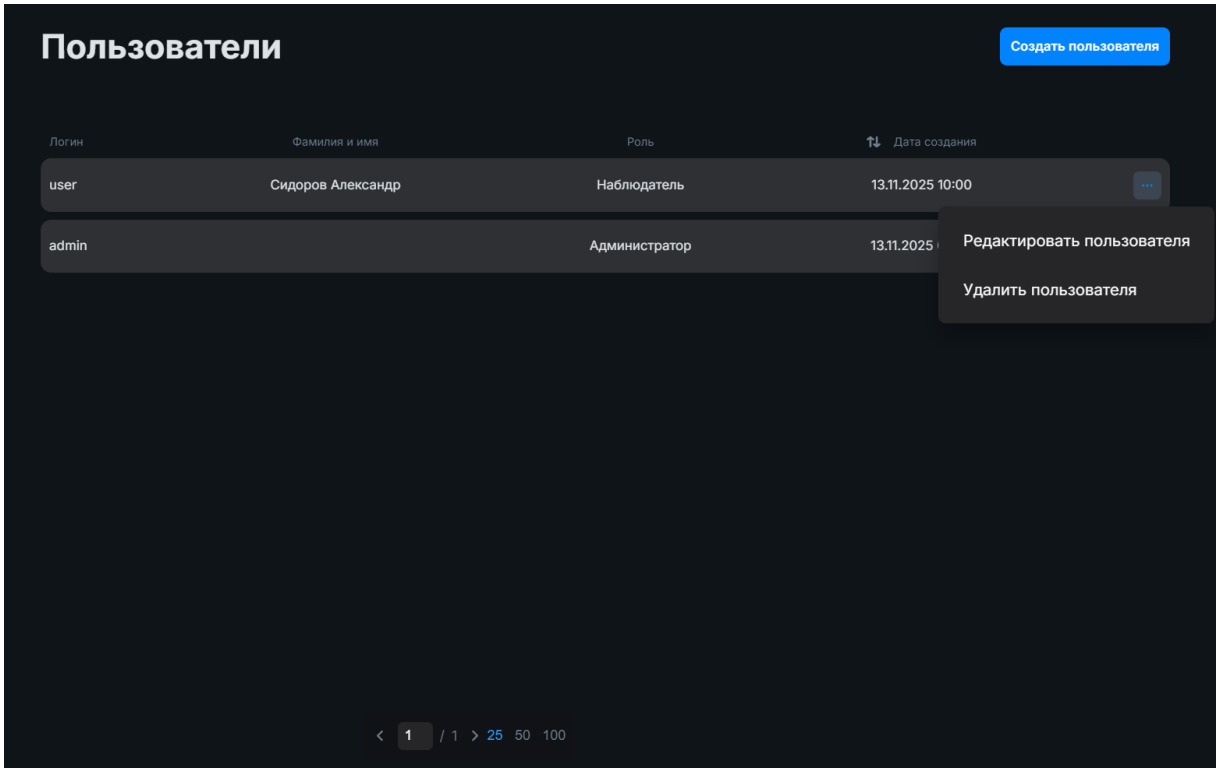


Рисунок 26. Окно пользователей интерфейса управления шлюзом

7.3. Создание нового пользователя

Для создания нового пользователя интерфейса управления, выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Пользователи**;
2. На странице меню, нажмите на кнопку [**Создать пользователя**];
3. В открывшемся окне введите имя и пароль нового пользователя, выберите его роль в системе из списка доступных ролей. Пароль должен быть не короче 14 символов и содержать заглавные буквы, цифры и спецсимволы;
4. Введите информацию о пользователе: фамилию, имя и адрес электронной почты;
5. Нажмите на кнопку [**Подтвердить**];
6. При успешном создании пользователя, появится соответствующее уведомление, и новый пользователь отобразится в списке.

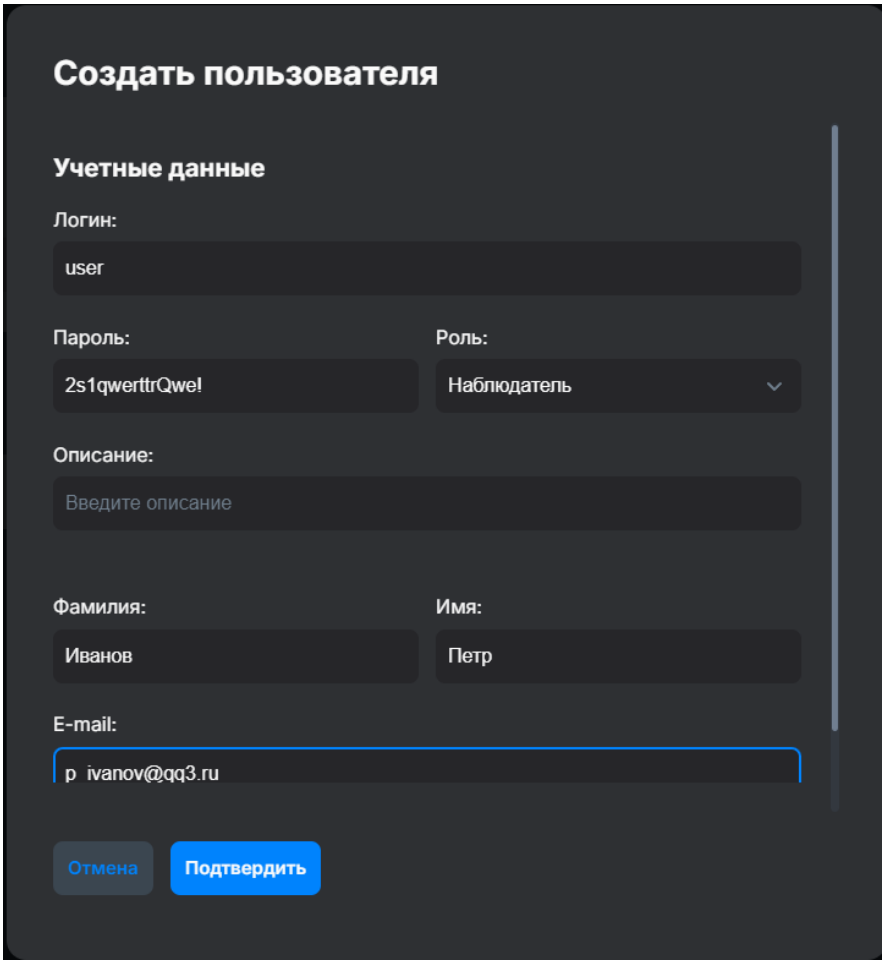


Рисунок 27. Окно создания пользователя

7.4. Редактирование свойств пользователя

Для редактирования свойств пользователя интерфейса управления, выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Пользователи**;
2. На странице меню, выберите из списка нужного пользователя;

3. Откройте контекстное меню для выбранного пользователя, нажав левой кнопкой мыши на значок многоточия, в правой части строки списка;
4. Выберите пункт контекстного меню **Редактировать пользователя**;
5. В открывшемся окне измените нужные свойства;
6. Нажмите на кнопку [**Подтвердить**];
7. При успешном сохранении изменений, появится соответствующее уведомление.

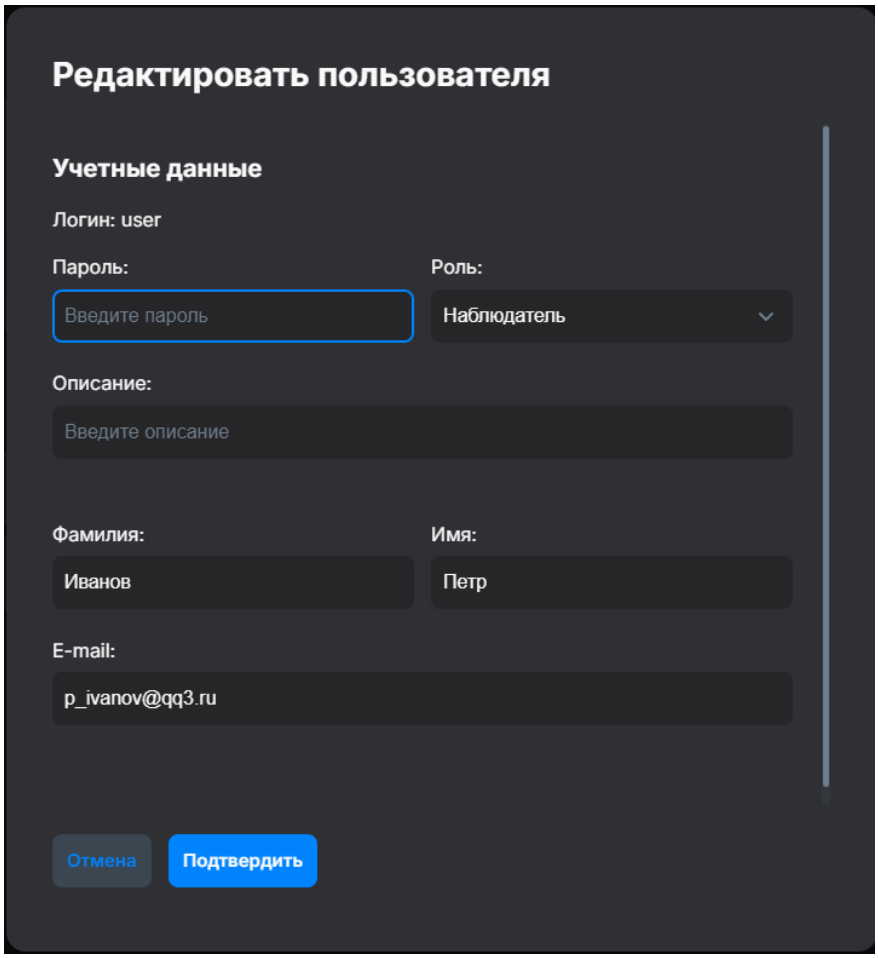


Рисунок 28. Окно редактирования свойств пользователя

7.5. Удаление пользователя

Внимание! Система не позволит удалить встроенного пользователя admin.

Для удаления пользователя интерфейса управления, выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Пользователи**;
2. На странице меню, выберите из списка нужного пользователя;
3. Откройте контекстное меню для выбранного пользователя, нажав левой кнопкой мыши на значок многоточия, в правой части строки списка;

4. Выберите пункт меню **Удалить пользователя**;
5. Подтвердите удаление;

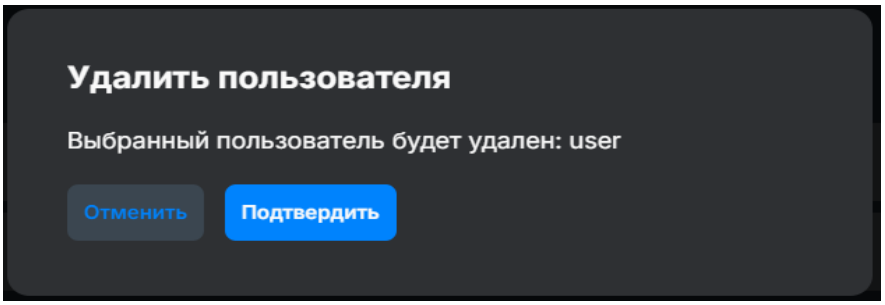


Рисунок 29. Окно подтверждения удаления пользователя

6. При успешном удалении пользователя, появится соответствующее уведомление.

8. УПРАВЛЕНИЕ РЕСУРСАМИ ХРАНЕНИЯ

Для управления ресурсами хранения, подключенными к шлюзу по протоколу NFS, служит страница меню **Администрирование > Ресурсы хранения**.

На данной странице отображается таблица всех подключенных NFS-папок со следующими сведениями:

- **Имя** — путь к папке на NFS-сервере (например, /nfs/rackA/export1);
- **Вес** — числовое значение, влияющее на распределение данных между папками;
- **Размер** — общая ёмкость ресурса в ГБ или ТБ;
- **% использования** — процент занятого места с цветовой индикацией (зелёный — менее 70%, жёлтый — 70–85%, красный — более 85%);
- **Теги** — метки для организации размещения данных (например, tier:Hot, rack:A);
- **Статус** — текущее состояние папки: ONLINE, OFFLINE, DRAINING, DEGRADED и т.п.

Таблица обновляется автоматически с заданным интервалом.

Управление NFS-папками выполняется при помощи кнопок, расположенных в верхней части страницы, а также через контекстное меню действий для каждой папки.

8.1. Добавление NFS-папки

Для подключения новой NFS-папки выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Ресурсы хранения**;
2. Нажмите на кнопку **[Добавить NFS папку]**.
3. В открывшемся окне мастера добавления, на шаге 1, введите **IP-адрес NFS-сервера** в соответствующее поле и нажмите кнопку **[Найти]**;
4. Система выполнит поиск доступных экспортов на указанном сервере и отобразит их список. Выберите одну папку из списка с помощью радиокнопки;
5. Нажмите кнопку **[Далее]** для перехода на шаг 2 мастера;
6. На шаге 2 отобразится информация о выбранной папке (IP-адрес и имя). Задайте следующие параметры:
   - **Вес папки** — целое положительное число (по умолчанию 100), влияющее на распределение данных;
   - **Теги** — метки в формате key:value, разделённые запятыми (например, tier:Hot, rack:B).
7. Нажмите кнопку **[Добавить]**.

