Руководство пользователя

Программного обеспечения

BlazeX

Версии 3.6 v1

BITBLAZE

ООО «Битблэйз Технологии» (ООО «БитТех»)

ОГРН 1177746396630, ИНН 7731360971 / КПП 773101001

121205, Российская Федерация г. Москва, вн. тер. г. муниципальный округ Можайский, тер. Инновационного центра «Сколково», Большой бульвар, д. 42, стр. 1, 599 р/м 02, этаж 1

https://bitblaze.tech/

СОГЛАШЕНИЕ ПО ОФОРМЛЕНИЮ

Для более наглядного представления различных команд, файлов и пр. в документе используется следующее форматирование:

Команды и командные утилиты

Параметры команд и файлов

Абзацы в тексте, содержащие важную информацию, выделены следующим образом:

ПРИМЕЧАНИЕ

Выделенные таким образом указания содержат важную информацию

ВНИМАНИЕ!

Выделенные таким образом указания настоятельно рекомендуется выполнять для обеспечения работоспособности СХД.

ВВЕДЕНИЕ

Данное Руководство содержит сведения по рабочему использованию управляющего ПО BlazeX в составе ПАКа и является обязательным документом для ознакомления перед началом и в процессе работ.

Руководство предназначено для администраторов системы. Установка и работа с данным ПО должны проводиться только опытными техническими сотрудниками.

Программное обеспечение BlazeX функционирует в составе ПАК СХД и предназначено для управления распределением дискового пространства и мониторинга рабочих процессов и состояния ПАКа.

BlazeX автоматизирует процесс работы с дисковым пространством путем:

- виртуализации нескольких физических накопителей данных в логическую группу (пул) для повышения отказоустойчивости и (или) производительности;
- организации отдельных областей данных поверх физических групп, отображаемые системой как отдельные блочные устройства (логические тома).

Руководство охватывает следующие ключевые аспекты работы с ПО BlazeX:

- управление ресурсами СХД (накопители, группы накопителей/RAID-массивы, логические тома);
- предоставление блочного доступа по протоколам iSCSI и FC;
- предоставление файлового доступа по протоколам NFS и SMB;
- технологии копирования и оптимизации данных (снимки, клоны, Thin provisioning, дедупликация, компрессия);
- фоновое сканирование и оптимизация для групп BlazeIO;
- мониторинг и наблюдаемость (обзор производительности СХД, SNMP, интеграция с Prometheus/Grafana и Zabbix, журналы команд, событий и аудита);
- безопасность (ролевой доступ, политики безопасности, AD/LDAP-аутентификация, SSH-ключи);
- настройки системы (сетевые интерфейсы, Syslog, SMTP-уведомления, NTP, CLI, REST API);
- аппаратная платформа (компоненты, сенсоры, дисковые полки);
- лицензирование (активация лицензионного ключа, режим «Только чтение» при отсутствии лицензии).

Данное Руководство составлено на управляющее ПО BlazeX. Приведенные иллюстрации подготовлены разработчиком BlazeX. Программное обеспечение разработано для работы с оборудованием ООО «Промобит».

1 ОБЩЕЕ ОПИСАНИЕ

ПО BlazeX предназначено для организации хранения массивов данных, выполнения оперативных задач и предоставления дискового пространства.

ПО BlazeX позволяет создавать высокопроизводительные отказоустойчивые СХД и применяться в составе управляющего ПО ПАКов. BlazeX предназначено как для управления, так и для мониторинга СХД в одно- или двухконтроллерном исполнении.

ПО BlazeX поддерживает как одноконтроллерный режим работы, так и двухконтроллерный, при котором оба контроллера активны и имеют постоянный доступ к общей корзине накопителей. Отказоустойчивость системы в таком режиме работы обеспечивается за счет горячего резервирования, позволяющего сохранить доступ ко всем ресурсам (группам дисков, логическим томам) при отказе одного из контроллеров и обеспечить следующие параметры надежности работы:

- защиту от выхода из строя аппаратных компонентов одного узла;
- защиту от отказа интерфейса подключения;
- защиту от сбоев ОС и ПО на отдельном контроллере.

ПО BlazeX позволяет реализовать сетевое хранилище данных (NAS), объединенное с сетью хранения данных (SAN).

Управление ПАК с установленным ПО BlazeX осуществляется через веб-интерфейс с предоставлением инструментария ГИП. Описание процесса работы с ГИП изложено в данном руководстве.

Дополнительно доступны следующие интерфейсы управления:

- REST API (интерактивная документация доступна по адресу https://<IP-адрес_узла>/api/);
- CLI (интерфейс командной строки) - подключение по SSH с использованием SSH-ключей или логина/пароля.

Обмен информацией о состоянии между узлами СХД осуществляется через heartbeat, обмен трафиком между контроллерами организован через высокоскоростное соединение (interconnect).

ПО BlazeX при использовании в составе 2-контроллерной аппаратной конфигурации СХД позволяет предоставлять доступ к данным по блочным протоколам в двух режимах отказоустойчивости: Active/Active (активный/активный) и Active/Passive (активный/пассивный).

В режиме Active/Active оба контроллера одновременно обслуживают операции ввода-вывода, что обеспечивает равномерное распределение нагрузки и высокую доступность данных.

В режиме ALUA (Asymmetric Logical Unit Access - асимметричный доступ к логическому устройству) ввод-вывод выполняется только через активный контроллер, резервный

вступает в работу при отказе основного. В этом режиме система автоматически выбирает оптимальные пути доступа к данным.

ПО BlazeX включает следующие функциональные блоки:

Функциональный блок	Описание
Управление СХД	Создание и управление накопителями, группами накопителей (RAID-массивами) и логическими томами. Поддержка драйверов BlazeIO, BlazeIO A/A, MDRAID.
Блочный доступ	Экспорт томов по протоколам iSCSI и FC. Управление таргетами и группами инициаторов.
Файловый доступ	Экспорт томов по протоколам NFS и SMB. Управление экспортами, пользователями и группами SMB.
Снимки и клоны	Создание моментальных копий (снимков) томов и групп. Создание полноценных клонов на основе снимков.
Фоновое сканирование и оптимизация	Планирование и запуск фонового сканирования дисков и оптимизации хранилища для групп BlazeIO.
Мониторинг	Обзор производительности СХД (IOPS, пропускная способность, время отклика, загрузка CPU/RAM/портов, FC-порты, скорость ребилдинга). SNMP (v2c, v3, трапы, MIB-файл). Интеграция с Prometheus/Grafana и Zabbix. Журналы команд, событий и аудита.
Аппаратная платформа	Просмотр компонентов (диски, контроллеры, дисковые полки, FC-порты, сетевые интерфейсы) и сенсоров (температура, вентиляторы, напряжение).
Безопасность	Ролевой доступ (Администратор, Оператор, Гость). Политики безопасности (парольная, сессий, защита входа). AD/LDAP-аутентификация. Управление SSH-ключами.
Настройки	Настройка сетевых интерфейсов (DHCP/статический, MTU). Syslog (UDP/TCP). SMTP-уведомления. NTP-серверы (синхронизация времени). CLI и REST API.
Лицензирование	Активация лицензионного ключа. Режим «Только чтение» (Read-Only) при отсутствии или недействительности лицензии.

Основные характеристики ПО Blazex отображены в следующей таблице:

Наименование критерия	**Значение критерия**
Поддерживаемые уровни RAID	RAID 0, 1, 5, 6 и 10, 50, 60[1*]
Композитные группы RAID	Объединение RAID + «Striped» том
Поддерживаемые блочные протоколы	FC, iSCSI
Поддерживаемые файловые протоколы	NFS (v3, v4), SMB/CIFS
Поддерживаемые интерфейсы дисков	SAS, SATA, NVMe
Максимальное количество дисков в RAID	20
Максимальное количество LUN	256
Технологии копирования данных	Снимки (Snapshot), Клоны (Snapclone)
Технологии оптимизации хранения	Thin provisioning, дедупликация, компрессия
Режимы работы контроллеров	Одноконтроллерный, двухконтроллерный Active/Active, ALUA
Поддерживаемые типы драйверов групп	BlazeIO (ALUA), BlazeIO A/A (Active/Active), MDRAID
Максимальное количество томов (LUN)	256
Максимальный размер тома (обычный)	Зависит от размера группы
Максимальный размер тома (Thin provisioning)	1 PB
Максимальный размер тома (дедуплицированный)	4 PB
Минимальный размер тома	1 GB (обычный и Thin), 6 GB (дедуплицированный)
Поддерживаемые типы доступа к томам	Block (блочный), File (файловый)
Поддерживаемые протоколы экспорта блочного доступа	iSCSI, Fibre Channel (FC)
Поддерживаемые протоколы экспорта файлового доступа	NFS, SMB
Аппаратная индикация накопителей	Поддержка Find Drive - мигание LED

[1*] Создание массивов аналогичных по свойства RAID 10, 50, 60. Смотреть описание в разделе 2.4.1

Фоновое сканирование и оптимизация	Поддерживается для групп BlazeIO
Планировщик задач	Поддерживается (расписание оптимизации и сканирования)
Управление пользователями и ролями	Администратор, Оператор, Гость
Аутентификация	Локальная, AD/LDAP
Политики безопасности	Парольная политика, политика сессий, защита входа (блокировка при неудачных попытках)
SSH-ключи	Поддерживаются (генерация, копирование, отключение)
Мониторинг и наблюдаемость	Обзор СХД (IOPS, пропускная способность, время отклика, загрузка CPU/RAM/портов)
SNMP	Поддержка SNMPv2c и SNMPv3, трапы, MIB-файл
Внешний мониторинг	Prometheus + Grafana, Zabbix
Журналирование	Журнал команд, журнал событий, журнал аудита
Интерфейс управления	Веб-интерфейс (ГИП), REST API, CLI (SSH)
Поддерживаемые браузеры для ГИП	Современные браузеры с поддержкой TLS (самоподписанный сертификат)
Уведомления	SMTP (email-уведомления)
Внешние логи	Syslog (UDP/TCP)
Синхронизация времени	NTP (поддержка burst, iburst, prefer)
Лицензирование	Активация по ключу (с учётом спецификации оборудования)
Режим при отсутствии/недействительности лицензии	«Только чтение» (Read-Only)

1.1 ОПИСАНИЕ ГИП И ОПЕРАЦИЙ ПО УПРАВЛЕНИЮ СХД

Администрирование и работа с СХД осуществляется через ГИП. Доступ к сервису осуществляется через Web–интерфейс в Интернет–браузере:

```
https://<IP–адрес_узла>
```

ПРИМЕЧАНИЕ

Проверка подлинности Web–интерфейса осуществляется самоподписанным SSL–сертификатом, выпускаемым компанией ООО «Промобит». В случае возникновения сообщения об ошибке, связанной с невозможностью установления безопасного соединения, требуется сделать исключение для посещаемого ресурса и подтвердить принятие сертификата (см. рисунок 1.1).

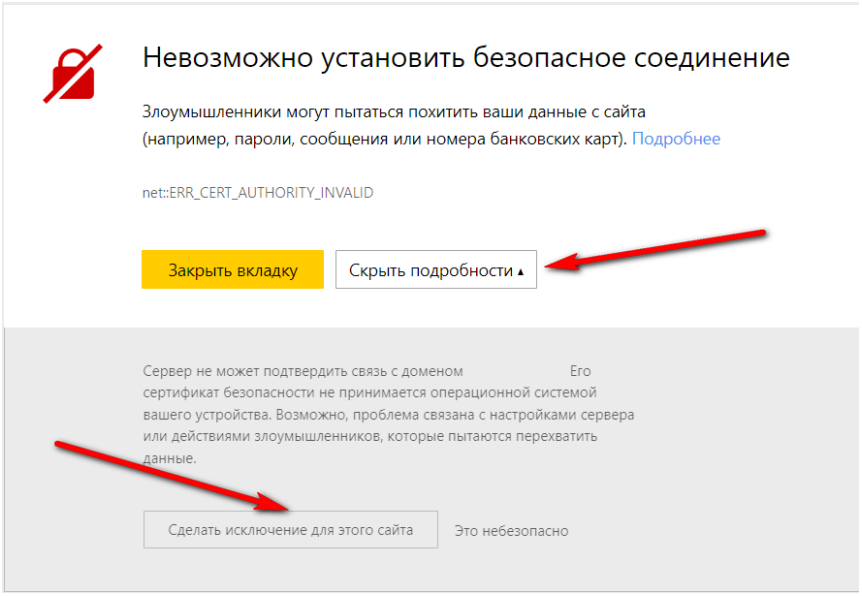


Рисунок 1.1 – Сообщение о невозможности установить безопасное соединение

1.2 АВТОРИЗАЦИЯ ПОЛЬЗОВАТЕЛЯ

Для работы в ГИП пользователь должен быть авторизован в системе. Окно авторизации показано на рисунке 1.2.

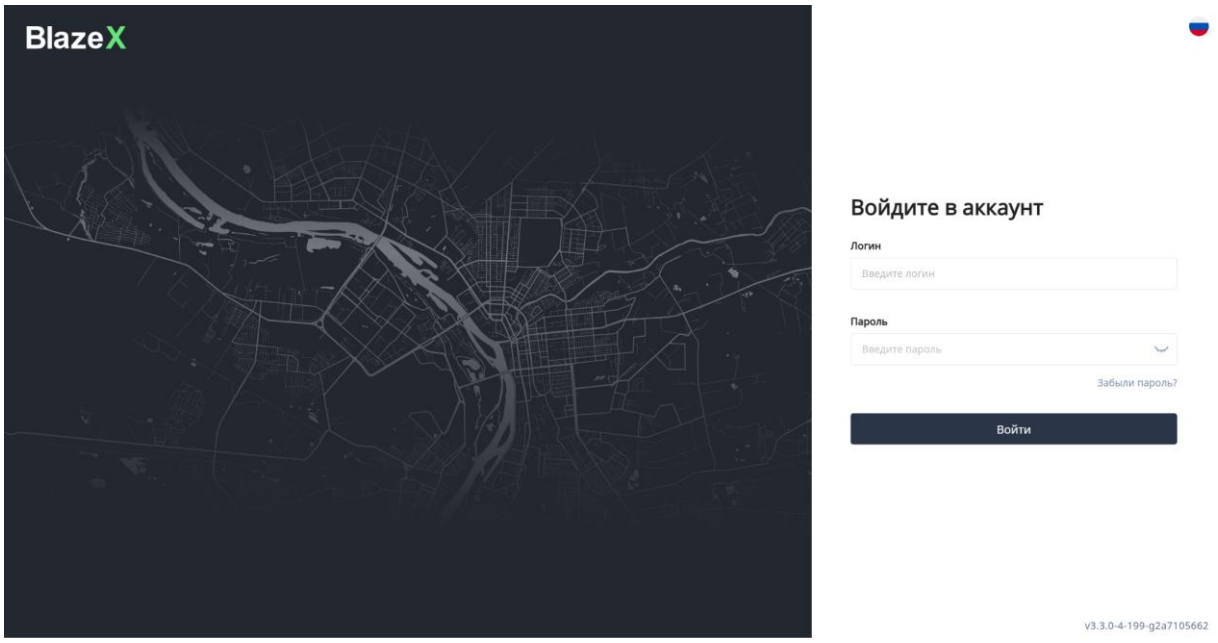


Рисунок 1.2 – Окно авторизации

Логин и пароль для первичной авторизации:

- Логин: admin
- Пароль: admin

Функция восстановления пароля (ссылка «Забыли пароль?» на рисунке 1.2) реализована в формате обращения в техническую поддержку компании ООО «Битблэйз Технологии» (рисунок 1.3.). При клике на «Забыли пароль» открывается страница службы поддержки, где можно оставить заявку:

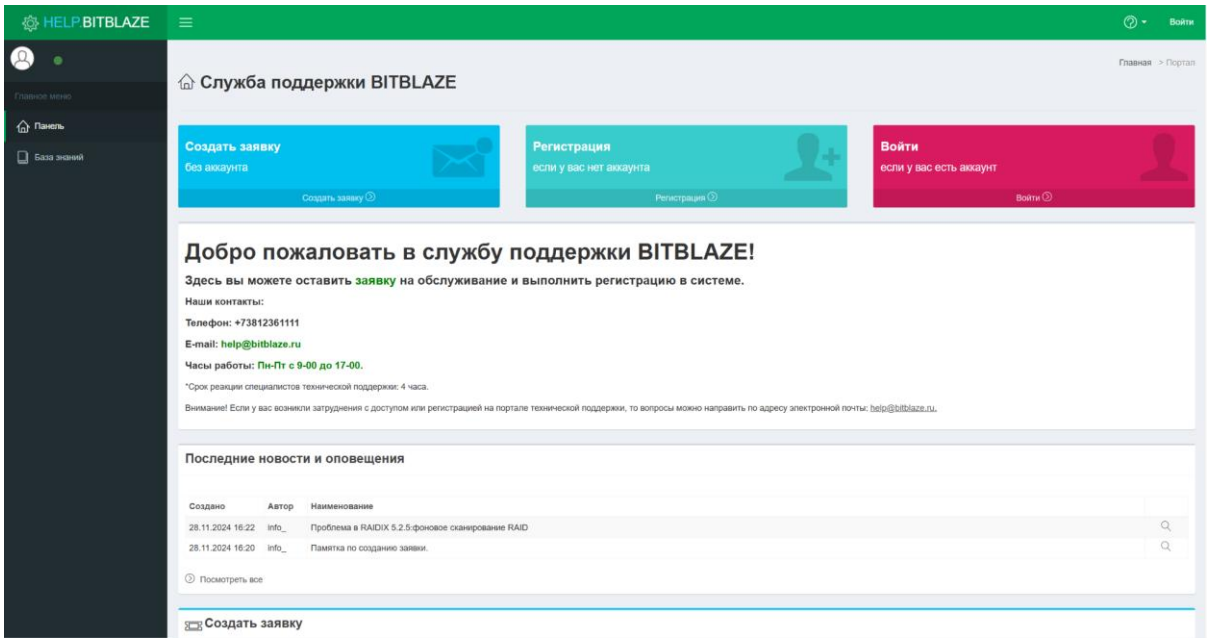


Рисунок 1.3 – Страница службы поддержки

1.3 ВЫБОР ЯЗЫКА ГИП

Смена языка ГИП (русский или английский) выполняется при вызове контекстного языкового меню, при клике на соответствующий графический элемент: (рисунок 1.4).

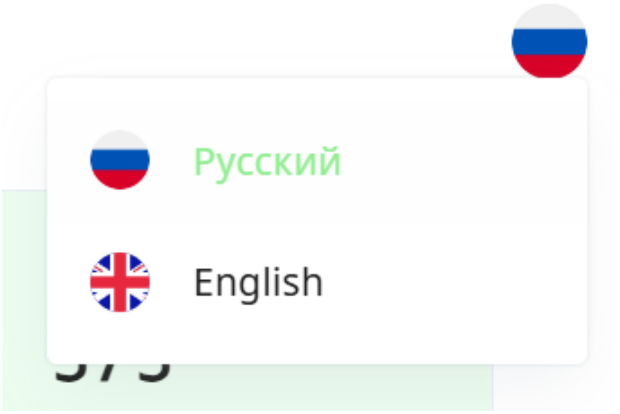


Рисунок 1.4 – Контекстное языковое меню

1.4 МЕНЮ ПОЛЬЗОВАТЕЛЯ

Контекстное меню пользователя предоставляет ролевой доступ, информационную справку об управляющем ПО и параметры системы. Доступ к меню осуществляется при вызове контекстного пользовательского меню, при клике на соответствующий графический элемент : (рисунок 1.5).

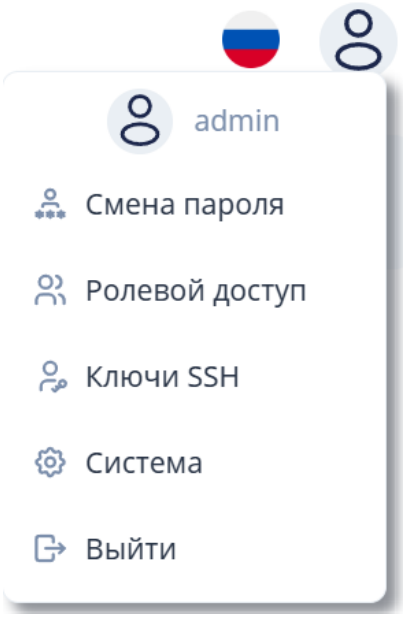


Рисунок 1.5 – Выбор контекстного меню

1.5 СМЕНА ПАРОЛЯ

Смена пароля авторизованного пользователя будет осуществлена при успешном заполнении всех пунктов меню (рисунок 1.6).

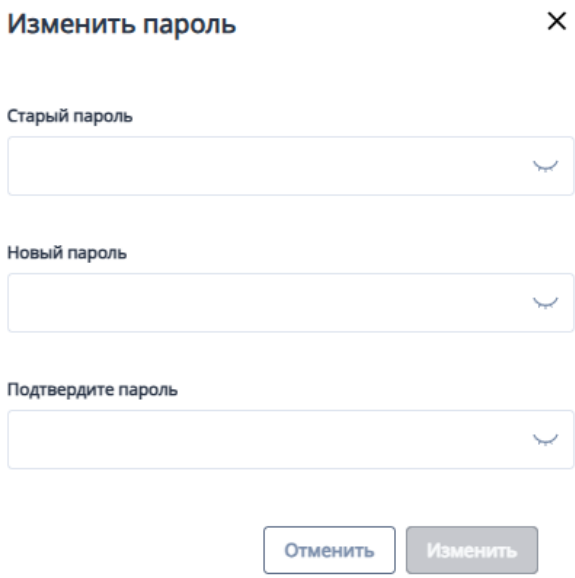


Рисунок 1.6 – Окно с меню смены пароля пользователя

ПРИМЕЧАНИЕ

Для самостоятельного сброса пароля необходимо использовать запуск *python* скрипта через консоль, для этого:

- перейдите в директорию: /opt/promobit/blazex/control/resources/recovery/
- введите команду: python3 password–recovery.py —username <ИМЯ_ПОЛЬЗОВАТЕЛЯ>
- введите и подтвердите новый пароль

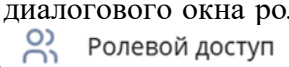
Смену пароля необходимо выполнять на том узле, который в данный момент является активным.

ВНИМАНИЕ!

Для обеспечения безопасности рекомендуется сменить пароль доступа после первой успешной авторизации!

При работе с ГИП следует учитывать, что время действия токена авторизации установлено равным 120 минутам. По истечению времени требуется повторная авторизация.

1.6 РОЛЕВОЙ ДОСТУП

Вызов диалогового окна ролевого доступа осуществляется выбором соответствующего пункта 

меню (рисунок 1.5). Работа с ролями производится в окне (рисунок 1.7).

Модель ролей и права:

Администратор: полный доступ ко всем ресурсам и операциям, включая управление пользователями и ролями, в т.ч. действия над Оператором и Гостем. Учетная запись Администратора создается по умолчанию, её редактирование запрещено.

Оператор: все операции над ресурсами, а также управление пользователями и ролями, кроме удаления/редактирования учетной записи Администратор.

Гость: роль с правами только на просмотр. Пользователь имеет доступ к интерфейсу и данным, но все функции создания, редактирования и удаления заблокированы. Формы можно открывать, но сохранение изменений запрещено.

Роль	Права					
	Смена пароля пользователя	Редактирование пользователя	Удаление пользователя	Создание новых пользователей	Доступно в приложении	Выдача доступа к CLI
Администратор	всех*	всех	всех	операторов и гостей	все операции	всем
Оператор	операторам и гостям	операторам и гостям	операторов и гостей	операторов и гостей	все операции	операторам и гостям
Гость	нет	нет	нет	нет	только просмотр, создать отчет, скачать отчет	нет

* *Примечание: Собственный пароль администратор может изменить только через смену пароля в меню пользователя, а не через панель управления ролями.*

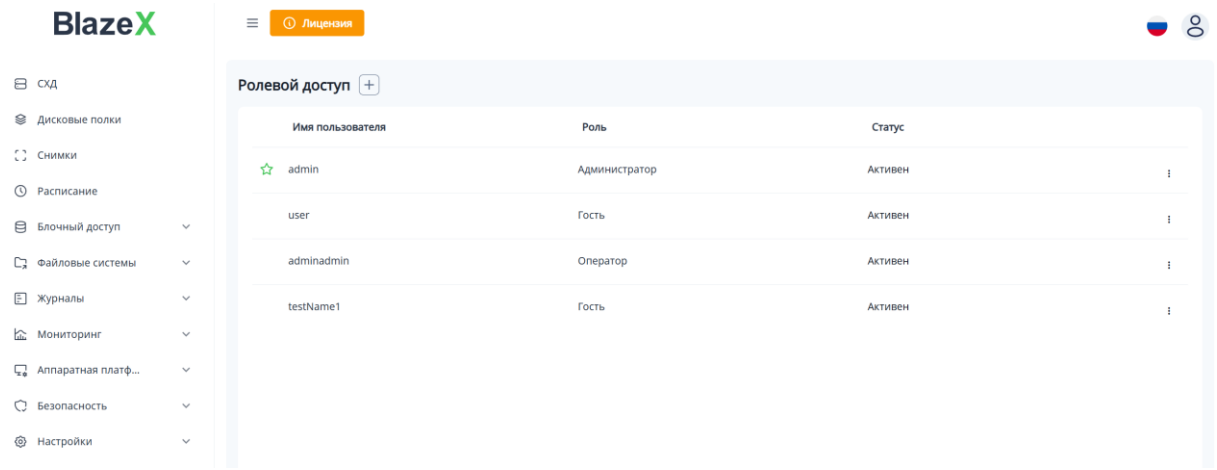


Рисунок 1.7 – Окно ролевого доступа

1.6.1 СОЗДАНИЕ НОВОГО ПОЛЬЗОВАТЕЛЯ

Для создания нового пользователя необходимо выполнить следующее:

1. В окне «Ролевой доступ» нажать «Добавить»  . В открывшемся окне необходимо (рисунок 1.8):

- выбрать роль (оператор или гость),

- ввести логин,

- ввести пароль,

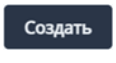
- подтвердить пароль,

- поставить\убрать галочку «Разрешить доступ в CLI»

ПРИМЕЧАНИЕ

Подробно о CLI в разделе 9.5 «Интерфейс командной строки CLI»

2. Для отмены создания пользователя необходимо нажать «Отменить»  или «Закрыть»  .

3. Для сохранения нового пользователя необходимо нажать на кнопку «Создать»  . При успешном выполнении команды ГИП отобразит нового пользователя в списке, как это показано на рисунке 1.7.

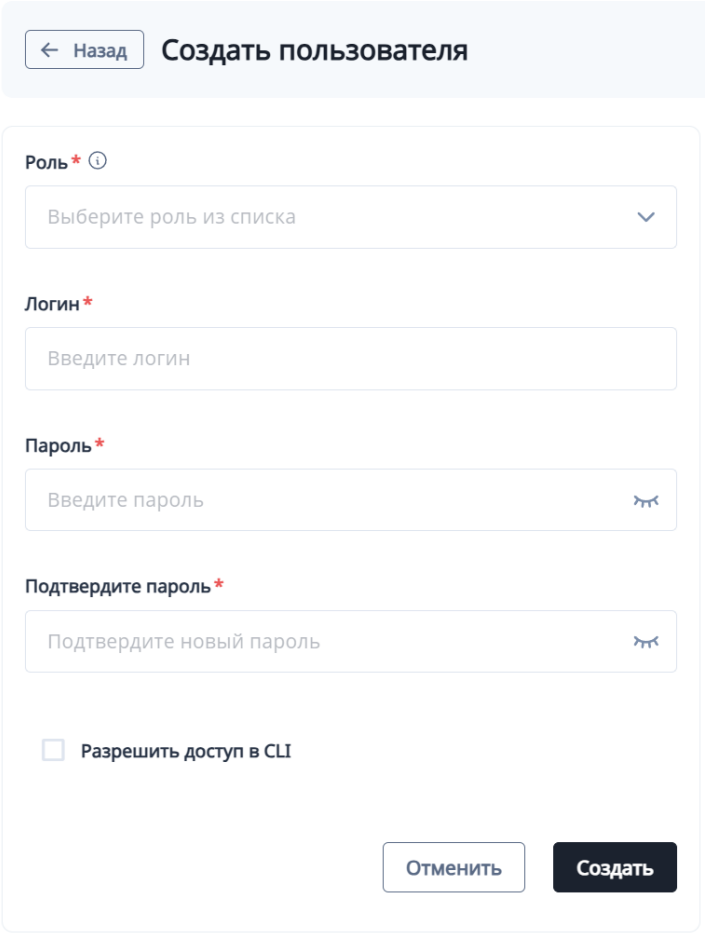


Рисунок 1.8 – Окно создания пользователя

1.6.2 РЕДАКТИРОВАНИЕ ПОЛЬЗОВАТЕЛЯ

Для редактирования параметров пользователя необходимо выполнить следующее:

1. В строке с ролью нажать на кнопку «Параметры» . На экране отобразится выбор действия, в котором нужно выбрать «Редактировать» (рисунок 1.9)

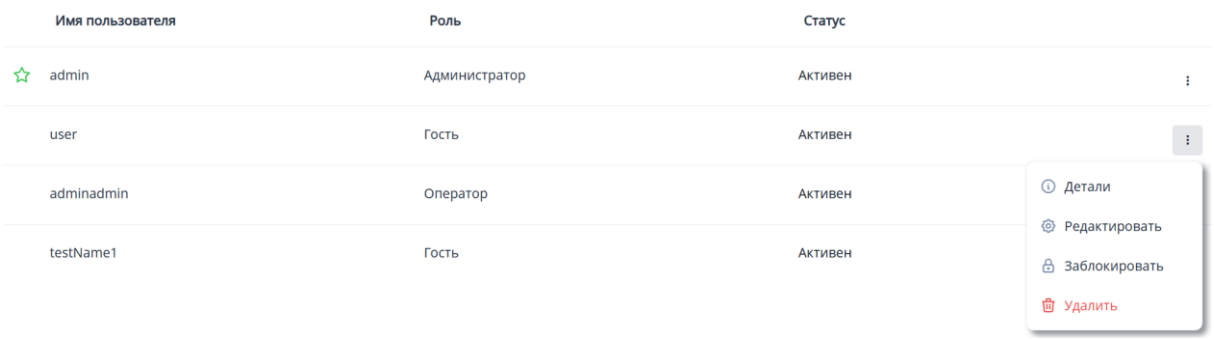


Рисунок 1.9 – Выбор действий с пользователем

2. В открывшемся окне «Редактирование пользователя» доступна смена роли пользователя, изменение его логина и пароля (рисунок 1.10)

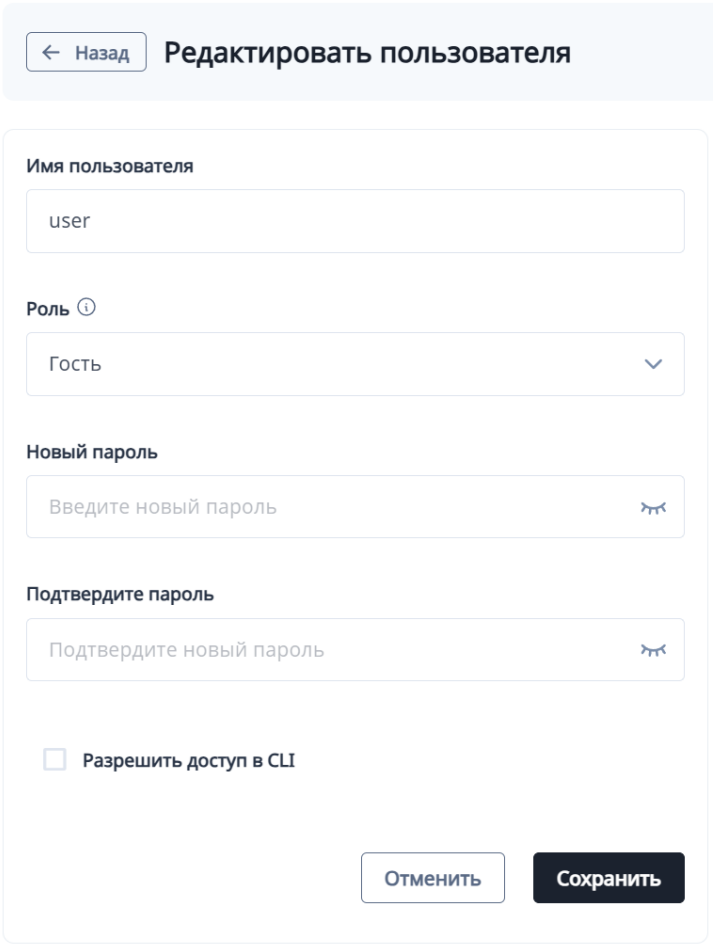


Рисунок 1.10 – Окно «Редактирование пользователя»

3. Чтобы отменить изменения редактирования необходимо нажать на кнопку «Отменить» 

.

4. Чтобы сохранить изменения необходимо нажать на кнопку «Сохранить» 

.

5. При успешном выполнении команды ГИП отобразит список пользователей, как это показано на рисунке 1.7.

1.6.3 УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ

Для удаления пользователя необходимо выполнить следующее:

1. В строке с необходимым пользователем нажать на кнопку «Параметры» (рисунок 1.9) и выбрать пункт «Удалить» 

.
2. В появившемся окне «Удаление роли» необходимо ввести логин пользователя в поле «Имя ресурса» как показано на рисунке 1.11

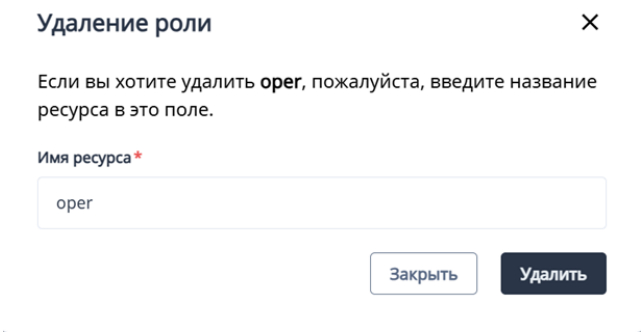


Рисунок 1.11 – Подтверждение имени ресурса при удалении

3. Чтобы отменить удаление пользователя необходимо нажать на кнопку «Закрыть» Закрыть.

4. Чтобы подтвердить удаление пользователя необходимо нажать на кнопку «Удалить» Удалить.

5. При успешном выполнении команды ГИП отобразит актуальный список пользователей, как это показано на рисунке 1.7.

1.6.4 БЛОКИРОВКА/РАЗБЛОКИРОВКА ПОЛЬЗОВАТЕЛЯ

Для блокировки строке с необходимым пользователем нажать на кнопку «Параметры» (рисунок 1.9) и выбрать пункт «Заблокировать» Заблокировать.

После подтверждения блокировки в основном окне ролевого доступа статус пользователя изменится с «Активен» на «Заблокирован» (рисунок 1.12).

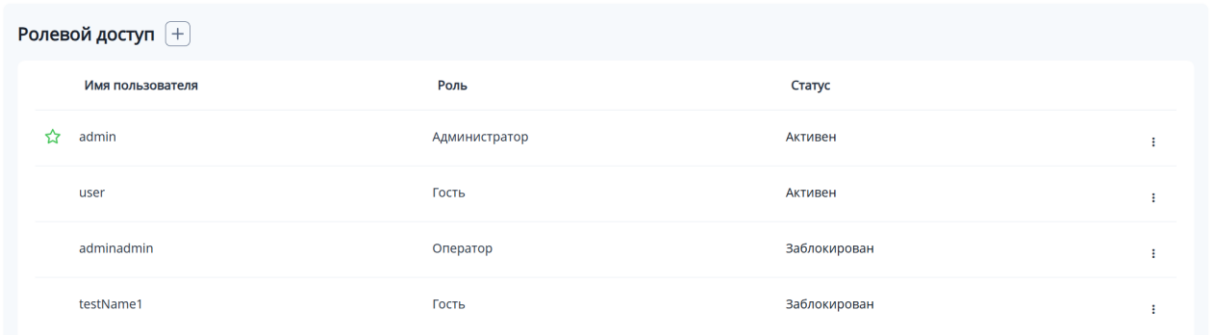


Рисунок 1.12 – Отображение заблокированных пользователей

Чтобы разблокировать нужно в строке с необходимым пользователем нажать на кнопку «Параметры» (рисунок 1.9) и выбрать пункт «Разблокировать» Разблокировать.

После подтверждения разблокировки в основном окне ролевого доступа статус пользователя изменится с «Заблокирован» на «Активен» (рисунок 1.7).

1.7 SSH-КЛЮЧИ

SSH-ключи используются для безопасного подключения к системе и состоят из двух частей:

- Приватный ключ (private key) - Конфиденциальная часть ключевой пары, которая должна храниться только у пользователя.
- Публичный ключ (public key) - Открытая часть ключевой пары, которая хранится в системе СХД для проверки подлинности подключения.

1.7.1 ПРОЦЕСС РАБОТЫ С КЛЮЧАМИ

Для начал работы с SSH ключами необходимо зайти в раздел «Безопасность» и выбрать подраздел «SSH-ключи» (рисунок 1.13).

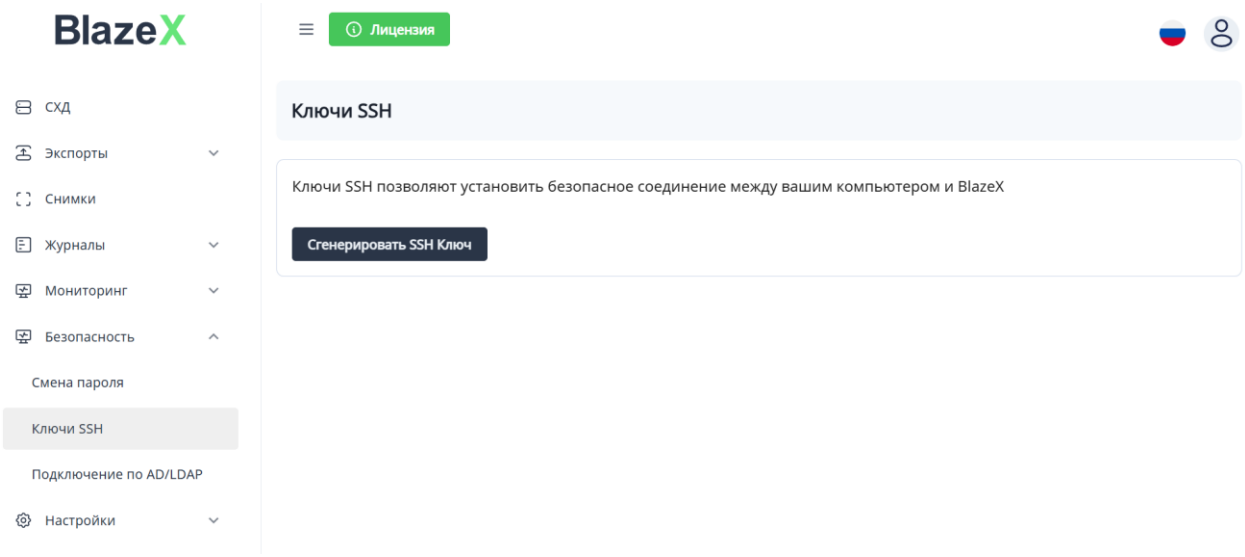


Рисунок 1.13 – Раздел «SSH-ключи»

Для генерации SSH-ключа необходимо нажать на «Сгенерировать SSH-ключ» Сгенерировать SSH Ключ. Появится модальное окно подтверждения генерации ключа (рисунок 1.14). Для продолжения необходимо нажать «Сгенерировать» Сгенерировать.

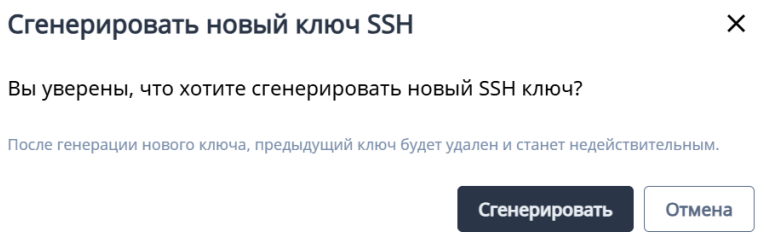


Рисунок 1.14 – Окно подтверждения создания SSH-ключа

В случае успешного выполнения команды созданный SSH-ключ отобразится в виде (рисунок 1.15)

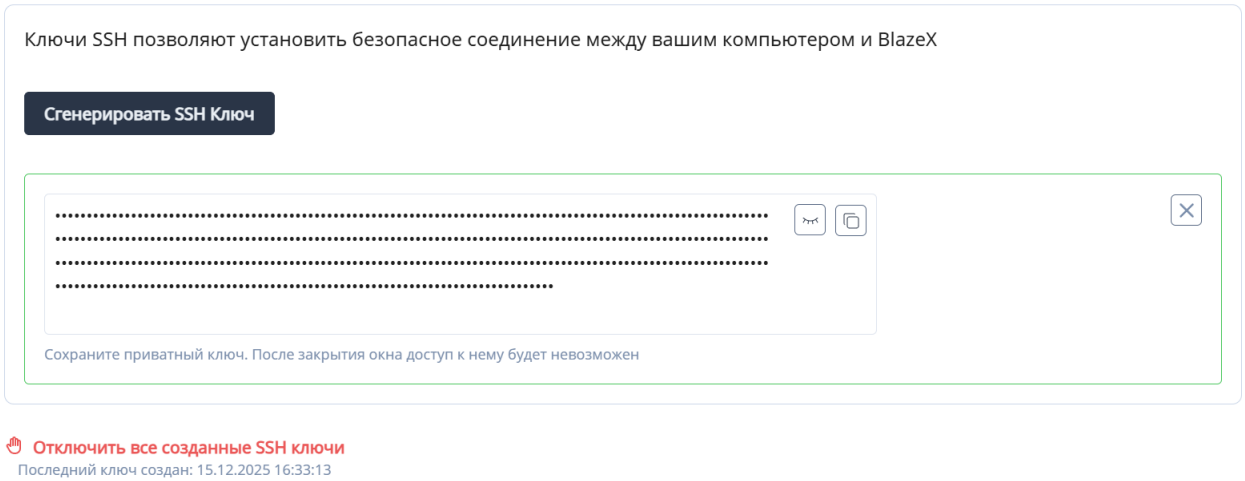


Рисунок 1.15 – Отображение сгенерированного SSH-ключа

Пользователю доступно:

1. Посмотреть SSH-ключ при нажатии на значок «Просмотр»  .
2. Скопировать SSH-ключ при нажатии на значок «Копировать»  . Ключ будет скопирован в буфер обмена.

3.

ПРИМЕЧАНИЕ.

Полученный приватный ключ необходимо сохранить в отдельный файл. Файл должен содержать только сам ключ целиком, без каких-либо изменений, дополнительных символов, комментариев и пробелов.

Для файла закрытого SSH-ключа требуются права 600 (read-only) для корректной и безопасной работы

Приватный ключ является конфиденциальной информацией и не должен передаваться третьим лицам.

4. Скрыть отображение SSH-ключа при нажатии на значок «Закрыть»  . Окно с ключом закроется, и в интерфейсе отобразится информация о последнем созданном ключе: **«Последний ключ создан: 15.12.2025 17:01:22»** (рисунок 1.16)

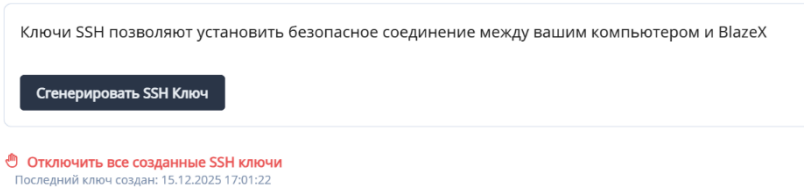


Рисунок 1.16 – Отображение в системе сгенерированного SSH-ключа

ПРИМЕЧАНИЕ.

Приватный ключ отображается только один раз при создании и не сохраняется в системе. После закрытия окна или перехода на другую вкладку он становится недоступен. Каждая новая генерация создаёт свежую пару ключей, при этом публичный ключ в системе обновляется, а старый - перестаёт действовать.

5. Удалить SSH-ключ при нажатии на кнопку «Отключить все созданные SSH-ключи» Отключить все созданные SSH ключи. В этом случает откроется модальное окно с подтвержденим удаления (рисунок 1.17).

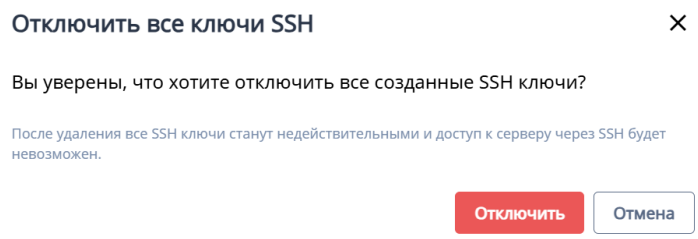


Рисунок 1.17 – Подтверждение отключения (удаления) SSH-ключа

В случае успешного выполнения команды раздел «SSH-ключи» будет отображаться в исходном виде (рисунок 1.13)

1.8 РАЗДЕЛ СИСТЕМА

Вызов раздела «Система» осуществляется выбором соответствующего пункта Система меню (рисунок 1.5).

Раздел «Система» предназначен для обновления системы и просмотра статической информации о системе хранения данных: общие сведения о системе, состояние узлов в режиме symmetric active-active, информация о ПО, технической поддержке и параметры каждого узла. Основные разделы (рисунок 1.18):

- Система
- Узел 1
- Узел 2
- Обновление системы

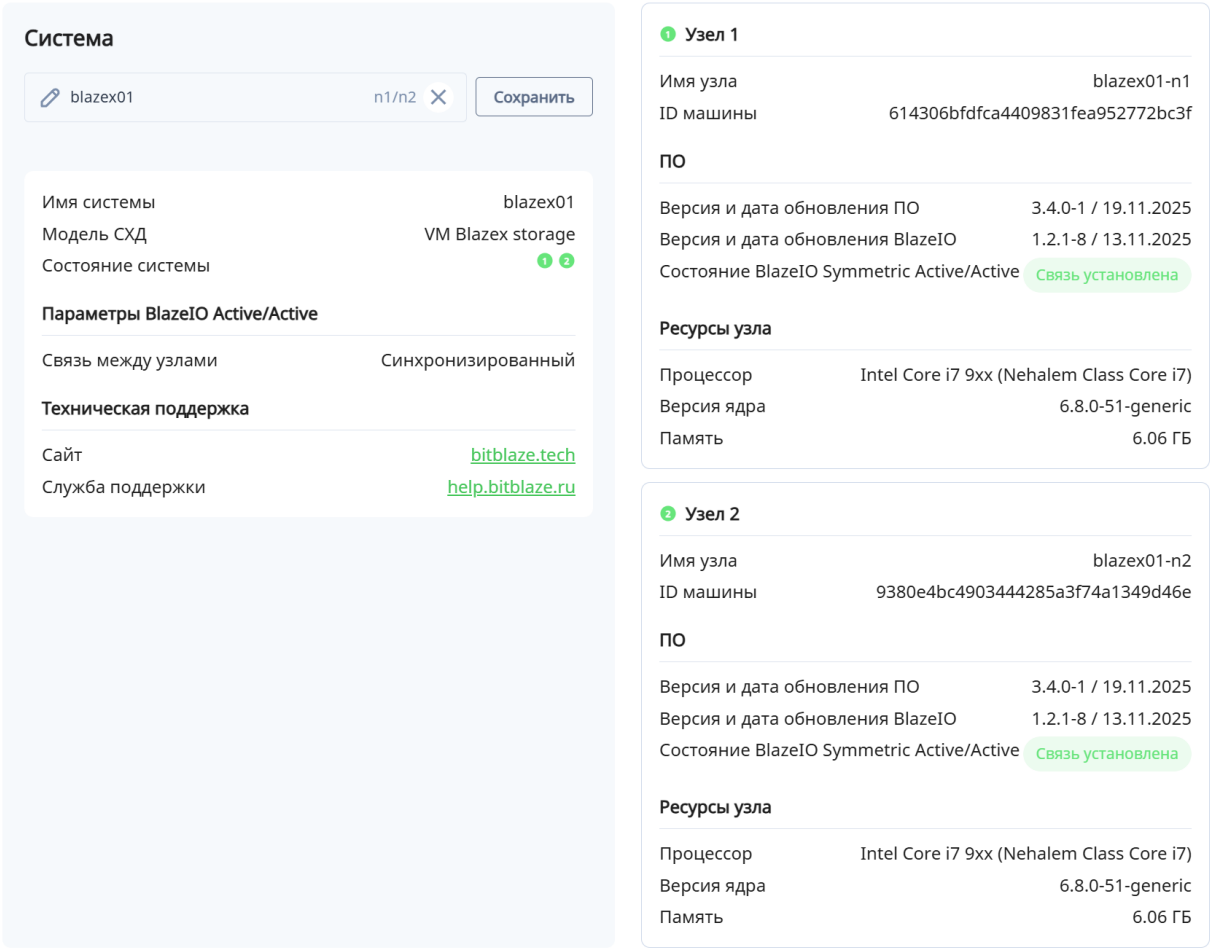


Рисунок 1.18 – Раздел «Система»

Окно **Система** содержит:

- Имя системы - наименование системы СХД

Для удобства администрирования большого парка СХД реализована возможность переименовывать систему. Для этого Сохранить истема необходимо ввести требуемое наименование и нажать «Сохранить» (рисунок 1.19).

Обозначение n1/n2 говорит о том, что имя узла будет определяться именем системы с добавлениям постфикса n1 - для Узла 1 и n2 - для Узла 2, которые формируется на основе порядкового номера узла в кластере.

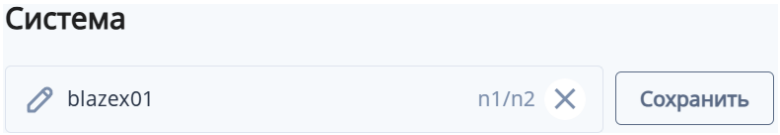


Рисунок 1.19 – Переименование системы

- Модель СХД - Модель СХД прописывается в паспорте изделия, и переносится вручную, при установке ПО
- Состояние системы 1 2 – отображает состояние узлов. Перечень состояний узлов представлен на рисунке 1.20. Состояния на обоих узлах должно быть идентичным, разное состояние узлов свидетельствует о проблемах.

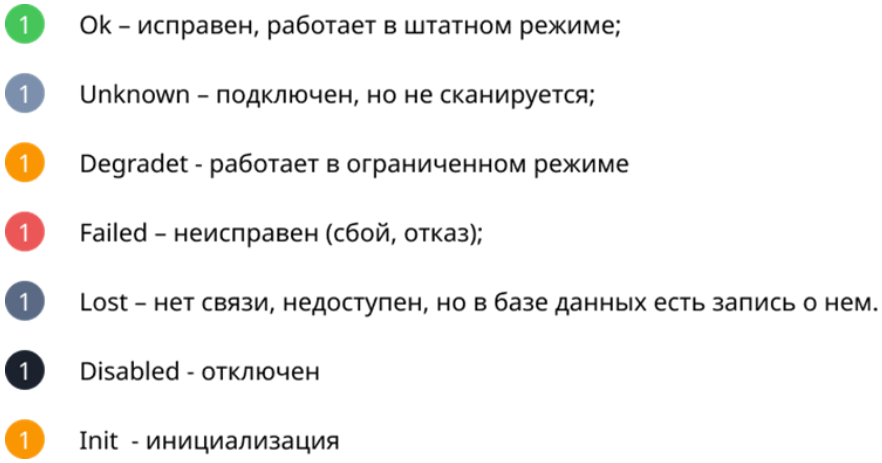


Рисунок 1.20 – Состояние узлов

Подраздел «Параметры Symmetric BlazeIO Active/Active»:

- Связь между узлами, которая может принимать следующие состояния:
  - ALONE - Независимый (одноконтроллерная)
  - IN SYNC - Синхронизированный (двухконтроллерная, оба узла работают корректно)
  - DISCONNECTED - Связь между узлами оборвалась, или еще не установлена

Подраздел «Техническая поддержка»:

- Сайт – отображается сайт компании BitTech https://bitblaze.tech/
- Служба поддержки - отображается сайт службы поддержки https://help.bitblaze.ru/site/

Область «Узел 1»

Перед именем узла 

отображается его здоровье согласно классификации на рисунке 1.20.

- Имя узла – состоит из названия СХД и постфикса с номером узла (например: blzx-773-readonly-n1)
- ID машины - Machine ID, генерируется при установке ОС

Подраздел «ПО»:

- Версия и дата обновления ПО - версия и дата последнего обновления программного обеспечения.
- Версия и дата обновления BlazeIO - версия и дата последнего обновления драйвера BlazeIO.
- Состояние BlazeIO Symmetric Active/Active – отображает состояние соединения по SAA. Перечень состояний представлен на рисунке 1.21.

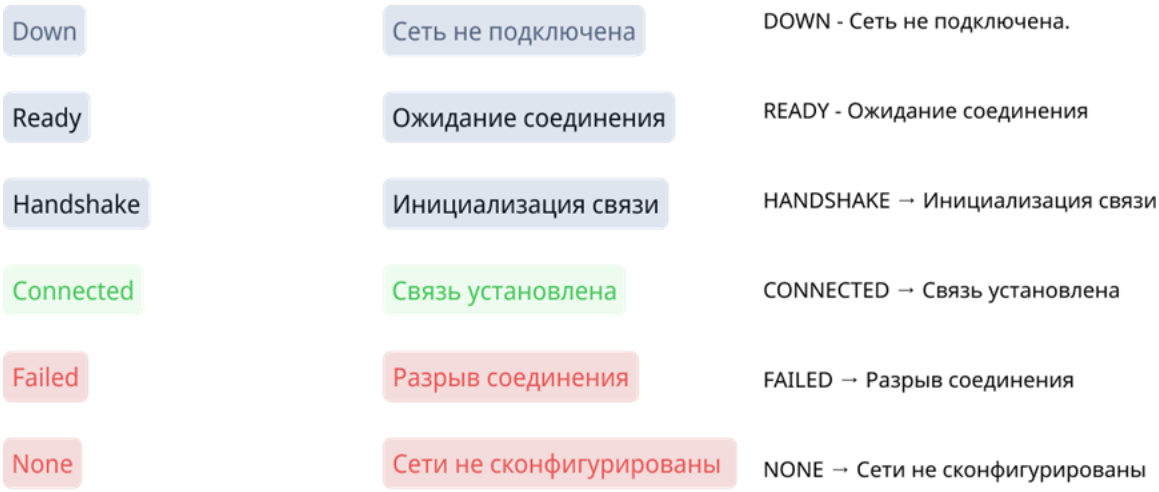


Рисунок 1.21 – Состояния BlazeIO Symmetric Active/Active

Подраздел «Ресурсы узла»:

- Процессор – марка и модель процессора
- Версия ядра - версия ядра операционной системы
- Память – Полная оперативная память узла.

При частичной недоступности отображаемых параметров система отображает «Н/Д».

Раздел «Система» при работе с одноконтроллерной СХД.

При одноконтроллерном исполнения раздел «Система» выглядит следующим образом (рисунок 1.22). В строке «Состояние системы» отображается здоровье одного узла, в параметрах Symmetric BlazeIO Active/Active статус «Независимый», в параметрах узла 1 отсутствует строка Состояние BlazeIO Symmetric Active/Active.

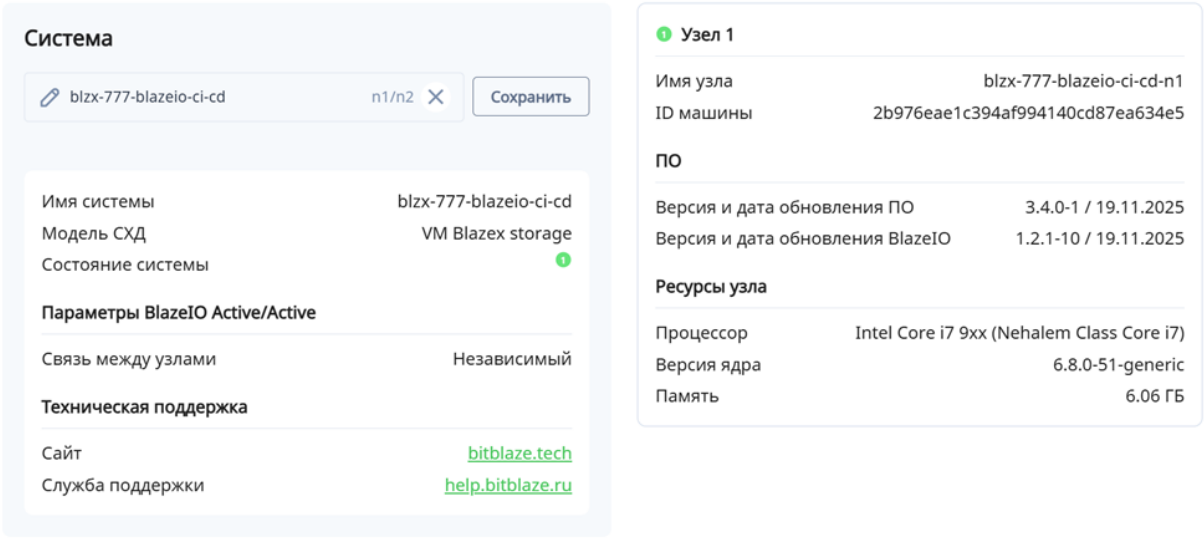


Рисунок 1.22 – Раздел «Система» при одноконтроллерном исполнении

1.8.1 ОНЛАЙН ОБНОВЛЕНИЕ

Подраздел «Обновление системы» предназначен для установки новых версий программного обеспечения BlazeX на СХД. Здесь администратор загружает образ обновления (BLZX-файл) и инициирует процесс обновления системы. (рисунок 1.23).

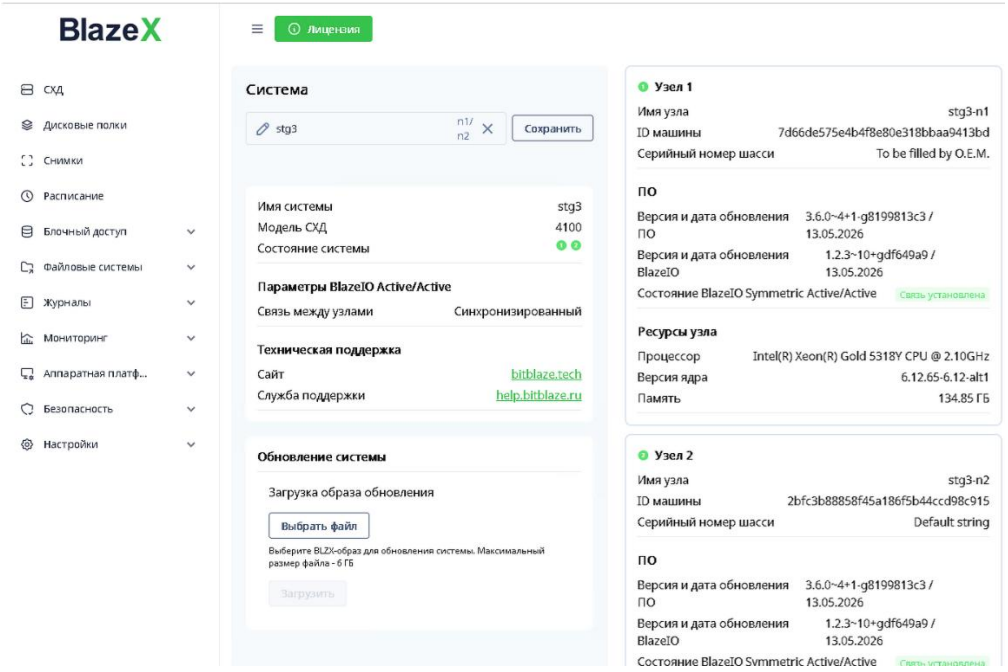


Рисунок 1.23 – Блок обновления системы в разделе «Система»

Сценарий обновления

Для обновления системы необходимо выполнить следующие действия:

1. Нажать на кнопку «Выбрать файл» 

для открытия диалога выбора файла в локальной файловой системе администратора (рисунок 1.24).

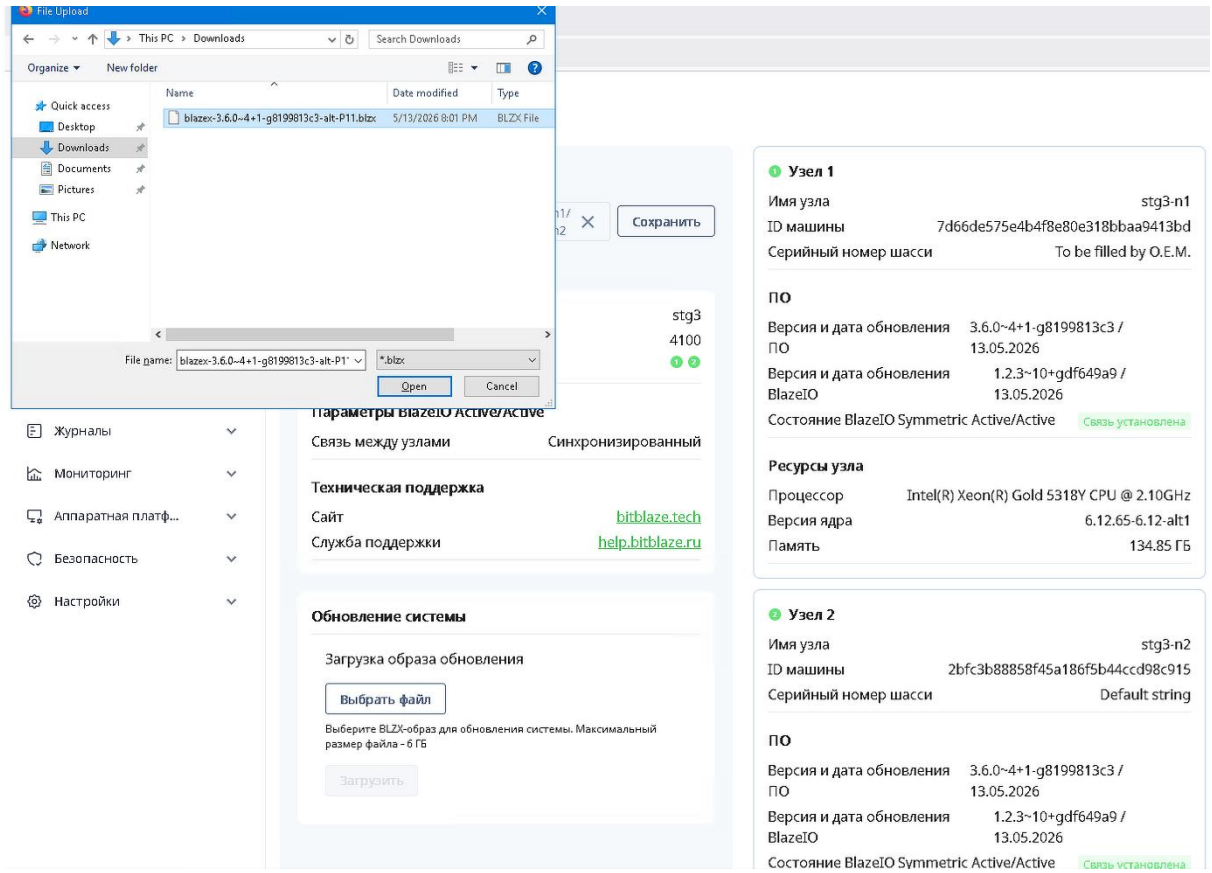


Рисунок 1.24 – Выбор файла для обновления системы

2. Нажать на кнопку «Открыть», что инициирует передачу выбранного файла на СХД для запуска процесса обновления. После подзагрузки файла блок обновления примет вид (рисунок 1.25):

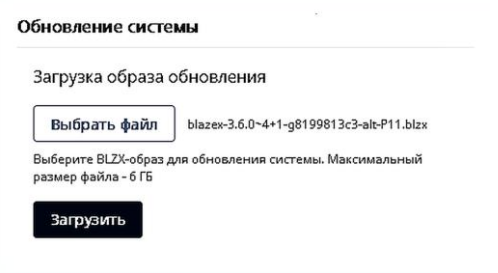


Рисунок 1.25 – Подгруженный образ обновления

3. Нажать кнопку «Загрузить» 

, чтобы инициировать загрузку файла обновления. Процесс загрузки отобразится на экране (рисунок 1.26):

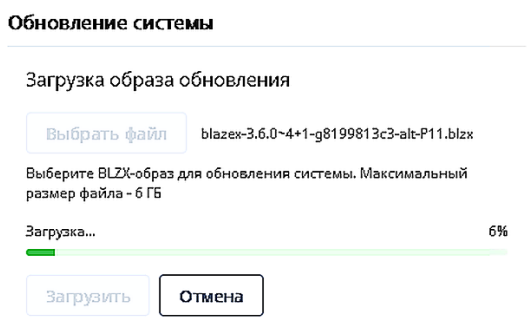
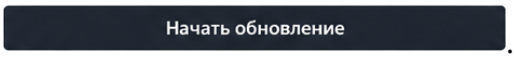


Рисунок 1.26 – Загрузка образа обновления

После загрузки образа система сообщит о готовности к обновлению системы. В блоке обновления отобразится «Готово к обновлению» (рисунок 1.27).

Рисунок 1.27 – Система готова к обновлению

Процесс обновления последовательный: сначала будет обновлен первый узел, затем второй. Перед обновлением каждого узла все его ресурсы будут автоматически перенесены на другой доступный узел.

4. Нажать кнопку «Начать обновление» 

.

Начнется обновление узла 1. Вверху окна появится статус «Выполняется обновление системы». (рисунок 1.28).

ПРИМЕЧАНИЕ

Не закрывайте браузер и не перезагружайте страницу. Процесс обновления продолжится даже после обновления страницы

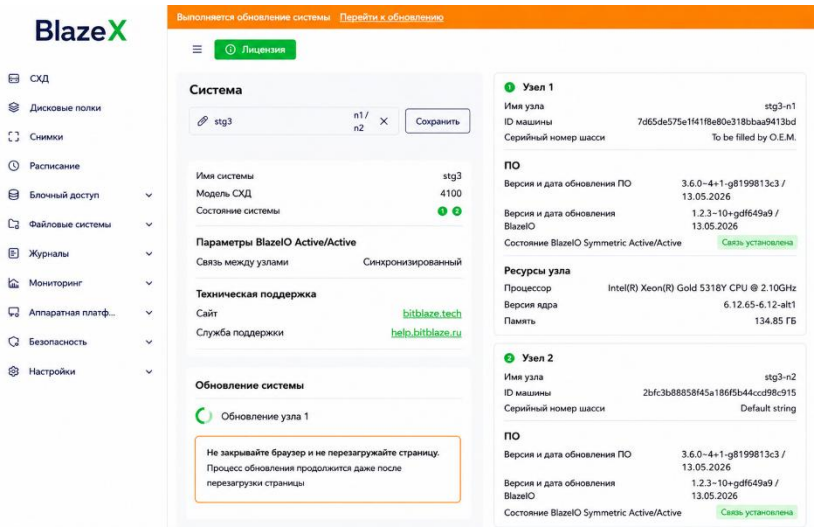


Рисунок 1.28 – Обновление узла 1

После обновления узла он должен перезагрузиться. Статус отобразится следующим образом (рисунок 1.29):

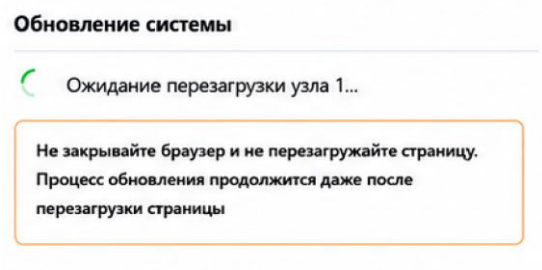


Рисунок 1.29 – Перезагрузка узла 1

Непосредственно во время перезагрузки узла вверху страницы отобразится сообщение, что включен режим «Только чтение» Соседний узел не доступен (рисунок 1.30)

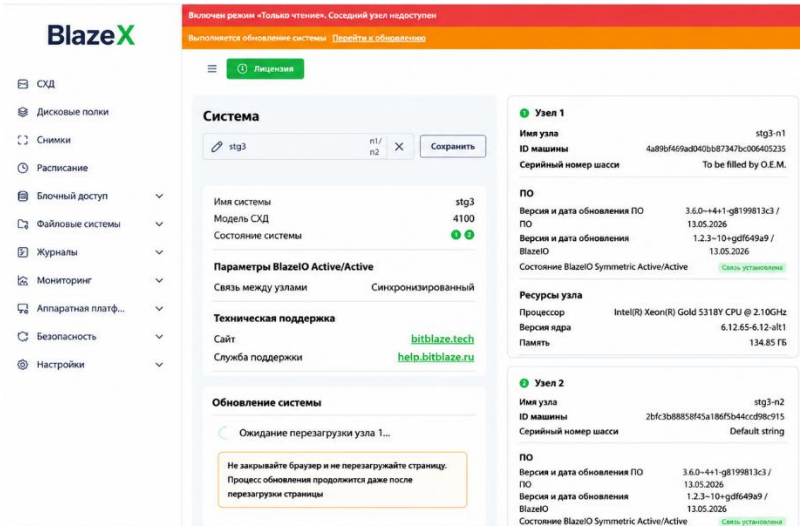


Рисунок 1.30 – Отображение процесса перезагрузки узла 1

После обновления и перезагрузки узла система сообщит об этом следующим сообщением (рисунок 1.30):

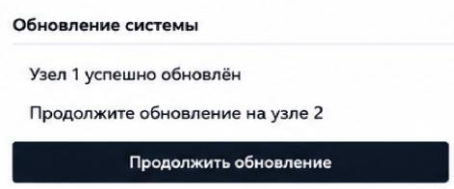


Рисунок 1.30 – Узел 1 успешно обновлен

4. Нажать кнопку «Продолжить обновление» 

. Запустится обновление узла 2 (рисунок 1.31)

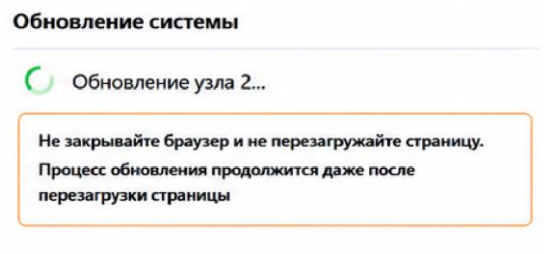


Рисунок 1.31 – Обновление узла 2

После обновления и перезагрузки второго узла обновление будет завершено. Система сообщит об этом следующим сообщением (рисунок 1.33):

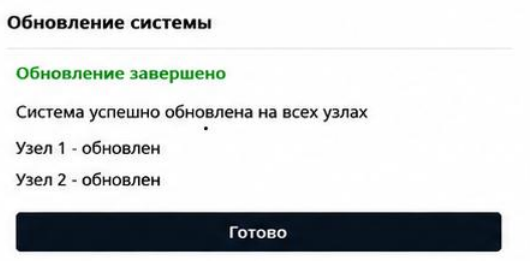


Рисунок 1.33 – Обновление завершено

После завершения обновления в разделе система произойдет обновление данных в строках «Версия и дата обновления ПО» в блоках Узел 1 и Узел 2 (рисунок 1.23).

2 СХД

Возможности ГИП сгруппированы по функциональным разделам, выбор которых осуществляется в левой боковой панели.

В раздел «СХД» осуществляется управление ресурсами: накопителями, группами накопителей (RAID–массивами) и логическими томами. Основные элементы страницы (см. рисунок 2.1):

- сводная информация о системе;
- сведения о состоянии узлов и выборе активного узла для создания ресурсов;
- сведения о накопителях;
- сведения о группах накопителей;
- сведения о логических томах.

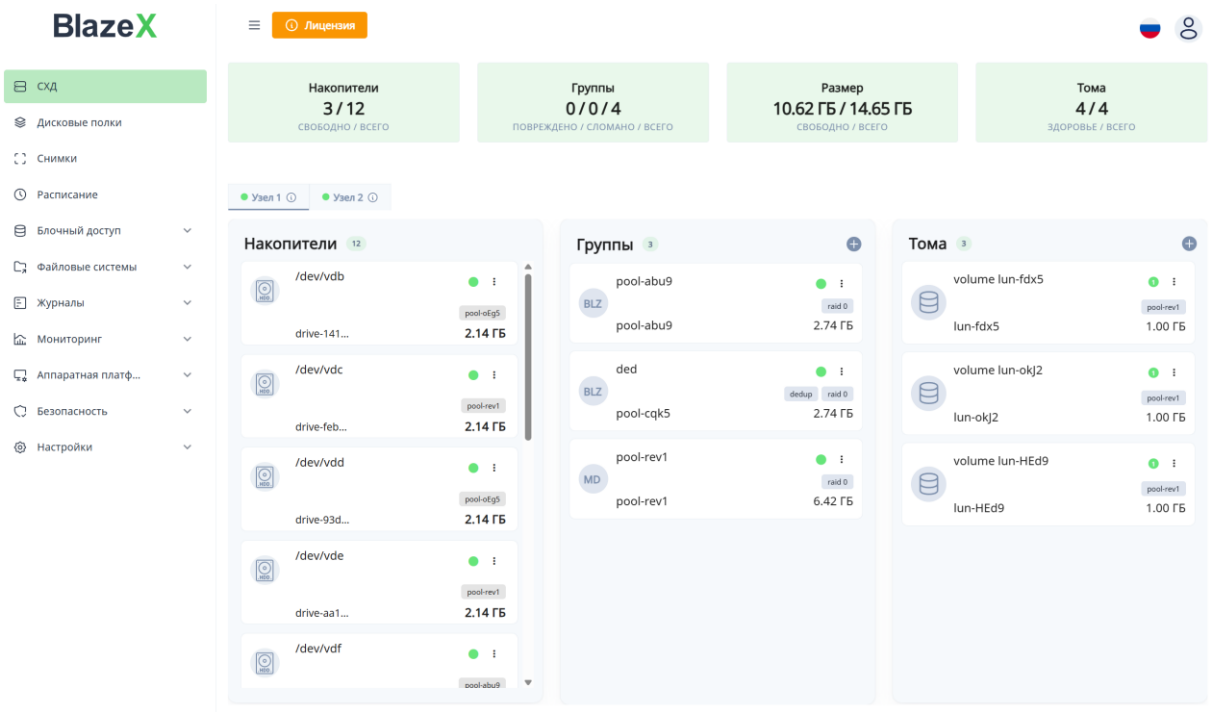


Рисунок 2.1 – Вкладка СХД

2.1 СВОДНАЯ ИНФОРМАЦИЯ О СИСТЕМЕ

Область сводной информации о системе состоит из четырех разделов: «Накопители», «Группы», «Размер», «Тома», и содержит сведения об используемых дисковых накопителях, отображает состояние логических групп, показывает соотношение экспортируемых логических томов к общему количеству.

Раздел «Накопители» указывает общее количество и количество незадействованных дисковых накопителей. Любая операция: включение в логическую группу, непосредственный экспорт дискового накопителя - снижают показатель свободных накопителей.

Раздел «Группы» отображает три ключевых значения:

- «Повреждено» - указывает на количество групп, работоспособность которых нарушена из–за отказа части дисковых накопителей, но не прекращена.
- «Сломано» - указывает на количество логических групп, работоспособность которых прекращена из–за критической ошибки.
- «Всего» - отображает общее количество созданных логических групп.

Раздел «Размер» содержит информацию о свободном пространстве памяти всех групп и общем объеме пространства всех групп.

Раздел «Тома» содержит информацию о количестве здоровых логических томов в текущий момент и общем числе созданных томов.

2.2 УЗЛЫ

2.2.1 ИНФОРМАЦИЯ ОБ УЗЛАХ

При нажатии на значок «Информация» на вкладке каждого из доступных узлов, показывается окно с системной информацией о данном узле (см. рисунок 2.2):

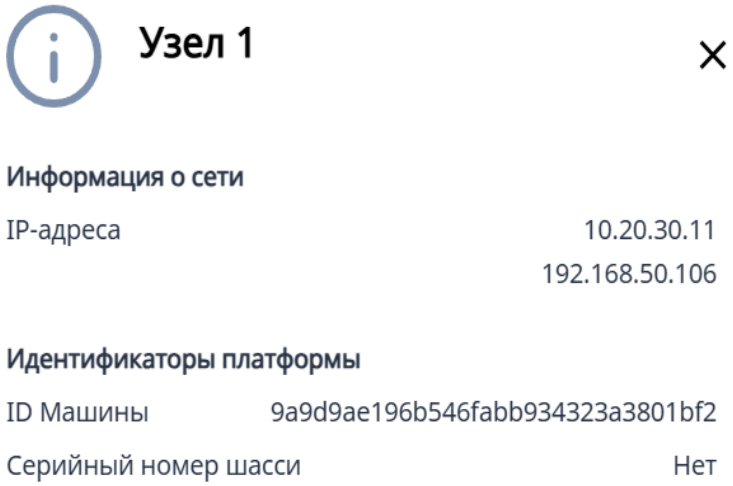


Рисунок 2.2 – Окно с системной информацией об узле

Выбор текущего узла выполняется кликом курсора на соответствующую вкладку и отображается подчеркиванием в соответствующей области. Выбор текущего узла влияет на организацию доступа к логическим ресурсам, позволяет регулировать нагрузку на

контроллер и определяет пути доступа от внешних источников к логическим ресурсам (см. рисунок 2.3).

Цветовой индикатор информирует о состоянии узла и может принимать следующие значения:

- Ok – узел работает в штатном режиме;
- Unknown – узел не сканируется в течении минуты;
- Lost – узел отключен.

Рисунок 2.3 – Вкладки узлов СХД

ВНИМАНИЕ!

При отображении черного (Lost) цветового индикатора необходимо обратиться в техническую поддержку. Контакты указаны в разделе ТЕХНИЧЕСКАЯ ПОДДЕРЖКА данного Руководства.

2.3 НАКОПИТЕЛИ

2.3.1 ИНФОРМАЦИЯ О НАКОПИТЕЛЯХ

Информация о состоянии имеющегося в системе накопителя отображается на карточке накопителя, как показано на рисунке 2.4:

- графическое отображение типа накопителя (HDD, SSD);
- наименование файла физического устройства;
- ID накопителя;
- размер накопителя в GB;
- цветовой индикатор информирует о состоянии здоровья накопителя и может принимать следующие значения:

- Ok – накопитель работает в штатном режиме;
- Unknown – накопитель подключен, но не сканируется;
- Failed – накопитель недоступен;

- Lost – накопитель отсутствует, но в базе данных есть запись о нем.

- вызов контекстного меню;
- указатель принадлежности к группе.

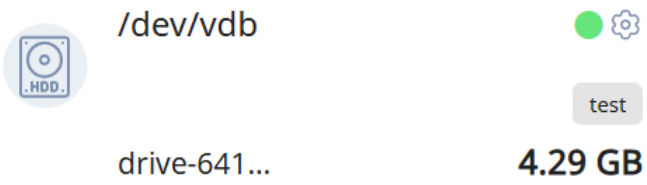


Рисунок 2.4 – Карточка накопителя

ВНИМАНИЕ!

При отображении серого (Unknown), красного (Failed) и черного (Lost) цветовых индикаторов необходимо обратиться в техническую поддержку. Контакты указаны в разделе ТЕХНИЧЕСКАЯ ПОДДЕРЖКА данного Руководства.

При нажатии на кнопку вызова контекстного меню и выборе пункта Детали (рисунок 2.4), будет показано окно деталей, содержащее подробную информацию о данном накопителе, а также ошибки, как показано на рисунках 2.5, 2.6, 2.7:

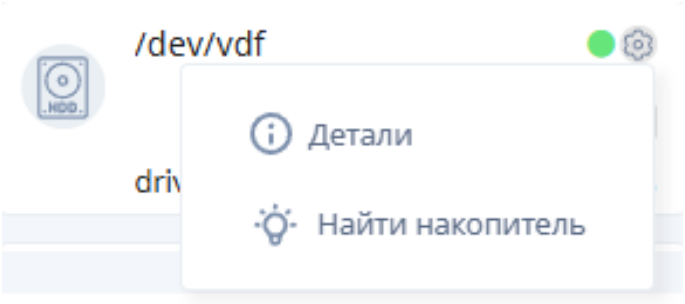


Рисунок 2.5 – Контекстное меню накопителя

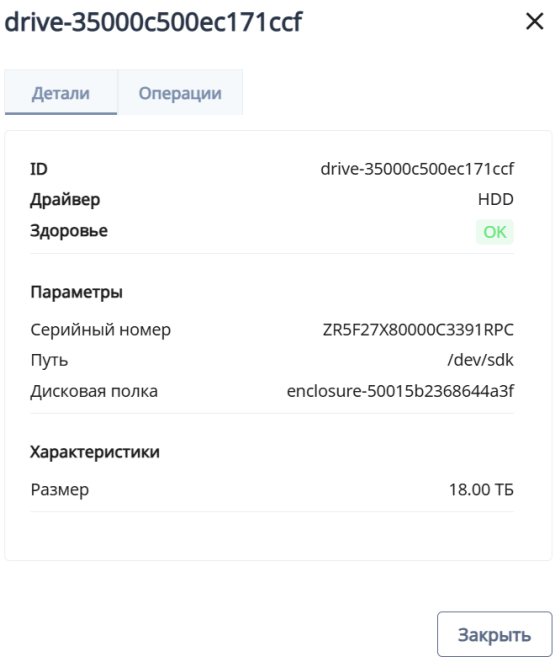


Рисунок 2.6 – Вкладка «Детали» информационного окна

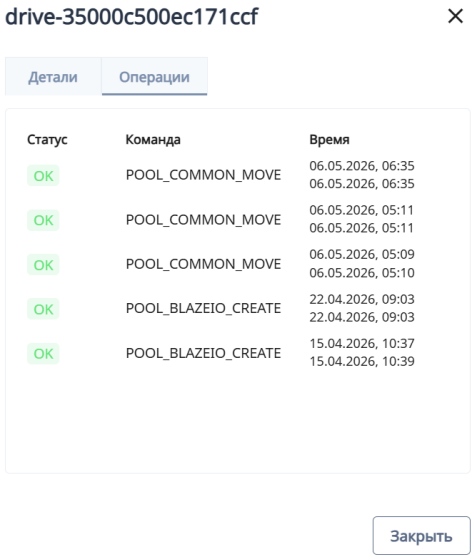


Рисунок 2.7 – Вкладка «Операции» информационного окна

2.3.2 АППАРАТНАЯ ИНДИКАЦИЯ НАКОПИТЕЛЯ

Для определения местоположения накопителя в аппаратной платформе необходимо выбрать опцию «Найти накопитель» в контекстном меню накопителя, как показано на рисунке 2.8.

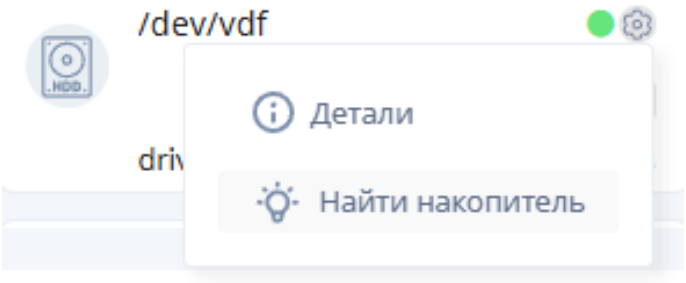


Рисунок 2.8 – Опция «Найти накопитель» в контекстном меню

После чего, в карточке накопителя, рядом с индикатором здоровья должна отобразиться мерцающая «Лампочка» (рисунок 2.9), светодиод активности и светодиод состояния на аппаратной платформе должны начать мерцать.

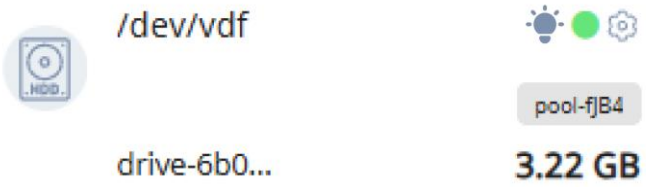


Рисунок 2.9 – Отображения включенной опции «Найти накопитель»

Чтобы отключить опцию, необходимо повторно выбрать опцию «Найти накопитель» в контекстном меню накопителя (рисунок 2.10)

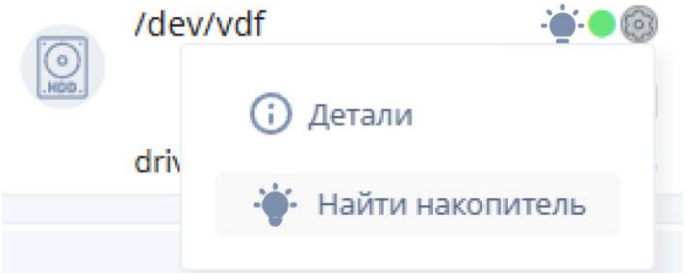


Рисунок 2.10 – Выключение опции «Найти накопитель» в контекстном меню

2.3.3 УДАЛЕНИЕ НАКОПИТЕЛЯ

Удалению подлежат только те накопители, здоровье которых:

- Unknown – накопитель находится в составе группы но не сканируется;
- Lost – накопитель отсутствует, но в базе данных есть запись о нем.

Для удаления накопителя необходимо нажать на кнопку вызова контекстного меню, как показано на рисунке 2.11 и выбрать опцию «Удалить».

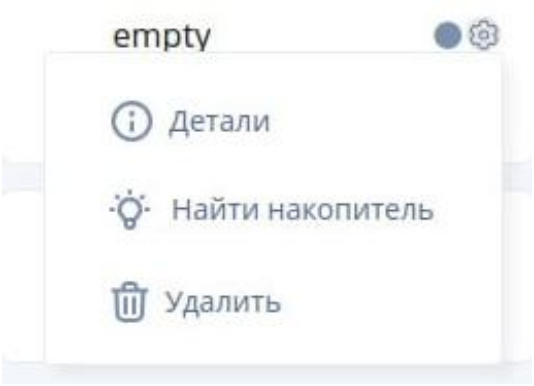


Рисунок 2.11 – Опция «Удалить» накопитель в контекстном меню

В открывшемся модальном окне, в поле «Имя ресурса» необходимо ввести имя удаляемого накопителя, как показано на рисунке 2.12, для подтверждения намерения.

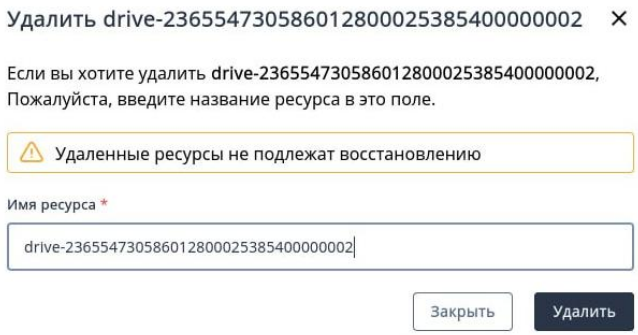


Рисунок 2.12 – Модельно окно «Удалить» накопитель

2.4 ГРУППЫ

2.4.1 СОЗДАНИЕ ГРУПП НАКОПИТЕЛЕЙ

Создание новой группы накопителей состоит из двух ключевых этапов – выбор драйвера и настройка группы.

BlazeX поддерживает три типа драйверов групп:

BlazeIO - Программный драйвер уровня ядра, оптимизированный для SSD/Flash-накопителей. Поддерживает отказоустойчивую работу хранилища при отказе до 4х дисков одновременно

BlazeIO A/A (Active/Active) – драйвер, работающий в режиме Active/Active (Symmetric) для равномерного распределения нагрузки между двумя контроллерами, и позволяющему нескольким узлам получать доступ к одному и тому же тому, что значительно повышает производительность системы

MDRaid - Классический механизм управления дисковыми массивами, рекомендованный для HDD (жёстких дисков). Поддерживает стандартные уровни избыточности

Выбор драйвера группы определяет следующие возможности:

- производительность;
- режимы отказоустойчивости:
- доступные уровни RAID;
- технологии оптимизации.

	BlazeIO A/A	**BlazeIO**	**MDRAID**
Режим отказоустойчивости	Active/Active	ALUA	ALUA
Уровни RAID	0; 1; N+M[2*]: 2+1; 4+1; 4+2; 8+1; 8+2; 8+3; 8+4	0, 1, N+M: 2+1; 4+1; 4+2; 8+1; 8+2; 8+3; 8+4	0; 1; 5; 6
Технология объединения RAID	Не поддерживается	Композитные группы[3*]	Композитные группы
Технологии оптимизации	Thin provisioning[4*]	Thin provisioning Дедупликация[5*]	Thin provisioning Дедупликация
Технологии копирования данных	Не поддерживается	Снимки[6*] Клоны[7*]	Снимки Клоны
Горячая замена	Не	Не поддерживается	Поддерживается

[2*] Расширенные схемы избыточности по модели N+M, где N — количество дисков с пользовательскими (данными) блоками, M — количество дисков, на которые записываются блоки четности (parity), обеспечивающих отказоустойчивость.

[3*] Логическое объединение нескольких RAID–групп, с применение метода распределения данных «Striping» на этапе создания тома. Позволяет создавать тома, аналогичные по свойствам и характеристикам RAID–массивам 10, 50, 60.

[4*] Этот режим позволяет выделять пространство хранения приложениям не сразу при создании, а по мере возникновения в нем потребности у приложения, что увеличивает эффективность использования ресурсов системы хранения данных.

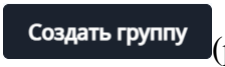
[5*] Этот режим позволяет оптимизировать емкость хранилища данных, благодаря устранению дублирующихся копий информации, тем самым снижая расходы на хранение.

[6*] Технология копирования данных, позволяющая зафиксировать состояния блочного устройства или файловой системы в определенный момент времени, быстро создавая точку восстановления, без дублирования всех данных. Подробнее в разделе 4.

[7*] Технология записи данных, сочетающая преимущества снимков (моментальное создание) и возможность их использования в качестве полноценных клонов томов. Подробнее в разделе 5.

накопителей	поддерживается		

Для выбора драйвера необходимо выполнить следующее:

1. В колонке «Группы» нажать «Добавить»  или кнопку «Создать группу»  (рисунок 2.13).

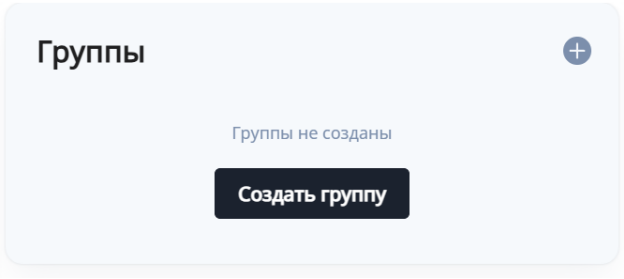


Рисунок 2.13 – Создание группы накопителей

2. После нажатия, открывается окно с настройками группы (рисунок 2.14):

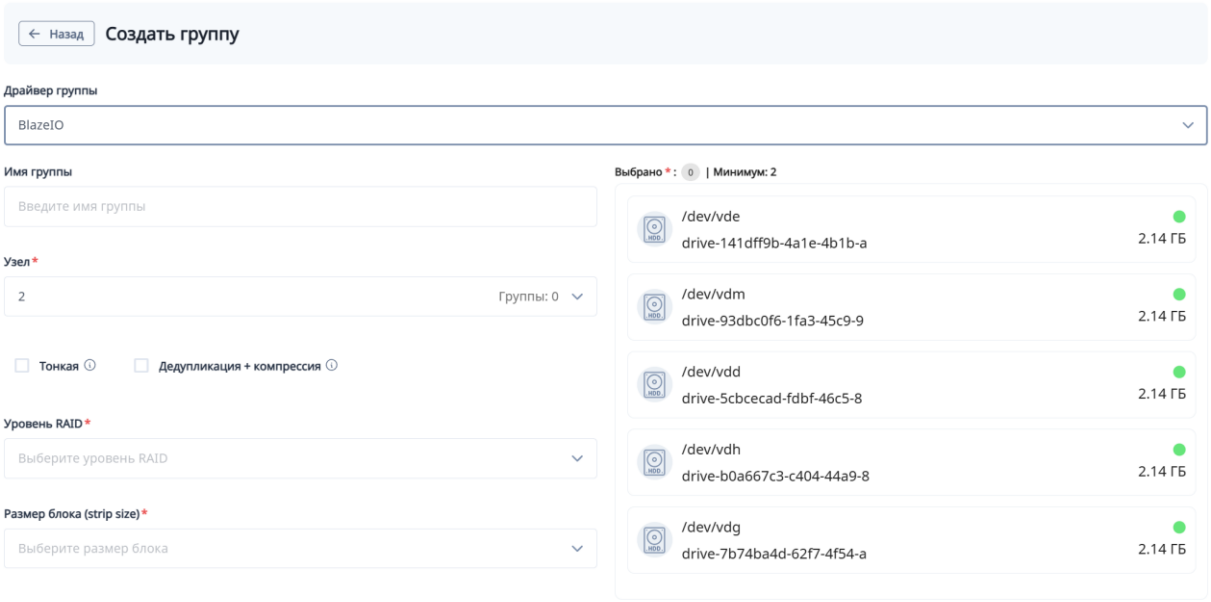


Рисунок 2.13 – Окно создания группы накопителей

В зависимости от выбора драйвера (рисунок 2.14) окна создания групп могут выглядеть следующим образом – рисунки 2.15, 2.16, 2.17

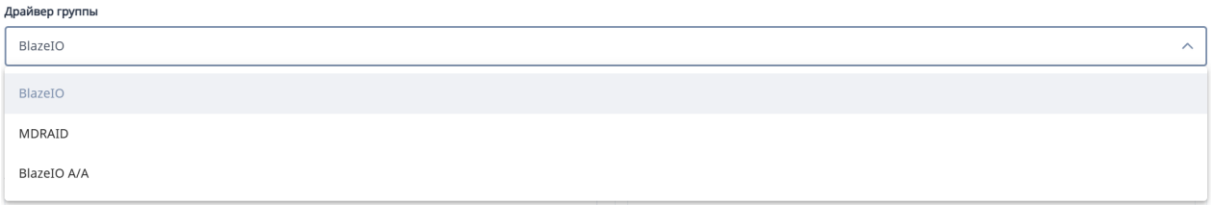


Рисунок 2.14 – Выбор драйвера при создании группы накопителей

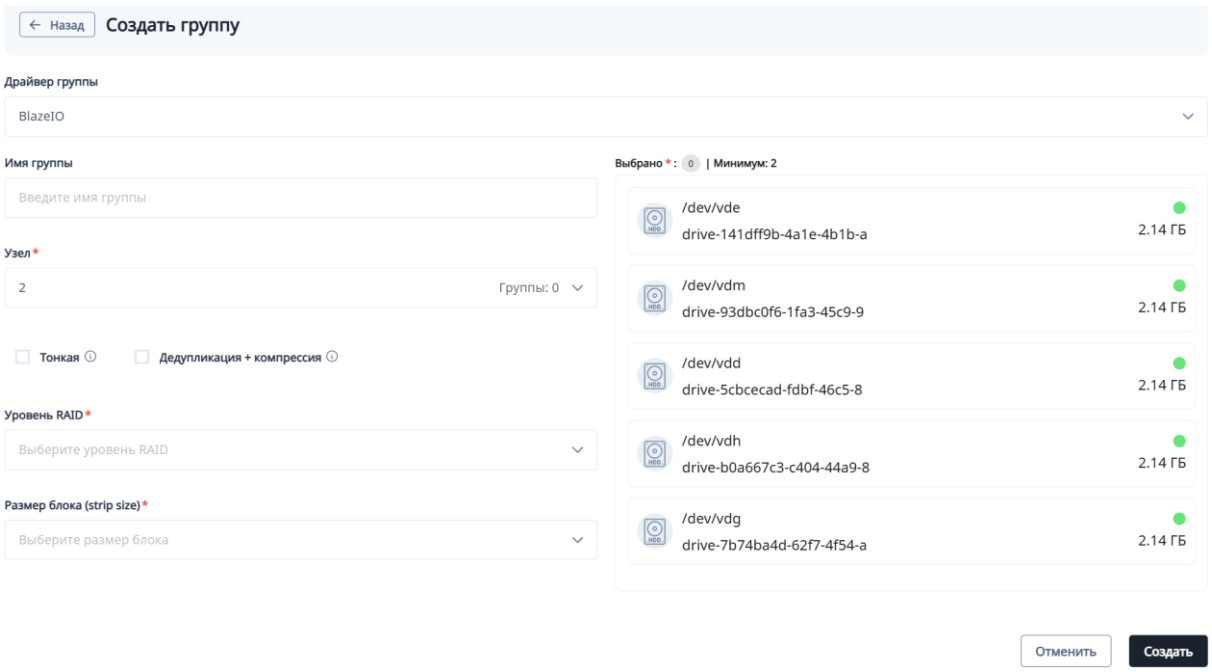


Рисунок 2.15 – Окно создания группы накопителей с драйвером BlazeIO.