При успешном добавлении папки, она появится в таблице со статусом ONLINE, а пользователь получит соответствующее уведомление.

Примечание. Если папка с таким именем уже существует в системе, добавление будет отклонено с сообщением об ошибке.

8.2. Редактирование NFS-папки

Для изменения параметров существующей NFS-папки выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Ресурсы хранения**;
2. В списке папок выберите нужную, откройте контекстное меню (значок многоточия в правой части строки) и выберите пункт **Редактировать**;
3. В открывшемся окне измените значения полей:
   - **Вес** — новое числовое значение;
   - **Теги** — новый набор меток.
4. Нажмите кнопку **[Подтвердить]** для сохранения изменений или **[Отмена]** для отмены.

При успешном сохранении изменений таблица обновится, и пользователь получит соответствующее уведомление.

8.3. Дренирование NFS-папки

Дренирование — это процесс переноса всех данных с выбранной NFS-папки на другие доступные ресурсы с сохранением условий размещения (весов и тегов). Данная операция выполняется перед удалением папки, содержащей данные.

Для запуска дренирования выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Ресурсы хранения**;
2. В списке папок выберите нужную, откройте контекстное меню и выберите пункт **Дренировать**;
3. В открывшемся окне подтверждения отобразится сообщение: *«Все данные с выбранной NFS-папки {Имя папки} будут перенесены на другие доступные ресурсы с сохранением указанных условий размещения.»;*
4. Нажмите кнопку **[Подтвердить]** для запуска процесса или **[Отмена]** для отмены.

После запуска дренирования статус папки изменится на DRAINING. Процесс выполняется асинхронно и не блокирует работу интерфейса. По завершении дренирования статус папки изменится на OFFLINE, и пользователь получит уведомление.

Примечание. Дренирование возможно только для папок, находящихся в состоянии ONLINE или DEGRADED. Нельзя дренировать уже дренируемую папку.

8.4. Удаление NFS-папки

Удаление папки из кластера возможно только после её успешного дренирования (статус OFFLINE) либо если папка не содержит данных.

Для удаления папки выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Ресурсы хранения**;
2. В списке папок выберите нужную, откройте контекстное меню и выберите пункт **Удалить** (пункт активен только для папок, допускающих удаление);
3. В открывшемся окне подтверждения отобразится сообщение: *«NFS папка {Имя папки} будет удалена из кластера.»;*
4. Нажмите кнопку **[Подтвердить]**.

При успешном удалении папка исчезнет из таблицы, и пользователь получит соответствующее уведомление. В случае ошибки (например, папка всё ещё содержит данные) будет выведено сообщение с требованием сначала выполнить дренирование.

9. РАБОТА С КЛИЕНТАМИ

Для создания и управления пользователями S3 API служит страница меню **Администрирование > Клиенты**.

9.1. Создание клиента

Внимание! В имени клиента допускаются только английские заглавные и строчные буквы и цифры. Имя должно начинаться с буквы и не превышать в длину 30 символов.

Для создания нового клиента, выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню, нажмите на кнопку [**Создать клиента**];
3. Введите имя клиента;
4. Введите адрес электронной почты и при необходимости описание;
5. Нажмите на кнопку [**Создать**];
6. При успешном создании клиента, появится соответствующее уведомление.

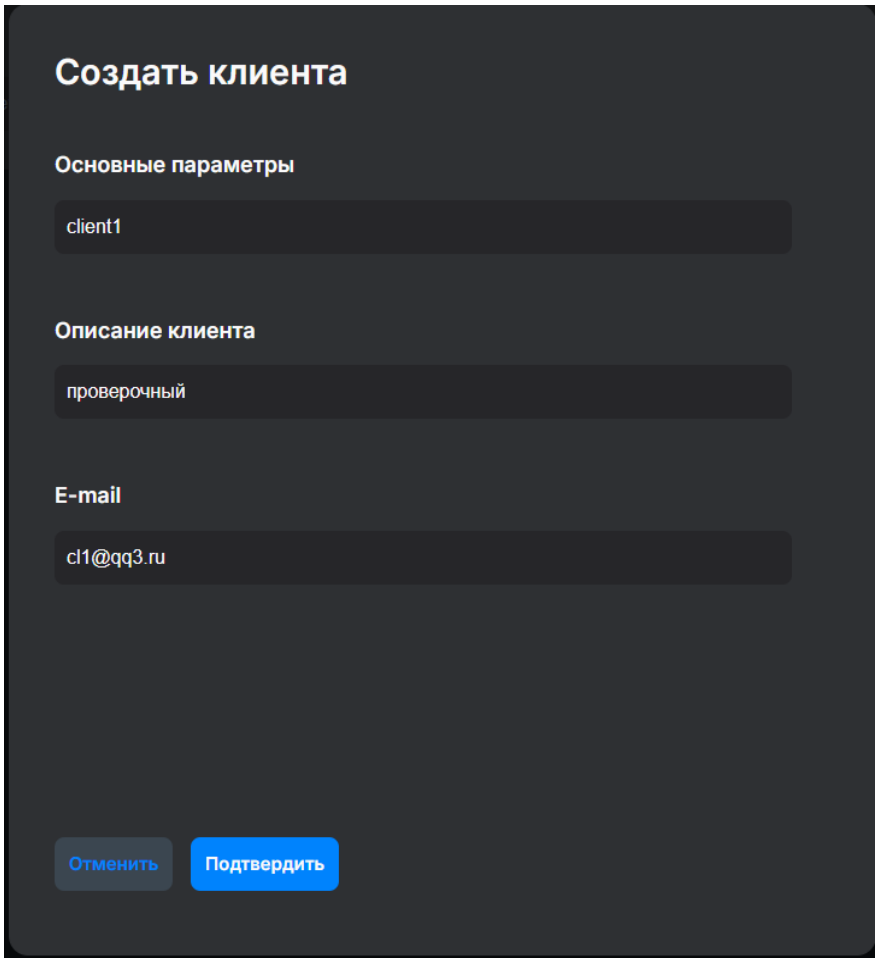


Рисунок 30. Окно создания клиента

9.2. Получение ключей доступа клиента

Ключи доступа для клиента генерируются в момент его создания. Для получения Access key и Secret key выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню Клиенты, выберите нужное имя клиента в списке;
3. Нажмите на значок **Копировать**  расположенный справа от поля Access key. Ключ доступа будет скопирован в буфер обмена;
4. Аналогичным способом скопируйте Secret key.

Обратите внимание на то, что в списке не отображаются полные значения ключей, и их можно получить только при помощи копирования в буфер обмена.

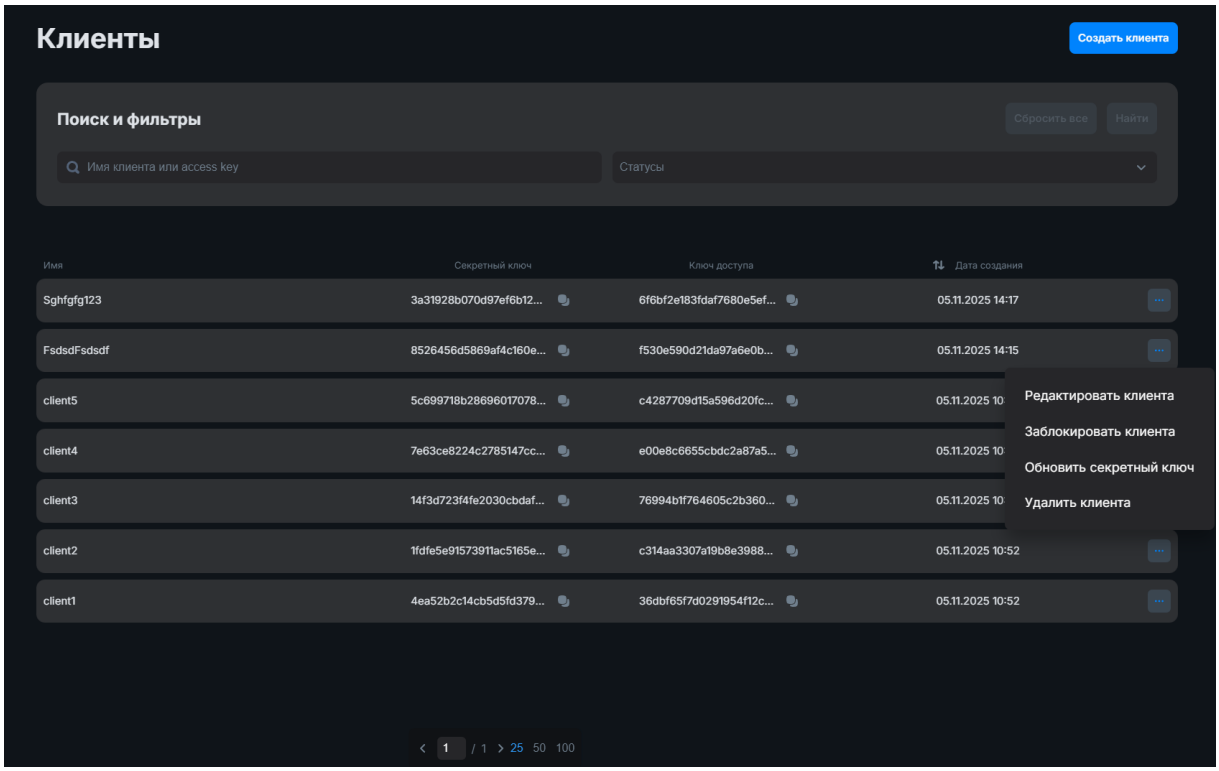


Рисунок 31. Окно страницы меню Клиенты

9.3. Редактирование свойств клиента

Для редактирования свойств клиента выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню Клиенты, выберите нужное имя клиента в списке;
3. В контекстном меню, выберите пункт **Редактировать клиента**;
4. В открывшемся окне редактирования свойств клиента, внесите изменения в поля **Описание** и **Адрес электронной почты**;

5. При необходимости, назначьте другую политику доступа, выбрав её из списка имеющихся. Используйте возможность поиска по имени политики;
6. Нажмите на кнопку [**Подтвердить**], для сохранения сделанных изменений;
7. При успешном сохранении изменений, появится соответствующее уведомление.

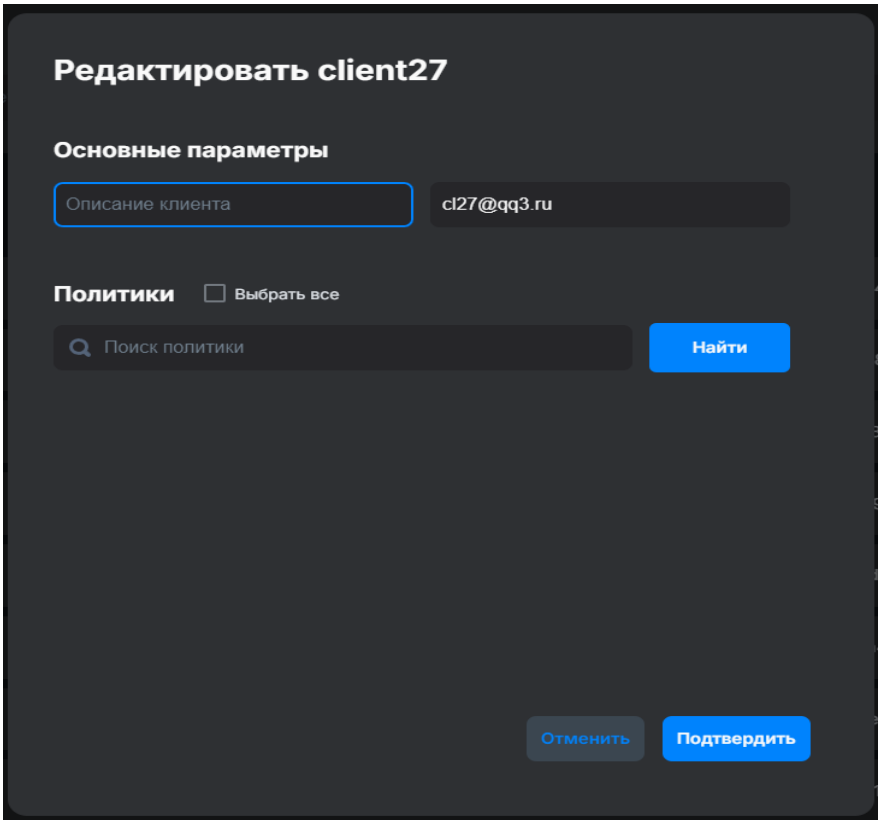


Рисунок 32.Окно редактирования свойств клиента

9.4. Удаление клиента

Внимание! Система не позволит удалить клиента, у которого имеются бакеты. Перед удалением клиента, удалите вначале все бакеты, владельцем которых он является.