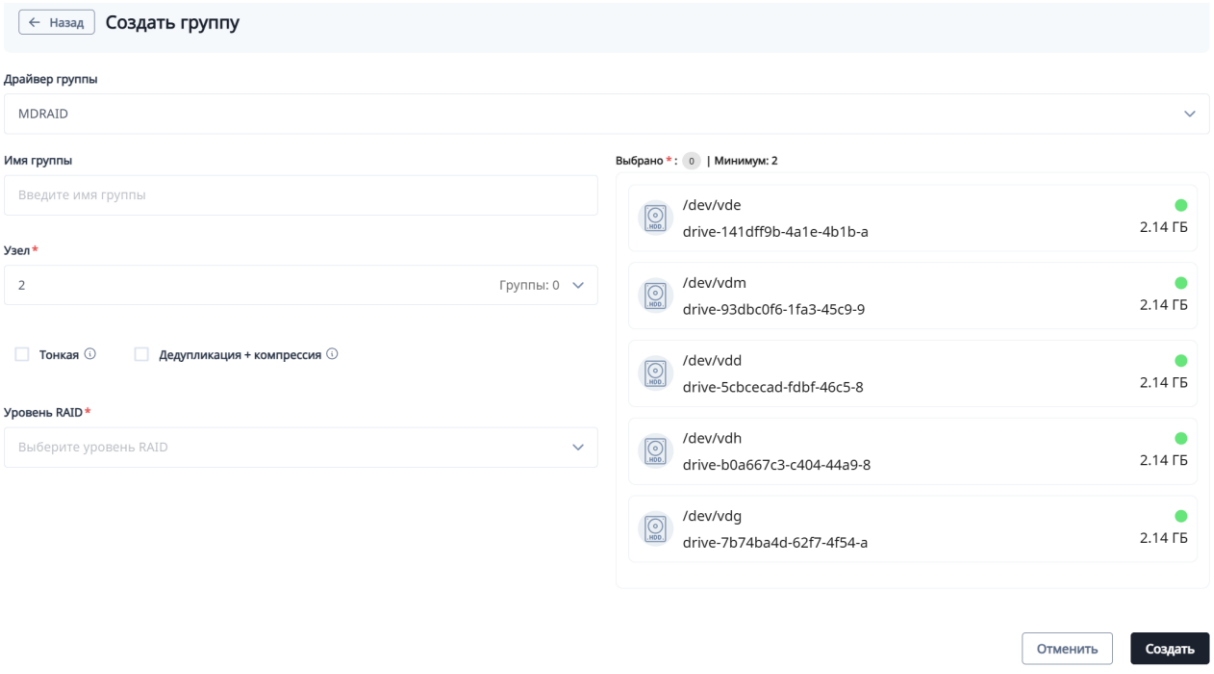


Рисунок 2.16 – Окно создания группы накопителей с драйвером MDRAID.

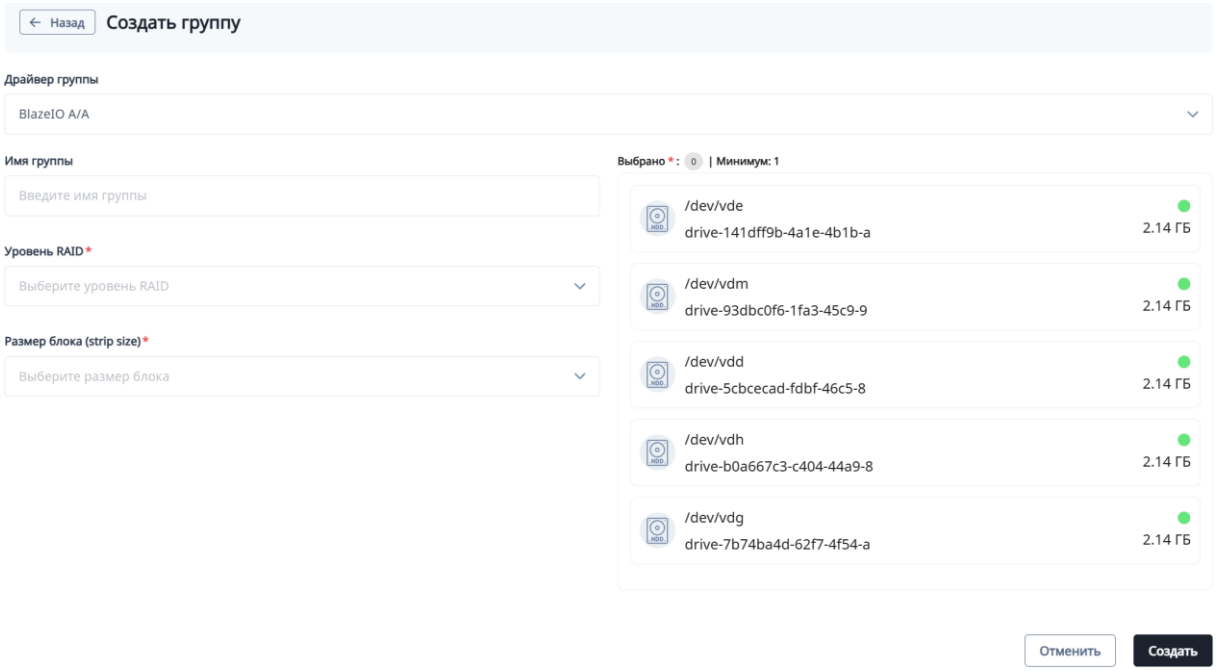


Рисунок 2.17 – Окно создания группы накопителей с драйвером BlazeIO A/A.

1. Задать имя группы накопителей (данный параметр не является обязательным для заполнения, если данное поле не будет заполнено, вместо имени будет отображаться ID группы накопителей).

2. Указать узел, который будет являться активным для создаваемой группы. Для группы с драйвером BlazeIO A/A оба узла будут являться активными.

3. При необходимости, выбрать технологию оптимизации. При выборе одного поля, второе автоматически становится заблокированным. Для группы с драйвером BlazeIO A/A

ПРИМЕЧАНИЕ. Особенности планирования массива

- При планировании массива, важно учесть, что от выбора технологии оптимизации будут зависеть доступные типы томов:

Технология оптимизации	**Тип тома**
Технология не выбрана	Обычный
Thin provisioning	Обычный, thin provisioning
Дедупликация	Обычный, дедуплицированный

- Выбирая «Thin provisioning» и «Дедупликацию» пользователь может задавать виртуальный размер тома на полный размер группы с динамическим предоставлением дискового пространства;
- Тип тома «Striped» будет доступен только при выборе «Объединенной» группы. Подробнее см. в разделе 2.5.1.

4. Указать уровень RAID, после чего, станет доступной область выбора накопителей и настройки размера блока (Strip size).
5. Выбрать размер блока из выпадающего списка.

Настройка параметра «Размер блока (Strip size)» зависит от драйвера и уровня RAID группы:

RAID	**BlazeIO A/A и BlazeIO**	**MDRAID**
RAID 0, 1,	4, 8, 16, 32, 64, 128 KB	512 K и изменению не подлежит
RAID 5, 6	—	4, 8, 16, 32, 64, 128, 256, 512, 1024 KB
N+M (Схемы: 2+1; 4+1; 4+2; 8+1; 8+2; 8+3; 8+4)	4, 8, 16, 32, 64, 128 KB	—

6. В колонке справа выбрать накопители, которые войдут в состав новой группы. Выбранные накопители подсвечиваются зеленым цветом. Над областью выбора накопителей подсказка о необходимом количестве накопителей, в зависимости от выбранного уровня RAID (рисунки 2.17, 2.18).

ПРИМЕЧАНИЕ

Количество накопителей должно соответствовать выбранному в п. 5 уровню RAID следующим образом:

	BlazeIO A/A и BlazeIO	**MDRAID**
RAID 0	2, 4, 8, 16 и т.д. – должно быть кратно двум в степени. В случае если количество накопителей отличное от рекомендованного, накопители будут присутствовать в группе, но не будут задействованы в записи данных.	минимум 2
RAID 1	2 - 5 – в случае, если количество накопителей превышает максимальное рекомендованное, накопители будут присутствовать в группе, но не будут задействованы в записи данных.	минимум 2
RAID 5	—	минимум 3
RAID 6	—	минимум 4
RAID N+M	Схемы: 2+1; 4+1; 4+2; 8+1 – количество накопителей должно соответствовать сумме значений выбранной схемы.	—

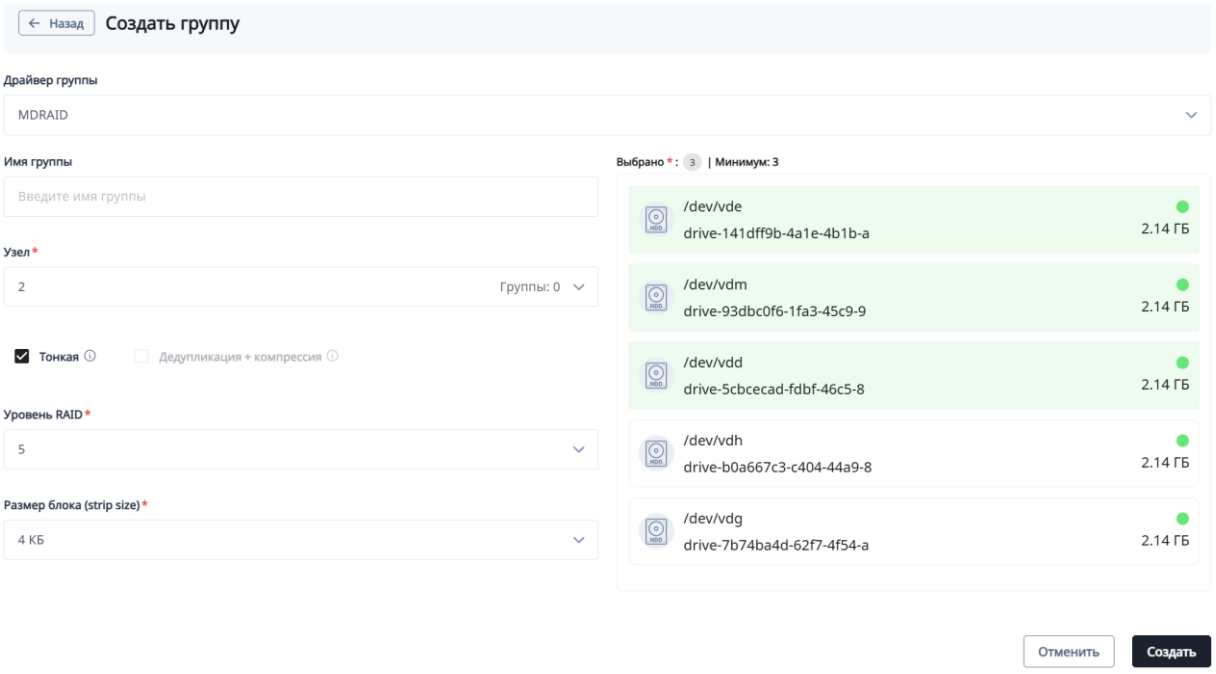


Рисунок 2.18 – Заполненное окно создания группы накопителей с драйвером MDRAID.

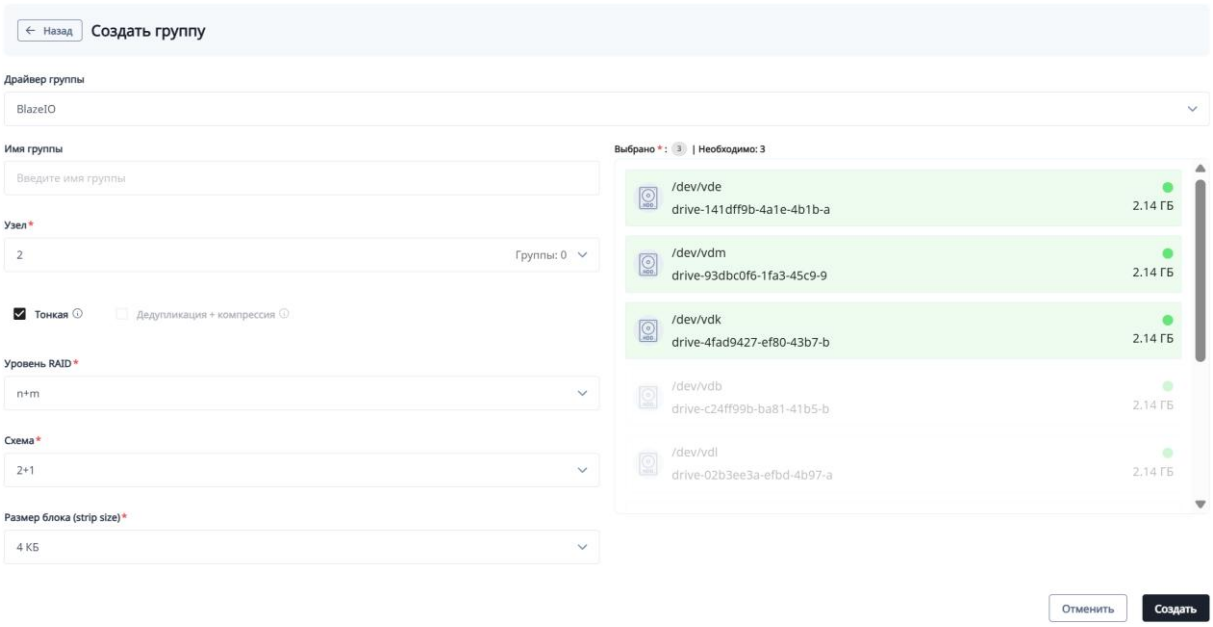


Рисунок 2.19 – Заполненное окно создания группы накопителей с драйвером BlazeIO.

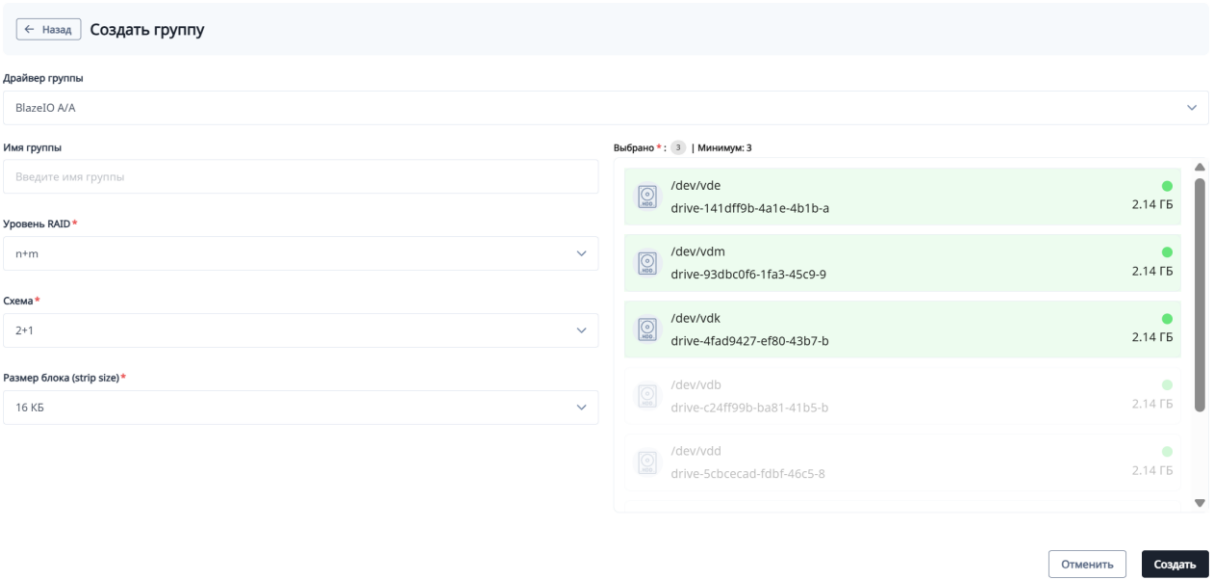


Рисунок 2.20 – Заполненное окно создания группы накопителей с драйвером BlazeIO A/A.

7. При успешном выполнении команды ГИП отобразит новую группу накопителей, как это показано на рисунке 2.21.

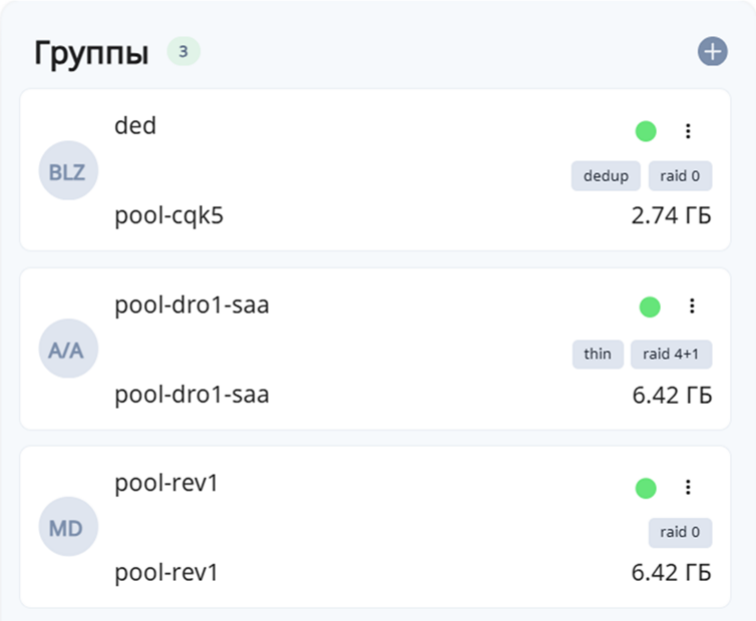


Рисунок 2.21 – Пример созданных групп накопителей

ВНИМАНИЕ!

Если при создании группы накопителей происходит ошибка, удалите группу и создайте ее заново. Если после нескольких попыток ошибки повторяются, то необходимо обратиться в техническую поддержку. Контакты указаны в разделе ТЕХНИЧЕСКАЯ ПОДДЕРЖКА данного Руководства.

2.4.1.1 СЦЕНАРИИ ПРИМЕНЕНИЯ SYMMETRIC ACTIVE-ACTIVE

Режим SAA является узкоспециализированным. Его применение оправдано исключительно в следующих случаях:

1. **Повышение пропускной способности для одного тома**

В системе создан **единственный том**, занимающий все доступное дисковое пространство, и этот том должен обслуживаться с максимально возможной скоростью.

В конфигурациях с двумя и более томами использование SAA приводит к снижению общей производительности системы по сравнению с ALUA из-за накладных расходов на внутреннюю синхронизацию и отсутствия редиректов.

2. **Минимизация времени восстановления (быстрый Failover)**

Критичность отказа оборудования превышает требования к производительности в штатном режиме. Необходимо обеспечить минимальное время переключения нагрузки при выходе из строя одного из контроллеров. Данный сценарий предполагает, что администратор готов пожертвовать общей производительностью системы в пользу скорости отказоустойчивости.

ПРИМЕЧАНИЕ

Режим SAA **не поддерживает** создание снапшотов, репликацию, дедупликацию и другие функции высокого уровня.

Критические ограничения и недопустимые сценарии

Использование Symmetric Active-Active **категорически запрещено** в перечисленных ниже случаях без предварительной технической доработки системы.

1. **Работа с файловыми системами VMFS (VMware)**

Использование томов в режиме SAA для размещения датасторов VMware ESXi (VMFS) строго запрещено. SAA не обеспечивает корректную атомарность SCSI-команд резервации (Persistent Reserve In/Out, Reserve, Release) между узлами. Это приводит к конфликтам записи и **повреждению данных** на датасторе. Для VMFS используйте только режим ALUA.

2. **Приложения с жесткой привязкой к SCSI-резервациям**

Запрещено любое ПО, использующее механизмы SCSI-2/SCSI-3 резерваций для синхронизации доступа к общему тому. В текущей реализации SAA данные команды обрабатываются локально на каждом узле и не синхронизируются с соседним контроллером, что нарушает логику работы кластерных файловых систем (кроме случаев, когда синхронизация вынесена на уровень приложения, например, через DLM).

ВНИМАНИЕ!

Перед включением режима SAA убедитесь, что ваше прикладное ПО не использует блокировки на уровне SCSI. В противном случае это приведет к нестабильности работы сервисов.

2.4.2 ИНФОРМАЦИЯ О ГРУППЕ

Информация о состоянии имеющейся в системе логической группы накопителей отображается на карточке группы, как показано на рисунке 2.22:

- наименование драйвера;
- имя логической группы;
- ID группы;
- общий размер логической группы, пересчитанный с учетом выбранного уровня RAID в GB;
- цветовой индикатор состояние здоровья группы;

- вызов контекстного меню;
- технология оптимизации пространства хранения данных;
- уровень RAID созданной группы.

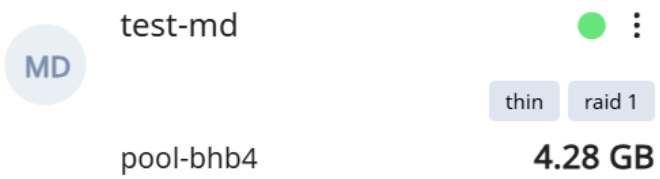


Рисунок 2.22 – Карточка группы

Цветовой индикатор информирует о состоянии группы и может принимать следующие значения:

- Ok – группа работает в штатном режиме;
- Degraded – группа пребывает в процессе восстановления или построения «Rebuilding», или возникла проблема с частью накопителей, но система продолжает функционировать на имеющихся ресурсах;
- Failed – группа недоступна;
- Unknown или Lost – группа отсутствует на сканере, но в базе данных есть запись о ней.

ВНИМАНИЕ! Рекомендуемые действия для восстановления работоспособности группы

- В случае если состояние здоровья остается «Degraded» по завершении процесса «Rebuilding», проверьте, все ли накопители принадлежащие к группе исправны в колонке «Накопители». Если в группе находится сбойный накопитель, проверьте его подключение к аппаратной платформе. При необходимости, замените на исправный.
- В случае если состав группы неполный, необходимо добавить количество накопителей соответствующее требованиям выбранного уровня RAID
- При отображении красного (Failed), или черного (Unknown или Lost) обратитесь техническую поддержку. Контакты указаны в разделе ТЕХНИЧЕСКАЯ ПОДДЕРЖКА данного Руководства.

При нажатии на кнопку вызова контекстного меню группы и выборе пункта меню Детали (рисунок 2.23), будет показано окно деталей, содержащее подробную информацию о данной группе: доступное пространство, технологию оптимизации

(тонкий том или дедупликация), уровень RAID, произведенные операции, как показано на рисунках 2.21 и 2.22.

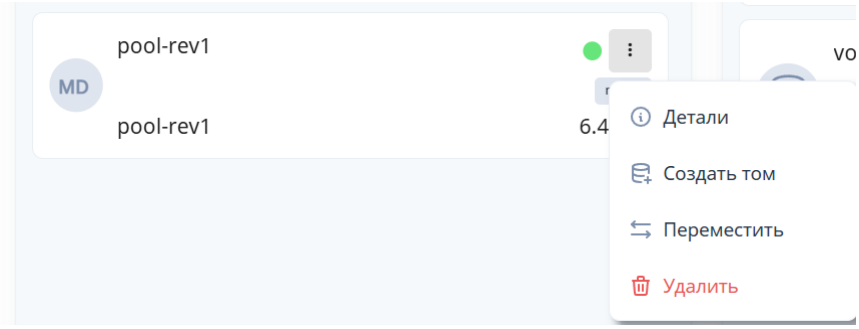


Рисунок 2.23 – Контекстное меню группы с драйвером MDRAID

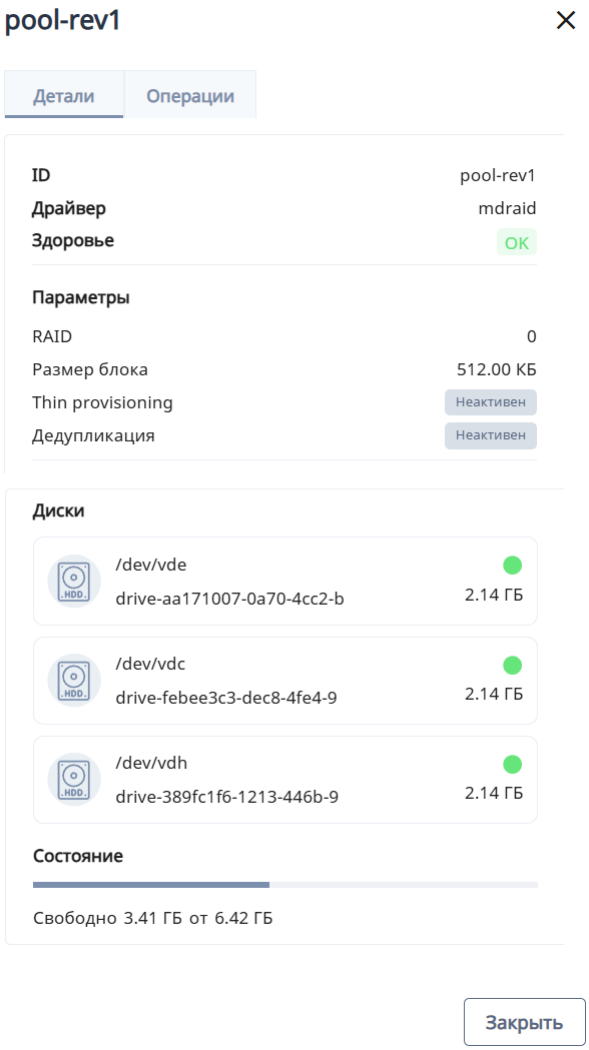


Рисунок 2.24 – Вкладка «Детали»

ВНИМАНИЕ!

При создании группы Blazeio часть пространства автоматически резервируется под метаданные, поэтому сразу после создания в информации о группе будет отображаться ненулевой занятый объём.

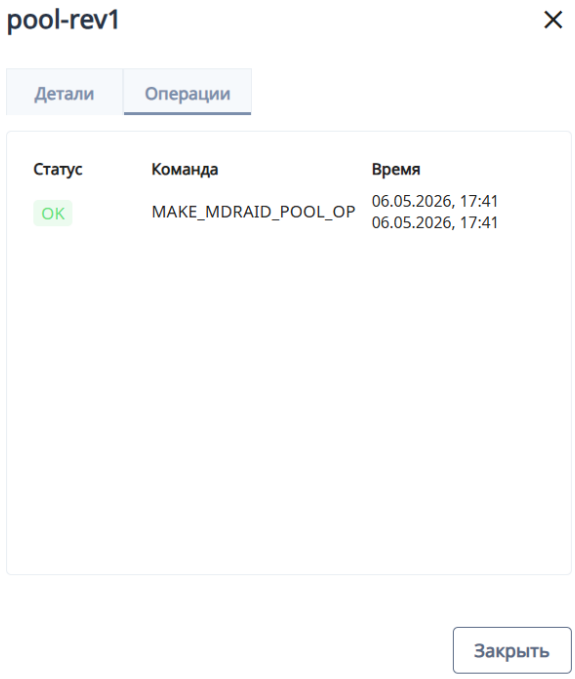


Рисунок 2.25 – Вкладка «Операции»

При нажатии на строку с операцией система перейдет в журнал команд.

ПРИМЕЧАНИЕ

Подробно о журнале команд в разделе 7.4 «Журнал команд» данного руководства

ВНИМАНИЕ!

При работе с ресурсами необходимо соблюдать последовательное выполнение операций. Например, необходимо дождаться завершения процесса создания группы для выполнения следующих действий в системе.

2.4.3 РЕДАКТИРОВАНИЕ ГРУППЫ НАКОПИТЕЛЕЙ

ПРИМЕЧАНИЕ

Опция «Редактировать» недоступна в случае, если группа пребывает в процессе создания/перестроения (rebuilding) и инициализации.

Опция «Редактировать» группу позволяет исключать, добавлять и заменять как сбойные, так и исправные накопители в уже созданной группе. Замена накопителей может осуществляться вручную или посредством опции горячей замены.

2.4.3.1. РУЧНАЯ ЗАМЕНА НАКОПИТЕЛЯ

ВНИМАНИЕ!

В случае, когда осуществляется редактирование группы со сбойным накопителем, в первую очередь необходимо заменить сбойный накопитель.

Для замены сбойного или исправного накопителя вручную, необходимо нажать на кнопку вызова контекстного меню и выбрать действие «Редактировать». Откроется окно редактирования, как показано на рисунке 2.26.

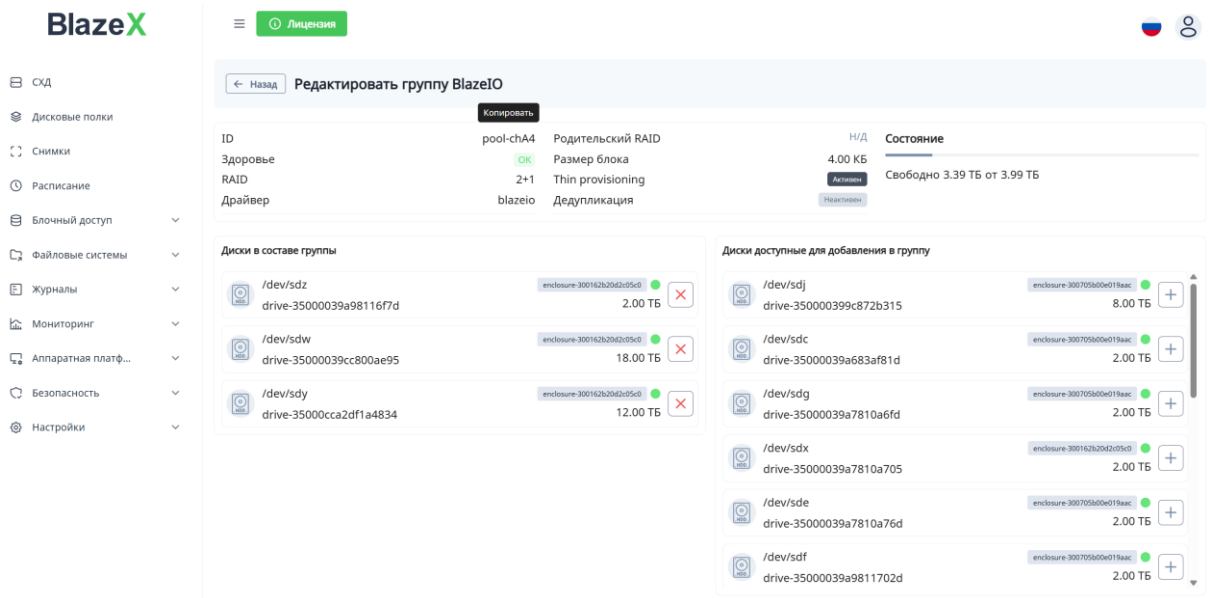


Рисунок 2.26 – Окно «Редактировать» группу накопителей

В окне редактирования группы, для изменения доступна только область выбора накопителей. Процесс замены накопителей состоит из двух этапов – исключение и добавление.

ПРИМЕЧАНИЕ

- Каждый этап является отдельной итерацией редактирования – за одну итерацию

возможно исключить или добавить лишь один накопитель.
- Для сохранения изменений конфигурации группы, после каждого действия, необходимо сохранять изменения, нажав кнопку «Сохранить».
- Для выполнения каждой новой итерации редактирования необходимо дождаться завершения процесса «Rebuilding»

Для того, чтобы исключить накопитель из группы необходимо нажать на него в поле выбора накопителей. Далее откроется окно подтверждения действия (рисунок 2.27).

Рисунок 2.27 – Окно «Исключения» накопителя из группы

Для того, чтобы добавить накопитель в группу, необходимо нажать на карточку любого доступного накопителя, в области выбора накопителей, и она окрасится в зеленый.

2.4.3.2. ГОРЯЧАЯ ЗАМЕНА НАКОПИТЕЛЯ

ПРИМЕЧАНИЕ

Горячая замена накопителей доступна только для групп с драйвером MDRAID и BlazeIO. Поддержка для драйвера Symmetric Active/Active отсутствует

Для использования функции горячей замены, после создания группы, необходимо добавить в массив резервный накопитель, который будет включён в состав группы, но не будет участвовать в записи данных, а в случае отказа одного из рабочих накопителей автоматически будет включен в процесс. Для этого необходимо выполнить следующие шаги:

1. Проверить в системе наличие одного или нескольких накопителей, не задействованных в группах.

2. Добавить свободный накопитель в созданную, здоровую группу, посредством опции «Редактировать»

3. После сохранения изменений в группе, добавленный накопитель будет маркирован как "Запасной", и станет частью группы, но не будет участвовать в записи данных.

В случае сбоя одного из накопителей в группе, замена на «Запасной» происходит автоматически, при этом:

1. Состояние здоровья группы меняется на "Degraded", система автоматически замещает сбойный накопитель на запасной. RAID остаётся работоспособным.
2. Лэйбл "Запасной" исчезает, накопитель перестаёт быть резервным и полноценно включается в RAID–массив.
3. Группа переходит в состояние "Rebuilding", а здоровье группы меняется на "Degraded", начинается процесс восстановления данных на новом накопителе.
4. По завершении восстановления, статус и здоровье группы возвращаются в состояние «Ok».
5. В окне редактирования группы остается сбойный накопитель, подсвеченный красным, его необходимо исключить вручную из состава группы, а также, из колонки "Накопители".

ПРИМЕЧАНИЕ. Особенности резервирования накопителей в RAID–массивах

RAID 1	1 резервный накопитель на каждую зеркальную пару. Возможно назначение нескольких резервных накопителей, но один уже покрывает отказ в типичной паре из двух накопителей.
RAID 5	Рекомендуется: 1–2 резервных накопителя на массив. Поддерживаются несколько резервных накопителей, но одновременно может выйти из строя только один накопитель без потери данных. Дополнительные резервные накопители остаются в очереди.
RAID 6	Рекомендуется: 1–3 резервных накопителя, в зависимости от размера массива. Способен выдержать отказ двух накопителей. Несколько резервных накопителей увеличивают общую отказоустойчивость.
RAID 0	Не поддерживает возможность добавления резервных накопителей из–за отсутствия избыточности. Выход одного накопителя приведет к полной потере данных.
Крупные массивы (>50 накопителей)	Крупные массивы (>50 накопителей) – рекомендуется 1 резервный накопитель на каждые 10–20 активных накопителей.

2.4.3.2.1 ДОБАВЛЕНИЕ ЗАПАСНОГО ДИСКА

Для добавления HotSpare накопителя пользователю необходимо:

1. Открыть веб-интерфейс BlazeX и выбрать вкладку «СХД» (рисунок 2.28)

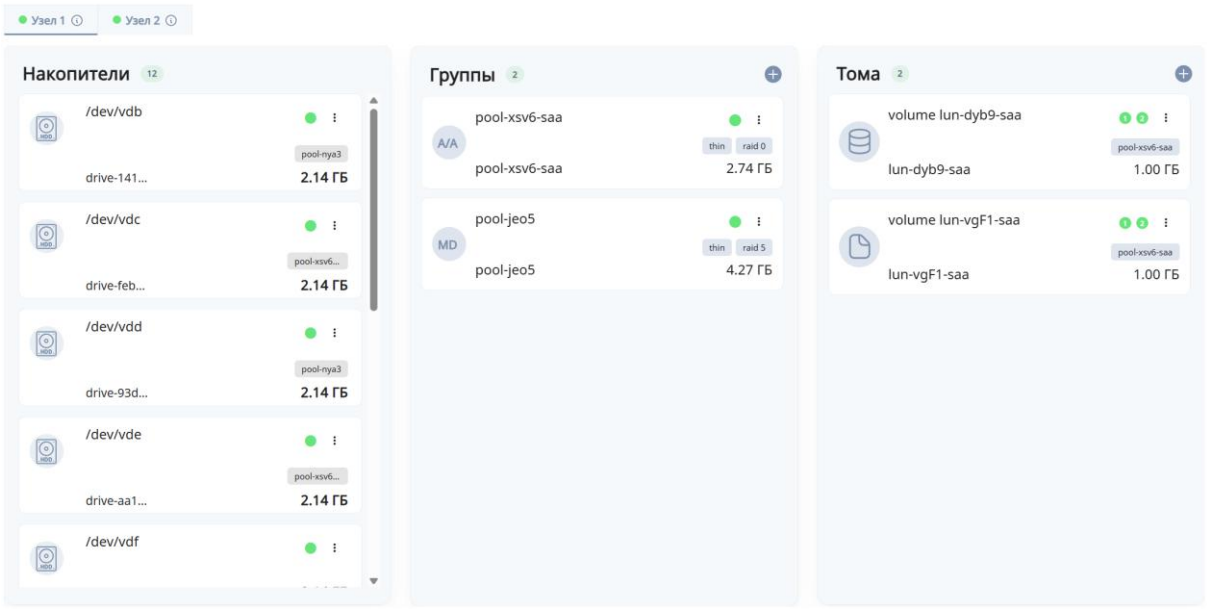


Рисунок 2.28 – Раздел СХД

2. В колонке «Группы» выберите нужную группу, например, «pool-jeo5».

ПРИМЕЧАНИЕ.

Убедитесь, что группа соответствует требованиям:

- Имеет полный набор накопителей согласно выбранной схеме RAID
- Находится в состоянии «Ok»

3. В разделе «параметры» ⋮ группы нажать «Редактировать» Редактировать (рисунок 2.29).

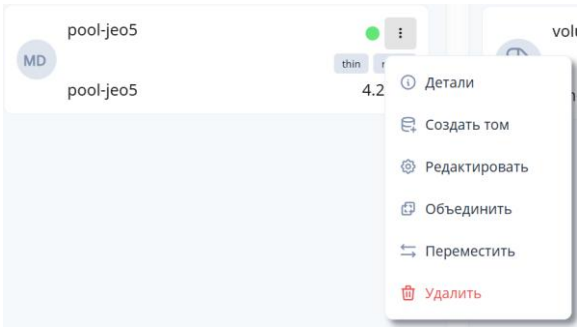


Рисунок 2.29 – Выбор редактирования группы

Откроется модальное окно редактирования группы (рисунок 2.30).

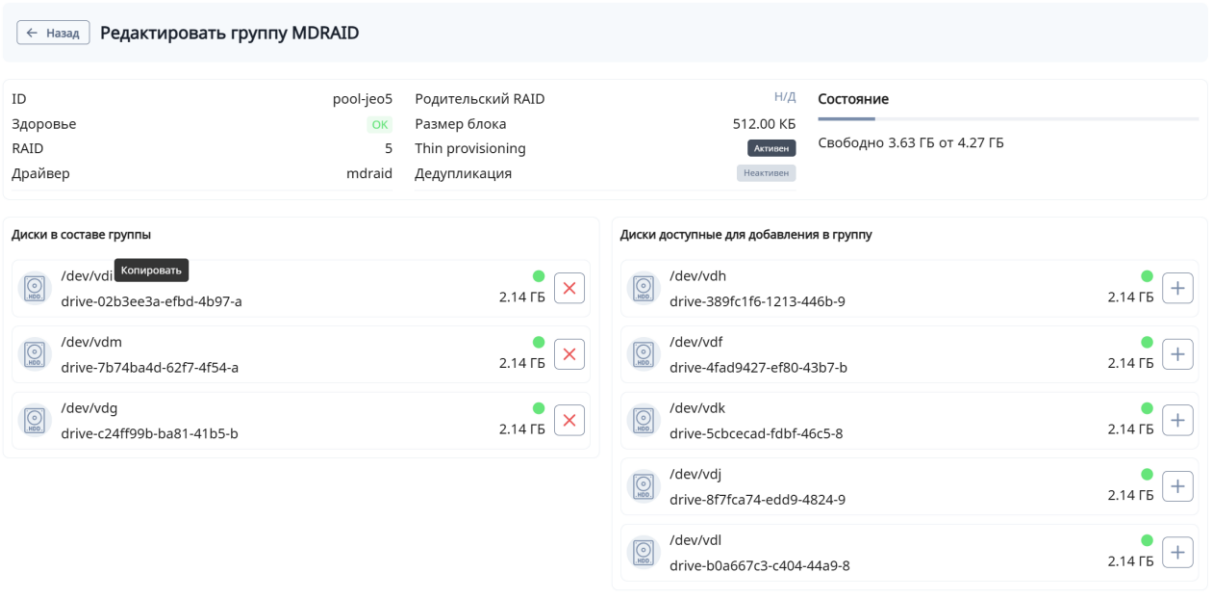


Рисунок 2.30 – Окно редактирования группы

4. В области «Диски доступные для добавления в группу» выберите доступный накопитель и нажмите «Добавить»  . Система попросит подтвердить действие сообщением (рисунок 2.31)

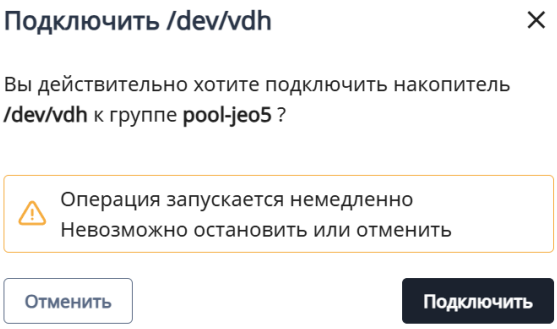


Рисунок 2.31 – Окно редактирования группы

5. После нажатия на кнопку «Подтвердить» система добавит накопитель в «Диски в составе группы» и пометит его как «Запасной» (рисунок 2.32).

ПРИМЕЧАНИЕ.

Система автоматически промаркирует накопитель как «Запасной» только если группа не деградирована (накопитель отключен или обнаружены ошибки ввода-вывода). Если группа деградирована, накопитель добавится как обычный.

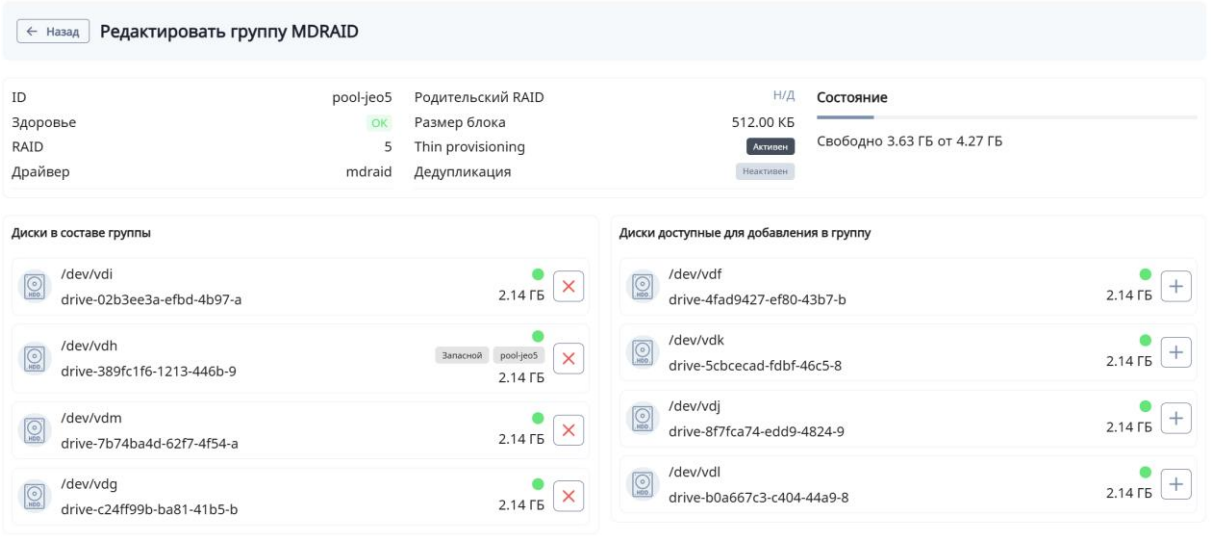


Рисунок 2.32 – Окно подтверждения сохранения изменений в группе

Система не ограничивает количество запасных дисков. Для каждой группы их может быть сколько угодно много (рисунок 2.33).

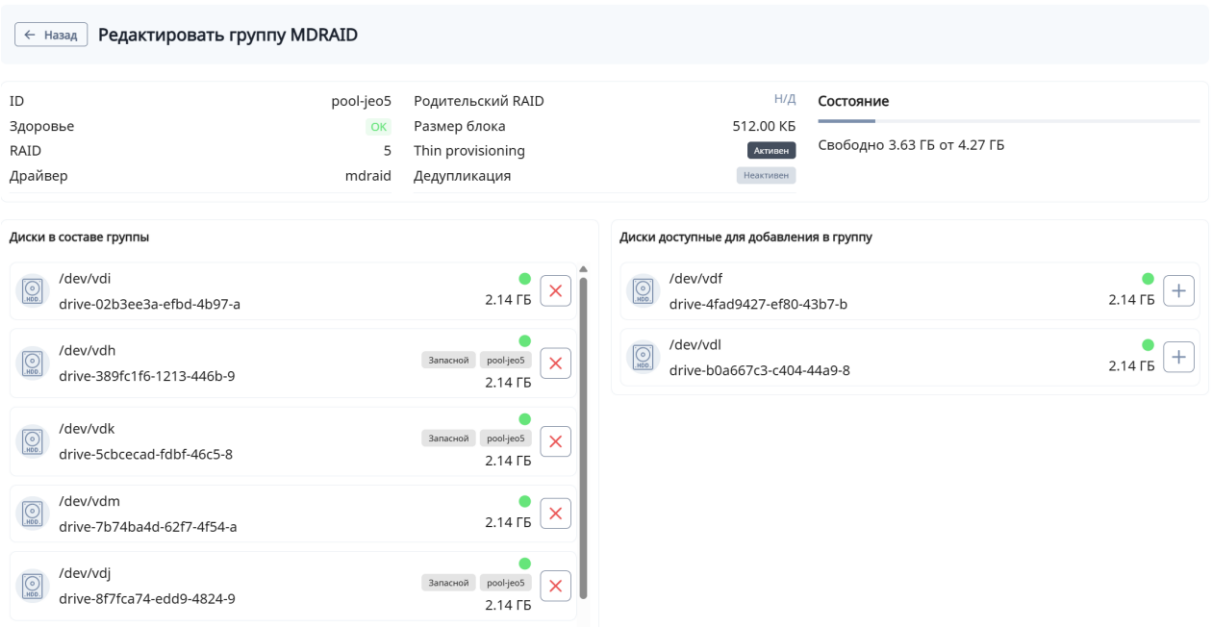


Рисунок 2.33 – Несколько запасных накопителей в группе

2.4.3.2.2 ИСКЛЮЧЕНИЕ ИЗ ГРУППЫ ЗАПАСНОГО ДИСКА

Для исключения запасного диска из группы необходимо:

1. Зайти в «Параметры» ⋮ группы и нажать «Редактировать» Редактировать.
2. В открывшемся окне у нужного диска нажать на «Исключить» ×.

3. В появившемся модальном окне «Исключить накопитель» нажать кнопку «Исключить» Исключить (рисунок 2.34)

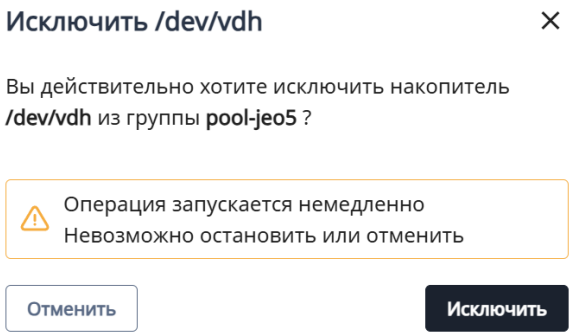


Рисунок 2.34 – Окно подтверждения исключения накопителя из группы

ПРИМЕЧАНИЕ.

Если исключить из группы основной накопитель, то система автоматически активирует запасной накопитель и группа перейдет в состояние «Rebuilding».

2.4.3.2.3 СЦЕНАРИЙ АВТОМАТИЧЕСКОГО ВОССТАНОВЛЕНИЕ ПРИ ОТКАЗЕ ДИСКА:

Обнаружение сбоя

- Система автоматически определяет отказ рабочего накопителя
- Состояние группы меняется на «Degraded»

Замена накопителя

- Система исключает сбойный накопитель из группы
- Автоматически активирует запасной диск
- Метка «Запасной» исчезает с карточки накопителя

Восстановление данных

- Группа переходит в состояние «Rebuilding»
- Система восстанавливает данные на замененном накопителе
- После завершения восстановления группа возвращается в состояние «Ok»

ПРИМЕЧАНИЕ.

Архитектурная особенность BlazeIO и порядок действий

После извлечения накопителя из группы система сохраняет его виртуальную привязку к исходной группе в БД управляющего сервиса для обеспечения отказоустойчивости.

Если физически вернуть извлечённый накопитель в систему, он будет отображаться в исходном пуле со статусом «Ok», но фактически не будет использоваться BlazeIO для

хранения данных. Такой накопитель нельзя добавить в другую группу, пока он не будет освобождён из текущей. Прежде чем вставить диск обратно, удалить диск в UI интерфейсе

Правильный порядок повторного использования накопителя:

1. Физически установить накопитель в систему.
2. В разделе СХД перейдите в параметры исходной группы.
3. Исключите этот накопитель из состава группы.
4. После освобождения диск можно добавить в нужный пул (исходный или новый).

2.4.4 ОБЪЕДИНЕНИЕ ГРУПП НАКОПИТЕЛЕЙ И СОЗДАНИЕ КОМПОЗИТНЫХ ГРУПП

Опция «Объединить» группы накопителей позволяет создавать более гибкие конфигурации RAID – «Композитных групп», которые объединяют и распределяют дисковое пространство, обеспечивая баланс между производительностью, отказоустойчивостью и эффективным использованием ресурсов.

ПРИМЕЧАНИЕ. Особенности создания композитной группы

- Опция «Объединить» доступна для групп с драйвером MDRAID и BlazeIO. Для BlazeIO A/A недоступна в текущей версии.
- Объединяемые группы должны быть созданы с одним и тем же драйвером
- Уровень RAID объединяемых групп может отличаться
- Конфигурации объединяемых RAID не ограничены
- В присоединяемой группе, которая впоследствии станет «Дочерней» не должно быть создано томов
- RAID 0 не может участвовать создании композитных групп
- При создании композитной группы, «разъединить» их будет невозможно. Опция «Удалить» композитную группы доступна только в контекстном меню родительской «Parent» группы.