Для удаления клиента выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню Клиенты, выберите нужное имя клиента в списке;
3. В контекстном меню, выберите пункт **Удалить клиента**;
4. Подтвердите удаление клиента;

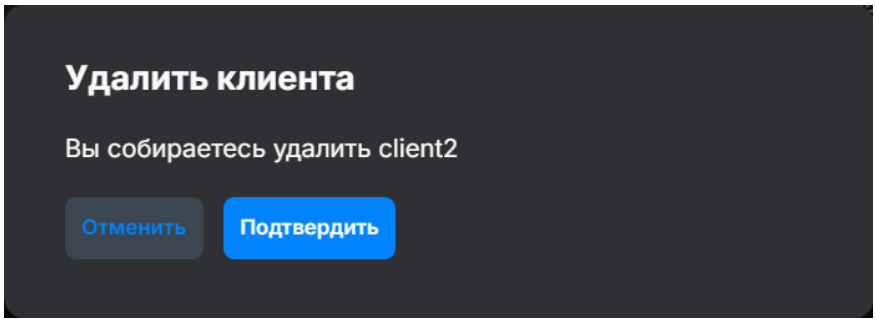


Рисунок 33. Окно подтверждения удаления клиента

5. При успешном удалении клиента, появится соответствующее уведомление.

9.5. Обновление Secret key

При потере или компрометации секретного ключа клиента, система позволяет Администратору заменить секретный ключ на новый.

Для обновления Secret key выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню Клиенты, выберите нужное имя клиента в списке;
3. В контекстном меню, выберите пункт **Обновить секретный ключ**;
4. Подтвердите создание нового ключа;
5. При успешном создании ключа, появится соответствующее уведомление;
6. Секретный ключ выбранного клиента будет заменен на новый.

9.6. Блокировка клиента

Система позволяет заблокировать доступ клиенту. Для этого выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню **Клиенты**, выберите нужное имя клиента в списке;
3. В контекстном меню, выберите пункт **Заблокировать клиента**;
4. При успешном выполнении команды, появится соответствующее уведомление.

Перед именем клиента в списке клиента отобразится значок замка  и доступ выбранному клиенту будет заблокирован. Строка заблокированного клиента в списке станет серого цвета.

В контекстном меню, пункт **Заблокировать клиента** изменит название на **Разблокировать клиента**.

Заблокированный клиент не сможет получить доступ к S3-API шлюза, пока на будет вновь разблокирован.

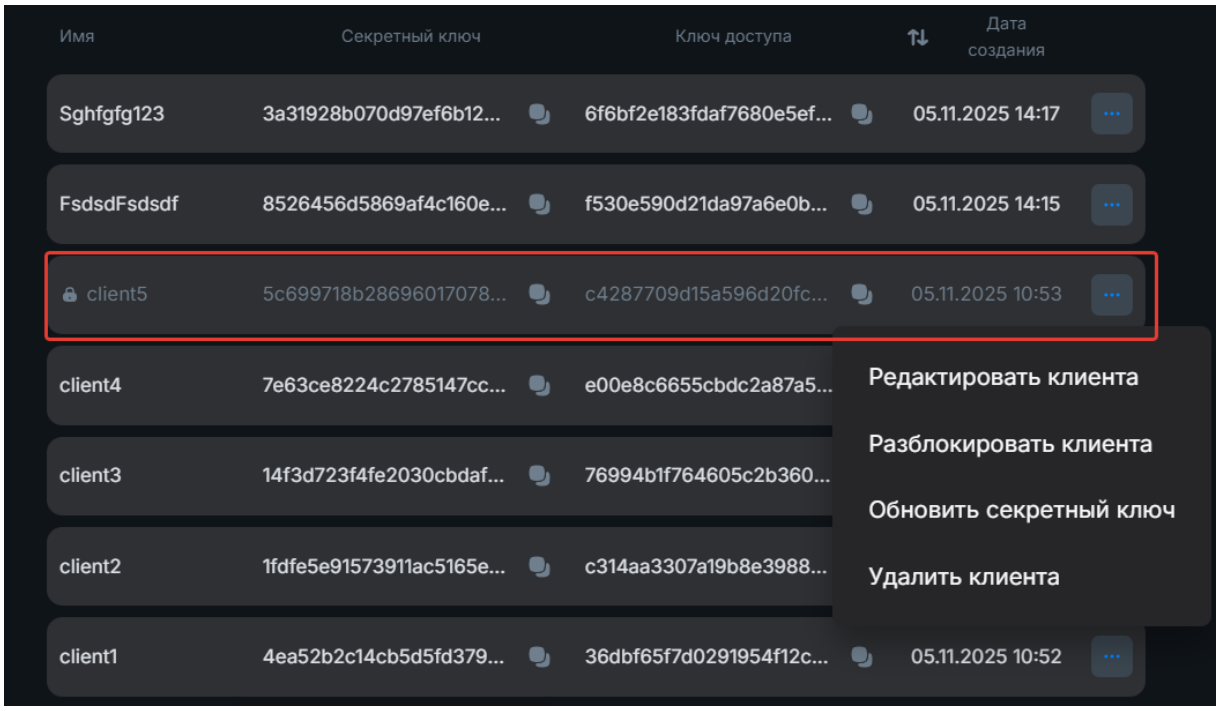


Рисунок 34. Отображение заблокированного клиента

9.7. Разблокирование клиента

Заблокированный клиент может быть разблокирован администратором, когда это потребуется.

Найти всех заблокированных клиентов можно используя фильтр статусов. Для этого, в области **Поиск и фильтры**, выберите статус Заблокированные и нажмите на кнопку [**Найти**].

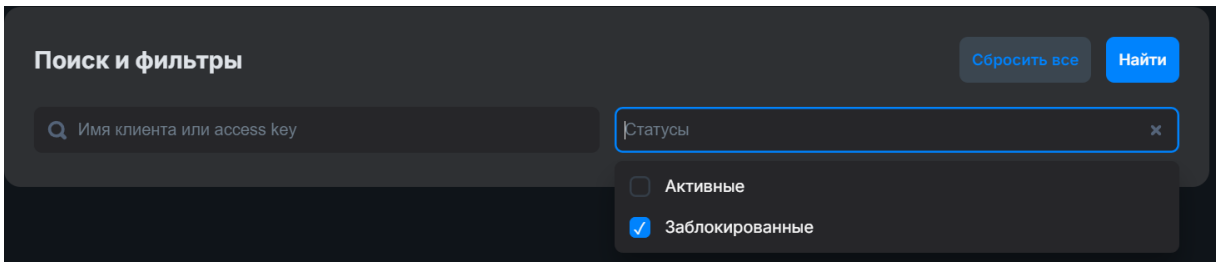


Рисунок 35. Выбор статуса клиентов в области фильтров

В списке клиентов отобразятся только заблокированные клиенты.

Для разблокировки клиента выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню Клиенты, выберите нужное имя клиента в списке;
3. В контекстном меню, выберите пункт **Разблокировать клиента**;
4. При успешном выполнении команды, появится соответствующее уведомление.

Перед именем клиента в списке клиента исчезнет значок замка и доступ выбранному клиенту будет разблокирован.

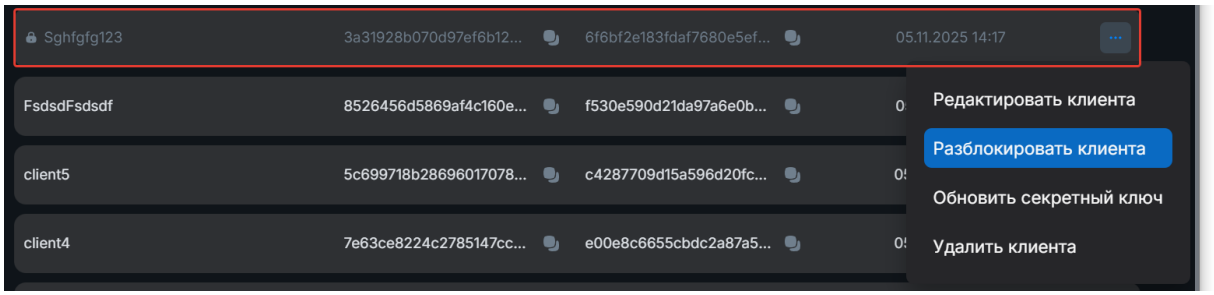


Рисунок 36. Пункт разблокировки клиента в контекстном меню списка клиентов

10. РАБОТА С БАКЕТАМИ

Для создания и управления бакетами служит страница меню Бакеты.

Бакет — это контейнер для хранения объектов (файлов) с гибкими настройками доступа. Имя бакета должно быть уникально для системы.

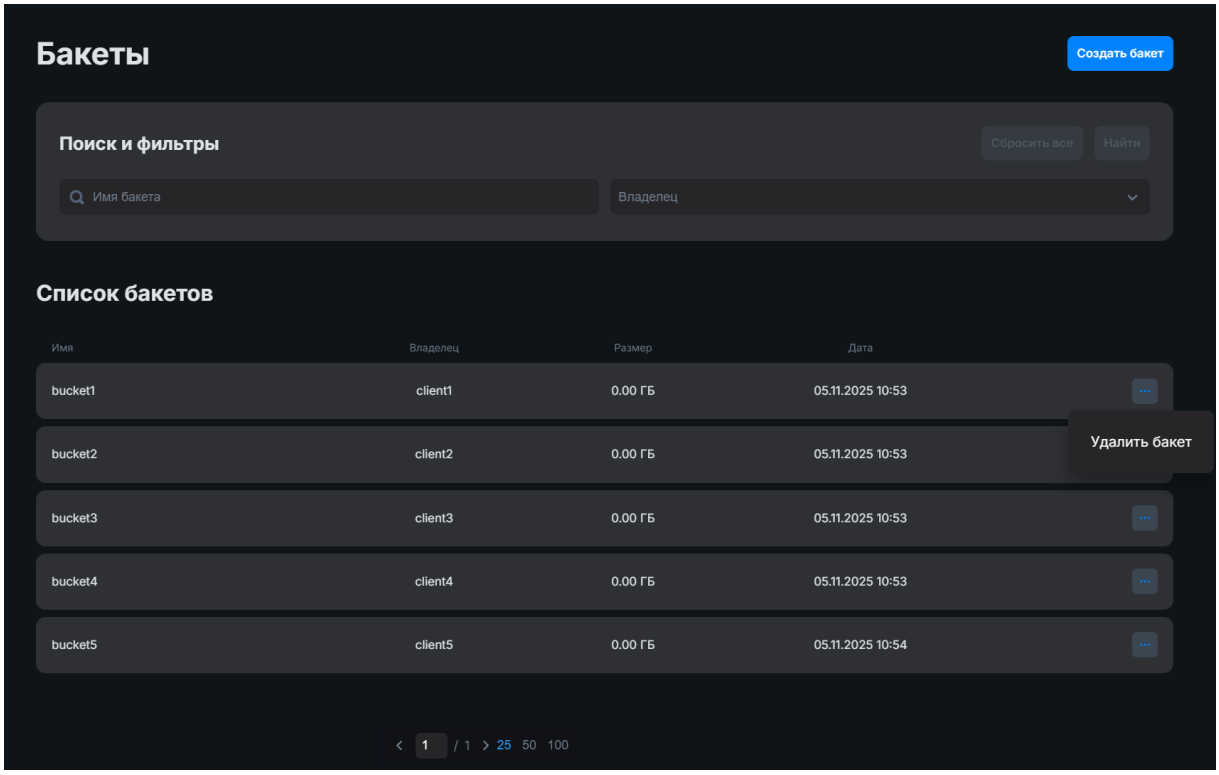


Рисунок 37. Окно управления бакетами

10.1. СОЗДАНИЕ БАКЕТА

Внимание! Имя бакета может состоять только из латинских строчных букв, цифр, точек (.) и дефисов (-).

Для создания нового бакета выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Бакеты**;
2. Нажмите на кнопку [**Создать бакет**];
3. В открывшемся окне создания бакета введите уникальное имя бакета и выберите клиента, который будет владельцем бакета.
4. Нажмите на кнопку [**Подтвердить**];
5. При успешном создании бакета, появится соответствующее уведомление.