Процесс создания композитной группы состоит из нескольких этапов:

1. Подготовка групп к объединению – создание новых или выбор уже созданных групп для объединения – минимум двух.

2. Объединение групп. Для объединения групп накопителей необходимо нажать на кнопку вызова контекстного меню, и выбрать действие «Объединить» как показано на рисунке 2.35.

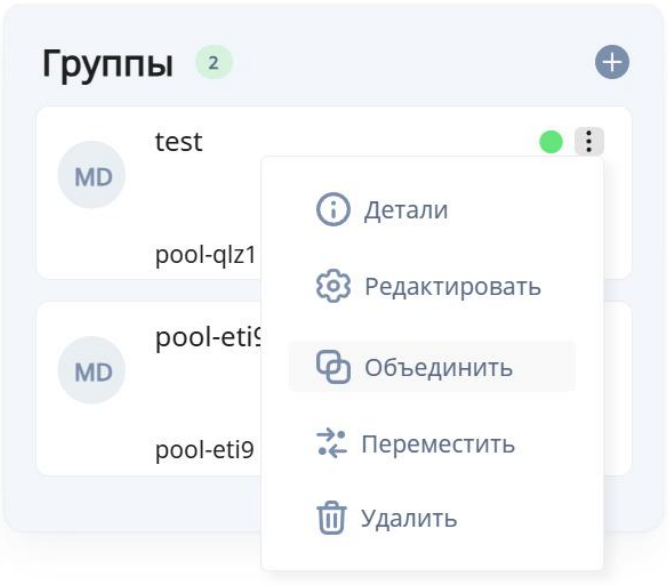


Рисунок 2.35 – Выбор опции «Объединить» группы накопителей

В открывшемся окне отобразится два поля «Дочерние группы» и «Доступные группы», в последнем должны быть доступные, соответствующие условиям группы накопителей (рисунок 2.36).

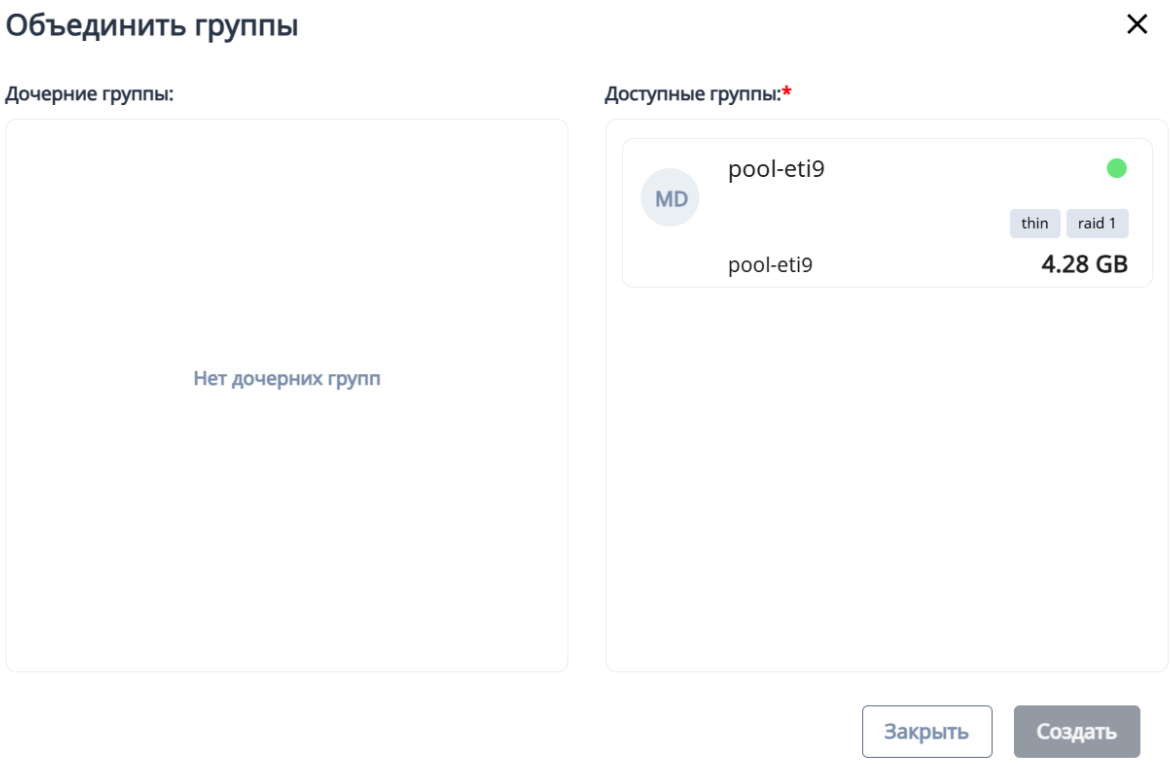


Рисунок 2.36 – Окно «Объединить группы» накопителей

После создания объединенной группы накопителей, группа к которой присоединялись другие группы маркируется как «Parent», а группа которая была присоединена «Child»,

а также ее объем памяти перемещается в родительскую «Parent» группу, как показано на рисунке 2.37.

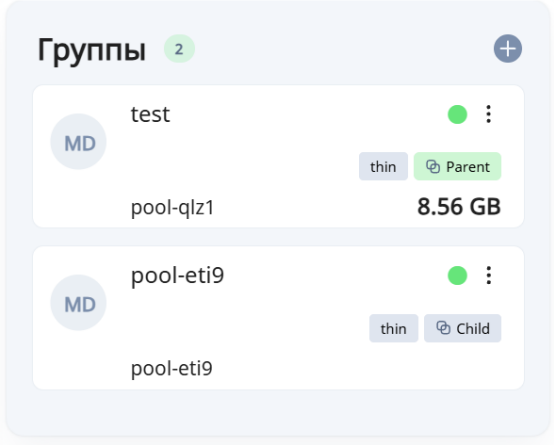


Рисунок 2.37 – Отображения групп накопителей с метками «Parent» и «Child»

ПРИМЕЧАНИЕ. Особенности функционирования композитной группы

- В случае сбоя одного из накопителей, меняется состояние здоровья той группы, в которой произошел сбой. Процесс восстановления осуществляется идентично обычной группе (см. п. 2.4.3).
- Группы могут сохранять работоспособность до тех пор, пока количество отказавших накопителей не превышает предел, допускаемый текущими RAID–группами, входящими в состав композитной структуры. Допустимый предел равен сумме накопителей, выделенных под отказоустойчивость, в зависимости от RAID–групп, образующих композитную.

3. Создание тома на объединенной группе. Более подробно про создание томов можно прочитать в разделе 2.5.

ПРИМЕЧАНИЕ. Особенности создания томов типа «Striped»

RAID 10	Том типа «Striped», созданный на композитной группе, состоящей из двух групп RAID 1
RAID 50	Том типа «Striped», созданный на композитной группе, состоящей из двух групп RAID 5
RAID 60	Том типа «Striped», созданный на композитной группе, состоящей из двух групп RAID 6

2.4.5 ПЕРЕМЕЩЕНИЕ ГРУППЫ НАКОПИТЕЛЕЙ

Опция «Перемещение» групп накопителей позволяет балансировать нагрузку между узлами, осуществлять техническое обслуживание, обновление или замену оборудования и выполнять управляемый failover.

ПРИМЕЧАНИЕ

Группы с драйвером BlazeIO A/A функционируют в режиме Active/Active, для этого не требуется опция ручного перемещения, так как оба узла одновременно используют все доступные пути без необходимости выбора оптимального и неоптимального.

Для перемещения группы накопителей необходимо нажать на кнопку вызова контекстного меню и выбрать действие «Переместить» как показано на рисунке 2.38.

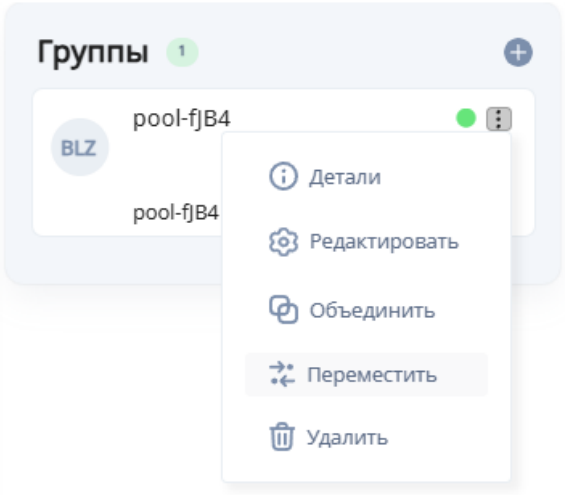


Рисунок 2.38 – Опция «Переместить» группу накопителей

Далее откроется окно «Переместить группу» в котором описывается, какую группу и на какой узел имеется возможность переместить и какие связанные с ней ресурсы будут перемещены, как показано на рисунке 2.39.

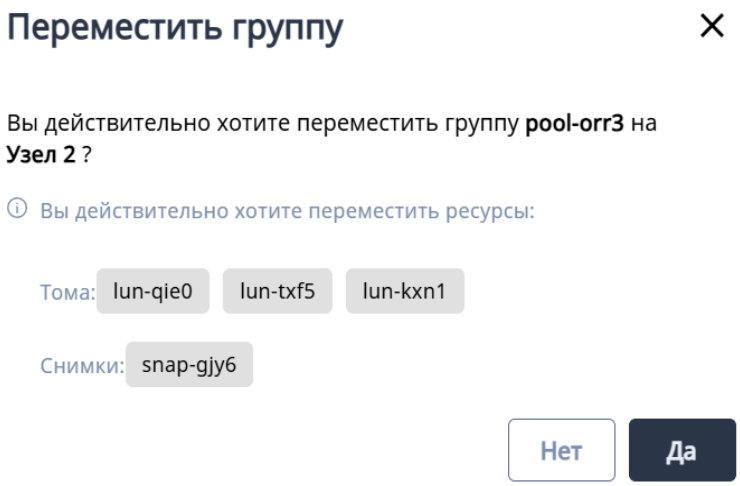


Рисунок 2.39 – Окно подтверждения «Переместить» группу накопителей

ПРИМЕЧАНИЕ

При возникновении сбоя одного из узлов произойдет перевод всех ресурсов на другой узел (failover). После восстановления первого узла необходимо вручную вернуть ресурсы на нее (failback).

2.4.6 УДАЛЕНИЕ ГРУПП НАКОПИТЕЛЕЙ

Для удаления группы накопителей необходимо нажать на кнопку вызова контекстного меню, как показано на рисунке 2.40, и выбрать пункт меню Удалить.

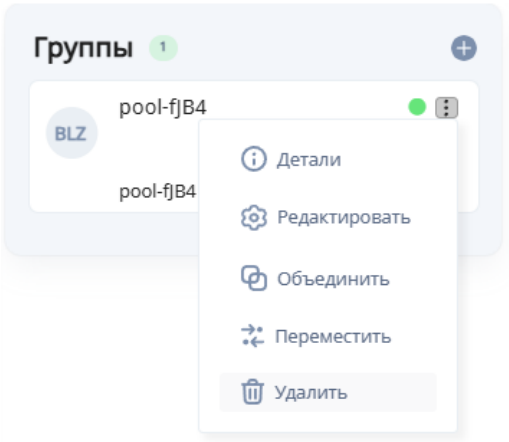


Рисунок 2.40 – Опция «Удалить» группу накопителей

ВНИМАНИЕ!

При удалении группы накопителей также будут удалены все относящиеся к ней дочерние ресурсы (тома, экспорты, снимки).

Перед удалением, необходимо прекратить экспорт и исключить из группы инициаторов ресурсы, связанные с удаляемой группой. В ином случае, попытка удаления завершится ошибкой.

При удалении выбранной группы накопителей, администратору СХД необходимо подтвердить данное решение. Для этого необходимо ввести название удаляемой группы, как показано на рисунке 2.41.

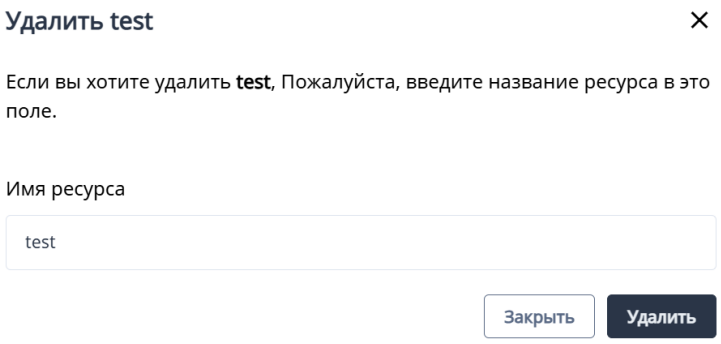


Рисунок 2.41 – Подтверждение удаления группы накопителей

2.5 ТОМА

2.5.1 СОЗДАНИЕ ТОМОВ

Для создания логического тома необходимо выполнить следующие действия:

1. В колонке «Тома» нажать «Добавить» или кнопку «Создать том». На экране отобразится окно создания нового логического тома, как показано на рисунке 2.42.

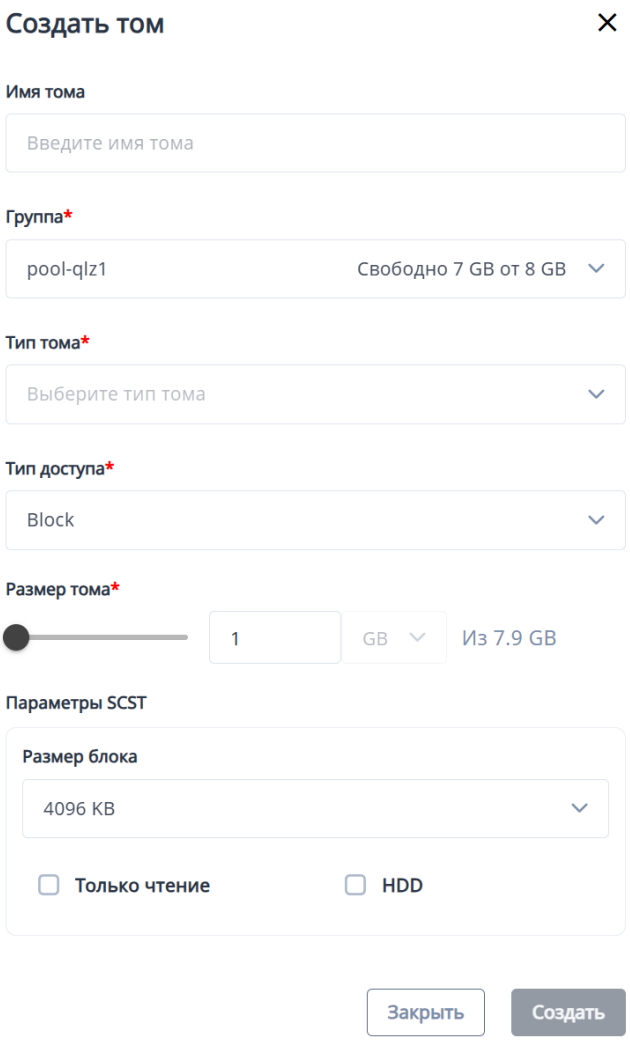


Рисунок 2.42 – Пример окна создания тома

2. В открывшемся окне в поле «Имя тома» задать имя создаваемого тома (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, вместо имени будет отображаться ID тома).
3. В поле «Группа» выбрать группу накопителей из открывшегося списка.
4. В поле «Тип тома» выбрать из выпадающего меню.

ПРИМЕЧАНИЕ. Тип тома

Доступные типы томов будут зависеть от того, группа с какой технологией оптимизации была выбрана:

Технология оптимизации	**Тип тома**
Технология не выбрана	Обычный
Thin provisioning	Обычный, thin provisioning
Дедупликация	Обычный, дедуплицированный

Тип тома «Striped» будет доступен только при выборе «Объединенной» группы. Подробнее в разделе 2.4.

5. В поле «Тип доступа» выбрать тип доступа к данным (файловый - «File» или блочный - «Block»).
6. Задать размер тома

ПРИМЕЧАНИЕ. Размер тома

Минимальный и максимальный размер тома зависят от выбранного типа тома:

Тип тома	Мин. размер	Макс. размер
Обычный	1 GB	Зависит от размера группы
Thin provisioning	1 GB	1 PB
Дедуплицированный	6 GB	4 PB

- Максимальный размер пространства доступного для создания тома зависит от суммы размеров других томов, созданных от этой группы, и от выбранной технологии оптимизации.
- Thin Provisioning - технология оптимизации, позволяющая предоставлять логический объем хранилища, превышающий фактический доступный физический ресурс группы.
    - Физическое пространство выделяется динамически только при записи данных, что повышает эффективность использования дисков и оптимизирует распределение ресурсов.
    - Технология необходима в случаях, когда приложения или пользователи запрашивают большие объемы, фактически используя лишь их часть.
    - Требуется контроль за заполнением группы: при полном исчерпании физического ресурса операции записи будут заблокированы, даже если логический объем остается доступным.
    - Эффективность оценивается по соотношению между выделенным и фактически занятым пространством, отображаемым в средствах мониторинга системы.
- Дедупликация - технология оптимизации использования дискового пространства основанная на дедупликации, компрессии (сжатии) и тонком выделении ресурсов. Анализирует входящие данные, исключает повторяющиеся блоки и блоки, заполненные нулями. Уникальные блоки дополнительно сжимает перед записью. При этом логические блоки динамически сопоставляются с физическим пространством, и фактическое место на диске выделяется только тогда, когда оно действительно требуется. Позволяет указывать логический размер, **превышающий физический максимум в 10 раз[8*], при соблюдении критериев технологии:**
    - Данные должны содержать много повторяющихся блоков, например, архивы виртуальных машин с большим количеством одинаковых операционных систем, резервные копии одних и тех же файлов.
    - Если пользователь хранит данные, которые уже сжаты или не имеют повторяющихся блоков, например, зашифрованные файлы, видео, аудио, то коэффициент дедупликации может быть равен 1.
    - Важно контролировать заполнение группы (физического, фактического размера), от которой был создан том, чтобы не допустить его переполнения - если данные заполнят физическое пространство, запись будет приостановлена, даже если пространство тома (логическое) еще не

заполнено.
- Отслеживать эффективность оптимизации пространства можно, просматривая раздел «Состояние» в деталях группы, от которой был создан том.

7. В разделе «Параметры SCST» содержатся настройки трех параметров – только чтение[9*], HDD[10*] и размер блока[11*].

ПРИМЕЧАНИЕ. Параметры SCST

Драйвер	Параметры SCST. Размер блока
BlazeIO	Размер блока 4096 В установлен по умолчанию, не отображается в окне создания тома, и не подлежит изменению
MDRAID	Выбор размера блока зависит от используемой версии VMware VAAI[12*]. В случае, если версия VMware VAAI ниже 8, размер блока должен быть 512 В. Если версия 8 и выше, размер блока должен быть 4096 В

8. Нажать кнопку «Создать».

2.5.2 ИНФОРМАЦИЯ О ЛОГИЧЕСКОМ ТОМЕ

При успешном выполнении операции будет создан новый логический том, который затем отобразится на экране, как показано на рисунке.

Информация о состоянии имеющегося в системе логического тома отображается на карточке тома, как показано на рисунке 2.43:

- графическое отображение вида тома: блочный/файловый;
- имя тома;
- ID тома;
- размер тома в MB;
- цветовой индикатор состояния тома;
- вызов контекстного меню;
- технология оптимизации пространства хранения данных;
- указатель принадлежности тома к группе накопителей.

[8*] Максимальный коэффициент фиксирован в текущей версии ПО и равен 10.
[9*] Параметр, определяющий режим доступа к экспортированному устройству.
[10*] Тип устройства, которым том будет представляться инициатору
[11*] Параметр, определяющий минимальную единицу чтения/записи, которую поддерживает экспортируемое устройство.
[12*] Набор API–интерфейсов, разработанных VMware, позволяющий перенести выполнение определенных операций с виртуальными дисками на уровень системы хранения данных. Это улучшает производительность, снижает нагрузку на сеть и ускоряет выполнение задач.

Рисунок 2.43 – Карточка тома

Цветовой индикатор ● информирует о состоянии здоровья логического тома и может принимать следующие значения:

- Ok – том работает в штатном режиме;
- Unknown – процесс сканирования;
- Failed – том недоступен;
- Lost – нарушена логическая связь с логическим томом.

ВНИМАНИЕ!

При отображении красного или черного цветового индикатора необходимо обратиться в техническую поддержку. Контакты указаны в разделе ТЕХНИЧЕСКАЯ ПОДДЕРЖКА данного Руководства.

При нажатии на кнопку вызова контекстного меню, и выборе пункта меню «Детали» (рисунок 2.44), будет показано диалоговое окно, содержащее подробную информацию о данном томе и операциях как показано на рисунках 2.45 и 2.46:

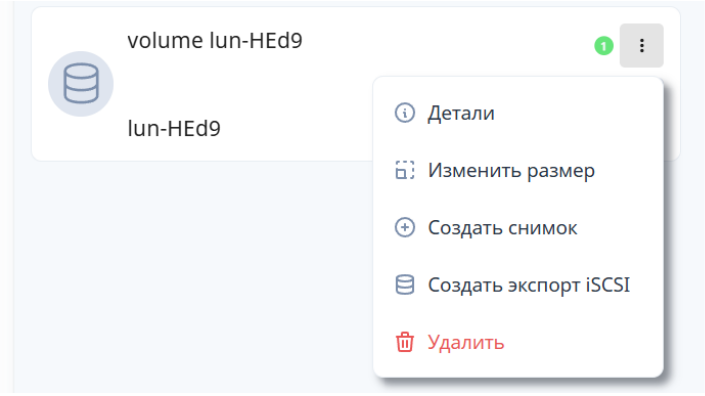


Рисунок 2.44 – Контекстное меню тома

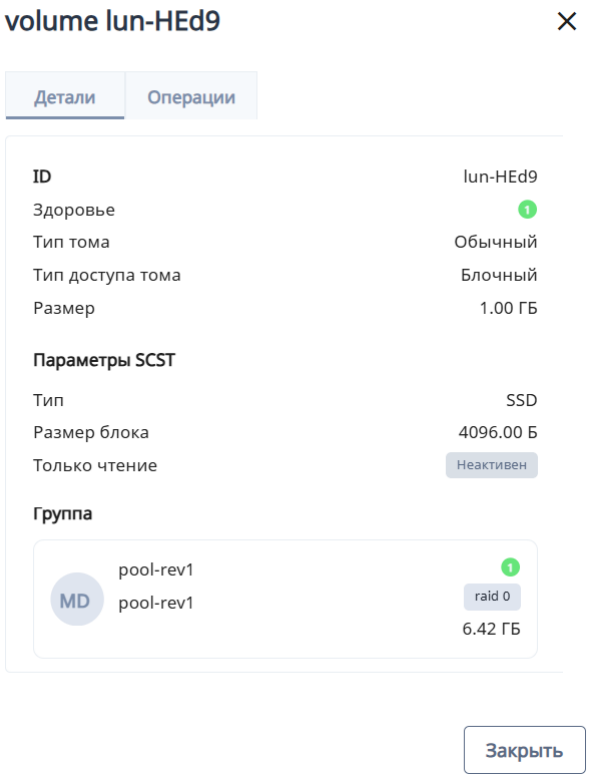


Рисунок 2.45 – Вкладка «Детали»

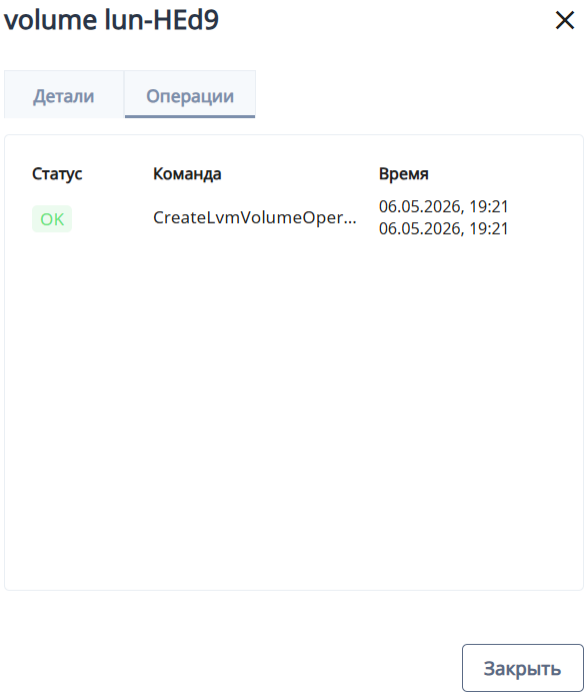


Рисунок 2.46 – Вкладка «Операции»

При нажатии на строку с операцией система перейдет в журнал команд.

ПРИМЕЧАНИЕ

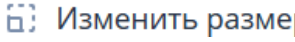
Подробно о журнале команд в разделе 7.4 «Журнал команд» данного руководства

2.5.3 РАСШИРЕНИЕ ТОМА

Расширение тома позволяет увеличить доступную ёмкость логического тома без остановки сервисов хранения данных. Процедура поддерживает онлайн-режим (без размонтирования файловой системы) для протоколов NFS и SMB.

Перед выполнением расширения тома система автоматически проверяет:

- Наличие свободного места в группе томов (расширение производится за счёт нераспределённого пространства группы).
- Новый размер тома должен быть строго больше текущего (уменьшение не допускается).
- Том должен быть здоров.

Для расширения тома в контекстном меню (рисунок 2.44) необходимо выбрать пункт «Изменить размер» 

. Откроется окно редактирование тома (рисунок 2.47).

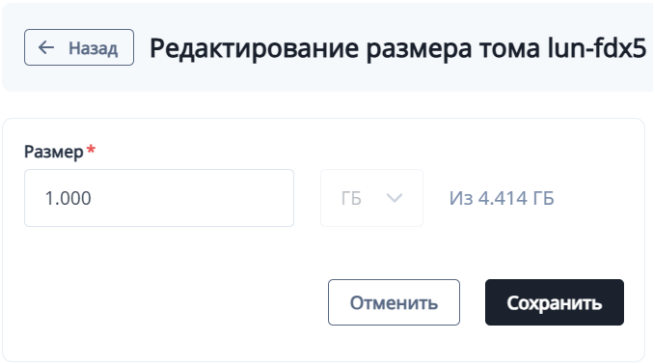
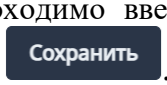


Рисунок 2.47 – Окно «Редактирование тома»

В окне необходимо ввести размер, выбрать единицы измерения и нажать кнопку «Сохранить» 

. После этого в исходном окне томов отобразится новый размер тома (рисунок 2.43).

2.5.4 ОГРАНИЧЕНИЯ ПРИ РАСШИРЕНИИ ТОМОВ

Операция расширения тома позволяет увеличить доступную ёмкость логического тома без остановки сервисов хранения данных. Настоящий раздел описывает ограничения, условия выполнения и поведение системы при расширении томов.

1. Поддерживаемые типы томов

Тип тома	Поддержка resize	Примечание
Block-том (блочный)	**Да**	Полная поддержка
File-том (файловый)	**Да**	Полная поддержка
Regular-том (обычный)	**Да**	Требуется свободное физическое место в группе
Thin-том	**Да**	Верхнее ограничение - 1 PB
Дедуплицированный том (VDO)	**Нет**	Расширение не поддерживается
Снапшот (снимок)	**Нет**	Снимки доступны только для чтения
Клон	**Да**	Клон является полноценным томом

2. Расширение тома может выполняться в онлайн-режиме, без отключения экспорта и без разрыва существующих соединений:

- для LUN, экспортированных по iSCSI/FC;
- для LUN, включённых в группу инициаторов.

3. Допустимые состояния

- Расширение допускается только при состоянии тома OK.
- Расширение допускается только при состоянии пула OK и наличии достаточного свободного места.
- При активации глобального режима «Только чтение» (отсутствие лицензии, нарушение синхронизации) операция расширения запрещена.
- Для тома с параметром «Только чтение» операция расширения запрещена.

4. Расчёт доступного места
Для обычного (Regular) тома: Физическое свободное пространство в группе накопителей за вычетом объёма всех существующих томов
Для тонкого (Thin) тома: Верхнее ограничение - 1 PB. Проверка физического свободного места при расширении не выполняется

5. Блокировка параллельных операций

На время выполнения операции расширения тома блокируются следующие операции над тем же томом:

- удаление тома;
- изменение параметров SCST;
- экспорт/отключение экспорта;
- создание снимка.

Первый запрос принимается в обработку, второй получает ошибку «Операция изменения размера уже выполняется для данного тома. Повторите запрос позже».

2.5.5 УДАЛЕНИЕ ТОМОВ

Для удаления выбранного логического тома необходимо нажать на кнопку вызова контекстного меню, как показано на рисунке 2.44 и выбрать опцию «Удалить».

В открывшемся модальном окне, в поле «Имя ресурса» необходимо ввести имя удаляемого логического тома как на рисунке 2.48, для подтверждения намерения.

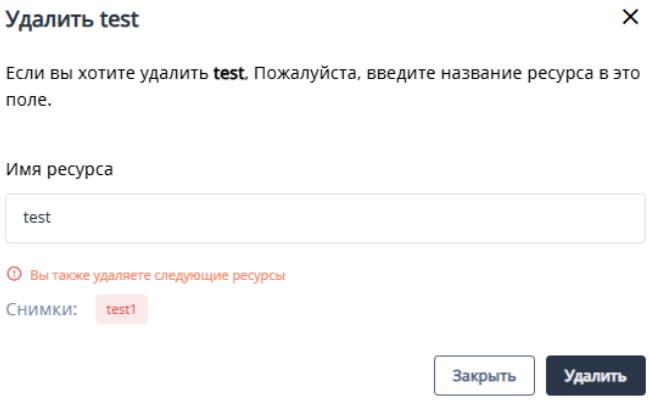


Рисунок 2.48 – Подтверждение удаления тома

ВНИМАНИЕ!

В случае, если удаляемый том экспортируется (включен в группу инициаторов) возникнет ошибка 400. Предварительно, необходимо исключить том из группы инициаторов.

3 ДИСКОВЫЕ ПОЛКИ

В данном разделе отображается информация о подключённых дисковых полках, их конфигурации и состоянии накопителей, как показано на рисунке 3.1.

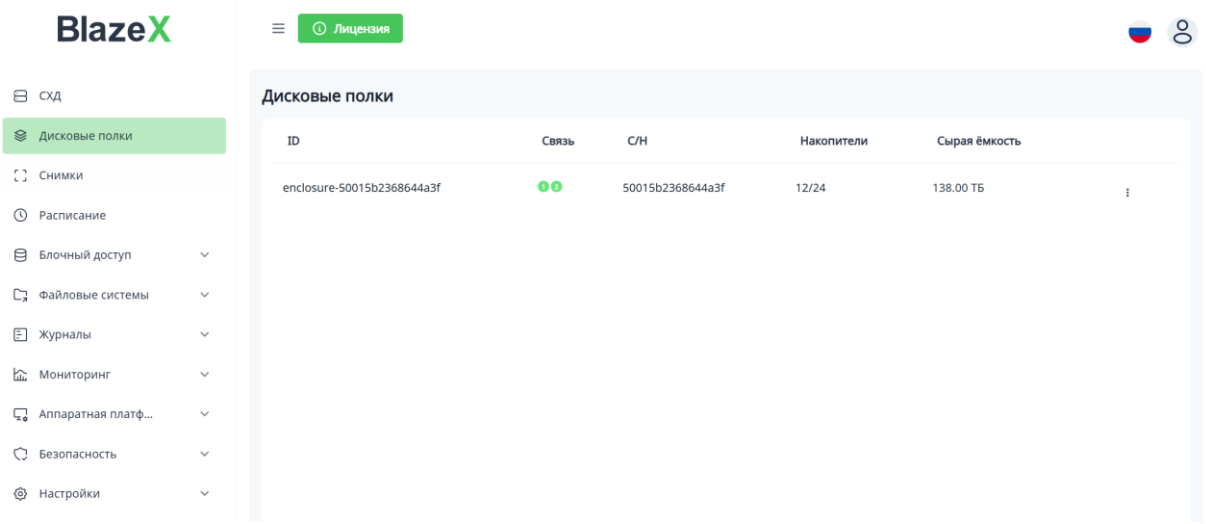


Рисунок 3.1 – Окно «Дисковые полки»

Окно содержит следующую информацию:

- ID - уникальный идентификатор полки
- Связь – показывает есть ли связь с контроллером 1 и 2
- С/Н – серийный номер дисковой полки
- Накопители - количество установленных накопителей в формате занято/всего
- Сырая ёмкость - общая физическая ёмкость всех дисков в полке

При нажатии на кнопку «Параметры» ⋮ можно посмотреть детали полки или физически подсветить полку нажав на кнопку «Включить индикацию» Включить индикацию (рисунок 3.2)

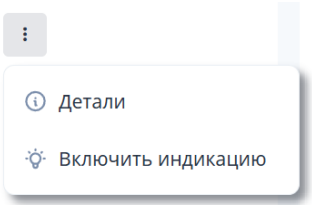


Рисунок 3.2 – Параметры «Дисковой полки»

Окно деталей содержит следующую информацию (рисунок 3.3):

- Модель – модель дисковой полки
- С/Н – серийный номер дисковой полки
- Объем - общая физическая ёмкость всех дисков в полке
- Здоровье – здоровье контроллера 1 и 2
- Окно «Накопители»
  - Связь – показывает есть ли связь с контроллером 1 и 2
  - С/Н – серийный номер дисковой полки

- Группа – группа в которой состоит накопитель
- Тип – тип накопителя HDD, SSD …
- Объем –- физическая ёмкость накопителя
- Кнопка «Параметры» ⋮ при нажатии на которую можно посмотреть детали накопителя или включить индикацию диска Включить индикацию.

ПРИМЕЧАНИЕ

Подробно о деталях накопителя в разделе 2.3.1 ИНФОРМАЦИЯ О НАКОПИТЕЛЯХ

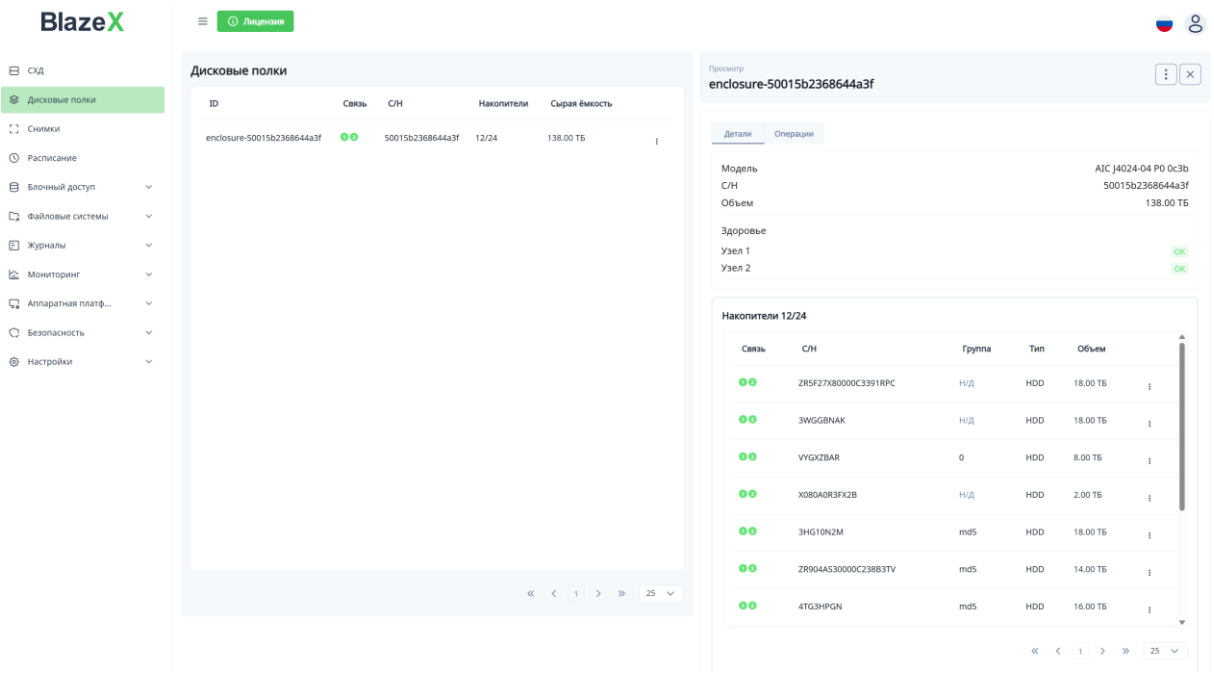


Рисунок 3.3 – Детали «Дисковой полки»

4 СНИМКИ

Раздел предназначен для управления моментальными копиями (снимками) томов и групп хранения. Позволяет просматривать существующие снимки, создавать на их основе клоны, экспортировать по iSCSI и удалять (рисунок 4.1)

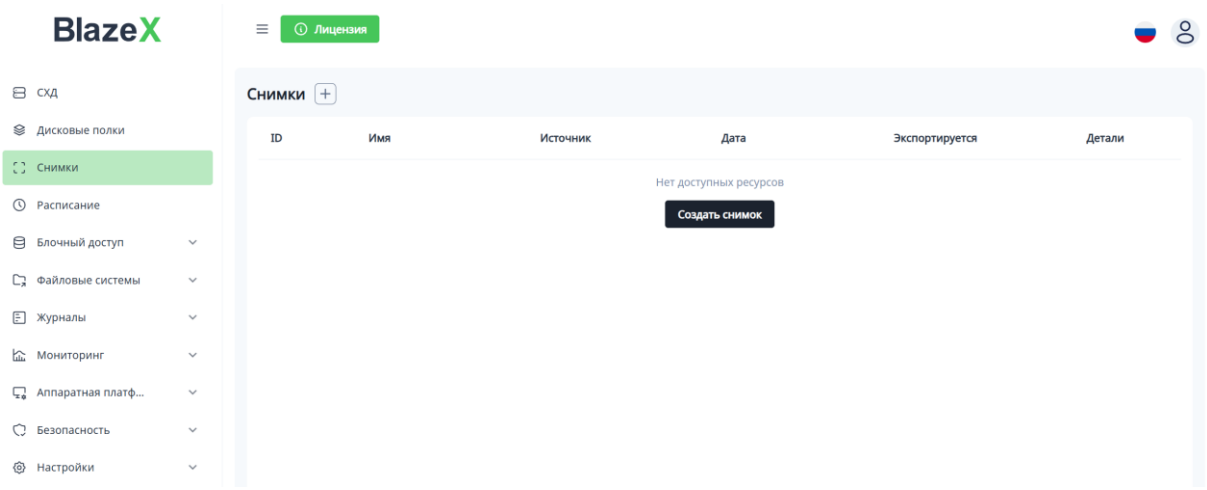


Рисунок 4.1 – Окно «Снимки»

Окно содержит следующую информацию:

- ID - уникальный идентификатор снимка
- Имя – пользовательское имя снимка
- Источник – исходный объект: том и группа хранения. Указывается в формате:
  - Том: <имя_lun>
  - Группа: <имя_pool>
- Дата - время создания снимка в формате дд.мм.гггг, чч:мм
- Экспортируется - Статус экспорта:
  - «Не экспортируется»
  - «Экспортируется» - активный экспорт
- Детали – кнопка ⋮ для просмотра дополнительной информации, создания клона, экспорта и удаления

ВНИМАНИЕ! Особенности создания снимков

Для создания снимка от тома, необходимо соблюдение следующих условий:

1. Тип тома от которого создается снимок может быть любым кроме SAA и VDO.
2. Состояние здоровья тома должно быть «Ok» (цветовой индикатор зеленого цвета)
3. Объем свободного места в группе от которой был создан том, должен быть достаточным для создания снимка:

- В случае, если пользователь создает снимок тома типа «Обычный» и «Striped», то размер снимка будет равен размеру тома, соответственно, в группе должно быть свободное место, равное размеру тома.
- В случае, если пользователь создает снимок от тома типа «Thin provisioning»,

ограничения по объему свободного места в группе отсутствуют.

4.1 СОЗДАНИЕ СНИМКОВ

Система позволяет создавать снимок двумя способами:

1. В «карточке» выбранного логического тома вызвать контекстное меню, далее выбрать пункт «Создать снимок» (см. рисунок 4.2).

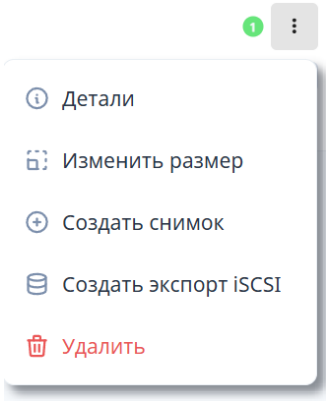


Рисунок 4.2 – Создание снимка из контекстного меню в «карточке» выбранного логического тома

2. Необходимо перейти во вкладку «Снимки» и активировать диалоговое окно создания снимка по нажатию на  над таблицей информации о созданных снимках или на кнопку 

. (см. рисунок 4.1). В открывшемся окне указать имя снимка и источник (том), как показано на рисунке 4.3.

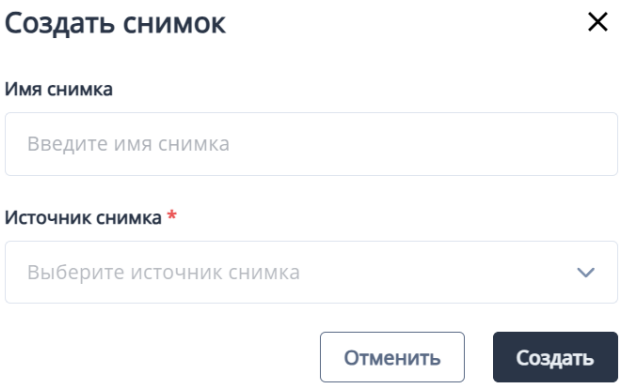


Рисунок 4.3 – Создание снимка через активацию диалогового окна

ПРИМЕЧАНИЕ

Созданные снимки (снапшоты) доступны для монтирования исключительно в режиме «только для чтения» (Read-Only) как по протоколу NFS (файловый доступ), так и по iSCSI (блочный доступ).

После выбора источника снимка и ввода имени (не обязательно) необходимо нажать на кнопку создать. Созданный снимок отобразится в окне снимки (рисунок 4.4)

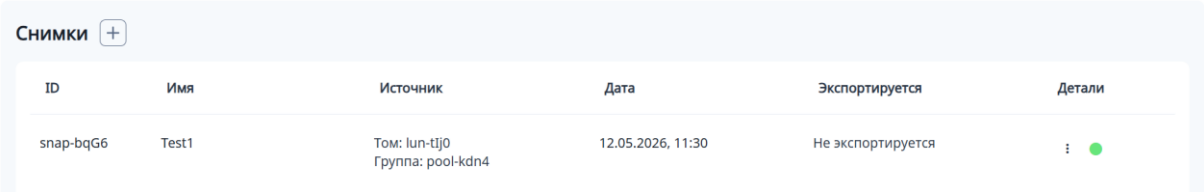


Рисунок 4.4 – Отображение снимка в итоговой таблице

4.2 ИНФОРМАЦИЯ О СНИМКАХ

После создания снимок получает одно из возможных состояний здоровья:

- Ok – снимок работает в штатном режиме;
- Unknown – снимок в процессе сканирования;
- Failed – недоступен, невозможно определить состояние.

При нажатии на кнопку «Параметры» ⋮ можно (рисунок 4.5):

- Посмотреть детали - просмотр расширенной информации о снимке
- Создать клон - создание полноценного клона (независимого тома) на основе снимка
- Создать экспорт iSCSI - Предоставление снимка по протоколу iSCSI хосту или инициатору
- Удалить - Безвозвратное удаление снимка (требует подтверждения)

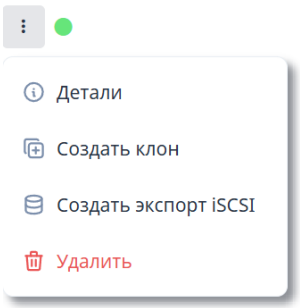


Рисунок 4.5 – Окно параметров снимка

Окно детали содержит следующую информацию:

- ID - уникальный идентификатор снимка
- Здоровье – состояние снимка
- Дата - время создания снимка
- Параметры – основные настройки хранения:
  - Том - имя исходного или связанного тома
  - Группа - имя пула хранения
  - Размер - общий размер логического устройства
  - Тип доступа - тип предоставляемого интерфейса (блочное устройство, файловый доступ)
  - Thin provisioning - признак тонкого выделения ресурсов, Активен (включен) / неактивен (отключён)
- Параметры SCST - подсистема для эмуляции SCSI-целей. Параметры:
  - Тип - эмулируемый тип носителя (SSD, HDD)
  - Размер блока - Логический размер блока в байтах
  - Только чтение - запрет записи на уровне цели. Статус «Активен» - запись запрещена, снимок защищён

Окно параметров снимка изображено на рисунке 4.6

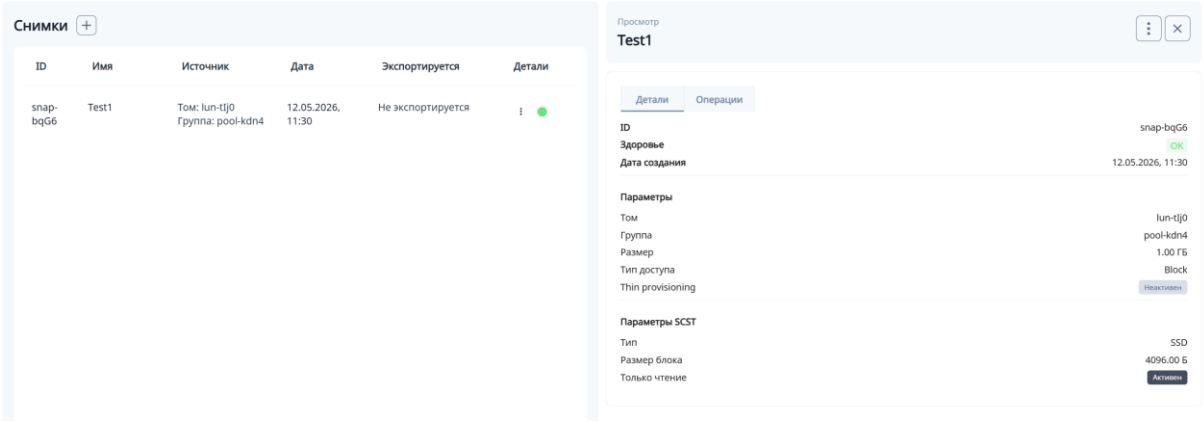


Рисунок 4.6 – Окно просмотра деталей снимка

4.3 УДАЛЕНИЕ СНИМКОВ

Для удаления снимка необходимо нажать кнопку вызова контекстного меню «Параметры» ⋮ , и выбрать пункт «Удалить» . Для подтверждения решения необходимо ввести имя ресурса в диалоговом окне формы на удаление (см. рисунок 4.7).

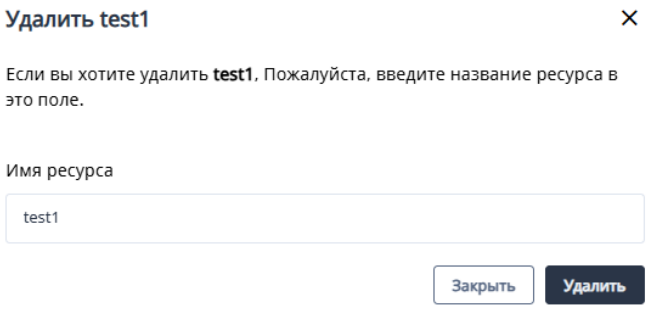


Рисунок 4.7 – Окно подтверждение удаления снимка

5 ФОНОВОЕ СКАНИРОВАНИЕ И ОПТИМИЗАЦИЯ

В системе BlazeX фоновое сканирование и оптимизация полностью поддерживаются и применяются к группам, созданным под управлением драйвера blazeio. Это ключевые механизмы для обеспечения целостности данных и производительности.

Фоновое сканирование

Фоновое сканирование - это автоматический процесс, предназначенный для проверки состояния носителей данных в составе группы blazeio.

Система в фоновом режиме считывает данные с дисков и проверяет их контрольные суммы. Это позволяет выявлять ошибки чтения, которые не были обнаружены в обычном рабочем процессе.

Оптимизация

Оптимизация для групп драйвера blazeio направлена на поддержание высокой производительности и эффективного использования емкости.

В процессе работы драйвера blazeio с данными файловая система может фрагментироваться. Оптимизация собирает разрозненные фрагменты файлов в непрерывные блоки, что ускоряет последовательный доступ и снижает нагрузку на механику.

Оптимизация также включает передачу команд драйверу для маркировки блоков, которые уже не используются операционной системой. Это позволяет драйверу blazeio физически очистить эти сектора, что улучшает скорость записи и информирует об актуальном свободном месте.