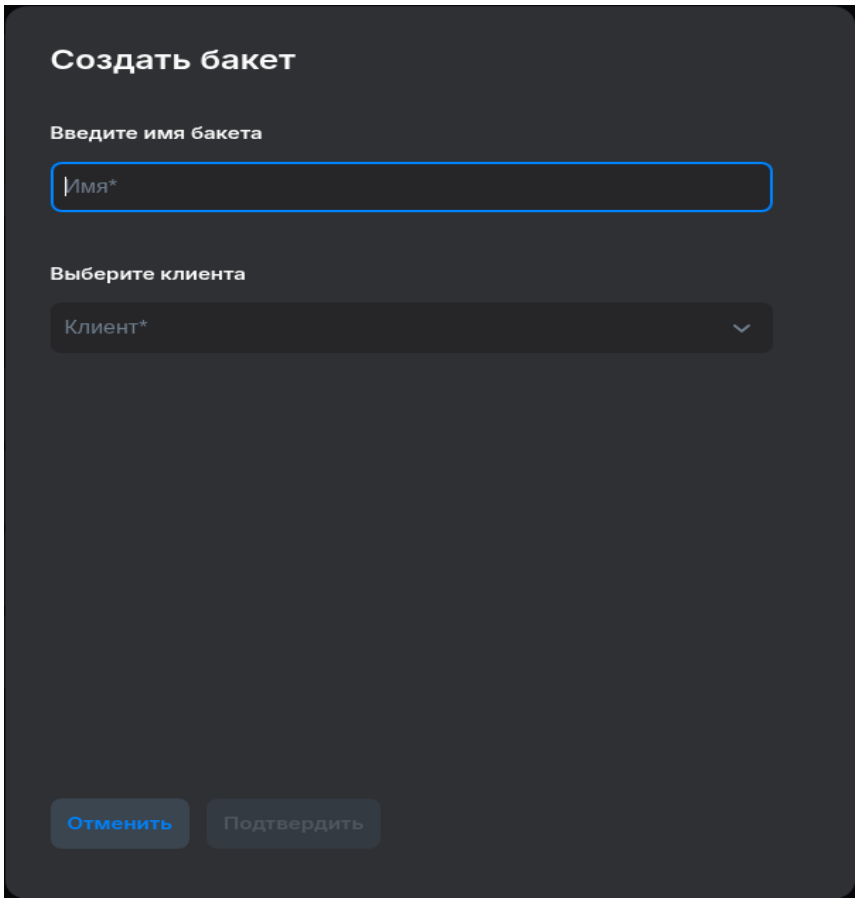


Рисунок 38. Окно создания бакета

10.2. Удаление бакета

Внимание! Система не позволит удалить бакет, в котором находятся объекты.

Для удаления бакета выполните следующие действия:

1. На странице меню **Администрирование > Бакеты**, выберите в списке нужное имя бакета. Используйте при необходимости поиск по имени или по владельцу бакета, расположенный на панели **Поиск и фильтры**;
2. В контекстном меню, выберите пункт **Удалить бакет**;
3. Подтвердите удаление бакета;

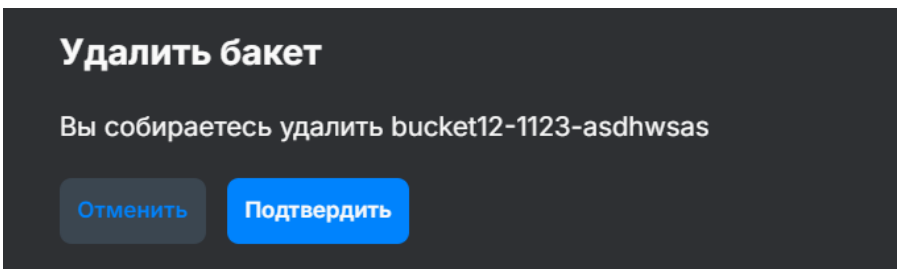


Рисунок 39. Окно подтверждения удаления бакета

4. При успешном удалении бакета, появится соответствующее уведомление.

11. РАБОТА С ПОЛИТИКАМИ

В текущей версии FORTEIA реализованы упрощенные Managed Policies.

Managed Policy (управляемая политика) — это тип IAM-политики, который создается пользователем, но существует как отдельный, независимый ресурс, который можно прикреплять к нескольким клиентам (пользователям S3 API). Изменение в политике применяется ко всем привязанным клиентам.

Основным элементом политики являются Statement, в которых декларируются правила доступа.

Statement — это неделимый элемент правила доступа, который однозначно отвечает на четыре вопроса:

- Кто? (Principal);

- Что может сделать? (Action);

- Над чем? (Resource);

- Разрешить или запретить? (Effect).

Ключевые поля внутри Statement:

Effect - определяет, является ли правило разрешающим ("Allow") или запрещающим ("Deny");

Action - перечень конкретных API-операций, к которым применяется правило, например: "s3:GetObject", "s3:PutObject", "s3:ListBucket";

Resource – в данном случае, это бакет, к которому предоставляется доступ.

В Managed Policy не используется поле Principal, так как это и есть клиент, к которому привязана политика.

Политика может содержать несколько Statement.

Внимание! При настройке политик доступа, следуйте принципу наименьших привилегий.

В текущей версии FORTEIA политики создаются только при помощи конструктора.

Для создания и редактирования политик доступа к бакетам служит страница меню **Администрирование > Политики**.

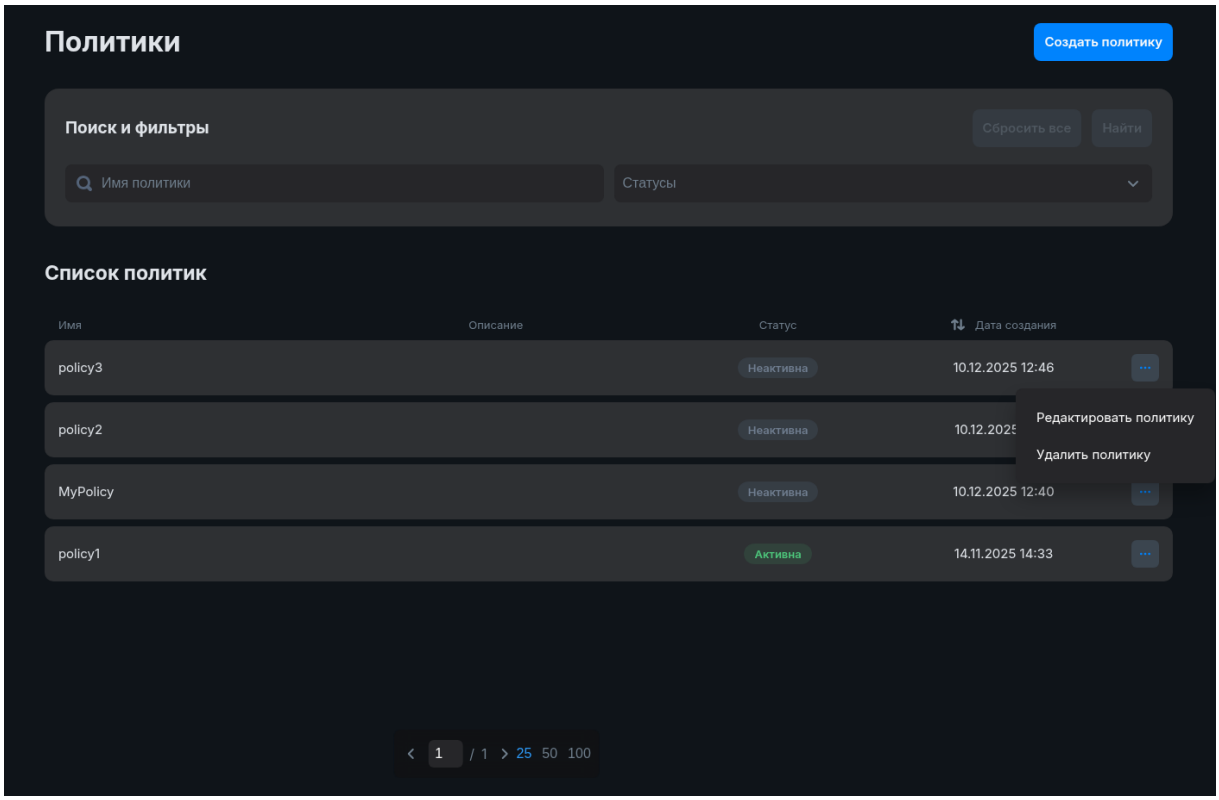


Рисунок 40. Окно управления политиками

Статус политики (активна/неактивна) показывает используется ли политика в данный момент времени.

11.1. Создание политики

Политика описывает что именно разрешается делать клиенту.

Внимание! Имя политики должно начинаться с буквы и состоять из латинских букв и цифр. Длина имени не более 30 символов.

Для создания новой политики доступа выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Политики**;
2. Нажмите на кнопку [**Создать политику**];
3. В открывшемся окне мастера создания политики введите уникальное имя политики и её краткое описание;

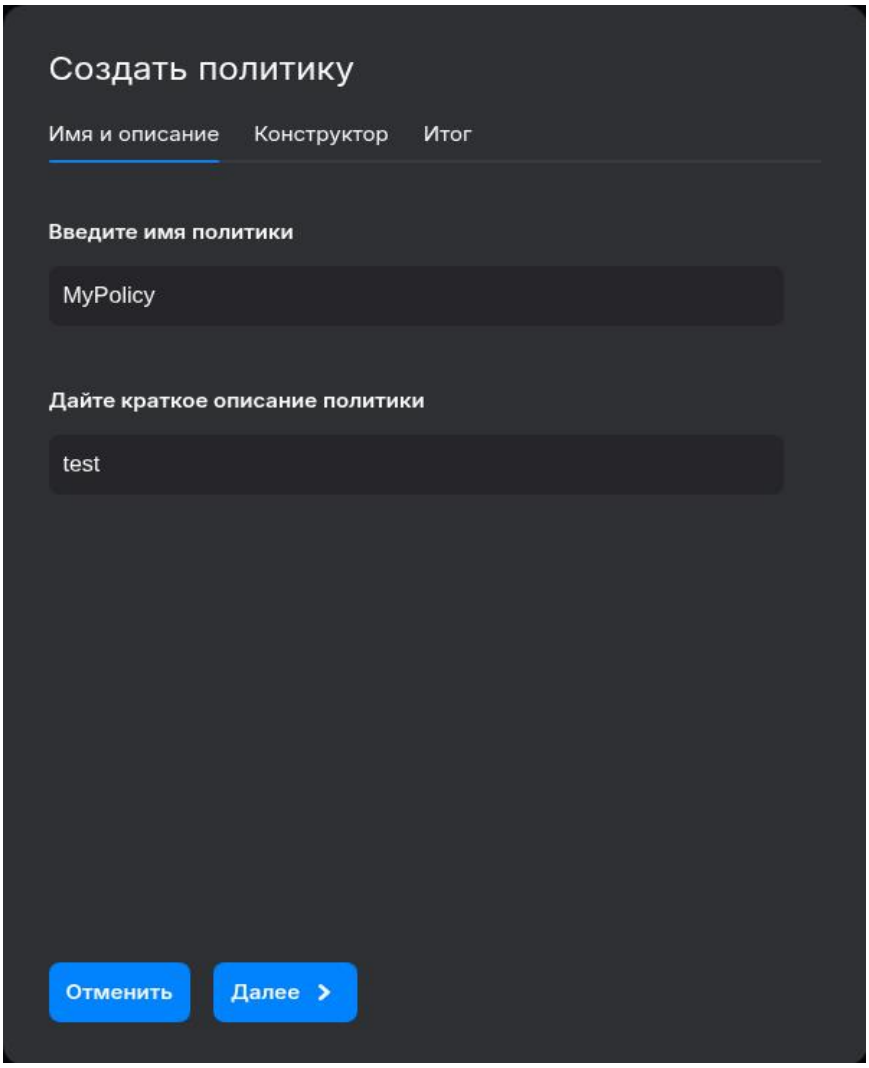


Рисунок 41. Окно мастера создания политики

4. Нажмите на кнопку [**Далее**] для перехода на следующую страницу мастера;
5. Создайте новый Statement, нажав на кнопку [**Создать**] находящуюся справа от имени **Statement1**;
6. В открывшейся области создания **Statement**, выберите эффект от применения данного Statement: **Allow** – разрешено, или **Deny** – запрещено;
7. Нажмите левой кнопкой мыши на области **Actions** и отметьте в списке S3 операции на которые будет распространятся действие политики;
8. Нажмите левой кнопкой мыши на области **Resourse** и отметьте в списке бакеты, на которые будет распространятся действие политики;
9. При необходимости аналогичным способом создайте дополнительные **Statement**, прокрутив панель со свойствами **Statement1** вниз до тех пор, пока не появится имя Statement2 и кнопка [**Создать**];