Для обеспечения стабильной работы групп blazeio рекомендуется настраивать расписание выполнения этих задач в окне «Расписание».

5.1 ПЛАНИРОВЩИК (РАСПИСАНИЕ)

Окно «Расписание» (или Планировщик) предназначено для настройки периодического автоматического выполнения двух типов сервисных операций (рисунок 5.1):

- Оптимизация хранилища
- Фоновое сканирование

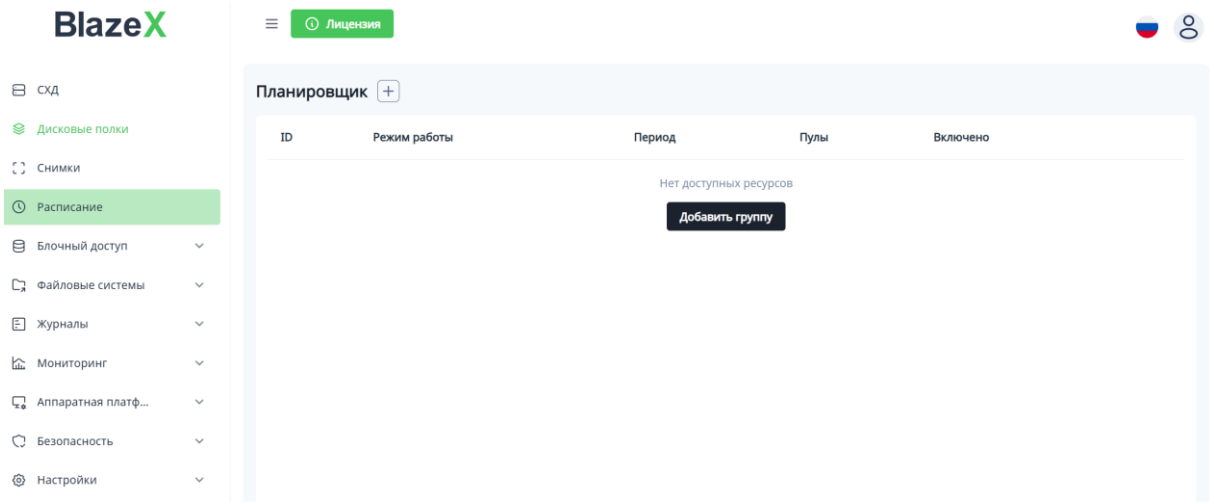


Рисунок 5.1 – Окно планировщика расписания оптимизации и фонового сканирования групп blazeio

Для создания расписания необходимо нажать на  или кнопку «Создать расписание». После нажатия откроется окно, в котором требуется выполнить следующую последовательность действий (рисунок 5.2).

1. В блоке выбора групп выделить одну или несколько групп, для которых нужно создать расписание (рисунок 5.2).

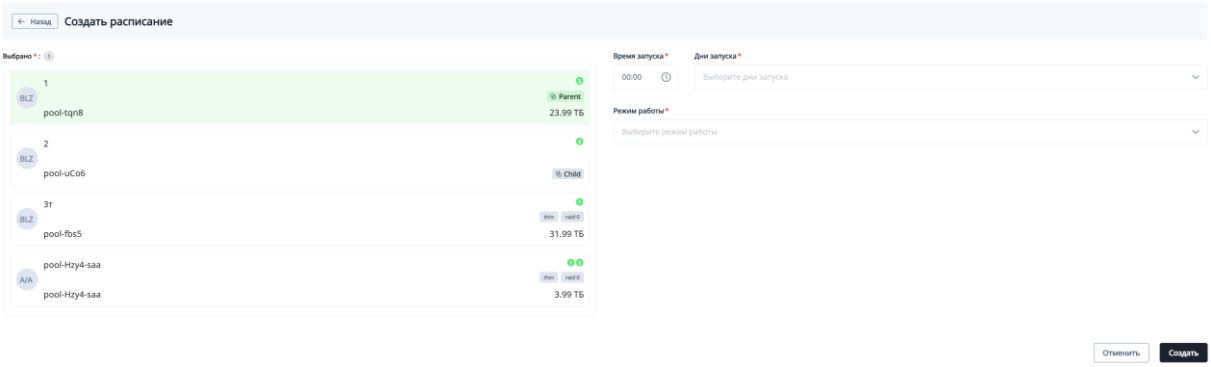


Рисунок 5.2 – Выбор групп

2. В блоке «Время запуска» выбрать необходимое время запуска фонового сканирования и/или оптимизации (рисунок 5.3).

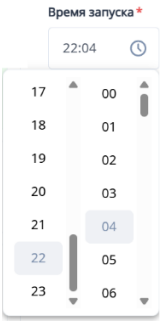


Рисунок 5.3 – Выбор времени запуска

3. В блоке «Дни запуска» выбрать необходимый день запуска фонового сканирования и/или оптимизации (рисунок 5.4).

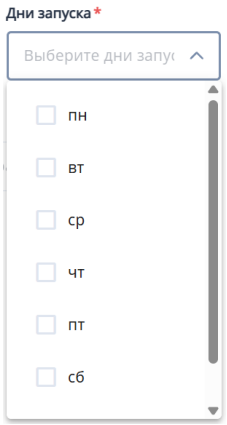


Рисунок 5.4 – Выбор дня запуска

4. В блоке «Режим работы» выбрать необходимый режим запуска фонового сканирования и/или оптимизации (рисунок 5.5).

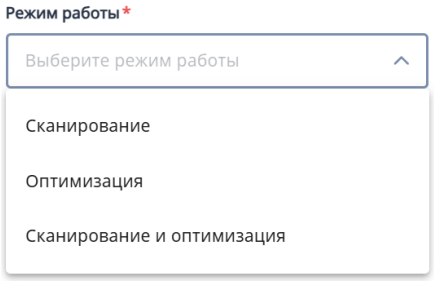


Рисунок 5.5 – Выбор режима работы

5. Для сохранения настроек необходимо нажать на кнопку «Создать» 

. При успешном выполнении операции итоговое расписание отобразится главном окне планировщика (рисунок 5.6).

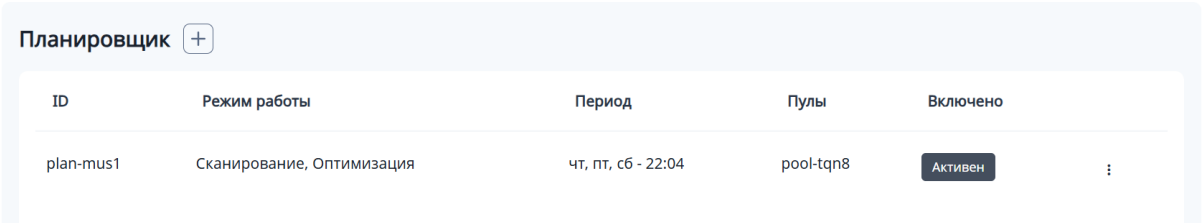


Рисунок 5.6 – Выбор режима работы

5.2 ИНФОРМАЦИЯ О РАСПИСАНИИ

При нажатии на кнопку параметры доступны следующие действия (рисунок 5.7):

- Детали - Вызов окна «Детали»
- Редактирование - Редактирование параметров расписания

- Запустить – принудительный запуск режима работы (оптимизации и/или сканирование) выбранного для данного расписания
- Включить/Выключить – Включение или отключение расписания
- Удалить – Удаление расписание

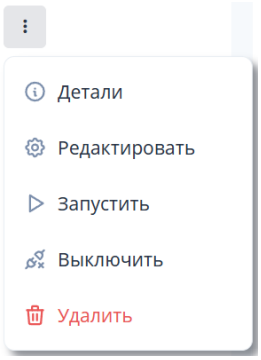


Рисунок 5.7 – Выбор режима работы

5.3 ДЕТАЛИ РАСПИСАНИЯ

При выборе пункта «Детали» Детали откроется окно показанное на рисунке 5.8. Оно содержит всю информацию о параметрах расписания

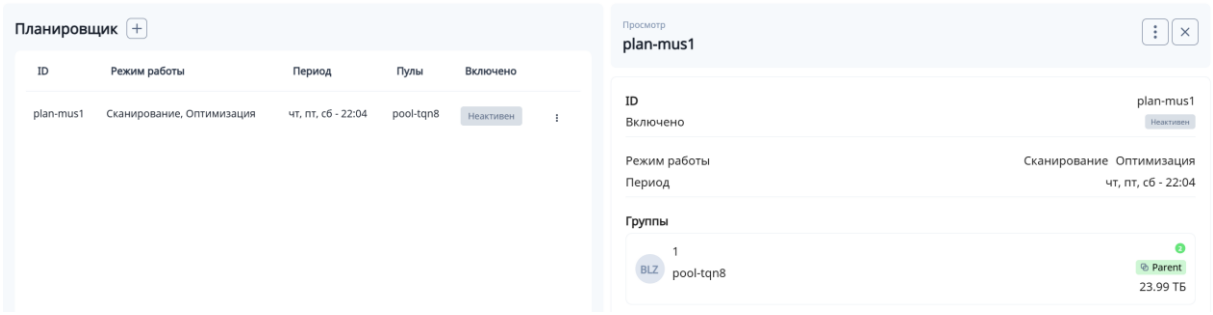


Рисунок 5.8 – Детали расписания

5.4 РЕДАКТИРОВАНИЕ РАСПИСАНИЯ

При выборе пункта «Редактировать» Редактировать откроется окно показанное на рисунке 5.9. Оно позволяет изменить параметры и сохранить изменения

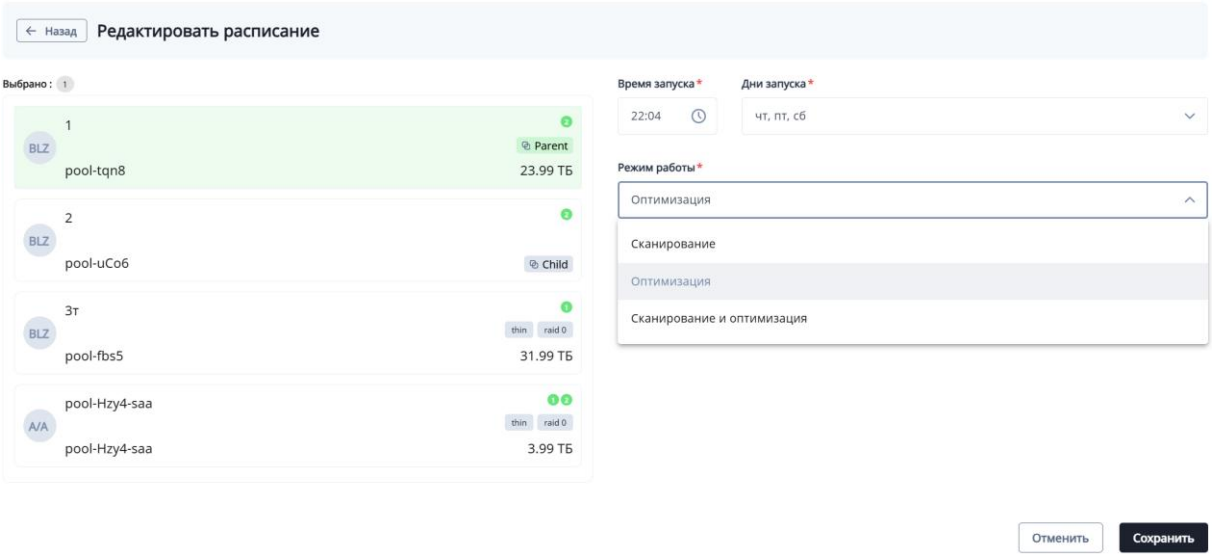


Рисунок 5.9 – Редактирование расписания

5.5 ПРИНУДИТЕЛЬНЫЙ ЗАПУСК РАСПИСАНИЯ

При выборе пункта «Запустить» ▷ Запустить в контекстном меню (рисунок 5.7) запустится выбранный режим работы. Отображения состояния оптимизации или сканирования можно посмотреть на странице СХД на карточке группы. Там отобразится название процесса и процент завершенности. Например, для процесса оптимизации карточка будет выглядеть так (рисунок 5.10):

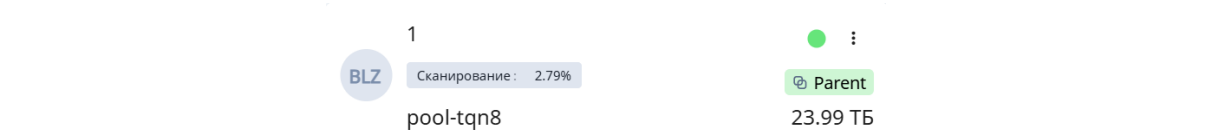


Рисунок 5.9 – Отображение операции «Оптимизация на карточке группы»

5.6 ВКЛЮЧЕНИЕ, ВЫКЛЮЧЕНИЕ РАСПИСАНИЯ

При выборе пункта «Выключить» Выключить расписание будет отключено и сменит статус в графе «Включено» с «Активен» Активен на «Неактивен» Неактивен в окне планировщика как показано на рисунке 5.10.

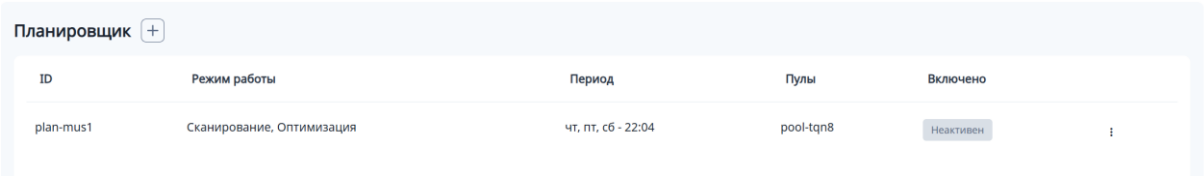


Рисунок 5.10 – Выключенное расписание

Включить расписание можно нажатием на кнопку Включить. В случае успешного применения изменений статус расписания изменится на Активен в графе «Включено» как показано на рисунке 5.6.

5.7 УДАЛЕНИЕ РАСПИСАНИЯ

При выборе пункта «Удалить» Удалить система попросит подтвердить удаление ресурса как показано на рисунке 5.11. В случае успешного выполнения операции расписание будет удалено и окно планировщика примет вид как на рисунке 5.1

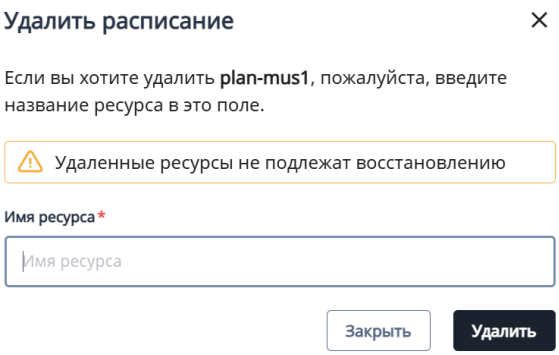


Рисунок 5.11 – Удаление расписания

5.8 ЗАПУСК ВНЕ РАСПИСАНИЯ

Оптимизацию или фоновое сканирование можно запустить в любой момент. Для этого необходимо:

1. Открыть окно «СХД» нажать на «Параметры» ⋮ группы Blazeio и в контекстном меню вырыть необходимый процесс нажав на кнопки «Оптимизация» ▷ Оптимизация или «Сканирование» ▷ Сканирование (рисунок 5.12).

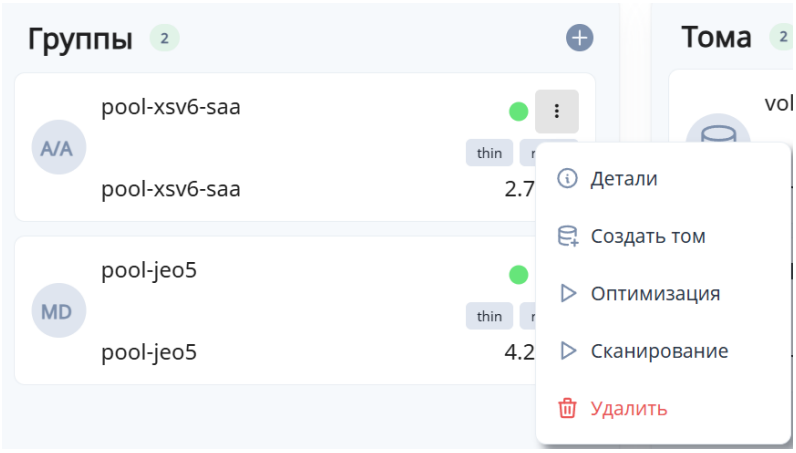


Рисунок 5.12 – Запуск оптимизации или сканирования

Статус процесса отобразится в карточке группы как на рисунке 5.9.

6 БЛОЧНЫЙ ДОСТУП

Раздел «Блочный доступ» содержит несколько дочерних разделов: «iSCSI / FC», «NVMe–oF», как показано на рисунке 6.1.

ПРИМЕЧАНИЕ. Особенности работы с экспортами

- В данной версии предоставляет только блочный доступ к данным, по протоколам iSCSI и FC
- В дочернем разделе «NVMe–oF» содержится анонс функциональности, которая будет доступна в будущих версиях BlazeX

В дочернем разделе «iSCSI / FC» расположены две таблицы (см. рисунок 6.2):

1. «iSCSI / FC», содержащая список экспортируемых (доступных извне) логических томов, и возможность ими управлять, и
2. «Группы инициаторов», в которой отображается список инициаторов, которым доступно подключения к таргету, и так же, возможность ими управлять.

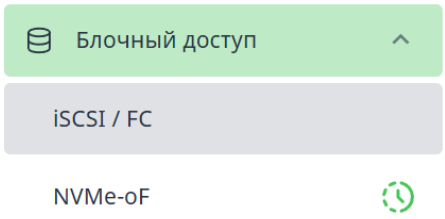


Рисунок 6.1 – Отображение вкладки «Блочный доступ»

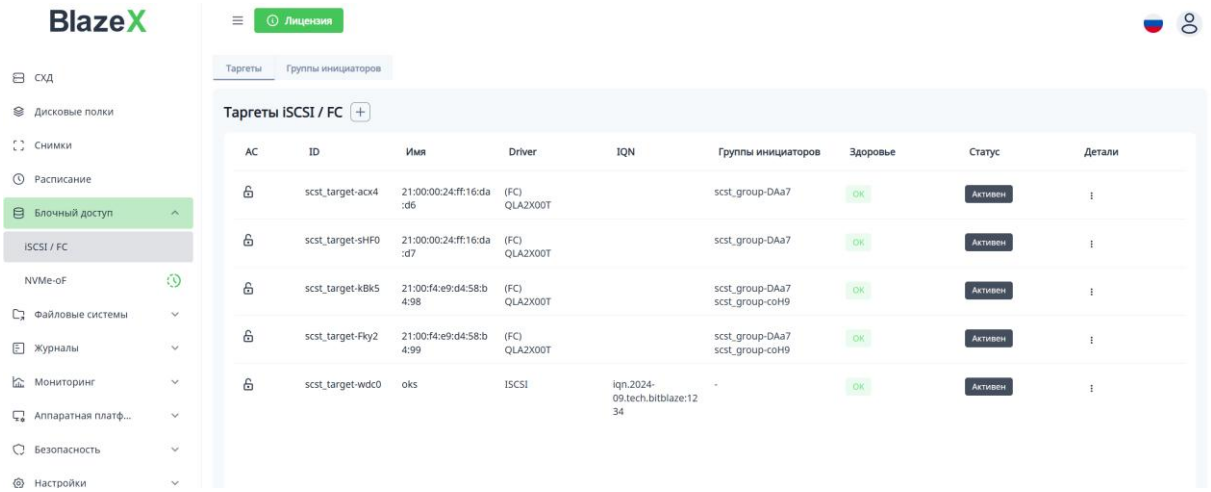


Рисунок 6.2 – Вид дочернего раздела «iSCSI / FC»

6.1 ISCSI

6.1.1 СОЗДАНИЕ ТАРГЕТА ISCSI

Для предоставления доступа к логическому тому с типом доступа «Block» в системе должен быть создан iSCSI–таргет.

Предоставить блочный доступ к логическому тому по транспортному протоколу iSCSI можно следующим образом:

1. В левом боковом меню перейти во вкладку «Экспорты», выбрать «iSCSI / FC». По умолчанию откроется вкладка «Таргеты SCSI / FC», содержащая соответствующую таблицу.
2. Нажать таблице нажать «Добавить»  , откроется модальное окно, как показано на рисунке 6.3.

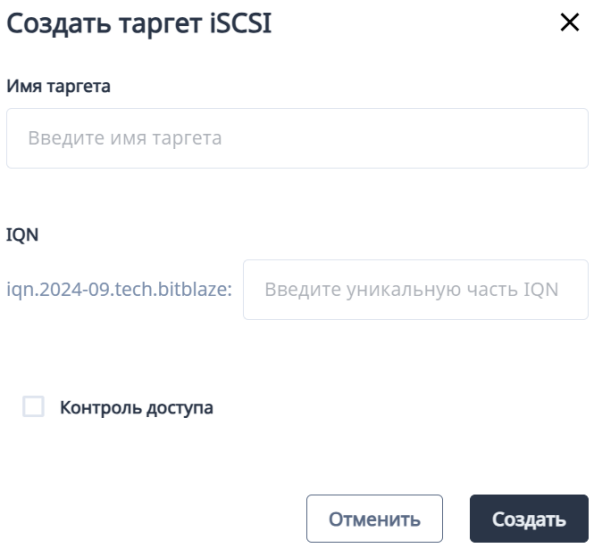


Рисунок 6.3 – Пример меню создания таргета iSCSI

3. В открывшемся окне «Создать таргет iSCSI» ввести в поле «Имя таргета» название таргета (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, то вместо имени будет отображаться ID таргета).
4. В поле «IQN» введите уникальный идентификатор (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, то вместо него будет отображаться IQN таргета).

При необходимости установления контроля доступа по логину и паролю к данному таргету поставить галочку в чек–боксе «Контроль доступа» и заполнить появившиеся поля «Логин» и «Пароль».

ПРИМЕЧАНИЕ. Особенности работы с контролем доступа

- Логин должен содержать от 2 до 8 символов.

- Пароль должен содержать от 12 до 16 символов, и не менее 2 цифр.

Нажать на кнопку «Создать».

6.1.2 ИНФОРМАЦИЯ О ТАРГЕТЕ

При успешном выполнении операции будет создан iSCSI–таргет, который затем отобразится в таблице «Таргеты iSCSI / FC», в соответствующем разделе (см. рисунок 6.4.), и получит один из двух статусов:

OK — Ok – информация о таргете получена

UNKNOWN — Unknown – информация о таргете в процессе получения

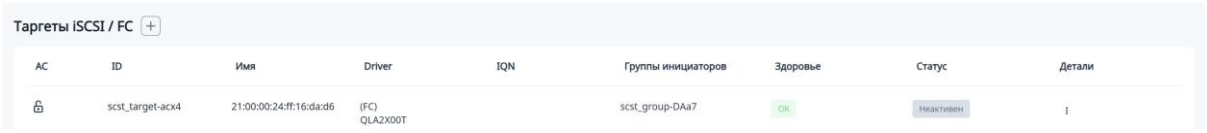


Рисунок 6.4 – Пример отображения таргета iSCSI с «зеленым» здоровьем и статусом «Неактивен»

При нажатии на кнопку вызова контекстного меню и выборе пункта меню «Детали» (см. рисунок 6.5), будет показано диалоговое окно, содержащее подробную информацию о данном таргете и присутствие ошибок в работе как показано на рисунке 6.6:

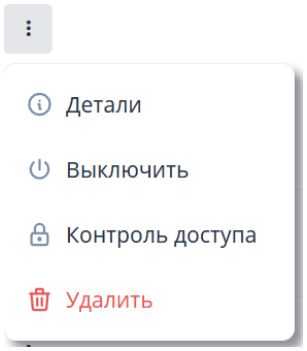


Рисунок 6.5 – Контекстное меню таргета iSCSI

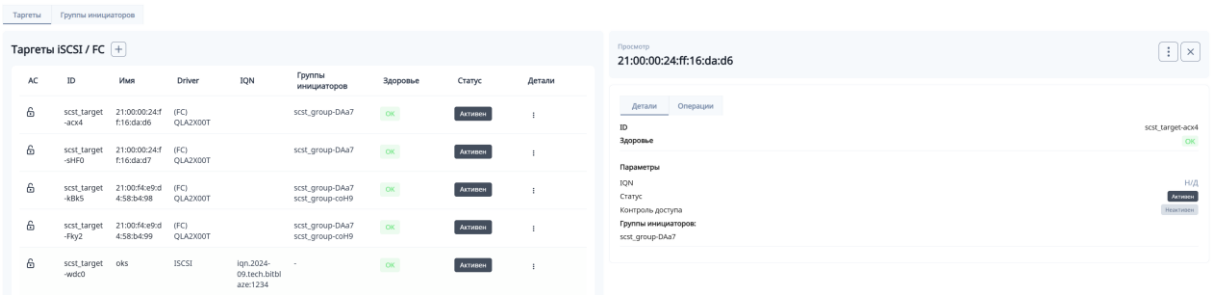


Рисунок 6.6 – Вкладка «Детали» таргета iSCSI

6.1.3 ВКЛЮЧЕНИЕ ТАРГЕТА

Для обнаружения таргета на стороне инициатора, необходимо активировать его видимость. Для этого в контекстном меню таргета необходимо выбрать опцию «Включить» (см. рисунок 6.7). после чего отобразится модальное окно, в котором необходимо подтвердить действие, как показано на рисунке 6.8.

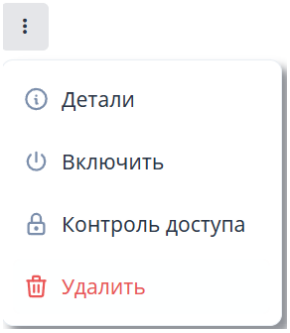


Рисунок 6.7 – Выбор опции «Включить» в контекстном меню

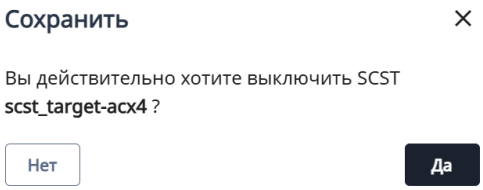


Рисунок 6.8 – Окно подтверждения включения таргета iSCSI

После подтверждения действия, в колонке «Включено» статус «Неактивен» Неактивен (рисунок 6.4) изменится на статус «Активен» Активен, что будет обозначать означает, что таргет стал видимым для инициатора (рисунок 6.9).

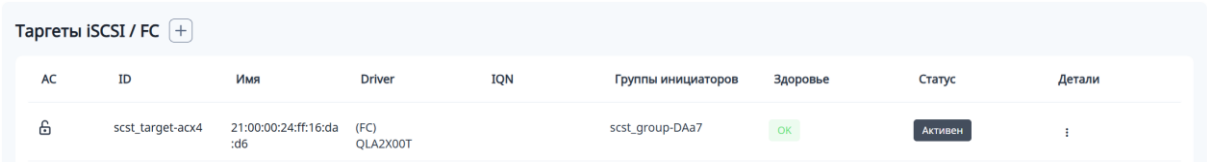


Рисунок 6.9 – Таргет iSCSI видим на стороне инициатора

ПРИМЕЧАНИЕ

Опция «Выключить» таргет iSCSI не прервет процесс экспортирования, но таргет перестанет быть видимым для инициатора.

6.1.4 УДАЛЕНИЕ ТАРГЕТА

Удаление выбранного таргета также осуществляется в контекстном меню, при выборе опции «Удалить». При удалении выбранного таргета необходимо подтвердить данное решение. Для этого введите название удаляемого таргета, как показано на рисунке 6.10:

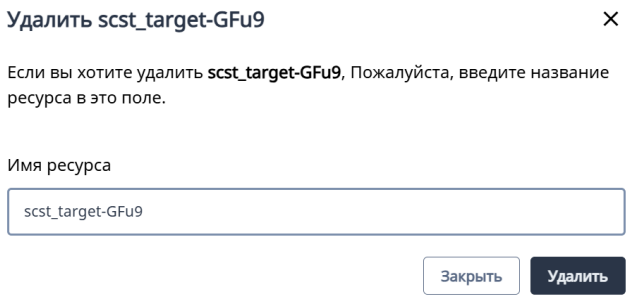


Рисунок 6.10 – Окно подтверждения удаления таргета iSCSI

6.1.5 СОЗДАНИЕ ТАРГЕТА FC

Для создания таргета по Fibre Channel, необходимо только подключить соответствующие коннекторы на стенде и они автоматически появятся в разделе таргетов, как показано на рисунке 6.11. Программно добавить или удалить таргеты по Fibre Channel – нельзя.

ПРИМЕЧАНИЕ

Если адаптер подключен физически, но не отображается в данном списке, необходимо обратиться в техническую поддержку. Контакты указаны в разделе ТЕХНИЧЕСКАЯ ПОДДЕРЖКА данного Руководства.

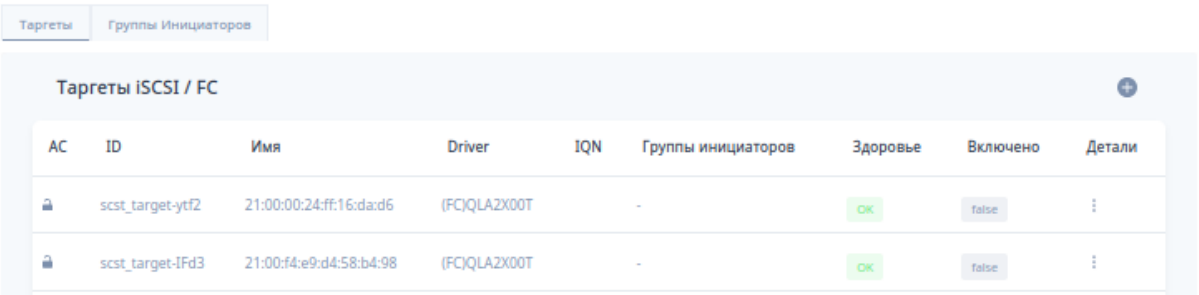


Рисунок 6.11 – Таргет Fibre Channel

6.1.6 СОЗДАНИЕ ГРУППЫ ИНИЦИАТОРОВ

Для того, чтобы создать группу инициаторов необходимо выполнить следующую последовательность действий:

1. Нажать на графический элемент  .
2. В открывшемся окне (рисунок 3.13) задать «Имя группы инициаторов» (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, то вместо имени будет отображаться ID группы инициаторов).
3. Далее выбрать «Таргеты» из выпадающего списка, отметив чек–бокс (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, то вместо таргета не будет отображаться ничего). Данное поле подразумевает возможность добавления нескольких значений.
4. Следующим этапом необходимо заполнить поле «Допустимые инициаторы» (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, то вместо допустимых инициаторов не будет отображаться ничего). Данное поле подразумевает возможность добавления нескольких инициаторов. Идентификационный номер инициатора вводится вручную. После ввода значение необходимо нажать «Enter» на клавиатуре, после чего значение отобразится в выпадающем списке.
5. В поле «Устройства» необходимо отметить доступные тома в открывшемся списке. Допускается выбор нескольких устройств (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, то вместо девайсов не будет отображаться ничего).
6. Чек-бокс «Только чтение» позволяет определить пользователю режим доступа. Если чек-бокс оставить пустым, инициатору будет доступен режим read/write, а если заполнить чек–бокс, то доступ к устройствам будет осуществляться в режиме read–only.
7. Нажать кнопку «Создать».

ВНИМАНИЕ!

Для любого заданного таргета, каждый инициатор должен быть ассоциирован ровно с одной группой доступа. Наличие одного инициатора в двух или более группах, подключённых к одному таргету, является недопустимой конфигурацией.

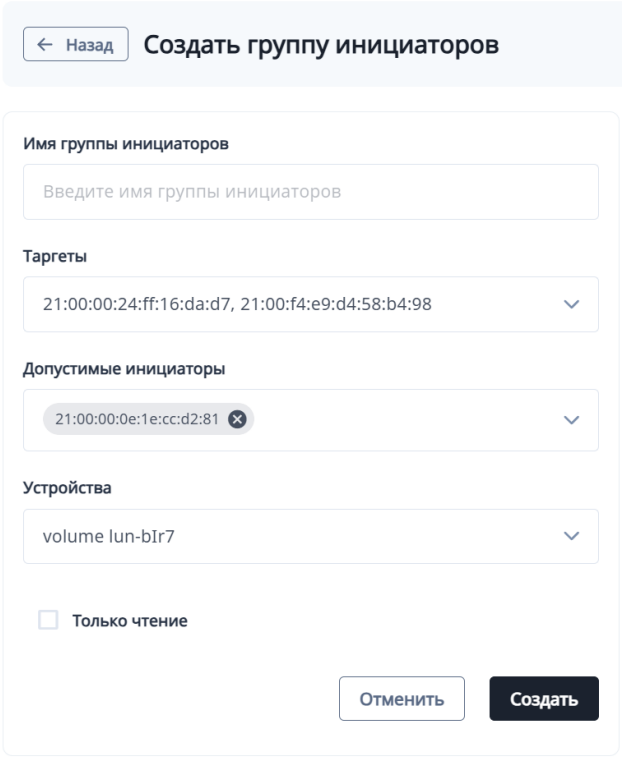


Рисунок 6.12 – Окно создания группы инициаторов

6.1.7 ИНФОРМАЦИЯ О ГРУППЕ ИНИЦИАТОРОВ

При успешном выполнении операции будет создана группа инициаторов, которая затем отобразится на вкладке «Группы инициаторов». Пример отображения приведен на рисунке 6.13.

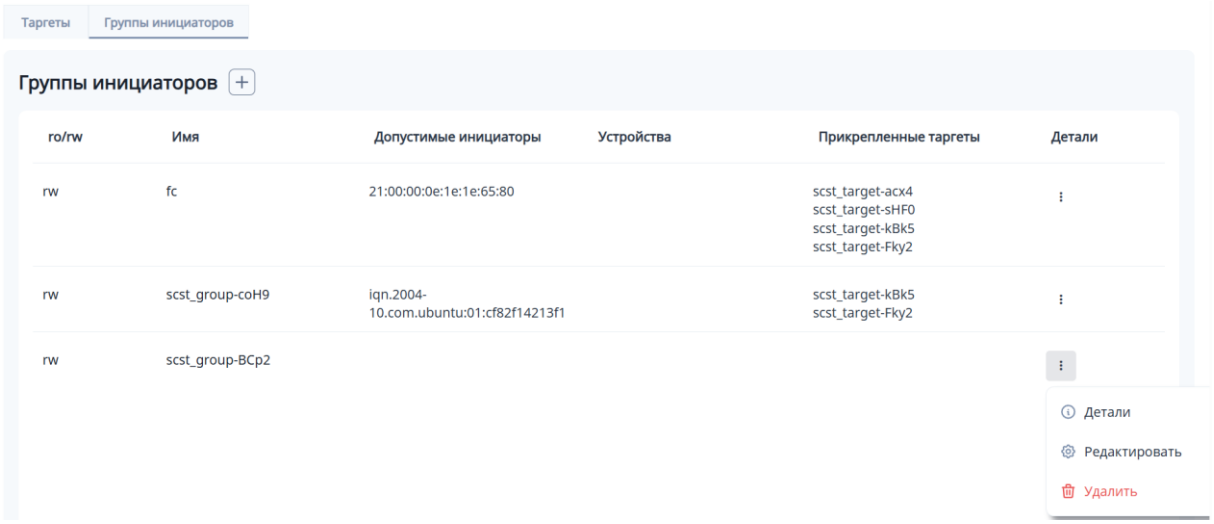


Рисунок 6.13 – Пример отображения окна списка групп инициаторов

При нажатии на кнопку вызова контекстно меню с группой инициаторов и выборе пункта меню Детали, будет показано диалоговое окно, содержащее подробную информацию о данной группе инициаторов и связанных с ней операциях, как показано на рисунках 3.14, и 3.15.

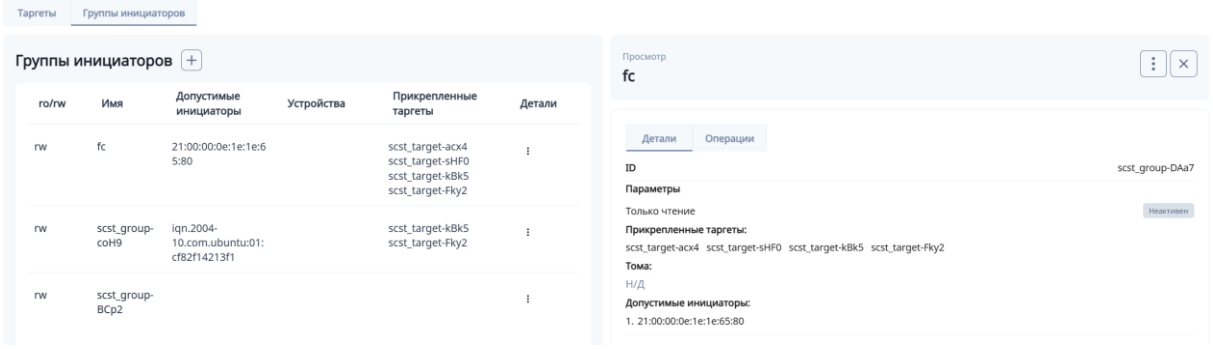


Рисунок 3.14 – Окно «Детали» группы инициаторов

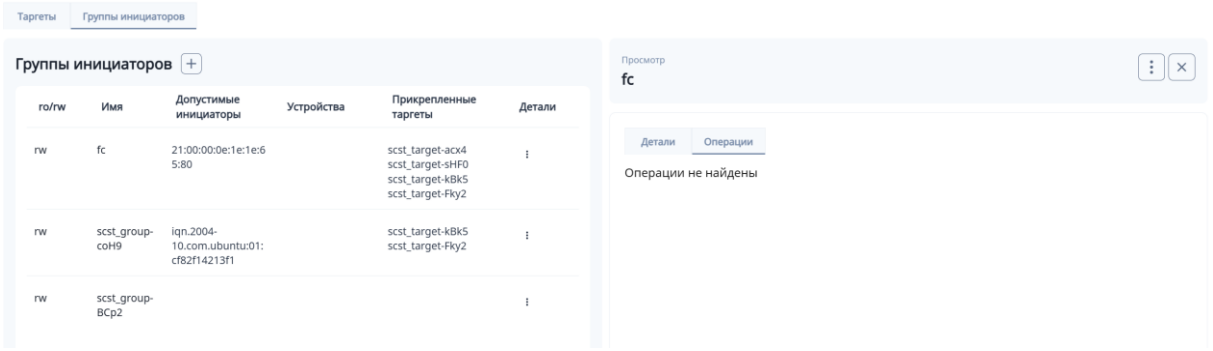


Рисунок 3.15 – Окно «Операции группы инициаторов

6.1.8 РЕДАКТИРОВАНИЕ ГРУППЫ ИНИЦИАТОРОВ

Для редактирования выбранной группы инициаторов, необходимо нажать на кнопку вызова контекстного меню группы инициаторов, как показано на рисунке 6.16 и выбрать пункт меню «Редактировать».

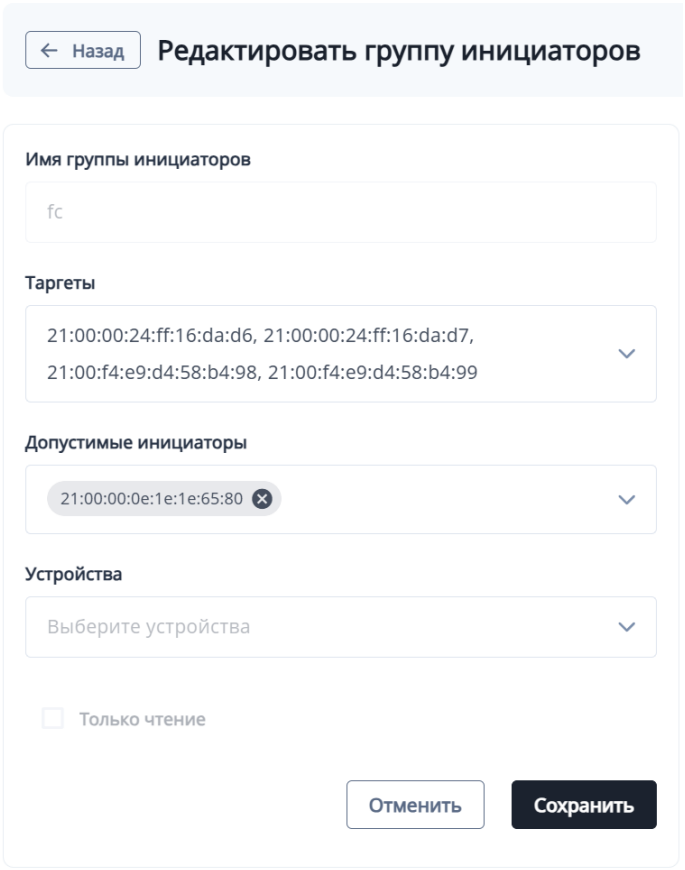


Рисунок 6.16 – Окно «Редактировать» группу инициаторов

В открывшемся окне доступна возможность редактирования (исключение и дополнение) следующих значений: «Таргеты», «Допустимые инициаторы», «Устройства». Изменив значения, необходимо нажать кнопку «Сохранить».

6.1.9 УДАЛЕНИЕ ГРУППЫ ИНИЦИАТОРОВ

Для удаления выбранной группы инициаторов необходимо выбрать опцию «Удалить» в контекстном меню таблицы. При удалении выбранной группы инициаторов администратору СХД необходимо подтвердить данное решение. Для этого введите название удаляемой группы, как показано на рисунке 6.17.

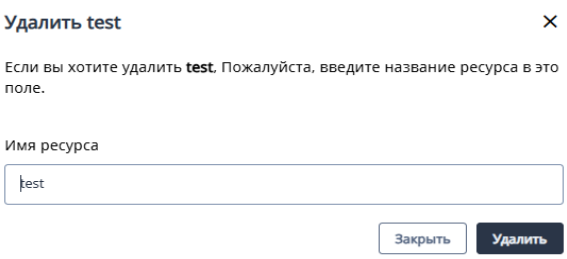


Рисунок 3.17 – Окно «Удалить» группу инициаторов

7 ФАЙЛОВЫЕ СИСТЕМЫ

Раздел «Файловые системы» содержит несколько дочерних разделов: «NFS» и «SMB», как показано на рисунке 7.1.

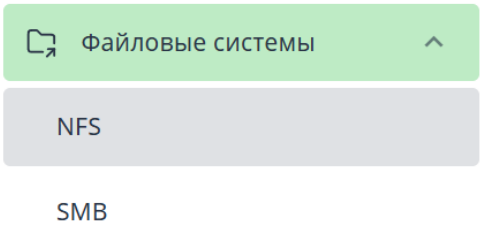


Рисунок 7.1 – Отображение вкладки «Блочный доступ»

7.1 ЭКСПОРТ NFS

ВНИМАНИЕ!

- В случае, если удаляемый том экспортируется (включен в экспорт) возникнет ошибка 400. Предварительно, необходимо исключить том из группы инициаторов.

7.1.1 СОЗДАНИЕ ЭКСПОРТА NFS

Для предоставления доступа к файловому логическому тому, в системе должен быть создан экспорт NFS.

Предоставление файлового доступа к логическому тому по протоколу сетевого доступа NFS, состоит из двух этапов:

Этап 1. Для создания экспорта, необходимо выполнить следующие шаги:

1. В левом боковом меню перейти во вкладку «Файловые системы», выбрать «NFS», откроется вкладка, содержащая соответствующую таблицу «Экспорты NFS» и информацию о состоянии NFS-сервера.
2. Нажать в таблице «Добавить»  , после чего откроется модальное окно, как показано на рисунке 7.2.

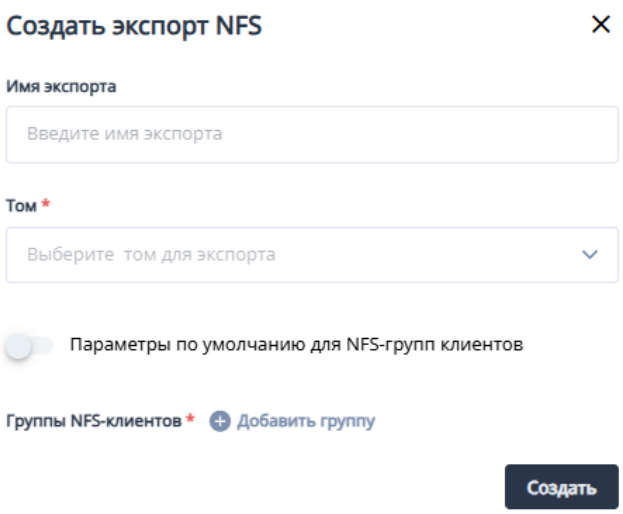


Рисунок 7.2– Окно создания экспорта NFS

3. В открывшемся окне «Создать экспорт NFS» ввести в поле «Имя экспорта» название (данный параметр не является обязательным для заполнения. Если данное поле не будет заполнено, то вместо имени будет отображаться ID таргета).

4. В поле «Том» необходимо выбрать том, который будет экспортироваться.

ПРИМЕЧАНИЕ.

В выпадающем списке, в поле «Том» отображаются только те тома, которые:

- Имеют тип «File». Тип тома указывается при его создании;
- Не экспортируются посредством NFS в данный момент.

5. Следующим шагом будет настройка раздела «Параметров для NFS-групп клиентов по умолчанию».

ПРИМЕЧАНИЕ. Доступные для настроек параметры для NFS-групп клиентов

rw / ro

- rw (чтение-запись) - клиенты, у которых есть доступ к экспортированному каталогу, могут как читать данные из него, так и записывать в него;
- ro (только чтение) - клиенты могут только читать данные из экспортированного каталога, но не могут вносить в него изменения.

sync / async

- sync (синхронный) - сервер NFS ждет завершения фактической записи данных на физический диск, прежде чем сообщать клиенту об успешном завершении

операции записи. Это гарантирует, что данные были сохранены на диск и не потеряются при сбое питания или других непредвиденных обстоятельствах. Однако, такая синхронная запись может значительно замедлять работу NFS, особенно при больших объемах записи или медленном диске;

- async - сервер NFS не ждет завершения записи на диск и сразу отвечает клиенту об успешном завершении операции. Запись данных на диск происходит в фоновом режиме. Это значительно увеличивает производительность, особенно при выполнении большого количества операций записи. Однако, в случае сбоя сервера до того, как данные будут записаны на диск, существует вероятность потери данных.

secure / insecure

- secure - требует, чтобы клиентские соединения NFS поступали с "защищенных" портов, то есть с номерами ниже 1024. Это сделано для предотвращения использования незащищенных портов для доступа к файловой системе, что может быть использовано злоумышленниками для подделки запросов;
- insecure - позволяет клиентским соединениям NFS приходить с любых портов, включая те, которые выше 1024. Хотя это может упростить настройку, оно делает NFS менее безопасным, так как позволяет неавторизованным пользователям и программам пытаться получить доступ к данным.

Заданные параметры впоследствии будут применены для всех создаваемых групп клиентов. Чтобы изменить эти параметры, необходимо переключить свитчер «Параметры по умолчанию для NFS-групп клиентов»

ПРИМЕЧАНИЕ.

По умолчанию выбраны значения:

- rw;
- sync;
- secure.

Этап 2. Для создания групп NFS-клиентов необходимо выполнить следующие шаги:

1. В том же модальном окне, в разделе «Группы NFS-клиентов» нажать «Добавить группу»  . Откроется область с настройками группы, как показано на рисунке 7.3.

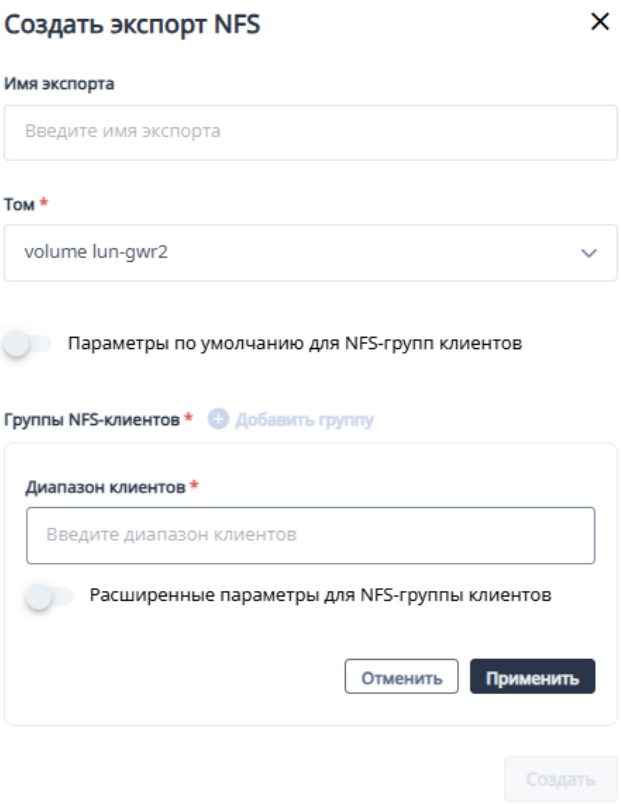


Рисунок 7.3 – Создание и настройка групп NFS-клиентов

2. В поле «Диапазон клиентов» указать данные о клиентах.

   «Параметры по умолчанию для NFS-групп клиентов»

ПРИМЕЧАНИЕ.

«Диапазон клиентов» может указываться в нескольких форматах из Machine Name Formats»:

- **Single host** – хост либо сокращенным именем, распознаваемым резолвером, либо полным доменным именем, адресом IPv4 или адресом IPv6.
- **Netgroups** – сетевые группы NIS могут быть заданы как @group . Только часть хоста каждого члена сетевой группы учитывается при проверке членства. Пустые части хоста или те, которые содержат один тире (-), игнорируются.
- **Wildcards** – имена машин могут содержать подстановочные знаки «*» и «?» или могут содержать списки классов символов в [квадратных скобках]. Это можно использовать для того, чтобы сделать файл экспорта более компактным; например, *.cs.foo.edu соответствует всем хостам в домене cs.foo.edu . Поскольку эти символы также соответствуют точкам в имени домена, заданный шаблон также будет соответствовать всем хостам в любом поддомене cs.foo.edu.

3. Следующим опциональным шагом будет настройка раздела «Расширенных параметры для NFS-групп клиентов» – настройка тех же параметров, что и в

разделе «Параметров для NFS-групп клиентов по умолчанию», но персонализированная для каждой группы клиентов, расширенная полем для свободного ввода значений дополнительных параметров (рисунок 7.4).

ПРИМЕЧАНИЕ. Дополнительные параметры NFS

Помимо параметров, настраиваемых с помощью радио-кнопок, существуют расширенные настройки NFS, которые можно изменить, введя значения в поле свободного ввода. По умолчанию установлены следующие параметры:

- **wdelay** - NFS-сервер будет пытаться объединить мелкие записи в одной операции записи на диск. Это может улучшить производительность, особенно при большом количестве небольших операций записи. Однако это может замедлить запись больших файлов.

  Обратное значение опции: **no_wdelay** (эта опция не действует, если выбрано « async») – каждая операция записи будет выполняться немедленно.

- **hide** - если подкаталог файловой системы также экспортируется, параметр hide предотвращает автоматический экспорт подкаталога, когда клиент монтирует экспортированный родительский каталог. Он "скрывает" этот подкаталог от клиентов, монтирующих родительский каталог.

  Обратное значение опции: **nohide** – разрешает клиентам просматривать и монтировать подкаталоги, которые также экспортируются.

- **no_subtree_check** - отключает проверку поддерева, что может повысить производительность, особенно, если часто экспортируются только подкаталоги файловой системы, но может незначительно снизить безопасность, поскольку сервер не будет так тщательно проверять доступ к файлам внутри подкаталогов. Эта опция часто используется, когда экспорт ограничен определенными подкаталогами и их содержимое редко меняется.

  Проверки поддерева обычно замедляют производительность. Использование no_subtree_check требует, чтобы на сервере было включено subtree_check=off в файле /etc/nfs.conf, если это действительно необходимо.

  Проверка поддеревьев также используется для того, чтобы убедиться, что файлы внутри каталогов, к которым имеет доступ только пользователь root, могут быть доступны только в том случае, если файловая система экспортирована с параметром **no_root_squash**, даже если сам файл допускает более общий доступ.

- **anounid=2000** - задает идентификатор пользователя (UID), которому будет присвоен анонимный доступ. Это означает, что все запросы от клиентов, чьи UID/GID не могут быть сопоставлены с существующими пользователями на сервере, будут рассматриваться как запросы от пользователя с UID 2000.

- **anoungid=2000** - задает идентификатор группы (GID), которому будет присвоен анонимный доступ. Как и anonuid, но для группы. Все запросы от клиентов, чьи

UID/GID не могут быть сопоставлены, будут рассматриваться как запросы от группы с GID 2000.

- **sec=sys** - использует стандартную аутентификацию на основе UID/GID. Это наиболее простая и наименее безопасная форма аутентификации. Она полагается на то, что клиенты правильно сообщают свои UID/GID.

  Доступные варианты безопасности включают:

  - **sec=krb5** - только аутентификация;
  - **sec=krb5i** - защита целостности;
  - **sec=krb5p** - защита конфиденциальности.

  Для целей согласования вариантов безопасности порядок имеет значение: предпочтительные варианты должны быть перечислены первыми.

- **root_squash** - отображает UID 0 (пользователь root) на сервере в UID анонимного пользователя (указанного в anonuid). Это важно для безопасности, поскольку предотвращает доступ пользователя root на клиенте к экспортируемой файловой системе с правами root на сервере.

  Обратное значение опции: **no_root_squash** – отключить сжатие корня. Эта опция в основном полезна для бездисковых клиентов.

- **no_all_squash** - в UID анонимного пользователя (указанного в anonuid). Это очень важно для безопасности, поскольку предотвращает доступ пользователя root на клиенте к экспортируемой файловой системе с правами root на сервере.

  Обратное значение параметра: **all_squash** - сопоставить все UID и GID с анонимным пользователем. Полезно для экспортированных по NFS публичных FTP-каталогов, каталогов новостных спулов и т. д.

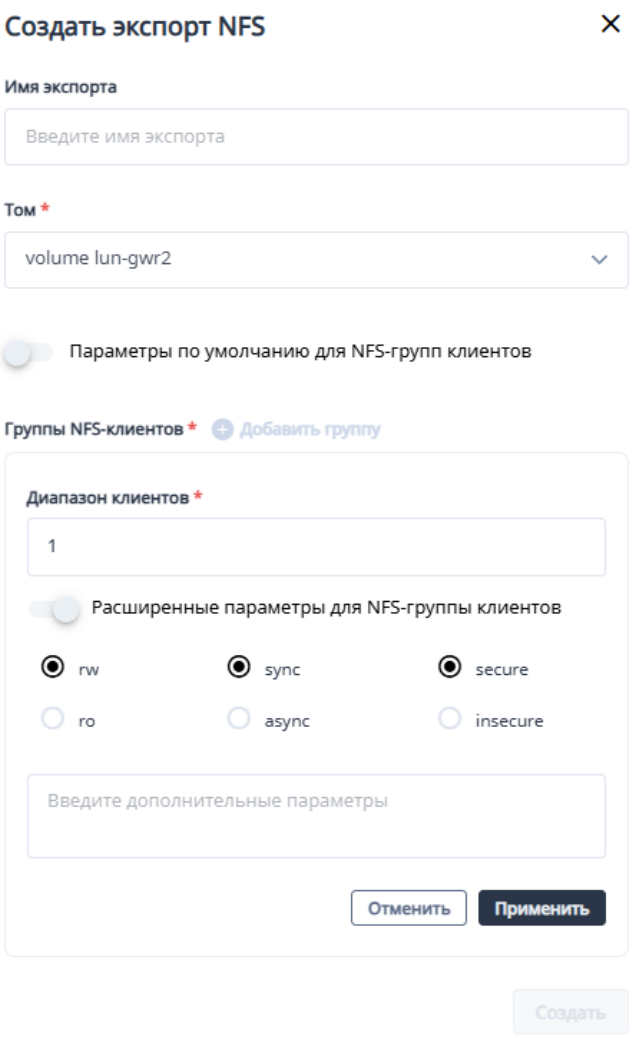


Рисунок 7.4 – Настройка расширенных параметров NFS-групп клиентов

4. Сохраните настройки NFS-групп клиентов, нажав «Применить». После этого, область настроек свернется, как показано на рисунке 7.5. Рядом со свернувшемся полем отобразится здорове группы клиентов, которое может принимать следующие значения:

- Ok – группа клиентов работает в штатном режиме;
- Unknown – новая группа, сканирование еще не произошло;
- Lost – группа отсутствует на сканере, но в базе данных есть запись о ней.

ПРИМЕЧАНИЕ.

В окне создания здоровье группы клиентов всегда будет «Unknown».

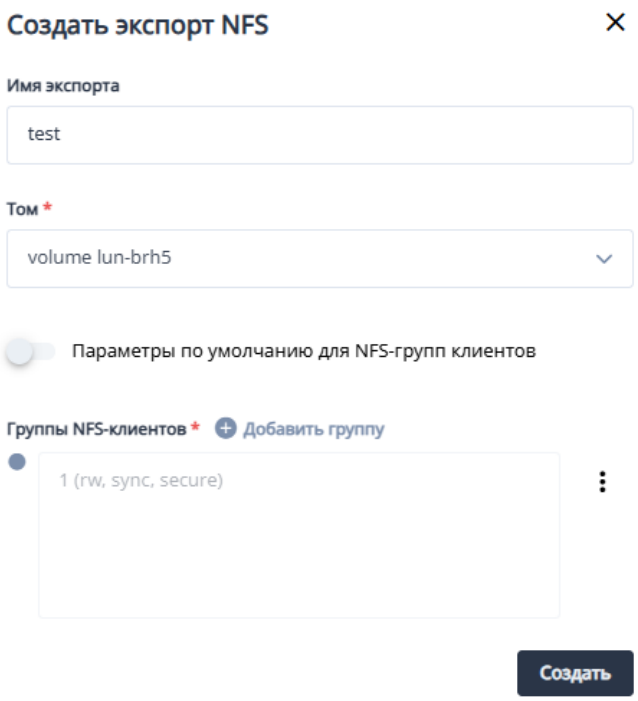


Рисунок 7.5 – Отображение примененных настроек NFS-групп клиентов

5. Нажмите «Создать».

7.1.2 ИНФОРМАЦИЯ ОБ ЭКСПОРТЕ И СЕРВЕРАХ NFS

После выполнения операции создания, будет создан экспорт NFS и группы NFS-клиентов. Экспорт отобразится в таблице «Экспорты NFS», в соответствующем разделе (рисунок 7.6).:

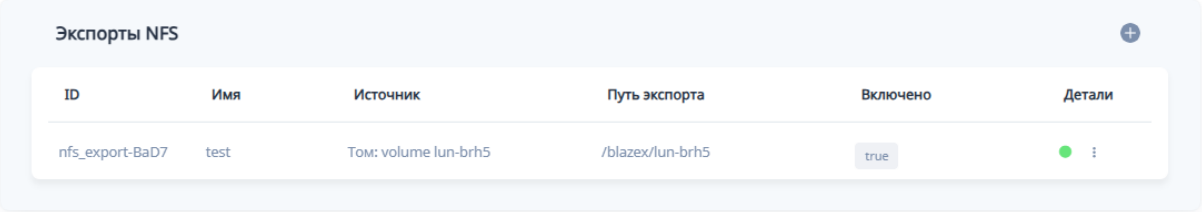


Рисунок 7.6 – Отображение экспорта NFS

Таблица содержит следующую информацию:

- ID;
- имя;
- источник;
- путь экспорта;

- включено (видимость экспорта на инициаторе);
- детали – кнопка вызова контекстного меню и состояние здоровья, принимающее следующие значения:

Ok – экспорт работает в штатном режиме;

Degraded – на узле отсутствует информация об одной и более группах клиентов, или некоторые параметры NFS имеют некорректное значение и были отклонены сервером;

Unknown – отключена видимость экспорта для инициатора.

Группы NFS-клиентов будут доступны для просмотра в окне деталей экспорта. Для этого необходимо вызвать контекстное меню экспорта в таблице, и выбрать опцию «Детали», после чего будет показано модальное окно, содержащее подробную информацию о данном экспорте, группах клиентов (рисунки 7.7, 7.8):

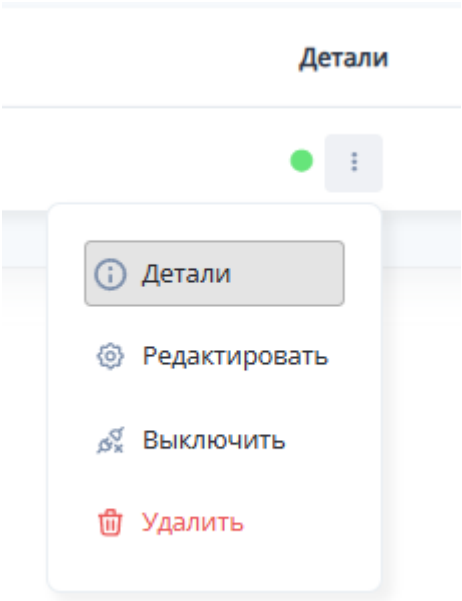


Рисунок 7.7 – Контекстное меню экспорта NFS

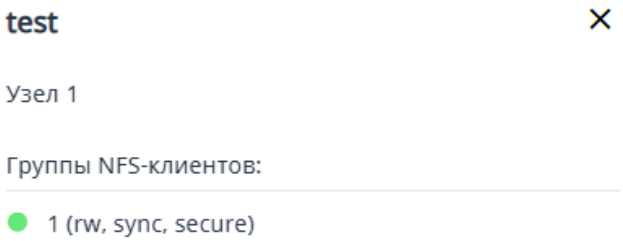


Рисунок 7.8 – Окно деталей экспорта NFS

NFS использует клиент-серверную архитектуру, где клиент отправляет запросы на сервер, а сервер обрабатывает их и предоставляет доступ к данным, поэтому, необходимо отслеживание состояния серверов. Для этого, над таблицей «Экспорты NFS», отображается область «Состояние NFS-сервера», как показано на рисунке 7.9.

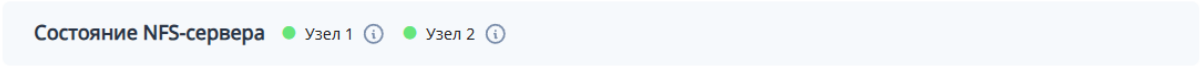


Рисунок 7.9 – Область «Состояние NFS-сервера»

Область содержит информацию о состоянии сервера на каждом из узлов и индикатор состояния здоровья, который может принимать следующие значения:

- Ok – сервер работает в штатном режиме (запущен и «слушает» запросы клиентов;
- Unknown – сервер в процессе сканирования или произошел сбой.

Для просмотра информации о поддерживаемой версии NFS, сетевых протоколах (tcp, udp, rdma) и портах, необходимо кликнуть на иконку «Информация» рядом с одним из узлов, после чего откроется окно деталей сервера, как показано на рисунке 7.10.

Рисунок 7.10 – Окно деталей сервера NFS

7.1.3 ВКЛЮЧЕНИЕ ЭКСПОРТА NFS

ПРИМЕЧАНИЕ

Экспорт NFS по умолчания виден для инициатора – в колонке «Включено» отображается статус «true».

Для того, чтобы скрыть экспорт на стороне инициатора, необходимо отключить его видимость. Для этого в контекстном меню экспорта необходимо выбрать опцию «Выключить» (см. рисунок 7.11). после чего отобразится модальное окно, в котором необходимо подтвердить действие, как показано на рисунке 7.12.

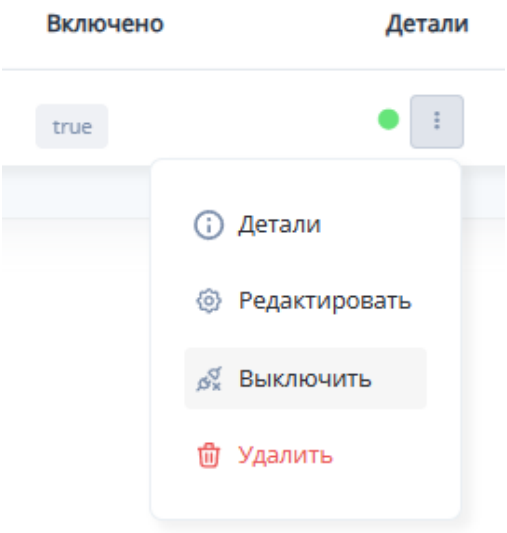


Рисунок 7.11 – Выбор опции «Выключить» в контекстном меню

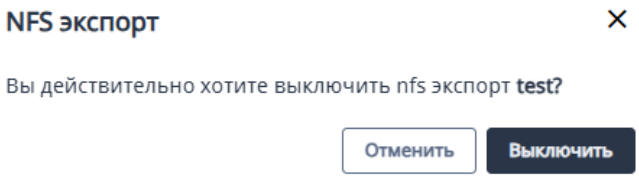


Рисунок 7.12 – Окно подтверждения выключения экспорта NFS

После подтверждения действия, в колонке «Включено» статус «true» изменится на статус «false», путь экспорта будет скрыт, а состояния здоровья в колонке «Детали» изменится на «Unknown» что означает, что экспорт стал невидимым для инициатора (рисунок 7.13).

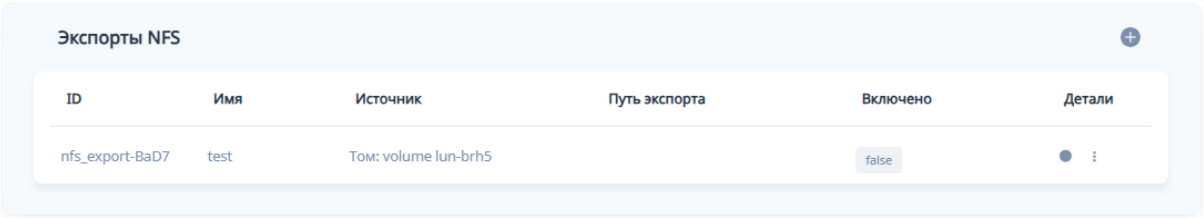


Рисунок 7.13 – Экспорт NFS невидим на стороне инициатора

ПРИМЕЧАНИЕ

Опция «Выключить» экспорт NFS не прервет процесс экспортирования, но экспорт перестанет быть видимым для инициатора.

7.1.4 РЕДАКТИРОВАНИЕ ЭКСПОРТА NFS

Для редактирования экспорта, необходимо нажать на кнопку вызова контекстного меню группы инициаторов, как показано на рисунке 7.14 и выбрать пункт меню «Редактировать».

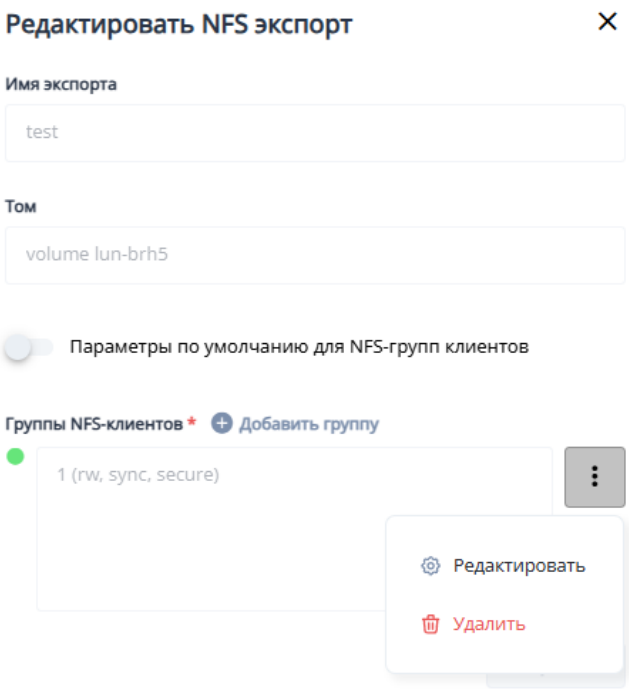


Рисунок 7.14 – Окно редактирования экспорта NFS

В открывшемся окне доступна возможность редактирования параметров по умолчанию для всех NFS-групп клиентов, редактирование параметров группы NFS-клиентов, удаление и создание новых групп.

Процесс редактирование аналогичен процессу создания. Изменив настройки групп клиентов, их необходимо применить, после изменений настроек экспорта необходимо нажать кнопку «Сохранить».

7.1.5 УДАЛЕНИЕ ЭКСПОРТА NFS

Удаление выбранного экспорта также осуществляется в контекстном меню, при выборе опции «Удалить». При удалении выбранного экспорта необходимо подтвердить данное решение. Для этого введите название удаляемого экспорта, как показано на рисунке 7.15:

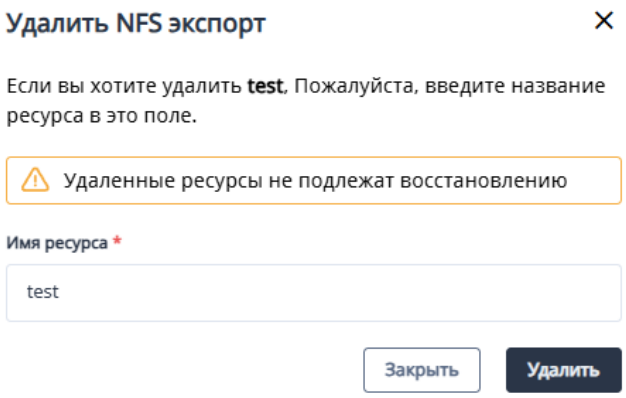


Рисунок 7.15 – Окно подтверждения удаления экспорта NFS

7.2 ЭКСПОРТ SMB

7.2.1 СОЗДАНИЕ SMB ЭКСПОРТА

Для предоставления доступа к файловому логическому тому, в системе должен быть создан экспорт SMB.

Предоставление файлового доступа к логическому тому по протоколу сетевого доступа SMB, состоит из двух этапов:

Для создания экспорта, необходимо выполнить следующие шаги:

1. В левом боковом меню перейти во вкладку «Файловые системы», выбрать «SMB», откроется вкладка, содержащая соответствующую таблицу «Экспорты SMB» (рисунок 7.16).

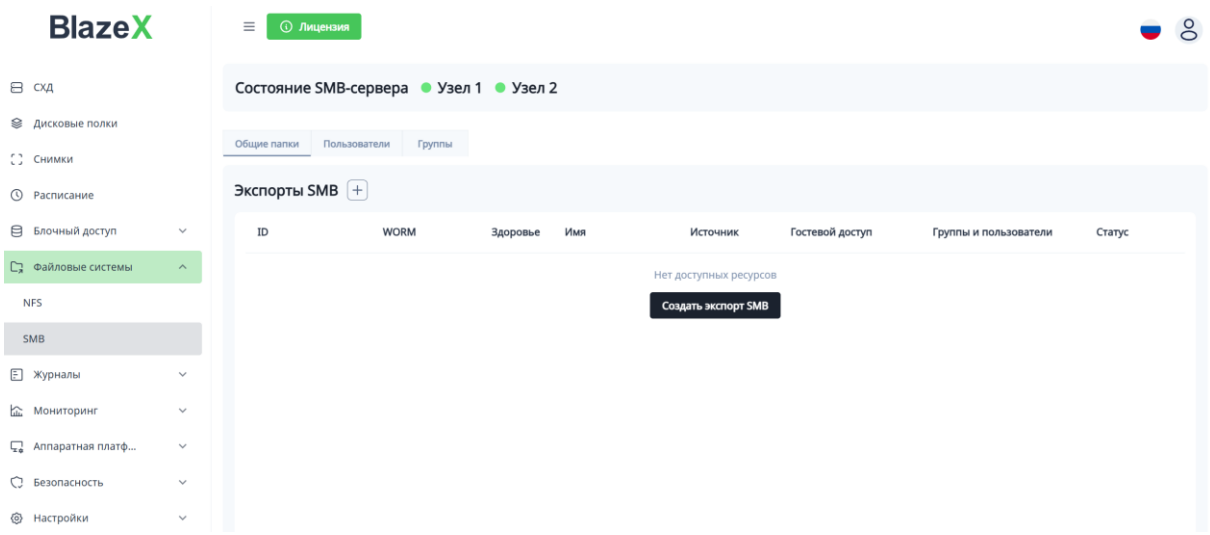


Рисунок 7.16 – Окно подтверждения удаления экспорта NFS

2. Нажать в таблице «Добавить»  или кнопку 

, после чего откроется модальное окно, как показано на рисунке 7.17.

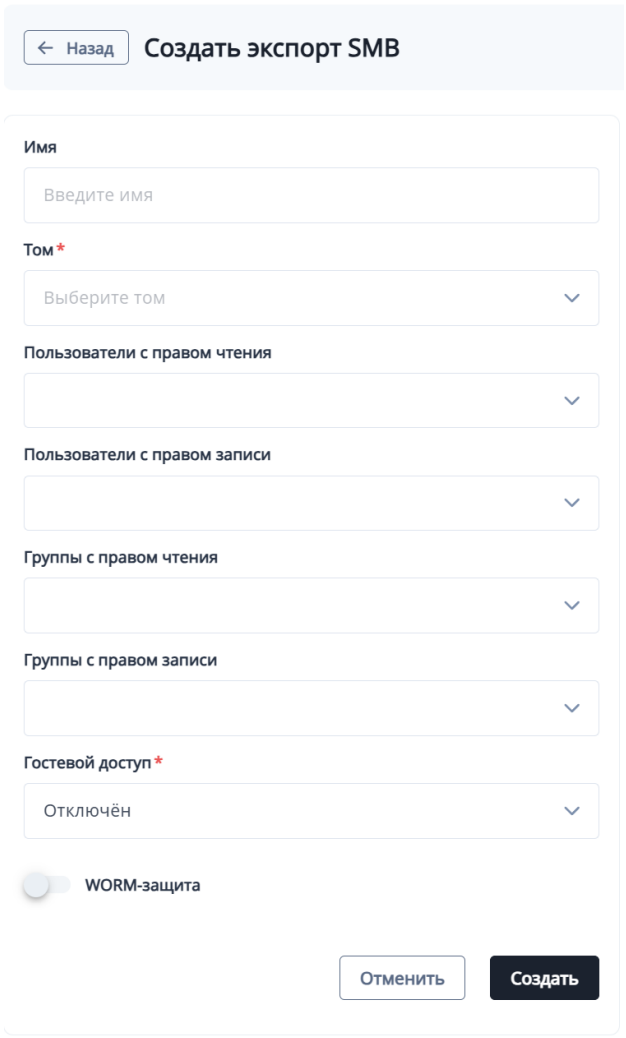


Рисунок 7.17 – Создание экспорта SMB

В окне создания SMB экспорта необходимо:

1. Ввести имя SMB папки (не обязательно)
2. Выбрать - выбрать том который будет роздан
3. Пользователи с правом чтения – в дропдауне выбрать пользователей которым будет выдано право только чтения
4. Пользователи с правом записи – в дропдауне выбрать пользователей которым будет выдано право чтения и записи
5. Группа с правом чтения – в дропдауне выбрать группу которой будет выдано право только чтения
6. Группа с правом записи – в дропдауне выбрать группу которой будет выдано право чтения и записи
7. Гостевой доступ – выбрать один из трех вариантов доступа для SMB экспорта (рисунок 7.18):
   - Отключен
   - Только чтение
   - Чтение и запись

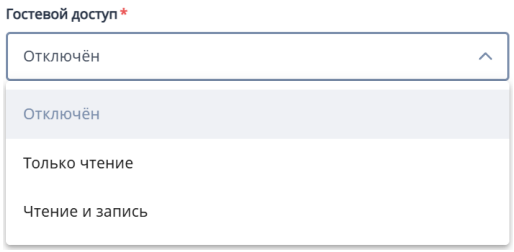


Рисунок 7.18 – Выбор доступа экспорта SMB

8. Включить или выключить защиту WORM.

WORM - это технология, которая защищает файлы от изменения или удаления в течение заданного срока хранения. Данные можно записать один раз, а после этого их можно только читать, но нельзя редактировать, перезаписывать или стирать до истечения срока. Защитить файлы или объект хранилища можно со следующими параметрами (рисунок 7.19):

- Время отсрочки - Время, после которого защита вступает в силу после записи объекта.
- Время хранения - Срок, на который файл блокируется от удаления/изменения.

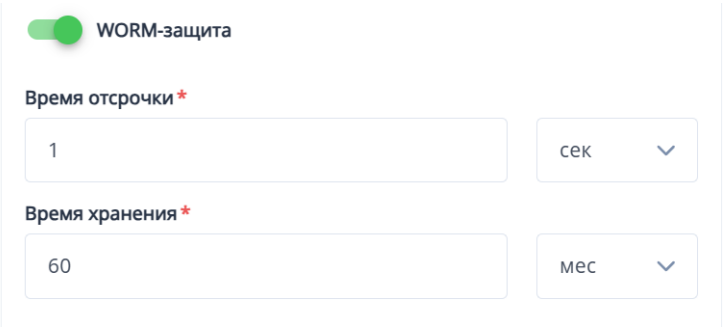


Рисунок 7.18 – Настройка параметров WORM защиты

9. Для сохранения настроек нажать на кнопку «Сохранить».

В результате выполнения новый SMB экспорт отобразится в итоговой таблице (рисунок 7.19)

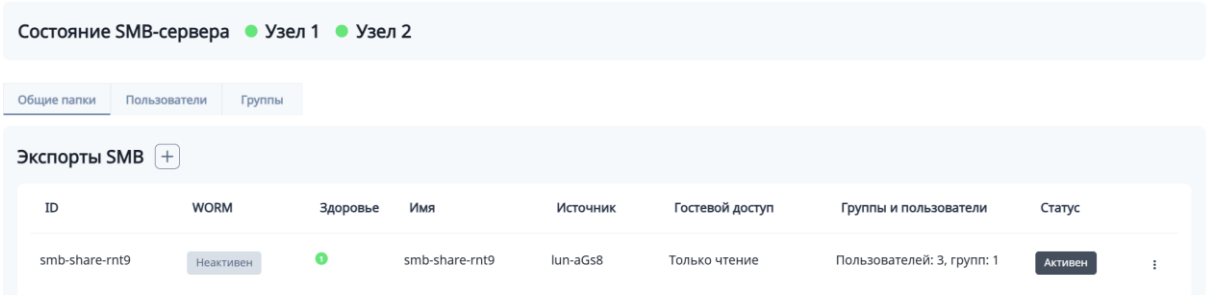


Рисунок 7.19 – Отображение SMB экспорта

7.2.2 ИНФОРМАЦИЯ О SMB ЭКСПОРТЕ

При нажатии на кнопку «Параметры» ⋮ доступны следующие действия (рисунок 7.20):

- Детали - Вызов окна «Детали»
- Редактирование - Редактирование параметров SMB экспорта
- Включить/Выключить – Включение или отключение доступа к SMB экспорту
- Удалить – Удаление SMB экспорта

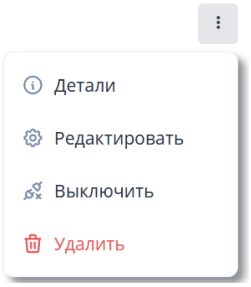


Рисунок 7.20 – Контекстное меню SMB экспорта

При выборе пункта меню Детали, будет показано диалоговое окно, содержащее подробную информацию о SMB экспорте и связанных с ним операциях (рисунок 7.21).

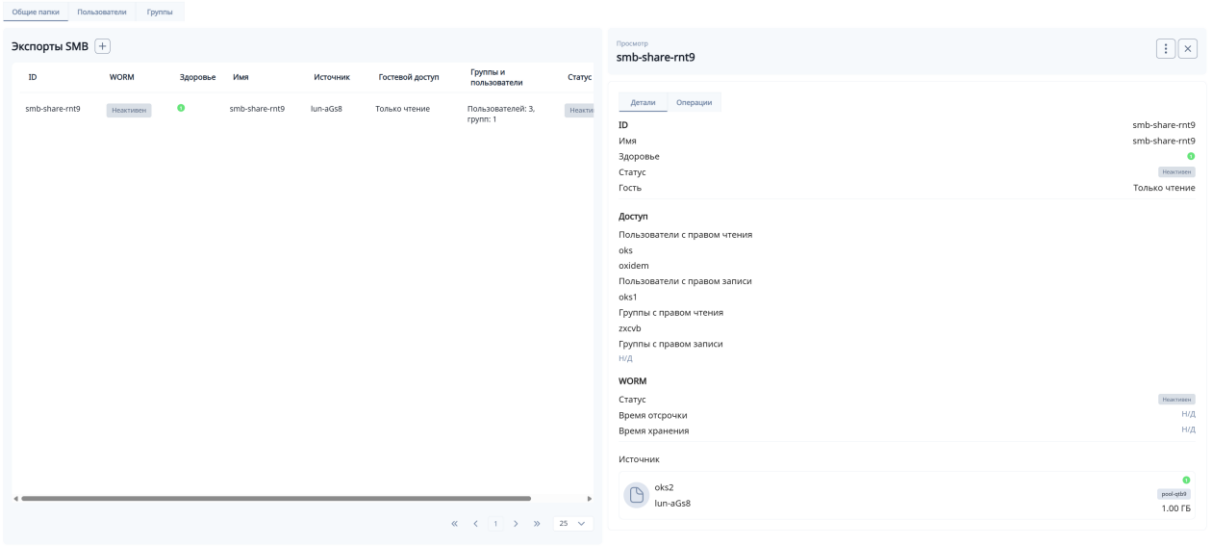


Рисунок 7.21 – Окно «Детали» SMB экспорта

7.2.3 РЕДАКТИРОВАНИЕ SMB ЭКСПОРТА

При выборе пункта «Редактировать» Редактировать откроется окно показанное на рисунке 7.22. Оно позволяет изменить параметры и сохранить изменения

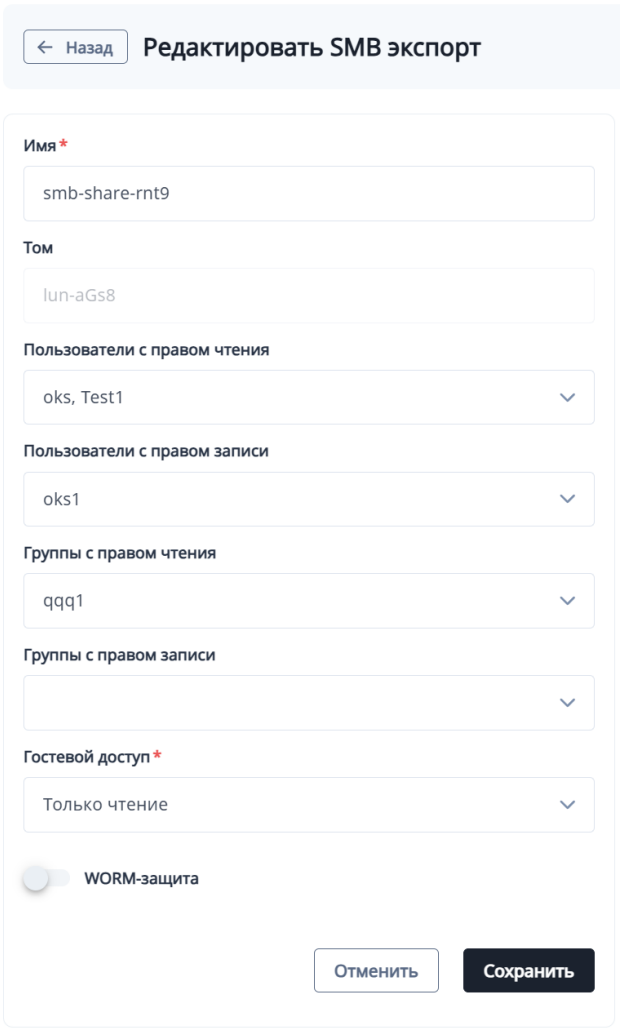


Рисунок 7.22 – Редактирование SMB экспорта

7.2.4 ВКЛЮЧЕНИЕ, ВЫКЛЮЧЕНИЕ SMB ЭКСПОРТА

Для обнаружения SMB экспорта, необходимо активировать его видимость. Для этого в контекстном меню необходимо выбрать опцию «Включить» (см. рисунок 7.20). после чего отобразится модальное окно, в котором необходимо подтвердить действие, как показано на рисунке 7.23.

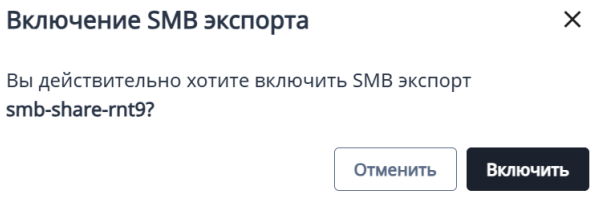


Рисунок 7.23 – Подтверждение включения SMB экспорта

После подтверждения действия, в колонке «Статус» статус «Неактивен» Неактивен (рисунок 7.21) изменится на статус «Активен» Активен, что будет обозначать означает, что SMB экспорт стал видимым (рисунок 7.22).

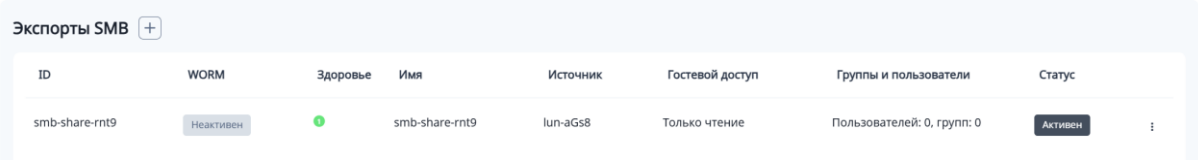


Рисунок 7.22 – Видимый SMB экспорт

7.2.5 УДАЛЕНИЕ ЭКСПОРТА SMB

Удаление выбранного экспорта также осуществляется в контекстном меню, при выборе опции «Удалить» Удалить. При удалении выбранного экспорта необходимо подтвердить данное решение. Для этого введите название удаляемого экспорта, как показано на рисунке 7.23:

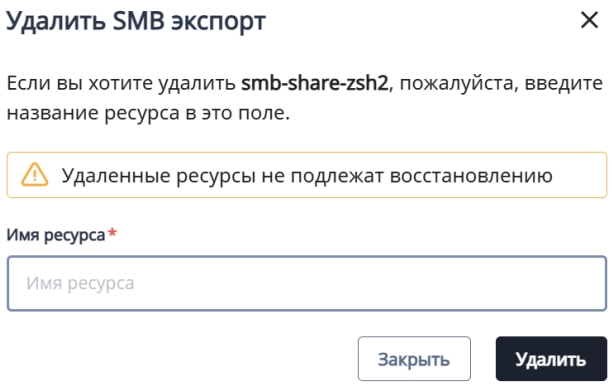


Рисунок 7.23 – Окно подтверждения удаления экспорта SMB

7.2.6 СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ SMB

Для создания SMB пользователей, необходимо выполнить следующие шаги:

1. В левом боковом меню перейти во вкладку «Файловые системы», выбрать «SMB», откроется вкладка, содержащая соответствующую таблицу «Экспорты SMB»? в ней нужно нажать на вкладку «Пользователи» (рисунок 7.16).
2. Нажать в таблице «Добавить» + или кнопку «Создать пользователя» Создать пользователя, после чего откроется модальное окно, как показано на рисунке 7.24.

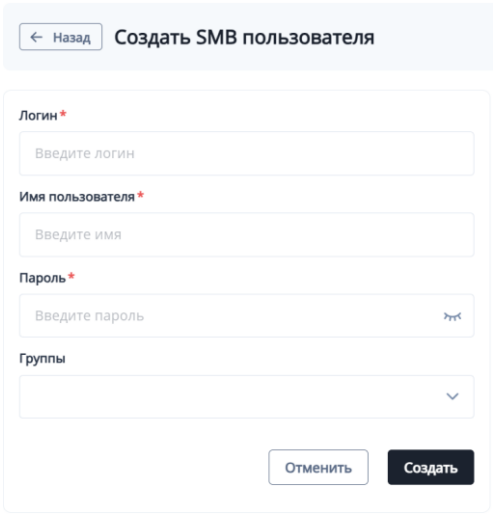


Рисунок 7.24 – Создание SMB пользователя

В данном окне необходимо задать:

- Логин пользователя
- Имя пользователя
- Пароль
- Группа – выбрать принадлежность к группе

После создания пользователь появится в окне «Пользователи» SMB (рисунок 7.25).

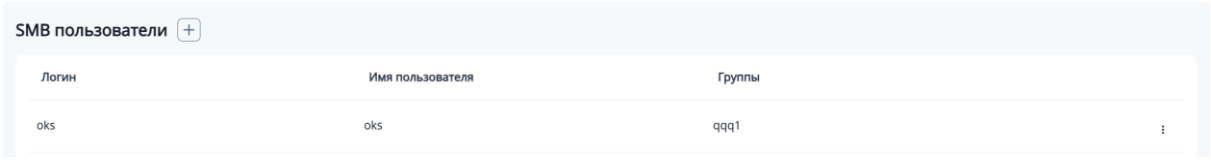


Рисунок 7.25 – Созданный пользователь SMB

7.2.7 ИНФОРМАЦИЯ ОБ SMB ПОЛЬЗОВАТЕЛЯХ

При нажатии на кнопку «Параметры» ⋮ доступны следующие действия (рисунок 7.26):

- Детали - Вызов окна «Детали»
- Редактирование - Редактирование параметров SMB пользователя
- Сменить пароль – Изменение пароля SMB пользователя
- Удалить – Удаление SMB пользователя

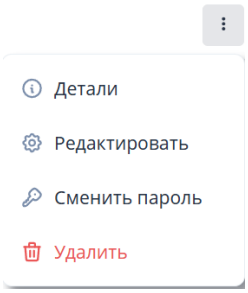


Рисунок 7.26 – Контекстное меню SMB пользователя

При выборе пункта меню Детали, будет показано диалоговое окно, содержащее информацию о SMB пользователе (рисунок 7.27).

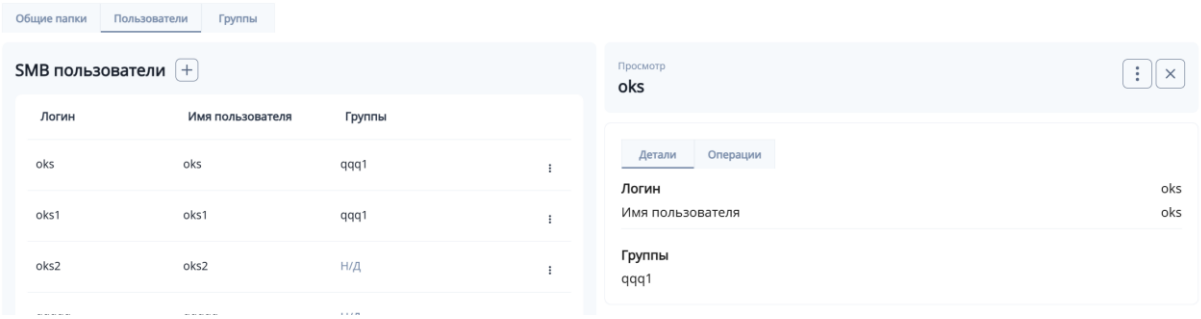


Рисунок 7.27 – Окно «Детали» SMB пользователя

7.2.8 РЕДАКТИРОВАНИЕ SMB ПОЛЬЗОВАТЕЛЯ

При нажатии на кнопку «Редактировать» (рисунок 7.26) открывается окно, в котором можно изменить имя пользователя и принадлежность к группе SMB пользователя (рисунок 7.28)

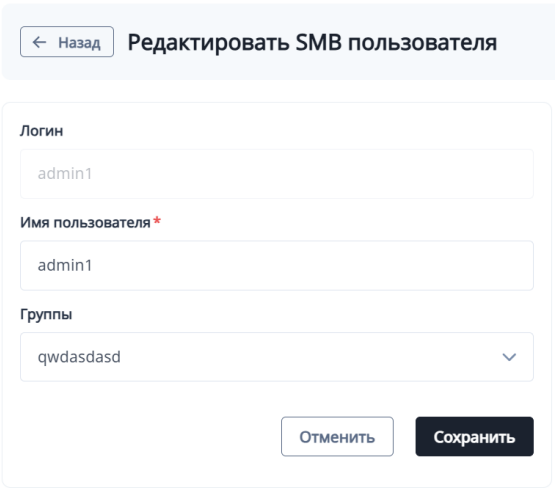


Рисунок 7.28 – Редактирование SMB пользователя

7.2.9 СМЕНА ПАРОЛЯ SMB ПОЛЬЗОВАТЕЛЯ

При нажатии на кнопку «Сменить пароль» открывается окно, в котором можно задать новый пароль SMB пользователя (рисунок 7.29)

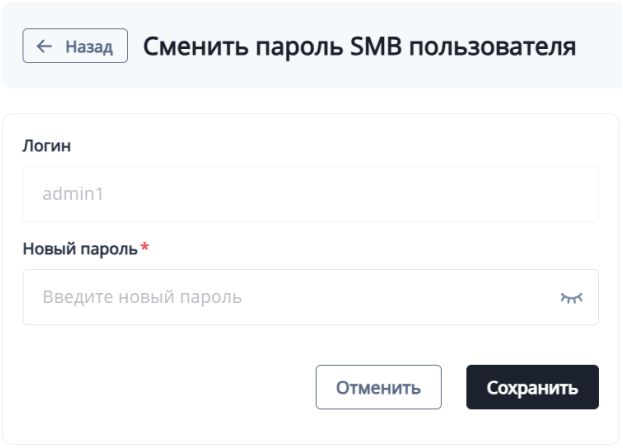


Рисунок 7.29 – Смена пароля SMB пользователя

7.2.10 УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ SMB

Удаление выбранного пользователя также осуществляется в контекстном меню, при выборе опции «Удалить» Удалить. При удалении выбранного пользователя необходимо подтвердить данное решение. Для этого введите название удаляемого экспорта, как показано на рисунке 7.30:

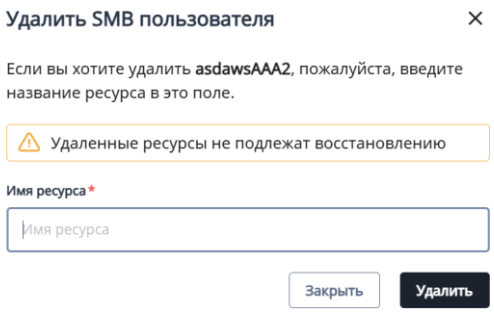


Рисунок 7.30 – Окно подтверждения удаления пользователя SMB

7.2.11 СОЗДАНИЕ ГРУПП ПОЛЬЗОВАТЕЛЕЙ SMB

Для создания групп SMB пользователей, необходимо выполнить следующие шаги:

1. В левом боковом меню перейти во вкладку «Файловые системы», выбрать «SMB», откроется вкладка, содержащая соответствующую таблицу «Экспорты SMB», в ней нужно нажать на вкладку «Группы» (рисунок 7.16).
2. Нажать в таблице «Добавить» + или кнопку «Создать группу» Создать группу, после чего откроется модальное окно, как показано на рисунке 7.31.

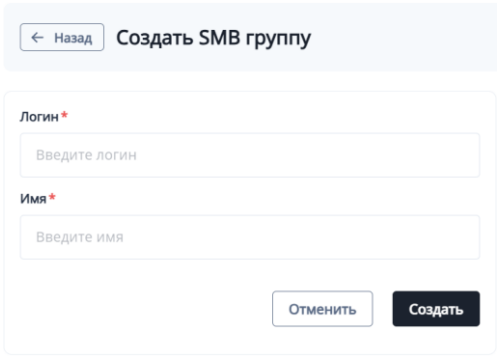


Рисунок 7.31 – Создание группы SMB пользователя

В данном окне необходимо задать:

- Логин группы
- Имя группы

После создания пользователь появится в окне «Группы» SMB (рисунок 7.32).

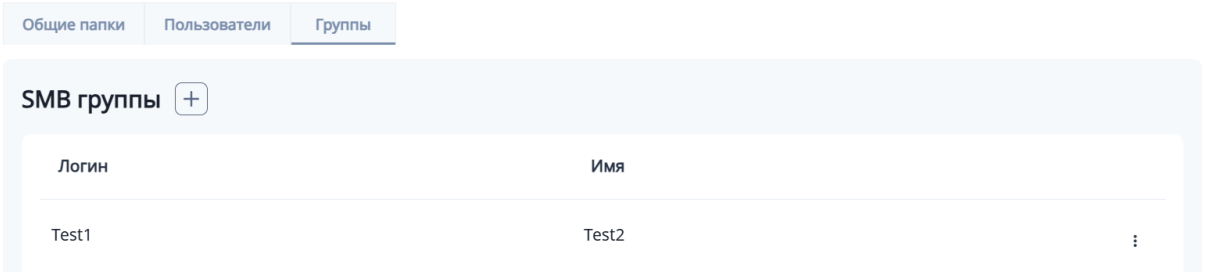


Рисунок 7.32 – Созданная группа SMB

7.2.12 УДАЛЕНИЕ ГРУППЫ SMB

Удаление выбранной группы также осуществляется в контекстном меню, при выборе опции «Удалить» Удалить. При удалении выбранного группы необходимо подтвердить данное решение. Для этого введите название удаляемого экспорта, как показано на рисунке 7.33:

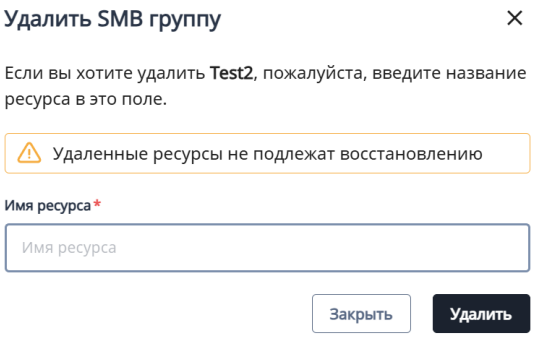


Рисунок 7.33 – Окно подтверждения удаления пользователя SMB

8 КЛОНЫ

BlazeX обеспечивает возможность создания клона тома посредством уже существующего снимка логического тома.