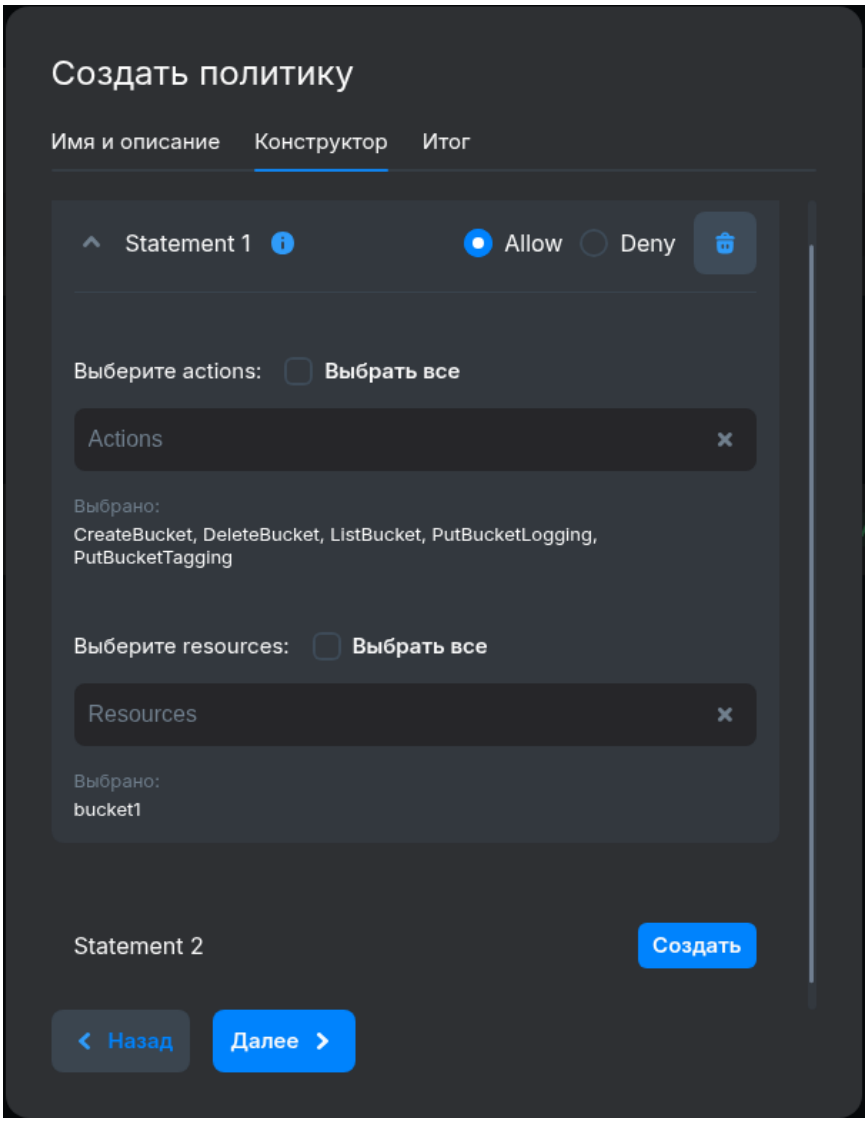


Рисунок 42. Окно мастера создания политики

10. Нажмите на кнопку [**Далее**] для перехода на следующую страницу мастера;
11. На завершающей странице мастера будет отображена итоговая информации о создаваемой политике;
12. Если требуется внести исправления, воспользуйтесь кнопкой [**Назад**], для перехода к нужной странице мастера;
13. Если нет ошибок, нажмите на кнопку [**Подтвердить**] для создания политики;

*Для удаления ошибочно созданного Statement, нажмите на кнопку  (Корзина), расположенную справа, напротив его имени.

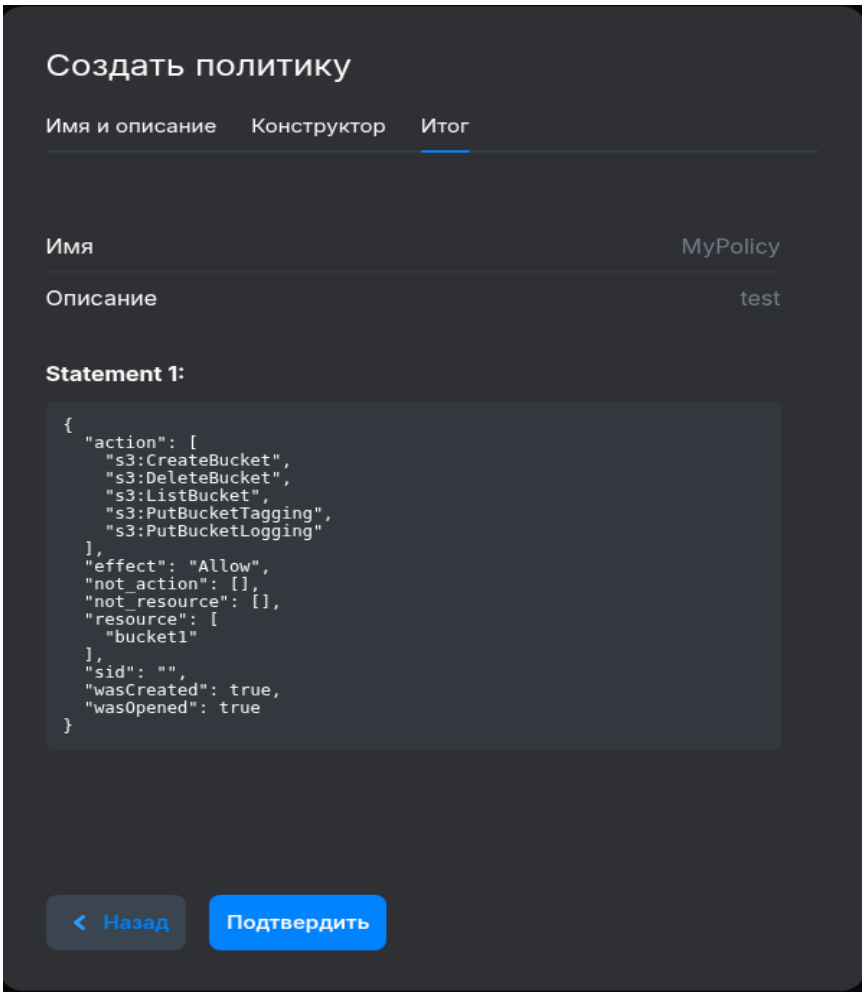


Рисунок 43. Окно мастера создания политики

14. При успешном создании политики, появится соответствующее уведомление.

11.2. Редактирование политики

Изменения, внесенные в политику, будут применены ко всем привязанным к ней клиентам.

Для редактирования политики выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Политики**;
2. На странице меню Клиенты, выберите в списке нужное имя политики;
3. В контекстном меню, выберите пункт **Редактировать политику**;
4. В открывшемся окне мастера редактирования политики, внесите необходимые изменения переключаясь между вкладками мастера при помощи кнопок навигации, аналогично тому, как это описано в пункте **Создание политики**;
5. Подтвердите сделанные изменения, нажав на кнопку [**Подтвердить**] на последней вкладке мастера;
6. При успешном сохранении изменений, появится соответствующее уведомление.

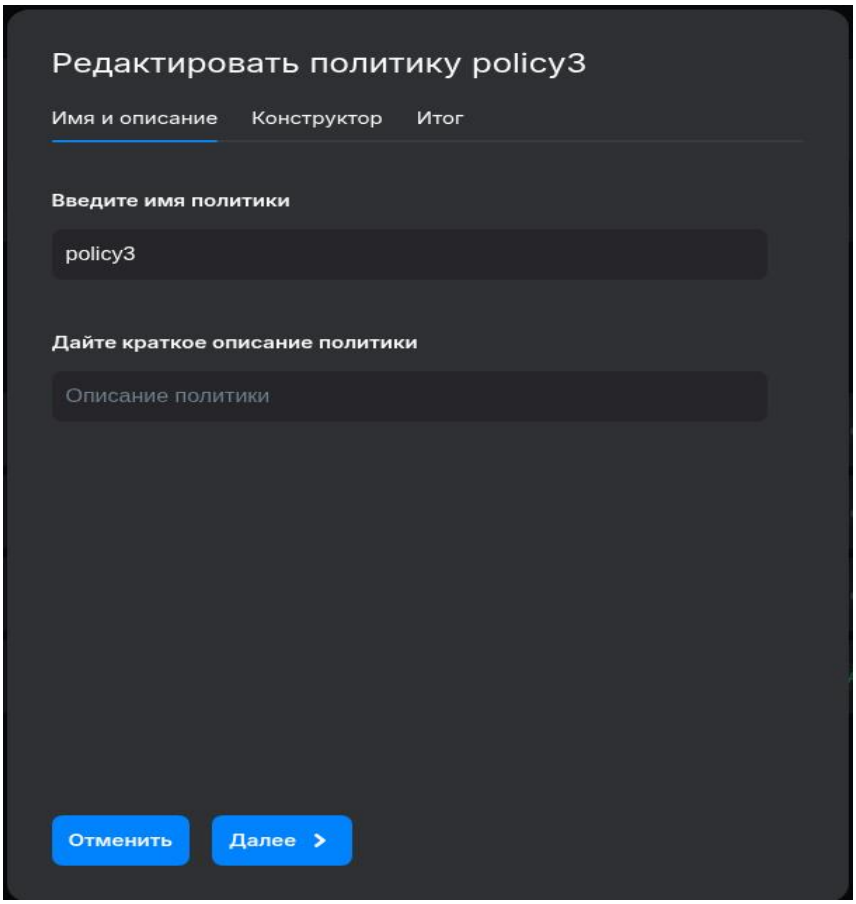


Рисунок 44. Окно мастера редактирования политик

11.3. Привязка политики к клиенту

Созданный клиент по умолчанию является владельцем своих бакетов и может записывать, читать и удалять в них данные. Однако ему не доступны другие возможности, например, создание нового бакета через S3 API. Для предоставления клиенту такой возможности, требуется создать политику, явно разрешающую эти действия, после чего привязать эту политику к клиенту.

Для привязки политики к клиенту выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Клиенты**;
2. На странице меню **Клиенты**, выберите нужное имя клиента в списке;
3. В контекстном меню, выберите пункт **Редактировать клиента**;
4. В открывшемся окне редактирования свойств клиента, в области **Политики**, отметьте флажком нужную политику. Если список большой, для удобства поиска воспользуйтесь возможностью поиска по имени политики;
5. Нажмите на кнопку [**Подтвердить**];
6. При успешном сохранении изменений, появится соответствующее уведомление.

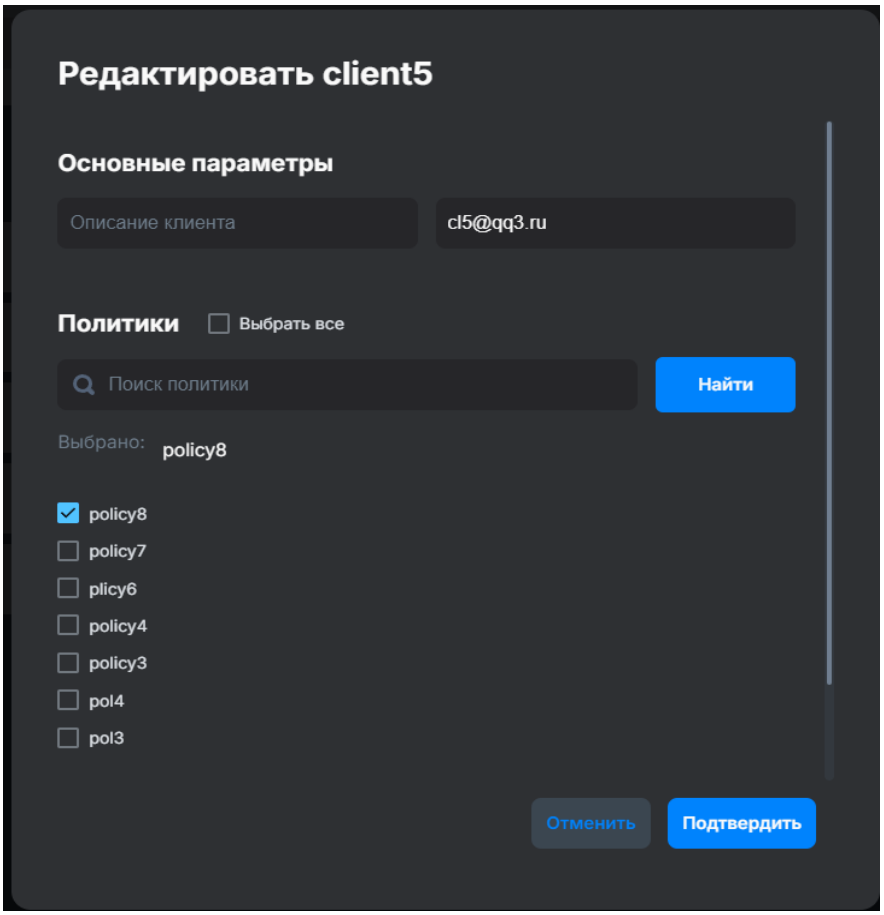


Рисунок 45. Назначение политики клиенту при редактировании его свойств

11.4. Удаление политики

Внимание! Система не разрешает удаление активной политики (которая привязана к клиенту).

Для удаления политики выполните следующие действия:

1. Перейдите на страницу меню **Администрирование > Политики**;
2. На странице меню **Клиенты**, выберите в списке нужное имя политики;
3. В контекстном меню, выберите пункт **Удалить политику**;
4. Подтвердите удаление политики;

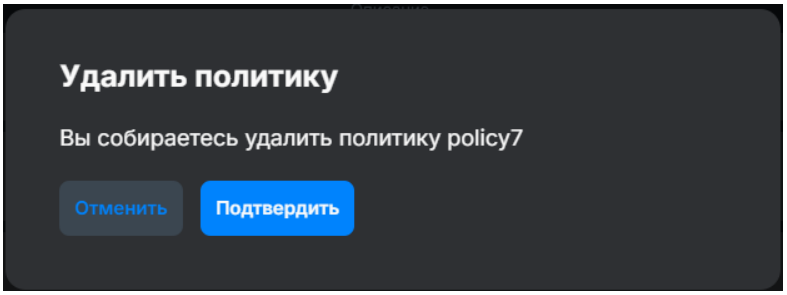


Рисунок 46. Окно подтверждения удаления

5. При успешном удалении политики, появится соответствующее уведомление.