ВНИМАНИЕ! Особенности работы с клонами

- Том, от которого был создан снимок, и сам снимок должны быть тонкими (при создании должна быть выбрана технология «Thin provisioning»)
- Клон тома становится полностью независимым от снимка, в момент удаления снимка из системы

Управление клонами доступно в разделе «СХД», в колонке «Тома», как показано на рисунке 8.1.

8.1 СОЗДАНИЕ КЛОНА

Процесс создания клона тома состоит из двух этапов: создание снимка тома и создание клона от снимка:

1. Создание снимка описано в разделе 4.1.
2. В таблице «Снимки», в соответствующем разделе, в строке снимка, от которого необходимо создать клон, необходимо вызвать контекстное меню, далее выбрать пункт «Создать клон» (см. рисунок 8.1).

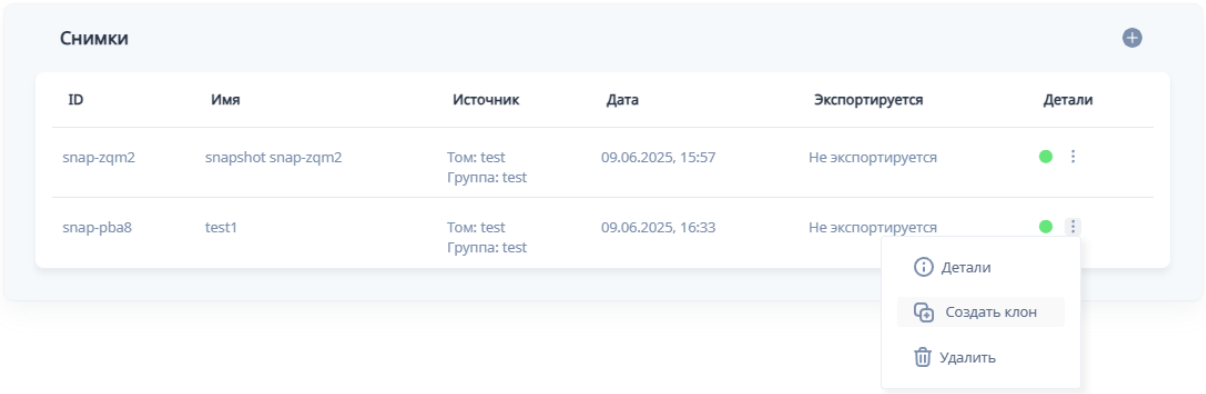


Рисунок 8.1 – Создание клона из контекстного меню в «карточке» выбранного логического тома

1. В открывшемся окне указать имя снимка, источник (том), и размер, как показано на рисунке 8.2.

ПРИМЕЧАНИЕ

Минимальный размер клона равен размеру тома.

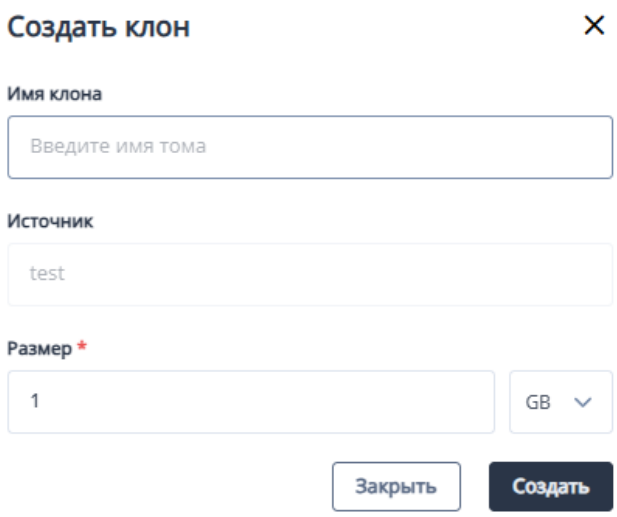


Рисунок 8.2 – Создание снимка через активацию диалогового окна

Отображение результата операции создания клона представлено на рисунке 4.4.

8.2 ИНФОРМАЦИЯ О КЛОНЕ

При успешном выполнении операции будет клон, который затем отобразится в разделе «СХД», в колонке «Тома», под карточкой исходного тома и получит один из возможных состояний здоровья:

- Ok – клон работает в штатном режиме;
- Unknown – процесс сканирования;
- Failed – клон недоступен;
- Lost – нарушена логическая связь с логическим томом.

Пример отображения приведен на рисунке 8.3.

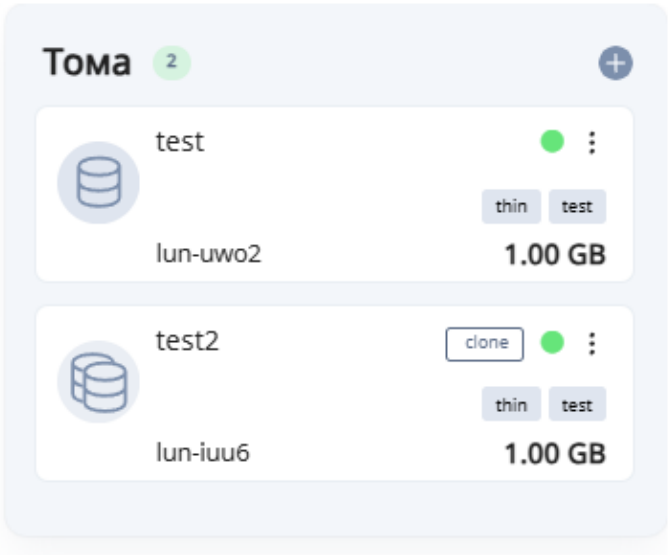


Рисунок 8.3 – Отображение карточки клона

При нажатии на кнопку вызова контекстного меню группы и выборе пункта меню Детали, откроется диалоговое окно, содержащее подробную информацию о клоне присутствующих ошибках в работе, как показано на рисунках 5.4.

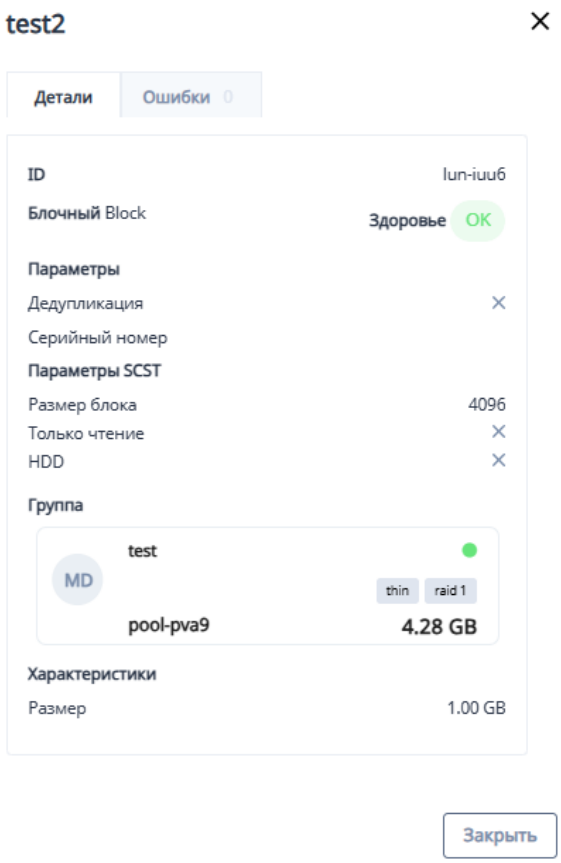


Рисунок 8.4 – Окно «Детали» клонов

8.3 УДАЛЕНИЕ КЛОНА

Для удаления клона необходимо в графе «Детали» необходимо вызвать контекстное меню и выбрать пункт 

. Для подтверждения решения необходимо ввести имя ресурса в диалоговом окне формы на удаление (см. рисунок 8.5).

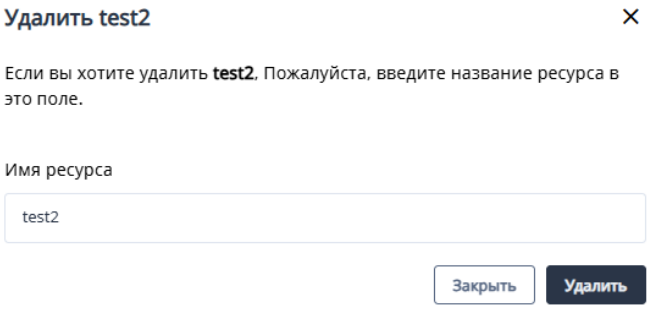


Рисунок 8.5 – Окно подтверждение удаления клона

9 МОНИТОРИНГ

Система мониторинга ПО «BlazeX» является гибридной, поддерживает:

- обзор СХД с отображением общей производительности,
- встроенный механизм отслеживания исполнения команд и событий, в разделе «Журнал команд», «Журнал сообщений» и «Журнал аудита»
- мониторинг состояния дисковых накопителей, здоровье пулов и сбор статистики по томам через SNMP и подключение сторонних систем: «Prometheus» с последующей визуализацией в системе «Grafana», и Zabbix.

9.1 ОБЗОР СХД

Раздел позволяет контролировать производительность СХД в реальном времени, что позволяет планировать конфигурацию, рассчитывать и повышать производительность как внутри системы хранения, так и на пути передачи данных
Раздел включает в себя:

- Производительность дисковой полки
- Пропускная способность дисковой полки
- Время отклика дисковой полки
- Загрузка процессоров
- Загрузка оперативной памяти
- Загрузка портов

При наведении указателя мыши на кривые графика можно посмотреть данные с определенным шагом измерений. Интервал измерений задается отдельно в правом верхнем углу окна и может быть равен: 5 мин, 15 мин, 30 мин, 1 ч, 7 дней, 90 дней или 1 год (рисунок 9.1).

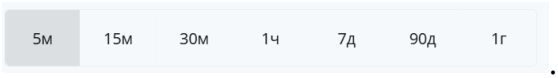


Рисунок 9.1 – Интервал измерения велечин

9.1.1 ПРОИЗВОДИТЕЛЬНОСТЬ ДИСКОВОЙ ПОЛКИ

Графики IOPS (Input/Output Operations per Second, количество операций ввода/вывода в секунду) в режиме реального времени позволяют получить подробную информацию о производительности дисковой полки на чтение и на запись в различные временные промежутки.
По вертикальной оси графиков указывается значение IOPS – количество операций ввода/вывода за секунду), по горизонтальной – временной диапазон. Графики для чтения и для записи обозначаются разными цветами. (рисунок 9.2).

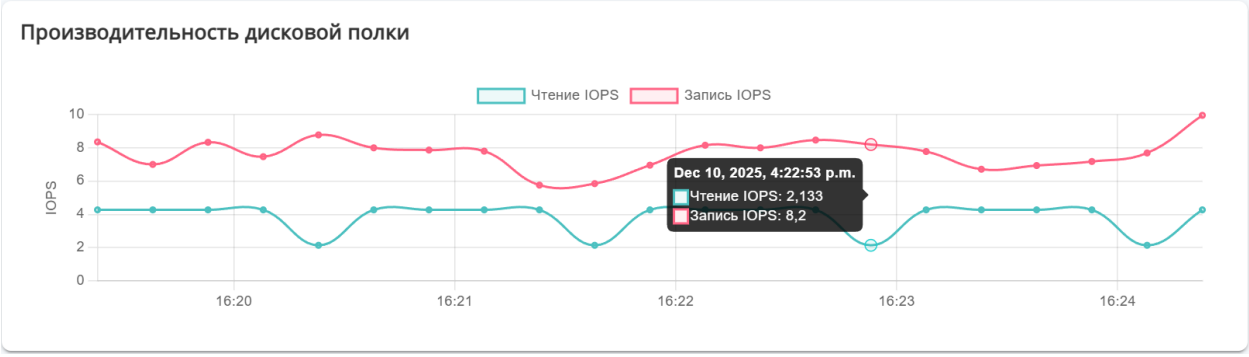


Рисунок 9.2 – Производительность дисковой полки

9.1.2 ПРОПУСКНАЯ СПОСОБНОСТЬ ДИСКОВОЙ ПОЛКИ

Скорость передачи данных или пропускная способность позволяет проводить оценку производительности системы.
По вертикальной оси графиков указывается значение МБ/с – количество переданной информации за секунду, по горизонтальной – временной диапазон. Графики «Чтение», «Запись» и «Всего» обозначаются разными цветами (рисунок 9.3).

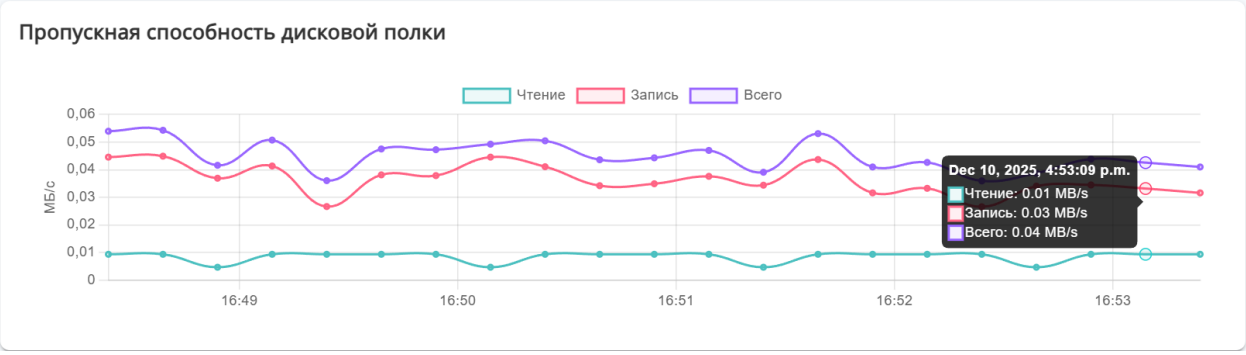


Рисунок 9.3 – Пропускная способность дисковой полки

9.1.3 ВРЕМЯ ОТКЛИКА ДИСКОВОЙ ПОЛКИ

Графики времени отклика позволяют получить информацию о времени отклика дисковой полки на команды в различные временные промежутки. По вертикальной оси графиков указывается время выполнения команды (миллисекунды), по горизонтальной – время. Графики «Чтение», «Запись» и «Среднее» обозначаются разными цветами (рисунок 9.4).

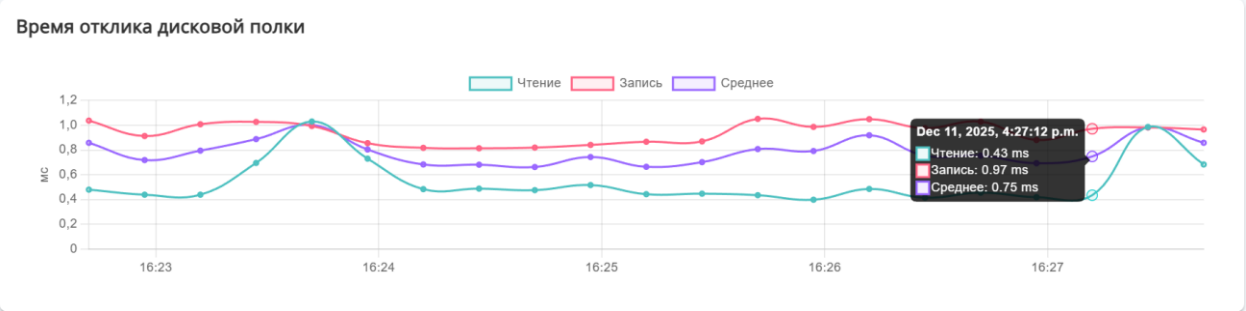


Рисунок 9.4 – Время отклика дисковой полки

9.1.4 ЗАГРУЗКА ПРОЦЕССОРОВ

График загрузки процессора позволяет получить информацию о степени использования вычислительных ресурсов центрального процессора каждого узла в различные временные промежутки. По вертикальной оси графика указывается уровень загрузки процессора (в процентах), по горизонтальной оси - время. График позволяет анализировать периоды пиковой нагрузки, общую производительность системы и выявлять потенциальные узкие места, связанные с нехваткой вычислительных

ресурсов. Графики загрузки процессора для узлов обозначаются разными цветами (рисунок 9.5).

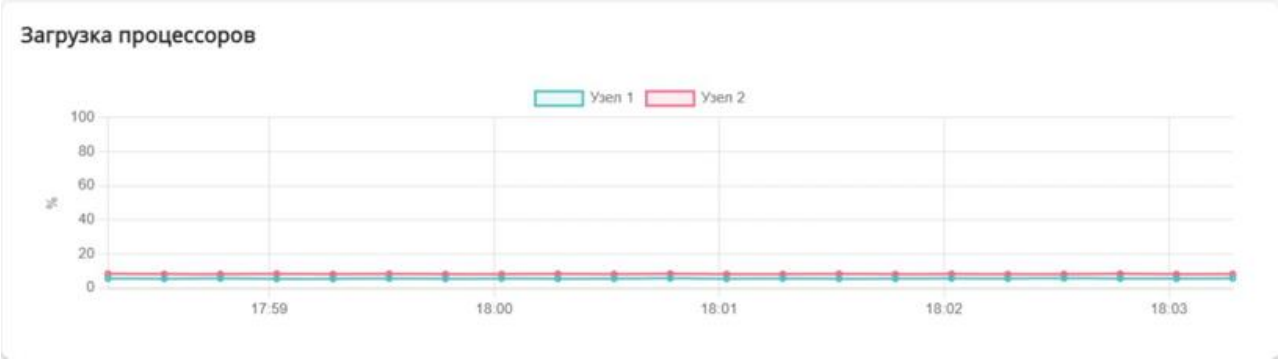


Рисунок 9.5 – Загрузка процессоров

9.1.5 ЗАГРУЗКА ОПЕРАТИВНОЙ ПАМЯТИ

График использования оперативной памяти позволяет получить информацию о степени занятости оперативной памяти в различные временные промежутки. По вертикальной оси графика указывается процент использования от общего доступного объёма оперативной памяти (%), по горизонтальной оси - время. График показывает отслеживать пики потребления, выявлять тенденции к нехватке ресурсов, анализировать работу приложений и эффективность работы системы в целом. Графики загрузки оперативной памяти для узлов обозначаются разными цветами (рисунок 9.6).

Рисунок 9.6 – Загрузка оперативной памяти

9.1.6 ЗАГРУЗКА СЕТЕВЫХ ПОРТОВ

График загрузки сетевых портов позволяет получить информацию об объёме передаваемого и принимаемого сетевого трафика через порты в различные временные промежутки. По вертикальной оси графика указывается скорость передачи данных (мегабиты в секунду, Мб/с), по горизонтальной оси - время. График позволяет анализировать периоды пиковой нагрузки, оценивать пропускную способность каналов связи, выявлять аномальную активность и планировать сетевую инфраструктуру. Графики загрузки портов на прием и передачу для разных узлов обозначаются разными цветами (рисунок 9.7).

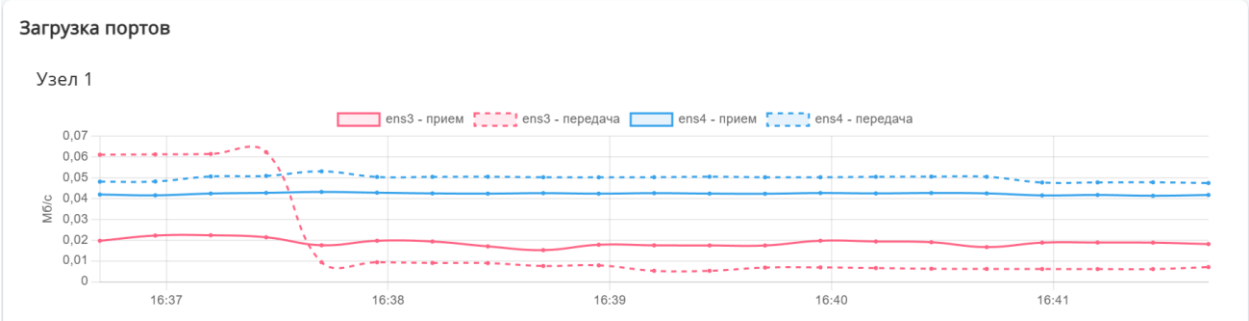


Рисунок 9.7 – Загрузка сетевых портов

9.1.7 ПРИЕМ FC ПОРТОВ

График приема FC портов позволяет получить информацию об объёме входящего трафика через волоконно-оптические порты в различные временные промежутки. По вертикальной оси графика указывается скорость приема данных (мегабайты в секунду, МБ/с), по горизонтальной оси - время. График позволяет анализировать периоды пиковой входящей нагрузки, оценивать пропускную способность каналов связи SAN, выявлять аномальную активность и планировать сетевую инфраструктуру хранения данных. Графики приема для разных FC портов обозначаются разными цветами (рисунок 9.8).

Рисунок 9.8 – Прием FC портов

9.1.8 ПЕРЕДАЧА FC ПОРТОВ

График передачи FC портов позволяет получить информацию об объёме исходящего трафика через волоконно-оптические порты в различные временные промежутки. По вертикальной оси графика указывается скорость передачи данных (мегабайты в секунду, МБ/с), по горизонтальной оси - время. График позволяет анализировать периоды пиковой исходящей нагрузки, оценивать пропускную способность каналов связи SAN, выявлять аномальную активность и планировать сетевую инфраструктуру хранения данных. Графики передачи для разных FC портов обозначаются разными цветами (рисунок 9.9).

Рисунок 9.9 – Передача FC портов

9.1.9 ОШИБКИ FC ПОРТОВ

График ошибок FC портов позволяет получить информацию о количестве сбоев и проблем при передаче данных через волоконно-оптические порты в различные временные промежутки. По вертикальной оси графика указывается интенсивность ошибок (количество ошибок в секунду), по горизонтальной оси - время. График позволяет анализировать периоды нестабильной работы каналов связи, оценивать качество физического соединения или оптических модулей, выявлять аномальную активность, связанную с повреждением кадров или потерей синхронизации, а также своевременно диагностировать деградацию сетевой инфраструктуры хранения данных. Графики ошибок для разных FC портов обозначаются разными цветами (рисунок 9.10).

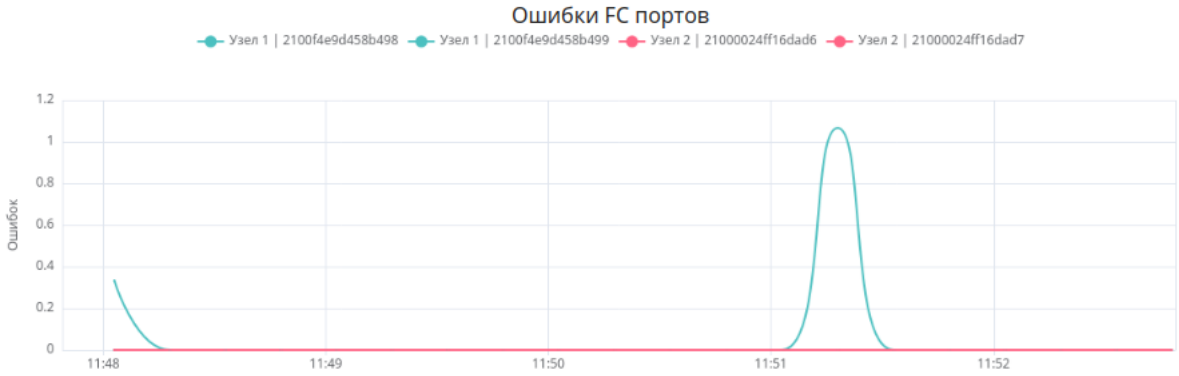


Рисунок 9.10 – Ошибки FC портов

9.1.10 ВРЕМЯ ОТКЛИКА ПО ХОСТАМ

График времени отклика по хостам позволяет получить информацию о задержках при обработке операций ввода-вывода на целевых хостах в различные временные промежутки. По вертикальной оси графика указывается время отклика (в миллисекундах или микросекундах), по горизонтальной оси - время. График позволяет анализировать периоды увеличения задержек при обработке запросов, выявлять хосты с аномально высоким временем ответа, оценивать влияние нагрузки на производительность целевых систем, а также своевременно диагностировать деградацию работы хостов, связанную с перегрузкой вычислительных ресурсов, проблемами с драйверами или некорректной настройкой целевых устройств. Показатели времени отклика для разных хостов обозначаются разными цветами или условными обозначениями, как показано на рисунке.9.11.

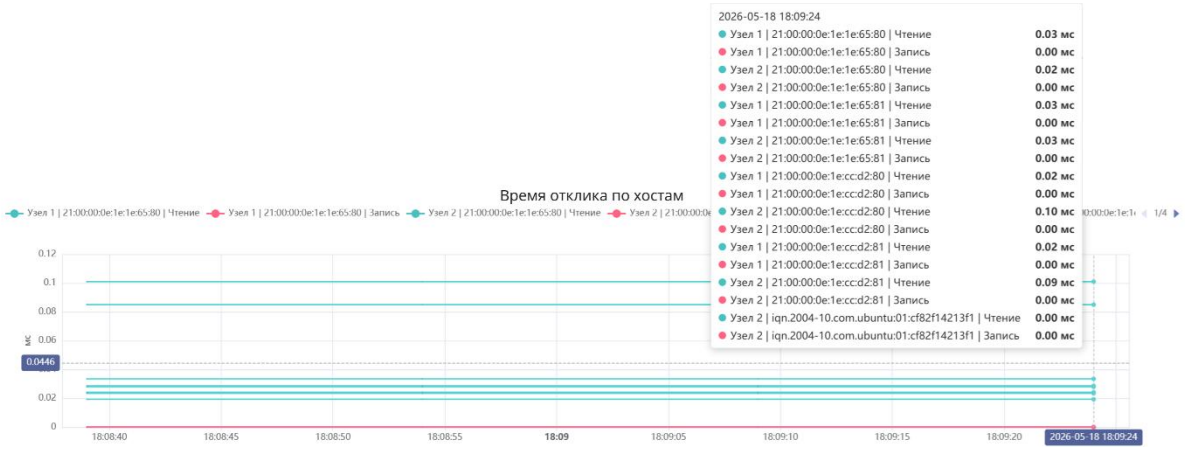


Рисунок 9.11 – Время отклика по хостам

9.1.11 СКОРОСТЬ РЕБИЛДИНГА ПУЛОВ

График скорости ребилдинга пулов позволяет получить информацию об интенсивности процесса восстановления данных после выхода из строя дисков, замены компонентов или сбоев в массиве. По вертикальной оси графика указывается скорость восстановления (МБ/с), по горизонтальной оси - время. График позволяет анализировать эффективность процесса ребилдинга, выявлять периоды нестабильной скорости, оценивать влияние фоновой нагрузки на восстановление данных, а также своевременно диагностировать проблемы с производительностью дисков, шины или контроллеров. Разные пулы и типы массивов (например, mdraid) обозначаются соответствующими подписями (Узел 1, pool-lop6, mdraid), что позволяет отслеживать ход ребилдинга в разрезе конкретных компонентов системы хранения данных (рисунок 9.12).

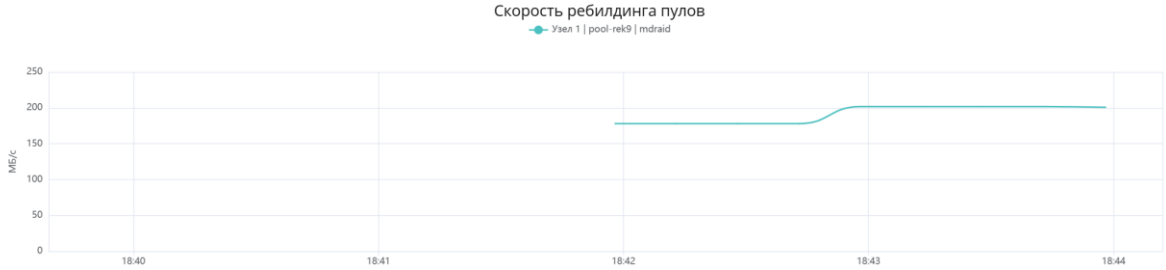


Рисунок 9.12 – Скорость ребилдинга пулов

9.2 SNMP

Раздел предназначен для мониторинга состояния дисковых накопителей СХД (сбои, ошибки, предупреждения, информационные сообщения), статистики по томам (чтение, запись, задержки) и здоровья пулов, посредством протокола SNMP.
Доступ в раздел доступен из раздела мониторинг, как показано на рисунке 9.11

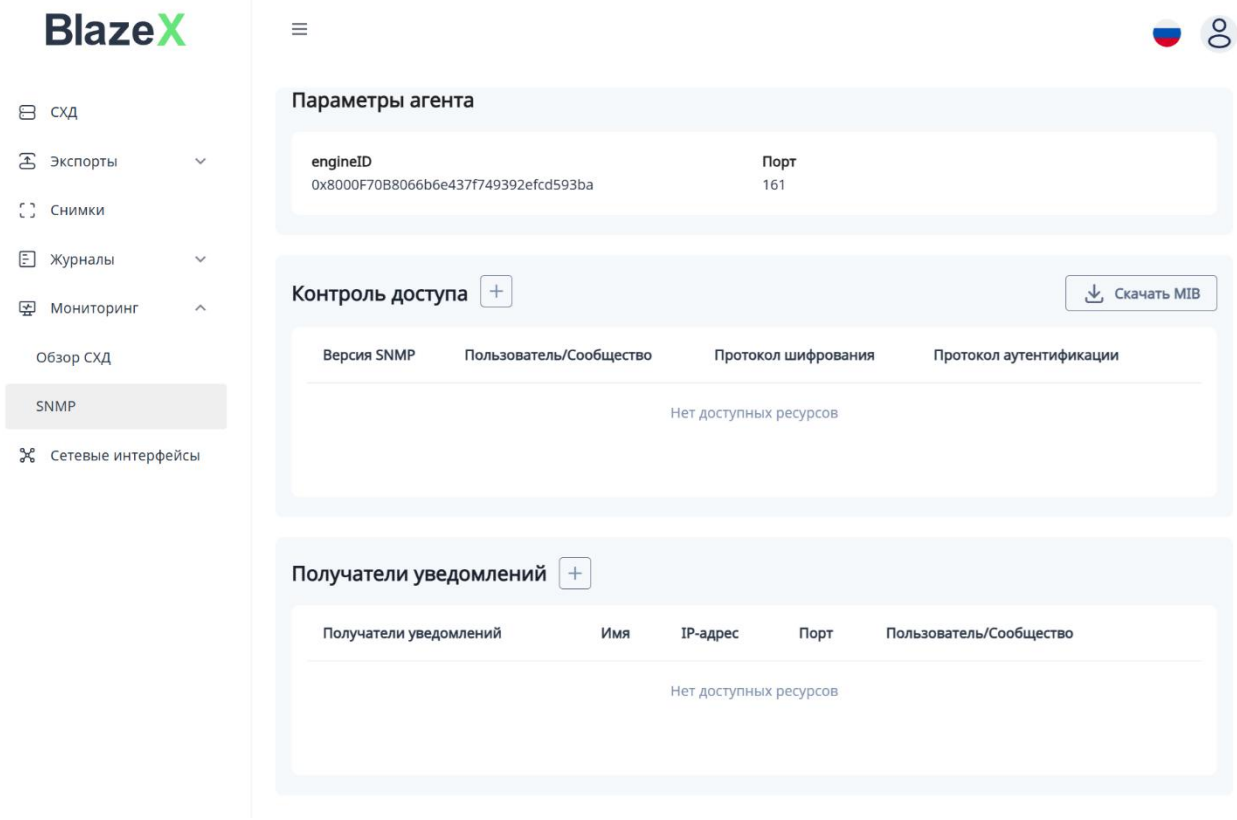


Рисунок 9.11 – Раздел SNMP

Раздел включает в себя

- Параметры агента
- Контроль доступа
- Получатели Уведомлений

Параметры агента
В параметрах агента указан порт и engineID (идентификатор модуля SNMP) - это уникальный, административно присвоенный идентификатор для каждой сущности SNMP (агента или менеджера), который используется для точного определения устройства, создания параметров безопасности (аутентификации/шифрования) и защиты от атак, таких как повторное воспроизведение, гарантируя, что сообщения поступают от правильного, доверенного узла.

9.2.1 НАСТРОЙКА SNMP

Настройка SNMP-агента с использованием SNMPv2c
Для настройки необходимо:

1. Нажать на плюс [+] в заголовке подраздела «Контроль доступа».

2. В открывшемся окне «Создание контроля доступа» Выбрать версию SNMP – «2c» (рисунок 9.12)

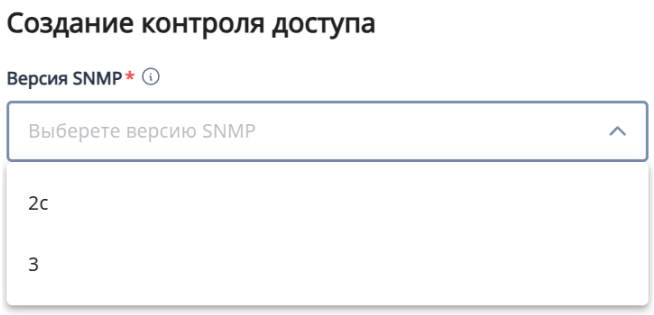


Рисунок 9.12 – выбор версии SNMP

3. В поле «Строка сообщества» укажите сообщество, например, «public» (рисунок 9.13).

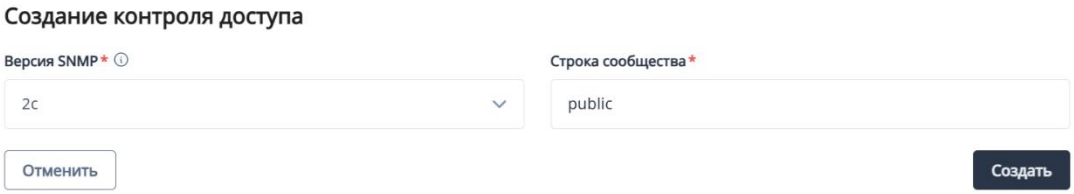


Рисунок 9.13 – Заполненное окно создания SNMP-агента с использованием SNMPv2c

4. Нажать кнопку «Создать» 

.

В случае успешного выполнения команды созданный контроль доступа отобразится в итоговой таблице (рисунок 9.14)

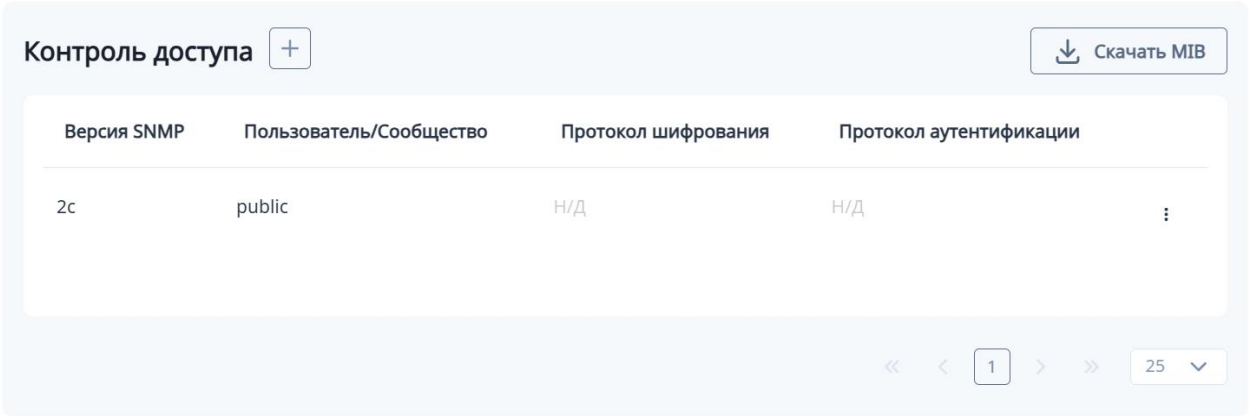


Рисунок 9.14 – Подраздел «Контроль доступа»

Настройка SNMP-агента с использованием SNMPv3
Для настройки необходимо:

1. Нажать на плюс 
в заголовке подраздела «Контроль доступа».
2. В открывшемся окне «Создание контроля доступа» Выбрать версию SNMP – «3» (рисунок 9.15)
3. В параметрах необходимо

a. Ввести **Имя пользователя,**
b. Выбрать **Протокол аутентификации** (**MD5** или **SHA),**
c. Ввести **Пароль аутентификации**,
d. Выбрать **Протокол шифрования** (**AES** или **DES**),
e. Ввести **Пароль шифрования**.

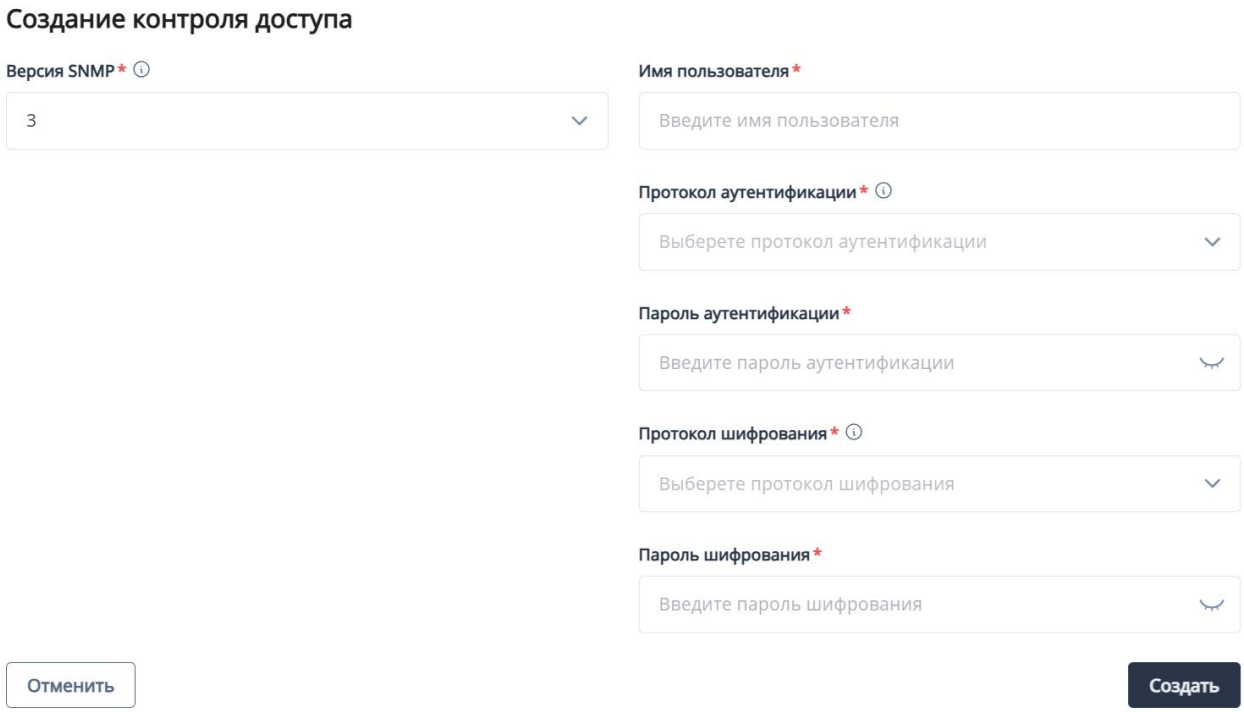


Рисунок 9.15 – параметры SNMP-агента с использованием SNMPv3

4. После ввода всех параметров нажать кнопку «Создать»  . (рисунок 9.16)

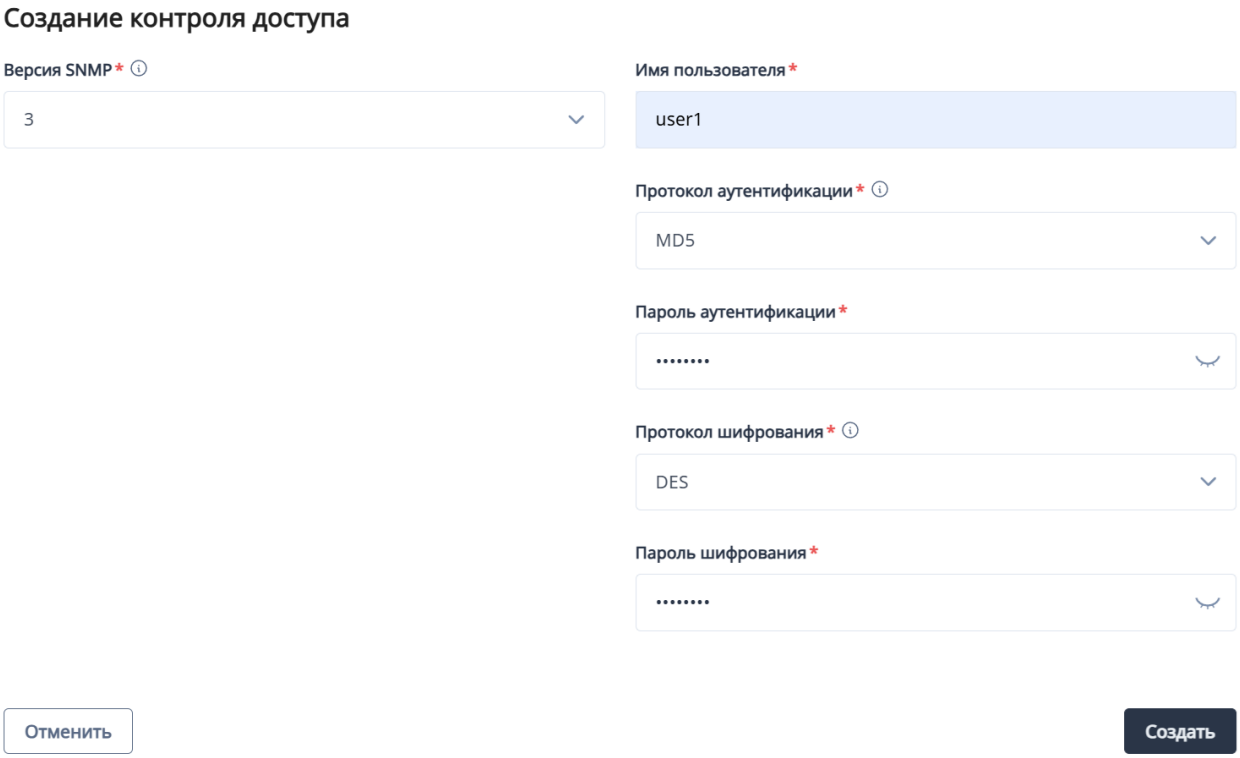


Рисунок 9.16 – Заполненное окно создания SNMP-агента с использованием SNMPv3

В случае успешного выполнения команды созданный контроль доступа отобразится в итоговой таблице (рисунок 9.17)

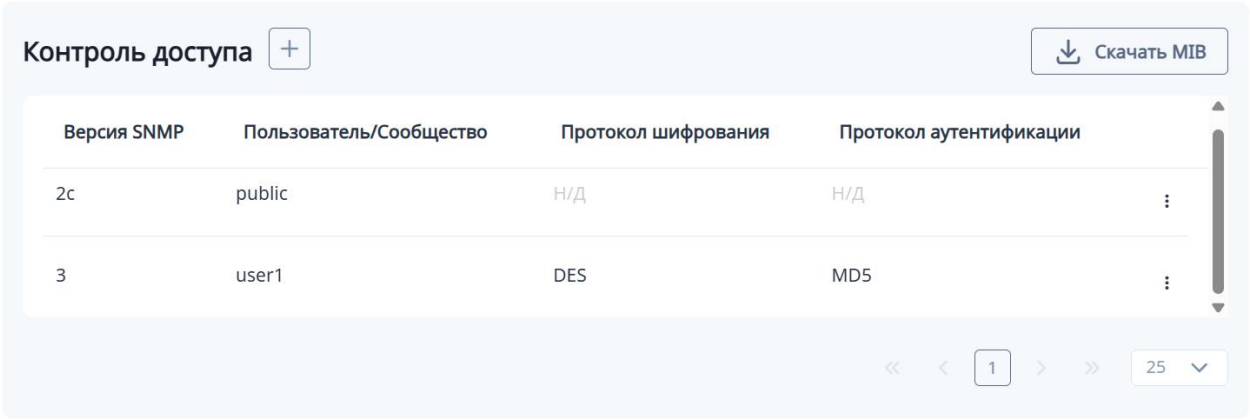
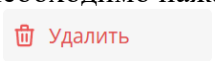


Рисунок 9.17 – Подраздел «Контроль доступа»

9.2.2 УДАЛЕНИЕ SNMP АГЕНТА

Для удаления SNMP агента (контроля доступа) необходимо нажать на кнопку «параметры» и выбрать действие «Удалить»  (рисунок 9.18).

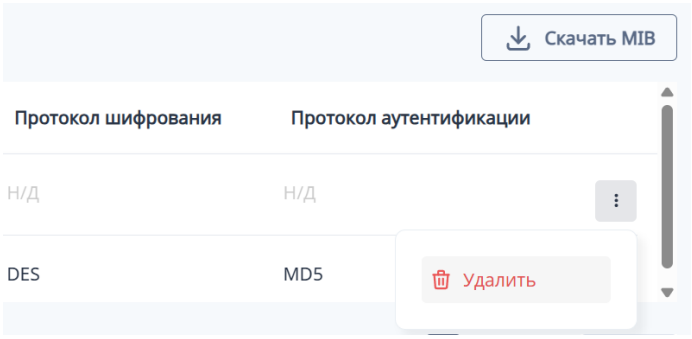


Рисунок 9.18 – Удаление SNMP агента

9.2.3 СКАЧИВАНИЕ MIB-ФАЙЛА

После завершения настройки можно загрузить MIB-файл – структурированный текстовый файл, содержащий информацию обо всех объектах устройства. Для загрузки кликните «Скачать MIB» 

в заголовке раздела контроль доступа (рисунок 9.17).

9.2.4 НАСТРОЙКА ПОЛУЧАТЕЛЕЙ УВЕДОМЛЕНИЙ SNMP

Для настройки необходимо:

1. Нажать на плюс 
в заголовке подраздела «Получатели уведомлений» (рисунок 9.11).
2. В открывшемся окне «Создание получателей уведомлений» необходимо:
    a. Ввести **Имя получателя,**
    b. Выбрать **IP-адрес получателя,**
    c. Ввести **Порт получателя**,
    d. Выбрать **Версию SNMP** (**2c** или **3**),
    e. В дропдауне выбрать созданный ранее агент контроля доступа (рисунок 9.19)

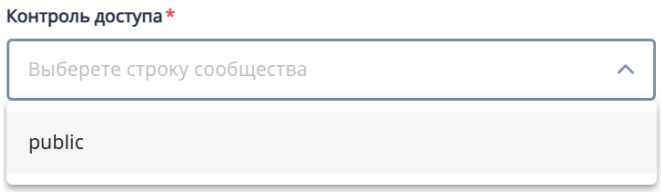


Рисунок 9.19 – Созданные ранее агенты SNMP

После ввода параметров для версии SNMP 2c заполненное окно выглядит следующим образом (рисунок 9.20)

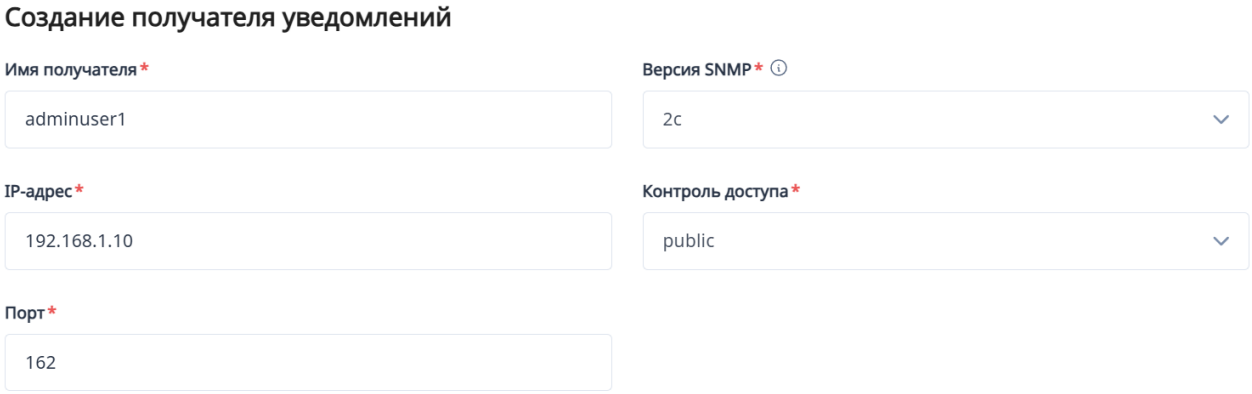


Рисунок 9.20 – Заполненное окно создания получателя уведомлений SMTP

В случае успешного выполнения команды созданный получатель уведомлений отобразится в итоговой таблице (рисунок 9.21)

Рисунок 9.21 – Подраздел «Получатели уведомлений»

9.2.5 УДАЛЕНИЕ ПОЛУЧАТЕЛЯ УВЕДОМЛЕНИЙ

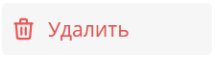
Для удаления Получателя уведомлений необходимо нажать на кнопку «параметры» и выбрать действие «Удалить»  (рисунок 9.22).