12. МОНИТОРИНГ И ЛОГИРОВАНИЕ

12.1. Мониторинг здоровья

Мониторинг здоровья шлюза проверяет доступность базы метаданных и ресурса СХД на который записываются данные.

Результат проверки выводится в виде состояния здоровья шлюза, который может принимать два значения: Норма или Ошибка.

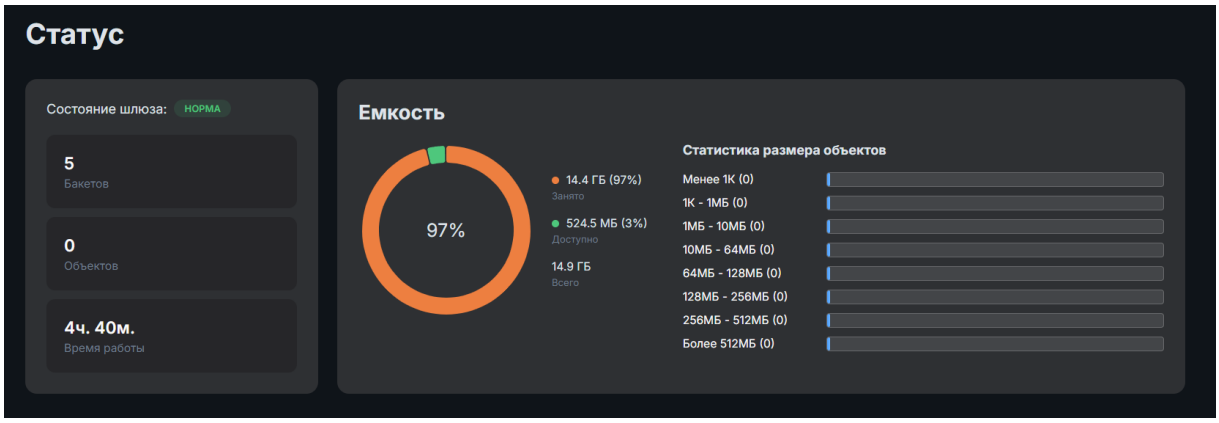


Рисунок 47. Окно меню Статус, с выводом состояния здоровья шлюза

12.2. Просмотр журнала событий

События, вызванные действиями пользователя в интерфейсе управления шлюзом, заносятся в журнал событий.

На странице меню **События**, расположены две вкладки: [**Журнал событий**] и [**Журнал аудита**].

Для просмотра журнала событий, перейдите на страницу меню **Система > События**.

Системные события имеют три статуса:

- **Уведомление** – информационные сообщения;
- **Предупреждение** – сообщения о потенциальной проблеме;
- **Ошибка** – сообщения о проблемах в работе системы.

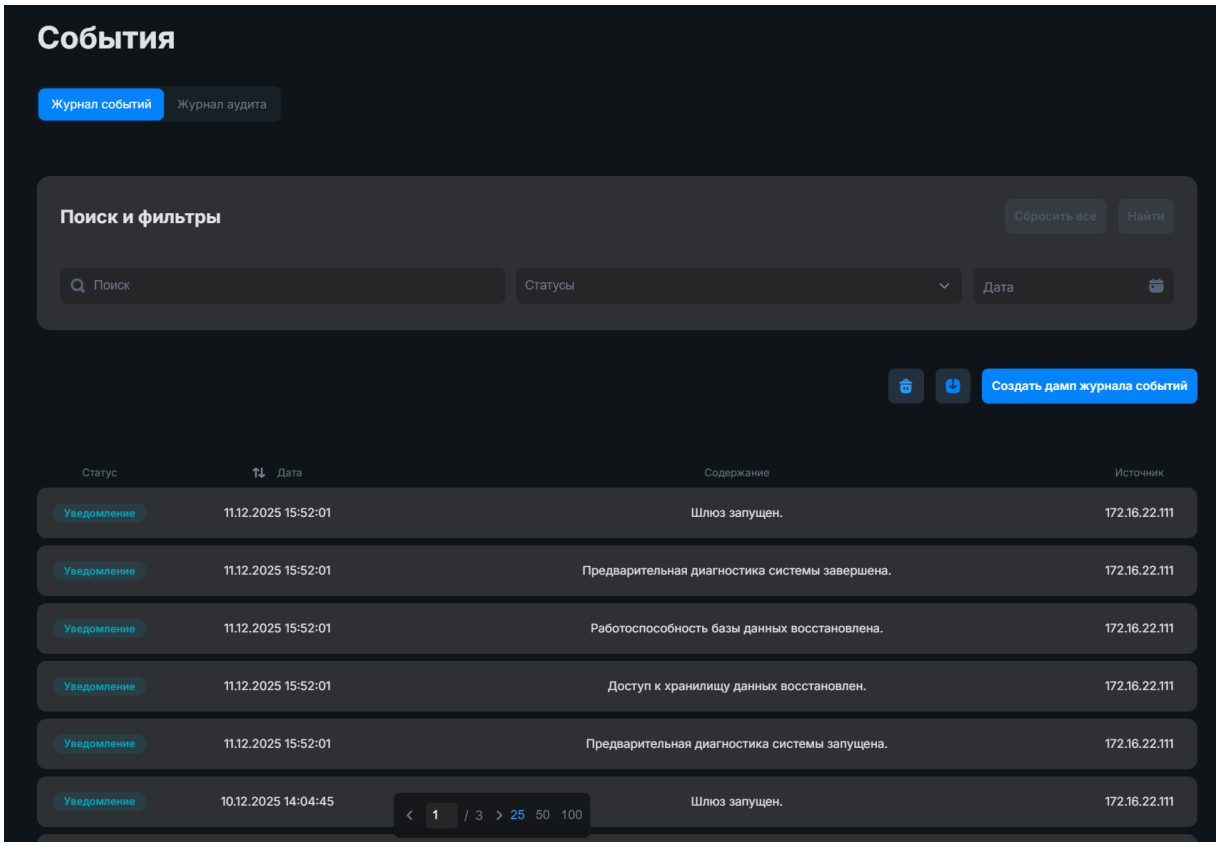


Рисунок 48. Окно меню События - Журнал событий

12.3. Просмотр журнала аудита

Вкладка [**Журнал аудита**], расположенная на странице меню События, содержит список записей событий аудита безопасности связанных с доступом пользователей в веб-интерфейс шлюза.

Внимание! События, генерируемые при работе клиентов с S3 объектами логируются, но в веб-интерфейсе не отображаются!

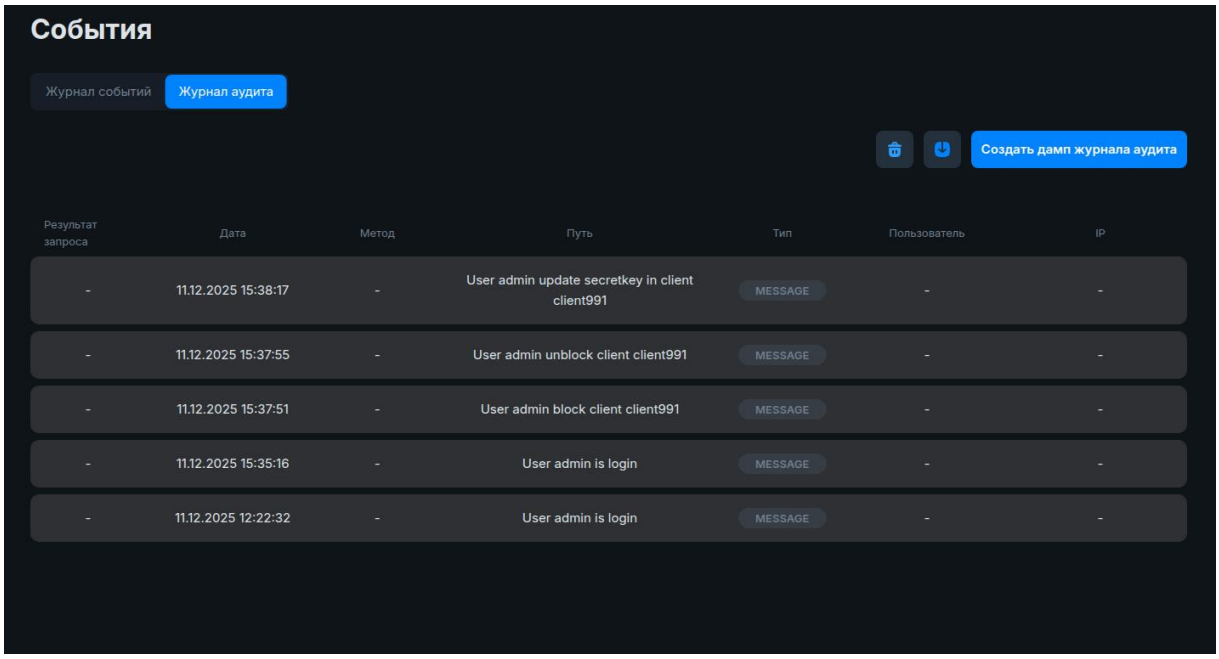


Рисунок 49. Окно меню События - Журнал аудита

12.4. Выгрузка лога событий

Система позволяет создать дамп событий за указанный интервал времени и выгрузить его в виде архива.

В правой части страницы меню, расположены кнопки для удаления, выгрузки и создания архива логов.

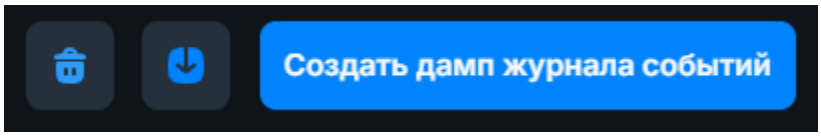


Рисунок 50. Кнопки для создания и выгрузки лога событий.

Для создания дампа событий и выгрузки архива выполните следующие действия:

1. Перейдите на вкладку меню **Система > События > Журнал событий**;
2. Нажмите на кнопку [**Создать дамп журнала событий**];
3. В открывшемся окне создания дампа, введите количество дней, за которые требуется создать дамп лога;
4. Нажмите на кнопку [**Подтвердить**];

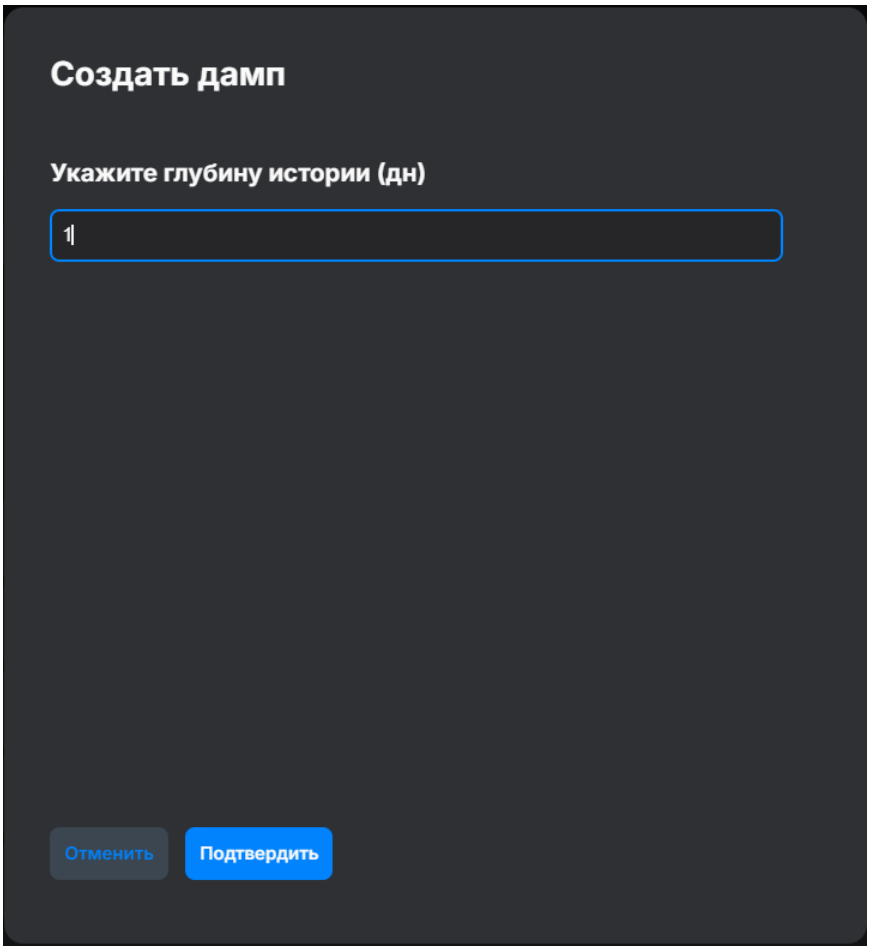


Рисунок 51. Окно создания дампа лога

5. Окно создания дампа закроется и начнется фоновый процесс создания дампа;
6. По окончанию процесса, появится уведомление об успешном создании дампа;
7. Нажмите на кнопку  чтобы скачать дамп журнала;
8. В открывшемся окне, выберите созданный дамп и нажмите на кнопку [**Подтвердить**];

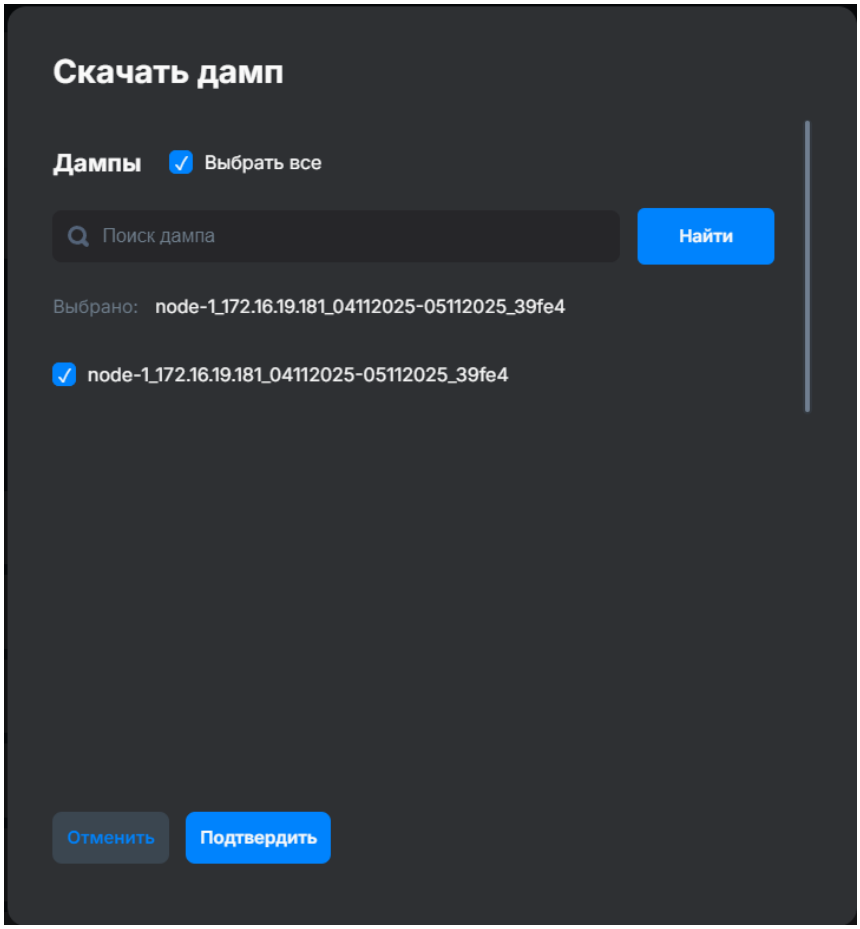


Рисунок 52. Окно скачивания дампа лога

9. Начнется скачивание дампа на компьютер пользователя. Возможно потребуется разрешить браузеру сохранить дамп. Файл дампа имеет расширение tar.gz.

12.5. Выгрузка лога аудита

Логи аудита содержат записи действий пользователей в веб-интерфейсе шлюза, а также действий клиентов шлюза с бакетами и объектами.

В правой части страницы журнала аудита расположены кнопки для удаления, выгрузки и создания дампа журнала событий аудита (лога аудита), содержащего список действий пользователей в веб-интерфейсе шлюза и действий клиентов с бакетами и объектами S3 API.

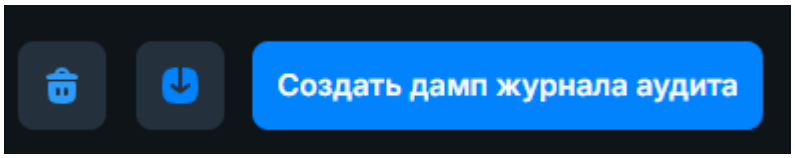


Рисунок 53. Кнопки для создания и выгрузки лога аудита.

Для создания дампа событий аудита и выгрузки архива выполните следующие действия:

1. Перейдите на вкладку меню **Система > События > Журнал аудита**;
2. Нажмите на кнопку [**Создать дамп журнала аудита**];
3. В открывшемся окне создания дампа, введите количество дней, за которые требуется создать дамп журнала;
4. Нажмите на кнопку [**Подтвердить**];
5. Окно создания дампа закроется и начнется фоновый процесс создания дампа;
6. По окончанию процесса, появится уведомление об успешном создании дампа;
7. Нажмите на кнопку  чтобы скачать дамп журнала;
8. В открывшемся окне, выберите созданный дамп и нажмите на кнопку [**Подтвердить**];
9. Начнется скачивание дампа журнала на компьютер пользователя. Возможно потребуется разрешить браузеру сохранить дамп. Файл дампа имеет расширение tar.gz.

12.6. Удаление созданных дампов журналов

После того, как созданный дамп лога будет скачан, удалите его из системы, чтобы он не занимал место.

Для удаление ненужных дампов выполните следующие действия:

1. Перейдите на вкладку меню **Система > События > Журнал событий**;
2. Нажмите на кнопку  чтобы удалить дамп журнала;
3. В открывшемся окне отметьте дампы журналов, которые хотите удалить;
4. Нажмите на кнопку [**Подтвердить**];
5. При успешном выполнении команды выбранные дампы будут удалены из системы.

Аналогичным способом удаляются дампы журнала аудита. Для этого используйте кнопку удаления дампа расположенную на вкладке меню **Система > События > Журнал аудита**.

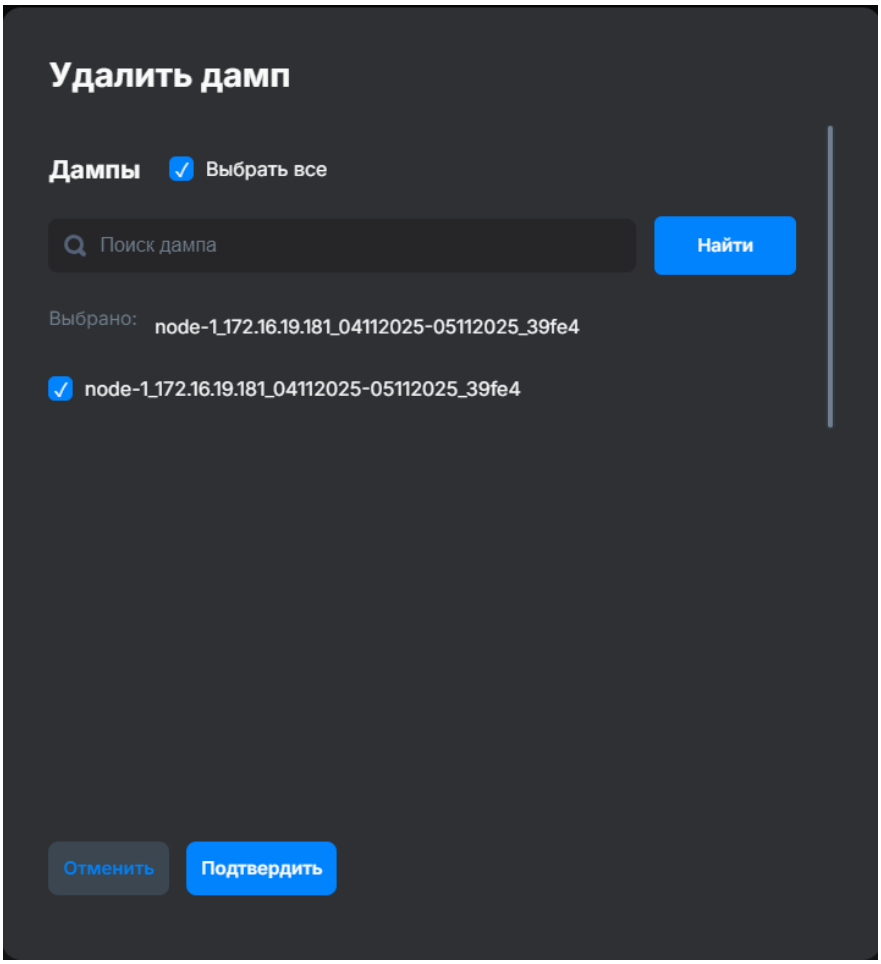


Рисунок 54. Окно удаления дампа журнала

12.7. Настройка логирования

Настройки логирования задаются на странице меню Система > Системный журнал.

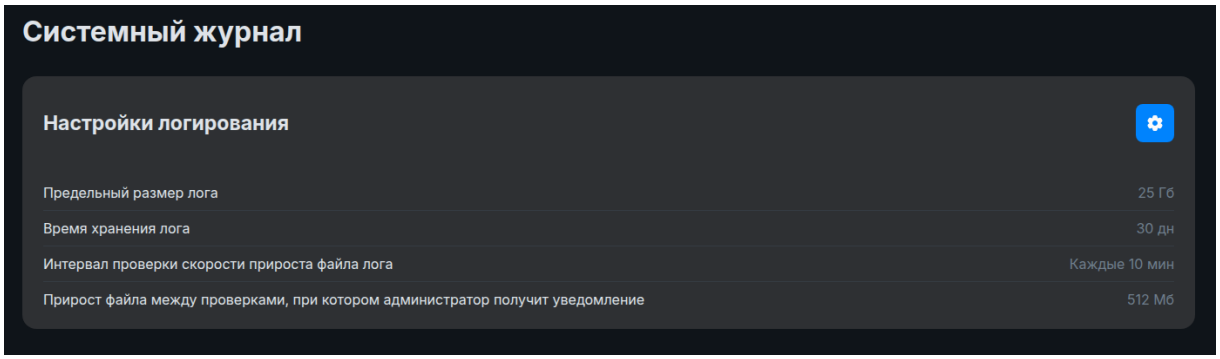


Рисунок 55. Окно меню Системный журнал

Для изменения настроек, нажмите на кнопку  справа на странице меню.

В открывшемся окне настроек логирования измените нужные параметры и нажмите на кнопку [**Подтвердить**].

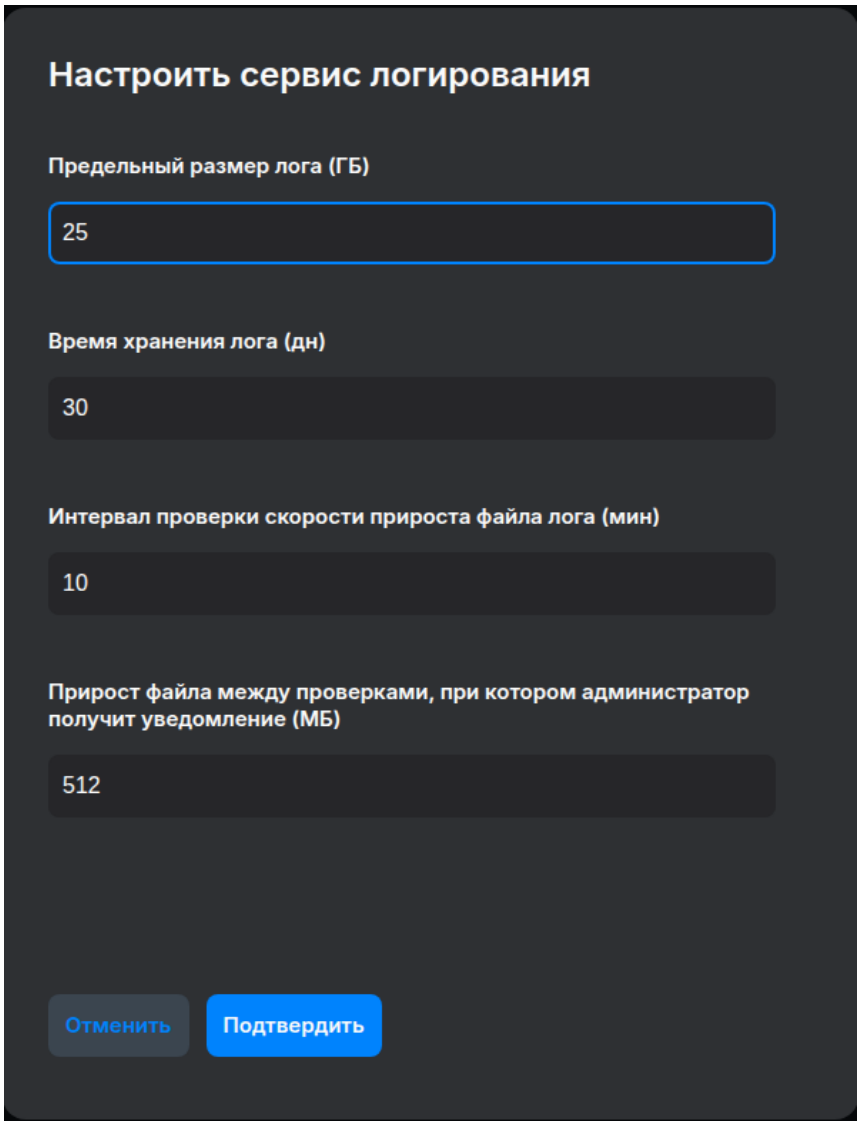


Рисунок 56. Окно настроек логирования

13. НАСТРОЙКА ШЛЮЗА ДЛЯ ПОДКЛЮЧЕНИЯ КЛИЕНТОВ

Перед подключением клиентов, необходимо создать и настроить учетные записи пользователей S3 шлюза, создать для них бакеты и назначить политики доступа.

Правами для настройки шлюза обладает пользователь с ролью Администратор.

Настройка учетных записей пользователей шлюза.

1. Войдите в веб-интерфейс управления шлюзом под учетной записью администратора;
2. Перейдите на страницу меню **Администрирование > Клиенты**;
3. Создайте нового клиента, как это описано в **разделе Работа с клиентами – Создание клиента**;
4. Скопируйте ключи доступа для клиента, воспользовавшись кнопками копирования в буфер, как это описано в разделе **Работа с клиентами – Получение ключей доступа клиента**;
5. Используйте полученные ключи для настройки подключения в клиентском приложении;
6. Перейдите на страницу меню **Администрирование > Бакеты** и создайте один либо несколько бакетов, в которых клиент будет хранить данные. При создании бакетов, укажите их владельцем клиента, созданного на шаге 2;
7. Перейдите на страницу меню **Администрирование > Политики**. Создайте политику доступа для созданных бакетов, как это описано в разделе **Работа с политиками – Создание политики**. Разрешите использование всех Actions для созданных бакетов;
8. Вернитесь на страницу меню **Администрирование > Клиенты**. Войдите в режим редактирования свойств созданного на шаге 2 клиента и привяжите к нему политику. Привязка политик описана в разделе Работа с политиками – Привязка политик к клиентам.

На этом настройка шлюза для подключения клиента завершена. Используйте полученные на шаге 3 ключи Access key и Secret key для доступа к шлюзу.

14. ОБНОВЛЕНИЕ ПО ШЛЮЗА

Процесс обновления ПО шлюза сводится к остановке запущенного контейнера и запуску контейнера с новой версией шлюза. Команды для выполнения этих операций описаны в разделе «Запуск и настройка шлюза» настоящего руководства.

15. РЕКОМЕНДАЦИИ ПО РЕЗЕРВНОМУ КОПИРОВАНИЮ

В кластерной архитектуре FORTEIA компоненты системы распределены следующим образом: метаданные находятся в реплика-сете MongoDB, развёрнутой на узлах шлюза, а объекты хранятся на внешних NFS-папках, доступных со всех узлов. Логи и метрики размещены локально на каждом узле. Для гарантированного восстановления системы при логических ошибках, случайном удалении или катастрофах необходимо выполнять резервное копирование следующих компонентов.

15.1. Метаданные (MongoDB)

Метаданные хранятся в базе данных MongoDB, работающей в режиме реплика-сета на тех же узлах, что и шлюз.

Рекомендации по резервному копированию метаданных:

Способ копирования: используйте штатные средства MongoDB – mongodump для логического дампа или создавайте файловые снапшоты с предварительной синхронизацией и блокировкой записи (db.fsyncLock()). В производственной среде предпочтительнее выполнять дамп с вторичного узла реплика-сета, чтобы не нагружать primary и не влиять на обслуживание клиентских запросов.

Периодичность: настройте регулярное выполнение резервного копирования в периоды минимальной нагрузки.

Хранение: храните резервные копии на отдельном надёжном хранилище для защиты от локальных отказов.

Проверка целостности: регулярно проверяйте возможность восстановления из резервной копии на тестовом стенде.

15.2. Данные (объекты)

Объекты записываются синхронно в несколько NFS-папок, что обеспечивает отказоустойчивость на уровне отдельных экспортов. Однако это не защищает от логических ошибок (например, массовое удаление или повреждение данных). Для таких случаев рекомендуется резервное копирование NFS-экспортов.

Способ копирования: предпочтительно использовать снапшоты томов на уровне СХД, если они поддерживается. Это гарантирует согласованность состояния файловой системы. Альтернативно применяйте утилиты rsync или tar для копирования содержимого NFS-папок на отдельное резервное хранилище.

Согласованность: при использовании rsync / tar старайтесь выполнять копирование в периоды минимальной записи, чтобы снизить риск копирования незавершённых файлов. Или, если это возможно, переведите кластер в режим обслуживания.

Периодичность: согласуйте с бизнес-требованиями, например, ежедневно для критичных данных, реже для архивных.

Хранение: резервные копии NFS-папок должны размещаться на физически независимых носителях, отличных от основных NFS-экспортов.

15.3. Логи и метрики

Логи работы шлюза (включая журналы событий и аудита) и метрики хранятся локально на каждом узле в каталогах, заданных при конфигурации системы (обычно /logs и /metrics). Эти данные не являются критичными для восстановления функциональности, но необходимы для аудита, расследования инцидентов и анализа производительности.

Способ копирования: настройте сбор и архивацию содержимого этих каталогов с каждого узла с помощью скриптов (например, tar + rsync) или используйте централизованную систему сбора логов (ELK, Graylog и т.п.) для автоматического переноса.

Периодичность и хранение: определяются политикой безопасности организации. Рекомендуется хранить архивы не менее 30 дней или дольше, если это требуется регуляторными нормами.

15.4. Общие рекомендации

- Разработайте и утвердите регламент резервного копирования с указанием периодичности, сроков хранения, ответственных лиц и процедур проверки восстанавливаемости.
- Автоматизируйте процесс с помощью планировщика (cron, systemd timers) и интегрируйте мониторинг успешности выполнения.
- Для MongoDB предпочтительно использовать mongodump с опцией --oplog при выполнении на вторичном узле, чтобы получить согласованный во времени дамп без остановки работы системы.
- Для NFS-экспортов отдавайте приоритет снапшотам СХД, они обеспечивают наилучшую согласованность и минимальное влияние на производительность.
- Регулярно, не реже одного раза в квартал, проводите учебные восстановления из резервных копий на изолированном стенде, чтобы подтвердить работоспособность процедур.

- Документируйте шаги по восстановлению системы и поддерживайте эту документацию в актуальном состоянии.
- Выполнение резервного копирования не требует обязательной остановки контейнеров шлюза, однако для создания согласованного дампа MongoDB следует использовать реплика-сет и снимать копии с вторичных узлов. Для NFS-папок наиболее безопасным способом являются снапшоты на уровне СХД.

16. REST-API

Управление шлюзом возможно при помощи REST-API. Поддерживаются все операции, которые есть в GUI шлюза.

Справочное руководство по методам REST-API доступно через эндпоинт /swagger/ на порту для подключения веб-интерфейса. Например: **http://172.16.19.181:8950/swagger/** .

Для получения токена сессии потребуется логин и пароль администратора.

1. Вычислите MD5 – хеш от пароля администратора:
   echo -n "Sd5vok7cls!" | md5sum

2. Выполните API операцию login для получения токена сессии, подставив полученный хеш вместо строки пароля, например,
   ***curl -X POST "http://localhost:8950/api/v2/login" ***
   ***-H "Content-Type: application/json" ***
   -d '{
   "device": "curl-client",
   "login": "admin",
   "password": "3b60f07e85367f48c3dae3c9f5761a73"
   }'

Рисунок 57. Пример ответа, содержащего токен сессии

17. СПИСОК ПОДДЕРЖИВАЕМЫХ ОПЕРАЦИЙ S3 API

Операции S3 API	Опции	Поддержка
HeadObject		Да
	Запрос по имени объекта от создателя бакета	Да
	Запрос на принадлежность конкретному пользователю	Нет
	Запрос по диапазону байтов (Range)	Да
	Запрос по номеру части (Part)	Да
	Поддержка версионирования объектов	Нет
	Запрос с учетом соответствия ETag (If-Match / If-None-Match)	Да
	Запрос с учетом времени модификации (If-Modified-Since / If-Unmodified-Since)	Да
	Поддержка проверки контрольной суммы	Да
	Поддержка шифрования на уровне сервера	Нет
	Поддержка request payer	Нет
HeadBucket		Да
	Запрос принадлежности бакета пользователю	Да
DeleteBucket		Да
	Удаление собственных бакетов	Да
	Удаление чужих бакетов	Нет
DeleteObject		Да
	Удаление объектов из собственного бакета	Да
	Использование блокировок	Нет
	Удаление чужих объектов	Нет
	Версионирование	Нет
	Поддержка request payer	Нет
	Поддержка MFA	Нет
DeleteObjects		Да
	Удаление объектов из собственного бакета	Да
	Использование блокировок	Нет
	Удаление чужих объектов	Нет
	Версионирование	Нет
	Поддержка request payer	Нет
	Поддержка MFA	Нет
	Реализация расширенного ответа (кто удалён, кто нет и почему)	Нет
GetBucketLocation		Да
	Возврат дефолтного региона для создателя бакета	Да
	Поддержка других регионов	Нет
	Возврат данных о бакетах других пользователей	Нет
GetBucketVersioning		Да
	Возврат текущего состояния версионирования бакета	Да
GetObject		Да
	Запрос по имени объекта от создателя бакета	Да
	Запрос на принадлежность конкретному пользователю	Нет
	Запрос по диапазону байтов (Range)	Да
	Запрос по номеру части (Part)	Да

	Поддержка версионирования объектов	Нет
	Запрос с учетом соответствия ETag (If-Match / If-None-Match)	Да
	Запрос с учетом времени модификации (If-Modified-Since / If-Unmodified-Since)	Да
	Поддержка проверки контрольной суммы	Да
	Поддержка шифрования на уровне сервера	Нет
	Поддержка request payer	Нет
	Поддержка данных для заголовков ответа в запросе	Нет
GetObjectAcl		Нет
ListBuckets		Да
ListObjects		Да
	Список объектов пользователя бакета	Да
	Список чужих объектов	Да
	Поддержка request payer	Нет
	Поддержка разделителей, маркеров, префиксов, ограничения выдачи	Да
ListObjectsV2		Да
	Список объектов пользователя бакета	Да
	Список чужих объектов	Да
	Поддержка request payer	Нет
	Поддержка разделителей, маркеров, префиксов, ограничения выдачи	Да
PutObject		Да
	Загрузка объекта в бакет	Да
	Поддержка проверки контрольной суммы	Да
	Поддержка шифрования на уровне сервера	Нет
	Поддержка request payer	Нет
	Поддержка данных для заголовков ответа в запросе	Нет
	Поддержка блокировок	Нет
	Поддержка времени жизни	Нет
	Поддержка Storage Class	Нет
	Поддержка прав пользователя на объект	Нет
	Поддержка версионирования	Нет
	Поддержка тегов объектов	Да
CreateBucket		Да
	Создание бакета текущим пользователем	Да
	Поддержка прав пользователей	Нет
	Поддержка ACL	Нет
	Поддержка блокировок	Нет
CreateMultipartUpload		Да
	Загрузка объекта в бакет	Да
	Поддержка проверки контрольной суммы	Да
	Поддержка шифрования на уровне сервера	Нет
	Поддержка request payer	Нет
	Поддержка данных для заголовков ответа в запросе	Нет
	Поддержка блокировок	Нет
	Поддержка времени жизни	Нет
	Поддержка Storage Class	Нет
	Поддержка прав пользователя на объект	Нет
	Поддержка версионирования	Нет
	Поддержка тегов объектов	Да
CompleteMultipartUpload		Да

	Завершение Upload, получение объекта	Да
	Поддержка проверки контрольной суммы	Да
	Поддержка шифрования на уровне сервера	Нет
	Поддержка request payer	Нет
UploadPart		Да
	Загрузка части	Да
	Поддержка проверки контрольной суммы	Да
	Поддержка шифрования на уровне сервера	Нет
	Поддержка request payer	Нет
	Загрузка в чужой бакет	Нет
AbortMultipartUploads		Да
	Отмена мультипарт загрузки, удаление частей	Да
	Поддержка request payer	Нет
	Загрузка в чужой бакет	Нет
ListMultipartUploads		Да
	Список объектов пользователя бакета	Да
	Список чужих объектов	Да
	Поддержка request payer	Нет
	Поддержка разделителей, маркеров, префиксов, ограничения выдачи, фильтров	Да
ListParts		Да
	Списое партов пользователя	Да
	Список чужих партов	Да
	Шифрование на уровне сервера	Нет
	Поддержка request payer	Нет
Реализована работа по https протоколу		Да
GetBucketTagging	Получение настроек работы с тегами бакетов	Да
PutBucketTagging	Установка настроек работы с тегами бакетов	Да
DeleteBucketTagging	Удаление настроек работы с тегами бакетов	Да
GetObjectTagging	Получение настроек работы с тегами объектов	Да
PutObjectTagging	Установка настроек работы с тегами объектов	Да
GetBucketLogging	Получение настроек работы с логгированием бакетов	Да
PutBucketLogging	Установка настроек работы с логгированием бакетов	Да
DeleteObjectTagging	Удаление настроек работы с тегами объектов	Да
GetBucketCORS	Получение настроек CORS для бакета	Да
PutBucketCORS	Установка настроек CORS для бакета	Да
DeleteBucketCORS	Удаление настроек CORS для бакета	Да
PreflightCORS	Проверка доступа через CORS	Да
CopyObject	Копирование объекта	Да
UploadPartCopy	Копирование части объекта в виде части другого объекта	Да