Рисунок 9.22 – Удаление SNMP агента

9.2.6 ТЕСТИРОВАНИЕ ПОЛУЧАТЕЛЯ УВЕДОМЛЕНИЙ

Для тестирования Получателя уведомлений необходимо нажать на кнопку «параметры» и выбрать действие «Тест» Тест (рисунок 9.23).
После нажатия кнопки «Тест» на SNMP сервер (например, Zabbix) отправляется SNMP-trap.

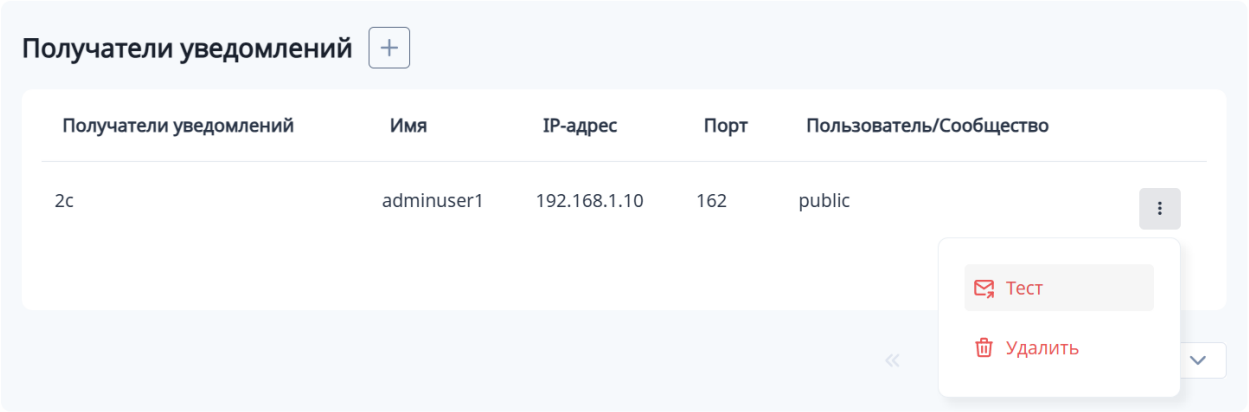


Рисунок 9.23 – Тестирование Получателя уведомлений

9.3 ПОДКЛЮЧЕНИЕ BLAZEX SNMP TRAPS К ZABBIX (SNMPTRAPD)

Zabbix использует стандартный демон snmptrapd для получения SNMP-trap. Данные передаются в скрипт Zabbix, который форматирует их для внутренней обработки в системе.

9.3.1 КОНФИГУРИРОВАНИЕ SNMPTRAPD НА ПРИЁМ TRAP ПО ВЕРСИИ SNMPV2C

Для того чтобы сконфигурировать snmptrapd на приём trap по версии SNMPv2c необходимо:

Добавить в файл /etc/snmp/snmptrapd.conf:

```
authCommunity log,execute,net <community-string>
```

Создать на вкладке Мониторинг - SNMP - Контроль доступа:

Версия SNMP - 2c

Строка сообщества - <community-string>

Создать на вкладке Мониторинг - SNMP - Получатели уведомлений, нового получателя:

Имя получателя - произвольное имя

IP-адрес - указать IP-адрес snmptrapd сервиса (Zabbix-сервера)

Версия SNMP - 2c

Контроль доступа - выбрать созданный в предыдущем пункте <community-string>

Порт - по умолчанию 162 (Заменить на свой, если в snmptrapd используется нестандартный)Версия SNMP - 2c

ПРИМЕЧАНИЕ.

Строки сообщества в файле snmptrapd.conf и контроле доступа должны совпадать

ПРИМЕЧАНИЕ.

Для применения изменений в конфигурации snmptrapd на сервере Zabbix необходимо выполнить перезагрузку сервиса snmptrapd: systemctl restart snmptrapd.service

9.3.2 КОНФИГУРИРОВАНИЕ SNMPTRAPD НА ПРИЁМ TRAP ПО ВЕРСИИ SNMPV3

Для конфигурации snmptrapd и SNMPv3 необходимо:

Добавить в файл /etc/snmp/snmptrapd.conf:

```
createUser -e <engine-id> '<snmp-v3-user>' <auth-method> <auth-passphrase> <priv-method> <priv-passphrase>
authuser log,execute <snmp-v3-user>
```

Создать на вкладке Мониторинг - SNMP - Контроль доступа:

Версия SNMP - 3

Имя пользователя - Имя пользователя которое будет использоваться для авторизации СХД при отправке trap в snmptrapd, должно соответствовать <snmp-v3-user> в snmptrapd.conf

Протокол аутентификации - SHA или MD5, должно соответствовать <auth-method> в snmptrapd.conf

ПРИМЕЧАНИЕ.

Пароль аутентификации - должен соответствовать <auth-passphrase> в snmptrapd.conf

Протокол шифрования - AES или DES, должен соответствовать <priv-method> в snmptrapd.conf

ПРИМЕЧАНИЕ.

Пароль шифрования - должен соответствовать <priv-passphrase> в snmptrapd.conf

После заполнения окно должно выглядеть следующим образом (рисунок 9.24)

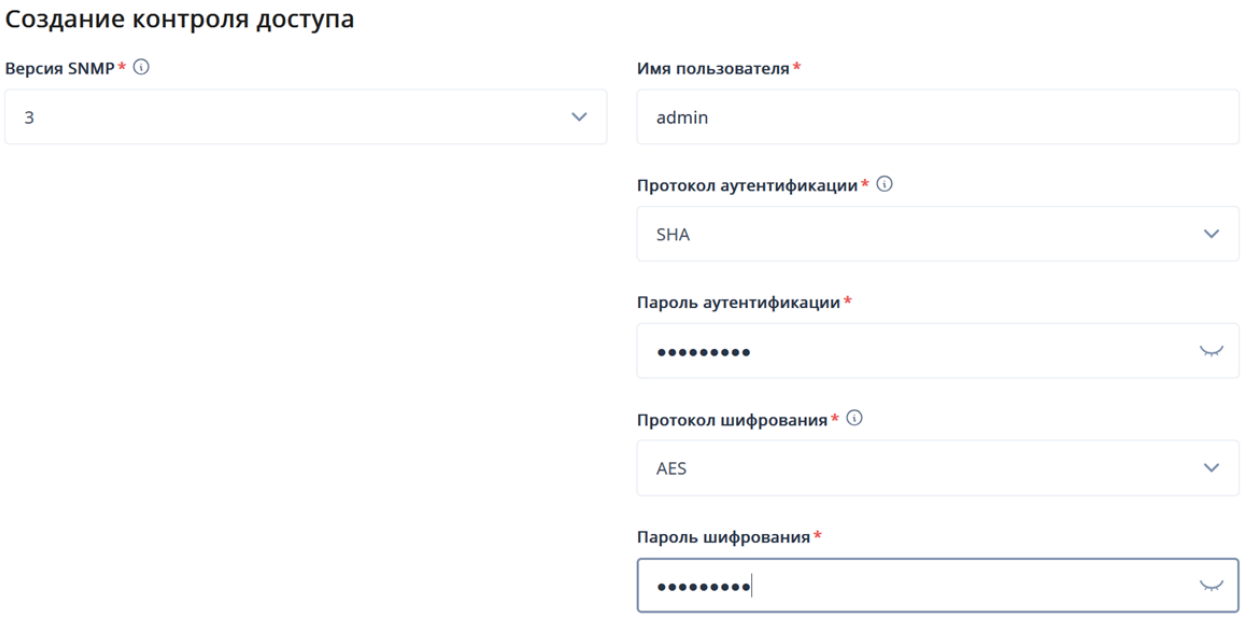


Рисунок 9.24 – Заполненное окно создания контроля доступа для конфигурации snmptrapd и SNMPv3

Создать на вкладке Мониторинг - SNMP - Получатели уведомлений:

Имя получателя - произвольное имя

Версия SNMP - 3

IP-адрес - указать IP-адрес snmptrapd сервиса (Zabbix-сервера)

Контроль доступа - выбрать созданного в предыдущем пункте пользователя <snmp-v3-user>

Порт - по умолчанию 162 (Заменить на свой, если в snmptrapd используется нестандартный)

После заполнения окно должно выглядеть следующим образом (рисунок 9.25)

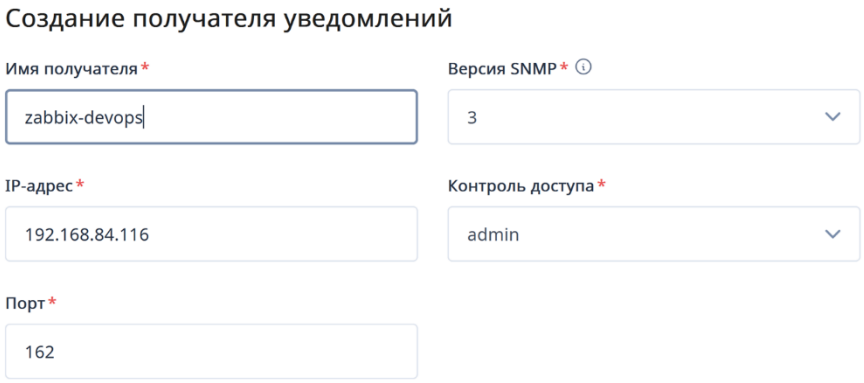


Рисунок 9.25 – Заполненное окно создания получателя уведомлений для конфигурации snmptrapd и SNMPv3

EngineID в snmptrapd.conf должен совпадать с EngineID указанным на вкладке Мониторинг - SNMP:

method> в snmptrapd.conf

ПРИМЕЧАНИЕ.

EngineID в snmptrapd.conf должен совпадать с EngineID указанным на вкладке Мониторинг – SNMP (рисунок 9.26)

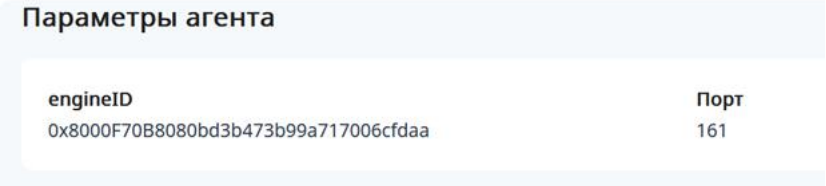


Рисунок 9.26 – EngineID в параметрах агента

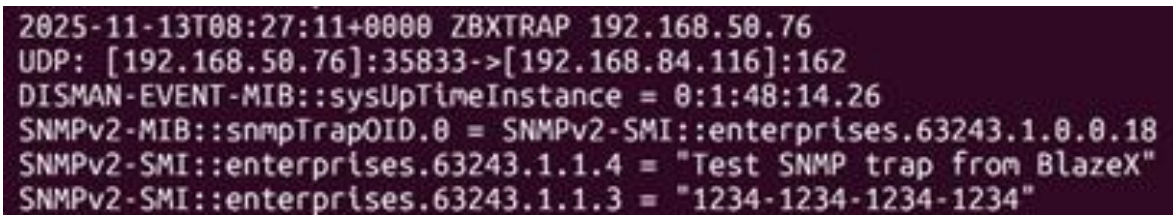
9.3.3 ПРОВЕРКА ПОДКЛЮЧЕНИЯ

Чтобы проверить подключение BlazeX к snmptrapd на сервере Zabbix есть возможность отправить тестовое уведомление, для этого:

1. Перейдите на вкладку Мониторинг - SNMP
2. В списке Получатели уведомлений найдите необходимого получателя
3. Нажатием на иконку слева, вызовите контекстное меню
4. Выберите пункт «Тест»
5. На сервере Zabbix, для просмотра лога уведомлений используйте команду:

```
cat /var/log/snmptrap/snmptrap.log | tail
```

6. Должен отобразиться лог со следующими строками:



В логе присутствует информация:
после ZBXTRAP - адрес узла СХД отправившего уведомление
в строке sysUpTimeInstance - время работы SNMP-агента на узле СХД
snmpTrapOID.0 - OID тестового (Debug) уведомления из MIB спецификации BLAZEX
63243.1.1.4 - Сообщение уведомления
63243.1.1.3 - Серийный номер СХД

9.4 ЖУРНАЛ КОМАНД

Раздел «Журнал команд» позволяет отслеживать процесс записи информации о пользовательских действиях, происходящих в системе (рисунок. 9.27).

В таблице «Журнал команд» отображаются ключевые параметры каждой команды, в соответствующих столбцах:

- Запуск и исполнение команды - дата и время запуска и исполнения команды;

- Команда - наименование команды;
- Статус исполнения команды - состояние исполнения команды:
- ID ресурса - ID ресурсов, задействованных в исполнении команды;
- Пользователь - пользователь, запустивший команду, в формате имя/ip.

NEW — Новая команда - статус соответствует событию "команда пришла на ресурс в результате действий пользователя в интерфейсе, например, нажата кнопка "Создать".

PROCESSING — В процессе - присваивается после того, как очередь введенных до этого команд выполнится и до получения результата исполнения

OK — Исполненная - команда успешно исполнения, результат исполнения получен

FAILED — Неудавшаяся - отрицательный результат исполнения команды, либо этот статус был присвоен по тайм–ауту (команда "ушла" на исполнение и завершилась без результата по истечении ожидаемого времени, чтобы перейти к исполнению следующей команды)

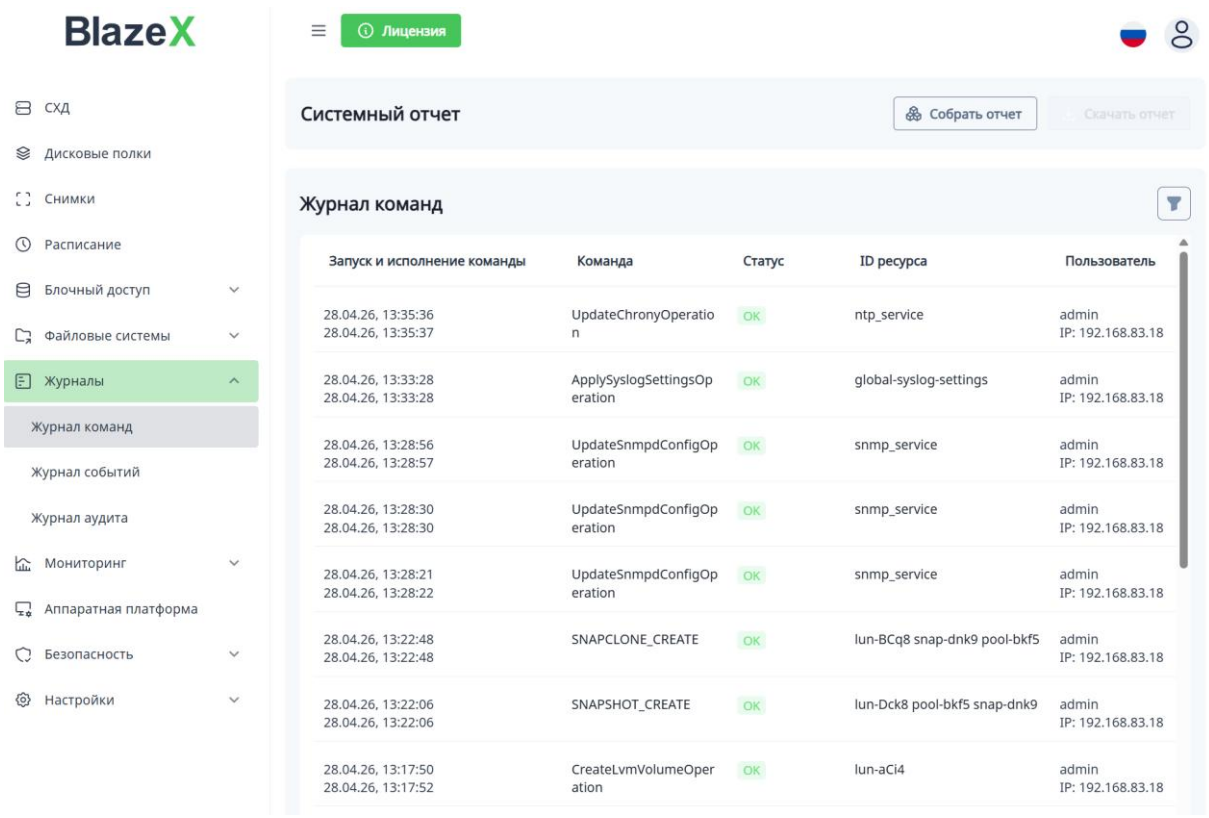


Рисунок 9.27 – Журнал команд

Для технического анализа, аудита безопасности и выявления причин сбоев, в Журнале команд реализован поиск по каждому из столбцов таблицы (открывается по нажатию на кнопку фильтрации). Изображено на рисунке 9.28

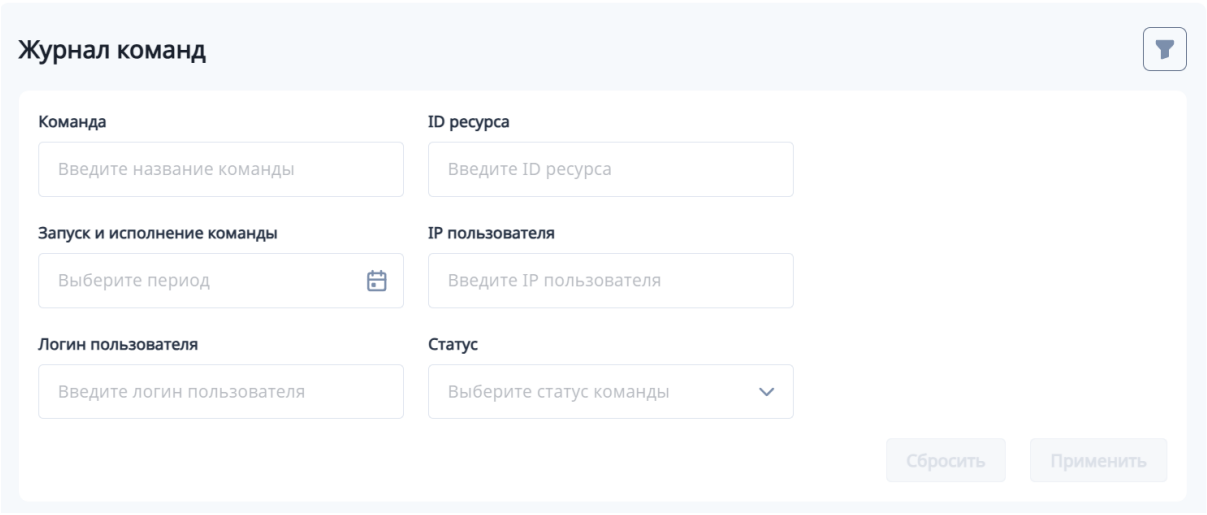


Рисунок 9.28 – Поиск и фильтры в Журнале команд

Для отображения детальной информации о команде необходимо нажать на соответствующую строку команды, чтобы открыть дополнительное окно и просмотреть все детали (рисунок 9.29)

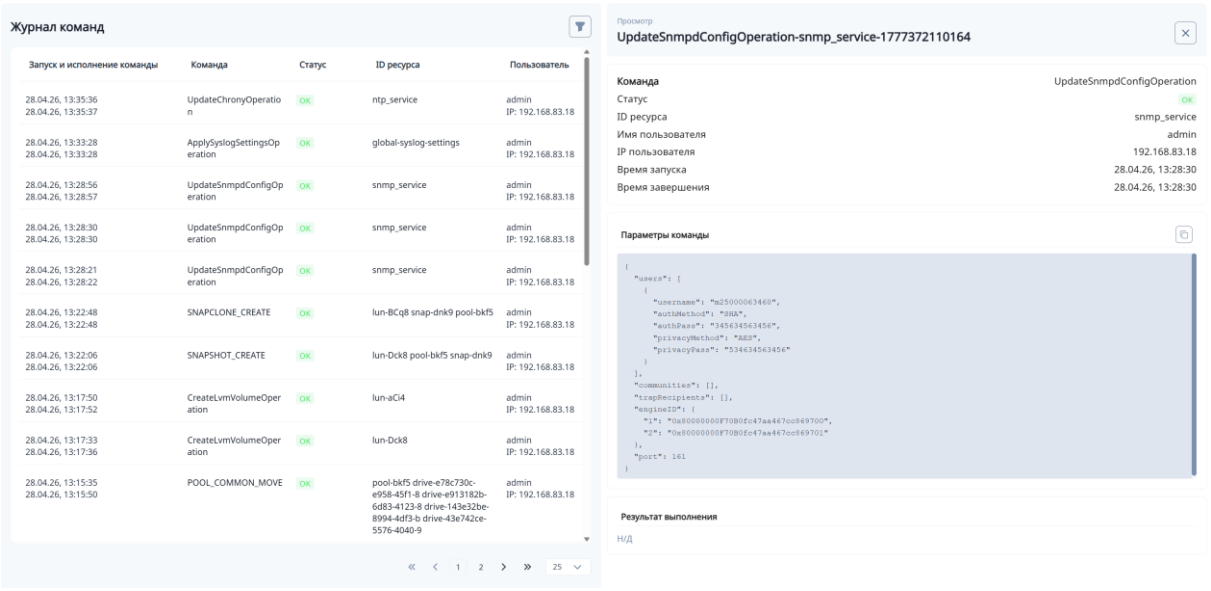
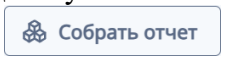


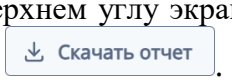
Рисунок 9.29 – Окно деталей в Журнале команд

Детали команды содержат информацию:

- Имя команды
- Статус
- ID ресурса
- Имя пользователя
- IP пользователя
- Время запуска
- Время завершения
- Параметры команды в формате json
- Результат выполнения

Сбор и сохранение отчета

Для просмотра полной информации о командах в системе можно собрать и скачать отчет. Он представляет собой архив с двумя json файлами, содержащими полный перечень команд для каждого узла. Чтобы сформировать отчет необходимо нажать на кнопку «Собрать отчет» 

в право верхнем углу экрана. Для сохранения отчета необходимо нажать кнопку «Скачать отчет» 

.

9.5 ЖУРНАЛ СОБЫТИЙ

Раздел «Журнал событий» позволяет отслеживать процесс записи информации о системных событиях, таких как сбои дисков, ошибки подключения, предупреждения, смену статуса компонентов и т.д. (рисунок 9.30).

В таблице «Журнал событий» отображаются ключевые параметры каждого события, в соответствующих столбцах:

- ID ресурса - уникальный идентификатор того компонента СХД, который сгенерировал событие или к которому оно относится;
- Узел - доказывает, какой физический или логический контроллер СХД зафиксировал событие
- Время события - момент наступления события, зафиксированный внутренними часами СХД
- Важность - Степень критичности события для работы СХД
    - **Emergency** (Emergency) - авария, система не работает.
    - **Critical** (Критическая) - серьезный сбой (например, потеря массива, смерть контроллера). Требует немедленного вмешательства.
    - **Error** (Ошибка) - неисправность, но система функционирует (сбой диска, сбой вентилятора). Требует планового ремонта.
    - **Warning** (Предупреждение) - есть риск проблемы (истечение ресурса, превышение порога температуры). Требует внимания.
    - **Info** (Информационная) - нормальное системное событие (создание группы, включение порта). Для сведения.
    - **Debug** (Отладочная) - для разработчиков/поддержки.
- Сообщение - Краткое описание проблемы
- Источник - Указывает на подсистему или модуль ПО, который сгенерировал событие

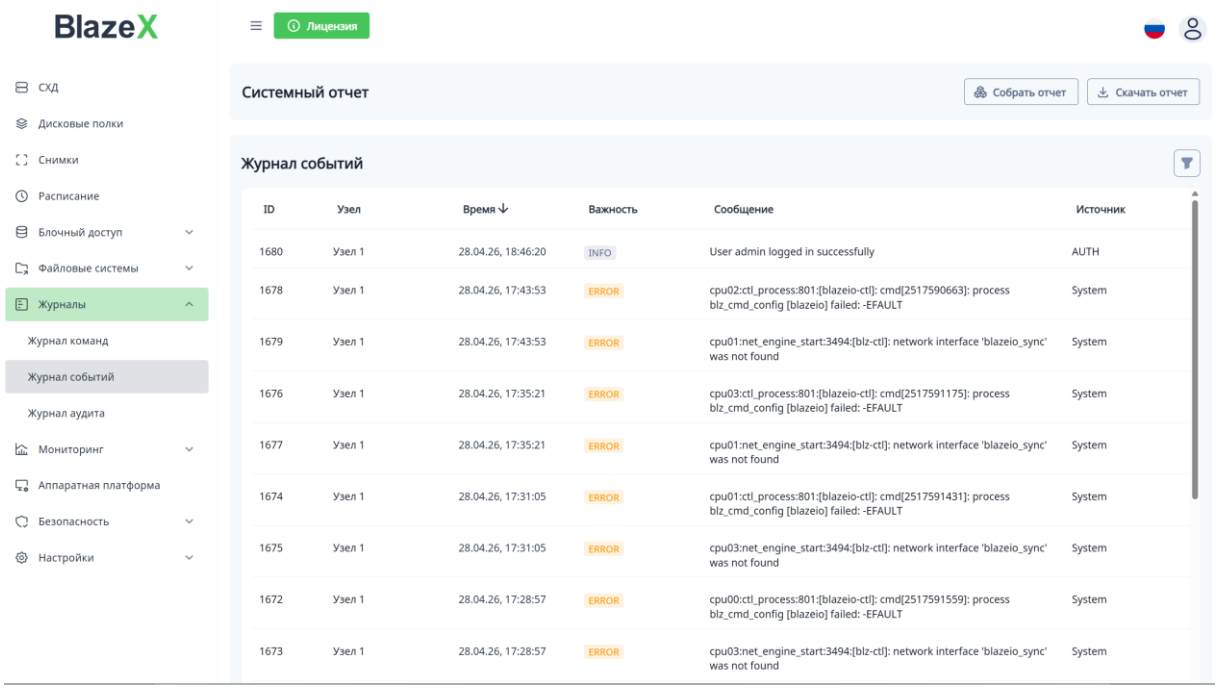


Рисунок 9.30 – Журнал событий

Для технического анализа и выявления причин сбоев, в журнале событий реализован поиск по каждому из столбцов таблицы (открывается по нажатию на кнопку фильтрации). Изображено на рисунке 9.31

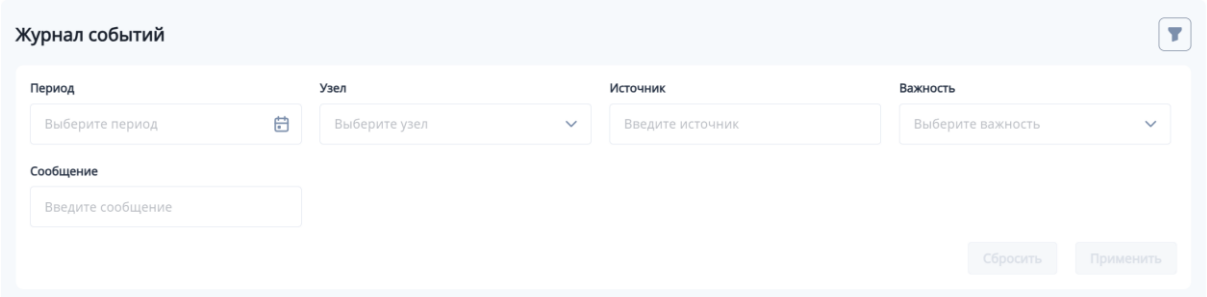


Рисунок 9.31 – Поиск и фильтры в Журнале команд

Для отображения детальной информации о событии необходимо нажать на соответствующую строку события, чтобы открыть дополнительное окно и просмотреть все детали (рисунок 9.32)

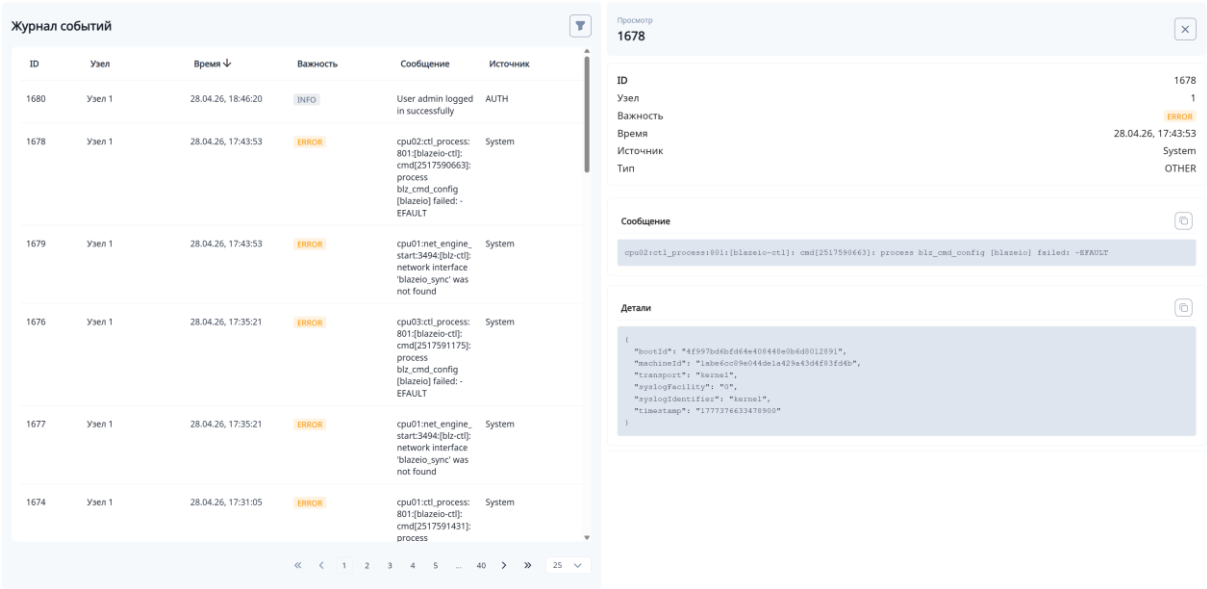


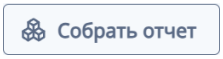
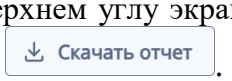
Рисунок 9.32 – Окно деталей в Журнале команд

Детали события содержат информацию:

- ID ресурса;
- Узел
- Важность
- Время
- Источник
- Тип
- Сообщение
- Детали в формате json

Сбор и сохранение отчета

Для просмотра полной информации о событиях в системе можно собрать и скачать отчет. Он представляет собой архив с двумя json файлами, содержащими полный перечень событий для каждого узла. Чтобы сформировать отчет необходимо нажать на кнопку

«Собрать отчет»  в право верхнем углу экрана. Для сохранения отчета необходимо нажать кнопку «Скачать отчет»  .

9.6 ЖУРНАЛ АУДИТА

Раздел «Журнал аудита» позволяет отслеживать процесс записи информации о действиях пользователя. (рисунок 9.33).

В таблице «Журнал аудита» отображаются ключевые параметры каждого события, в соответствующих столбцах:

- ID ресурса - уникальный идентификатор компонента СХД, к которому относится событие;
- Время события - момент наступления события
- Важность - Степень критичности события для работы СХД (аналогичная журналу событий)
- Сообщение - Краткое описание проблемы
- Источник - Указывает на подсистему или модуль ПО, который сгенерировал событие

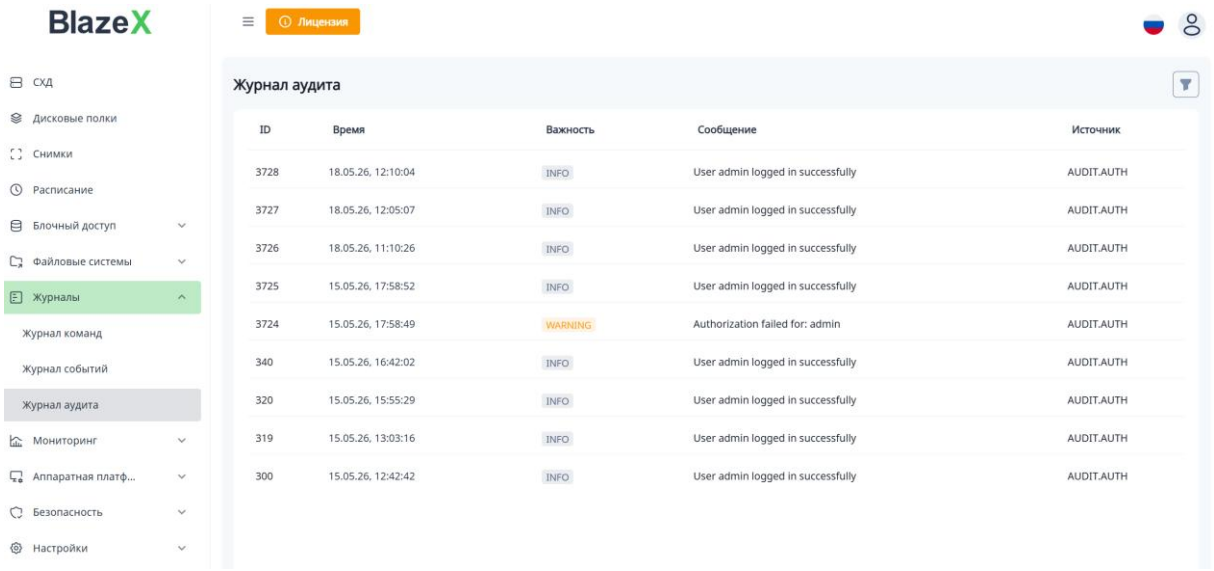


Рисунок 9.33 – Журнал аудита

Для технического анализа и выявления причин сбоев, в журнале событий реализован поиск по каждому из столбцов таблицы (открывается по нажатию на кнопку фильтрации ). Изображено на рисунке 9.34

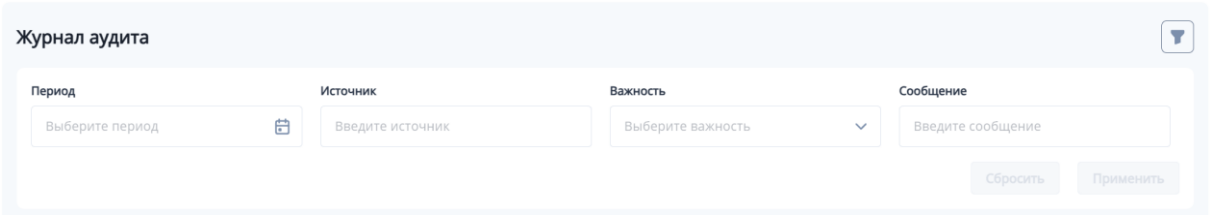


Рисунок 9.34 – Поиск и фильтры в Журнале аудита

Для отображения детальной информации о событии необходимо нажать на соответствующую строку события, чтобы открыть дополнительное окно и просмотреть все детали (рисунок 9.36)

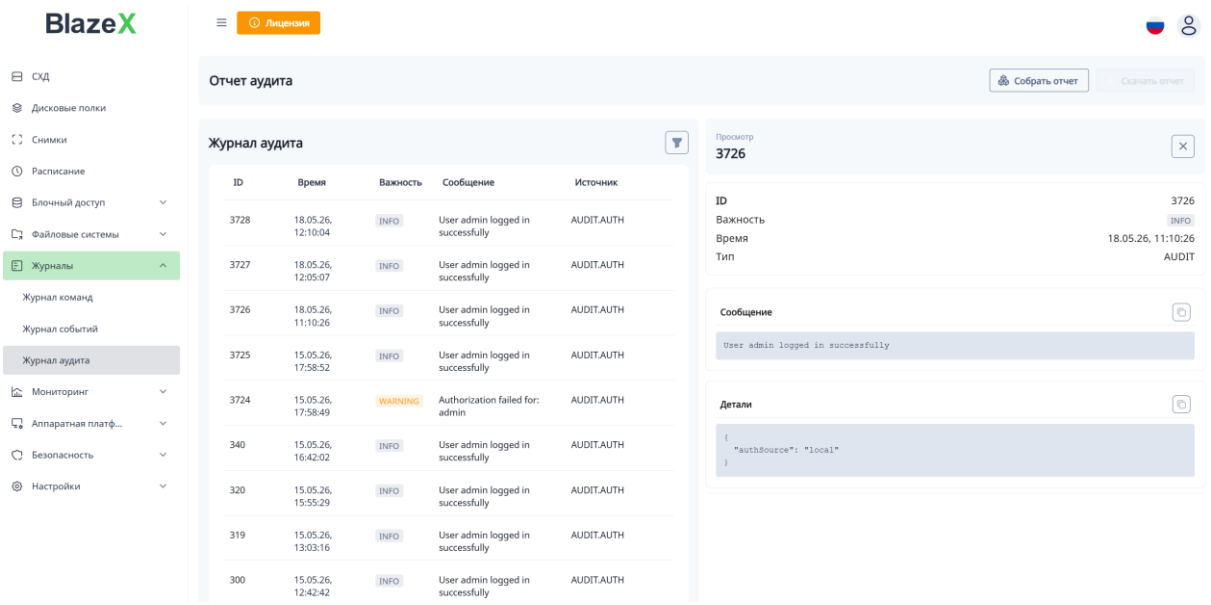
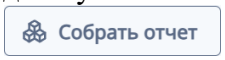


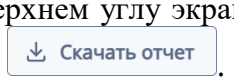
Рисунок 9.36 – Окно деталей в Журнале аудита

Детали события содержат информацию:

- ID ресурса;
- Узел
- Важность
- Время
- Источник
- Тип
- Сообщение
- Детали в формате json

Сбор и сохранение отчета

Для просмотра полной информации о событиях в системе можно собрать и скачать отчет. Он представляет собой архив с двумя json файлами, содержащими полный перечень событий для каждого узла. Чтобы сформировать отчет необходимо нажать на кнопку «Собрать отчет» 

в право верхнем углу экрана. Для сохранения отчета необходимо нажать кнопку «Скачать отчет» 

.

9.7 ВНЕШНИЙ МОНИТОРИНГ

9.7.1 НАСТРОЙКА PROMETHEUS И GRAFANA

Система мониторинга предназначена для вывода информации о состоянии системы в реальном времени и выявления отклонений с последующей локализацией сбоев в работе СХД. Настройка источников данных Prometheus:

https://prometheus.io/docs/prometheus/latest/configuration/configuration/

Настройка Prometheus для работы с Grafana:

https://prometheus.io/docs/visualization/grafana/

Настройка Grafana для работы с Prometheus:

https://grafana.com/grafana/plugins/prometheus/

Метрики СХД доступны по следующему URL (его нужно использовать при настройке Prometheus):

```
https://<IP–адрес_узла>/api/metrics
```

Пример ответа на запрос по указанному URL (выдержка):

```
# HELP blz_disks count of disks
# TYPE blz_disks gauge
blz_disks 6              # Количество накопителей

# HELP blz_pools count of pools
# TYPE blz_pools gauge
blz_pools 2              # Количество групп накопителей (RAID–массивов)

# HELP blz_volumes count of volumes
# TYPE blz_volumes gauge
blz_volumes 2            # Количество логических томов

# HELP blz_fileExports count of file exports
# TYPE blz_fileExports gauge
```

```
blz_fileExports 2 # Количество экспортируемых томов с файловым типом доступа


# HELP blz_blockExports count of block exports
# TYPE blz_blockExports gauge
blz_blockExports 1  # Количество экспортируемых томов с блочным типом доступа


# HELP blz_errors count of errors
# TYPE blz_errors gauge
blz_errors 0          # Количество ошибок
```

Краткое описание предоставляемых метрик:

Метрика	Описание
blz_disks	Количество накопителей
blz_pools	Количество групп накопителей (RAID–массивов)
blz_volumes	Количество логических томов
blz_fileExports	Количество экспортируемых томов с файловым типом доступа
blz_blockExports	Количество экспортируемых томов с блоковым типом доступа
blz_errors	Количество ошибок

9.7.2 НАСТРОЙКА ZABBIX

Для интеграции Zabbix с BlazeX, необходимо выполнить следующие шаги:

1. В inventory.ini требуется указать:

```
enable_zabbix_monitoring=True
zabbix_server_ip=(введите свой IP-адрес)
```

2. После чего необходимо запустить команду:

```
blazex–install
```

3. Для добавления шаблона, перейти в меню «Сбор данных», далее «Шаблоны», нажать кнопку "Импорт", добавить файл с шаблоном и нажать "Импорт", как показано на рисунке 9.37.

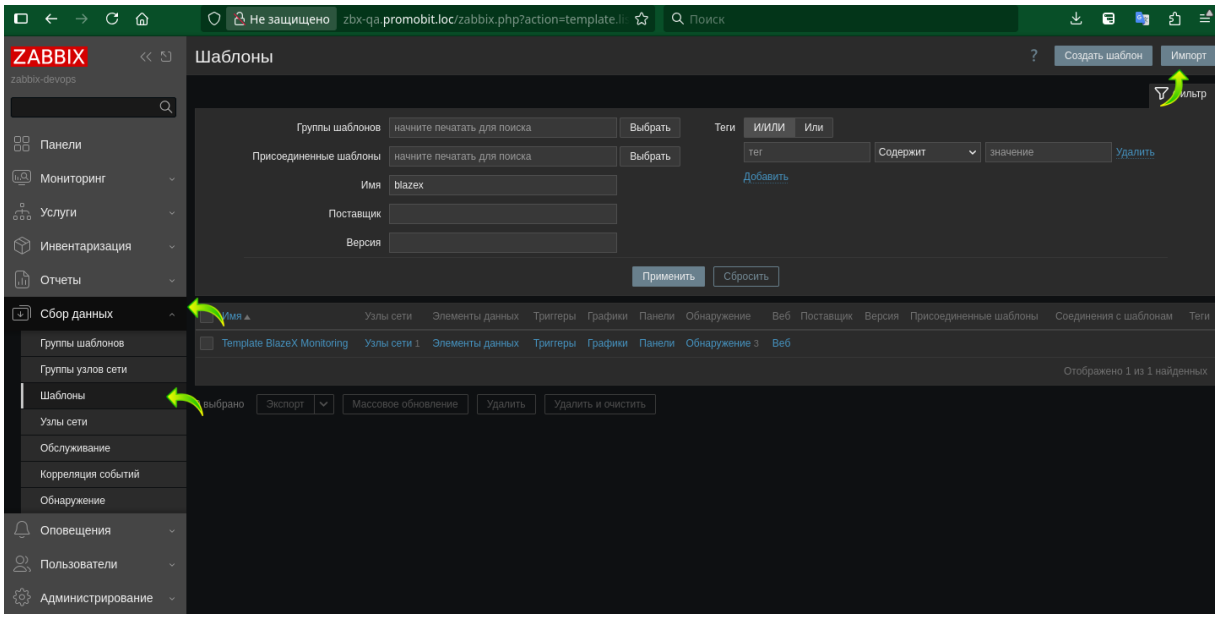


Рисунок 9.37 – Добавление шаблона

4. После добавления узла сети в Zabbix, необходимо авторизоваться в Zabbix, перейти в меню «Сбор данных», далее «Узлы сети» и нажать «Создать узел сети» как показано на рисунке 9.38.

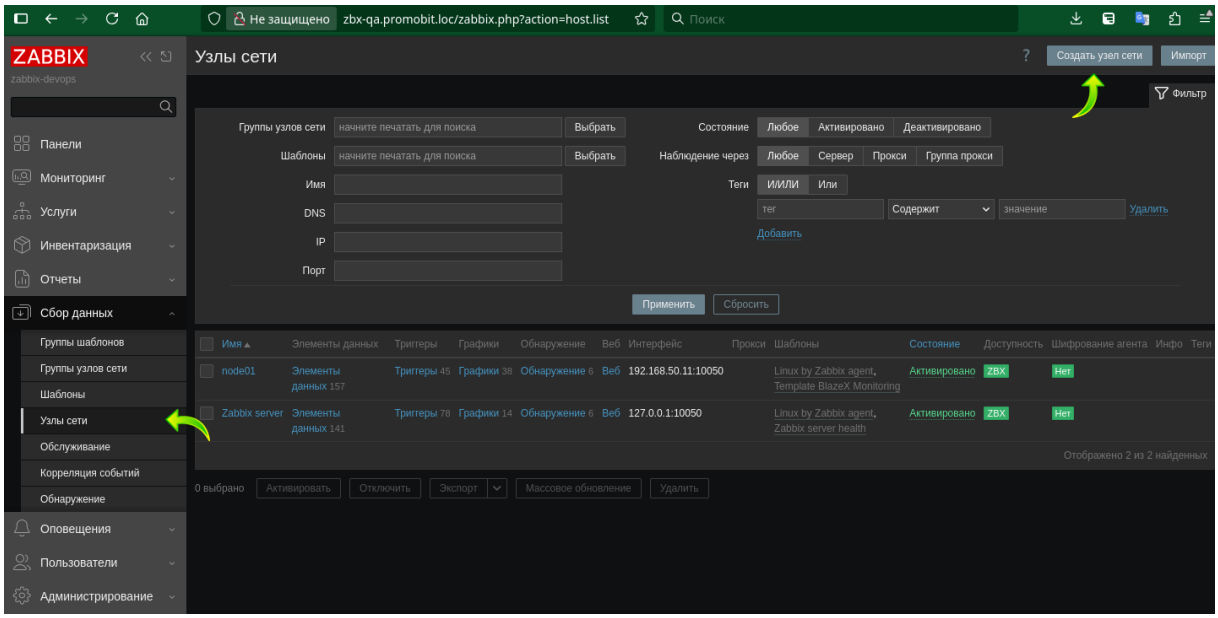


Рисунок 9.38 – Создание узлов сети

3. В появившемся окне заполнить обязательные поля, как показано на рисунке 9.39:

- Имя узла сети: задать произвольное имя
- Шаблоны: начать вводить "BlazeX" – во всплывающей подсказке можно выбрать шаблон "Template BlazeX Monitoring". При необходимости, для мониторинга остальных ресурсов системы, рекомендуется также добавить шаблон "Linux by Zabbix agent".
- Группы узлов сети: "Openstack_VM" – для виртуальных стендов, "HW_stand" – для железных
- Интерфейсы для мониторинга: выбираем "Агент" и вводим адрес сервера для мониторинга

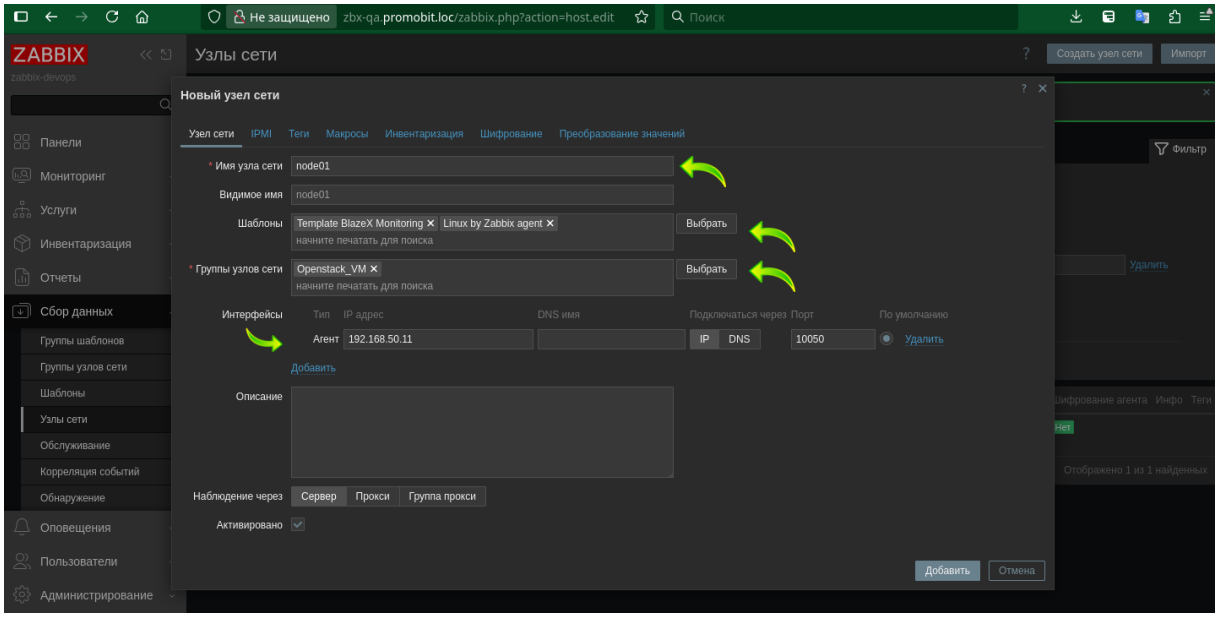


Рисунок 9.39– Заполнение обязательных полей

4. После добавления, если blazex–install прошел без ошибок и верно настроен узел сети, то спустя 1–3 минуты должен появиться зеленый значок "ZBX", как изображено на рисунке 9.40.

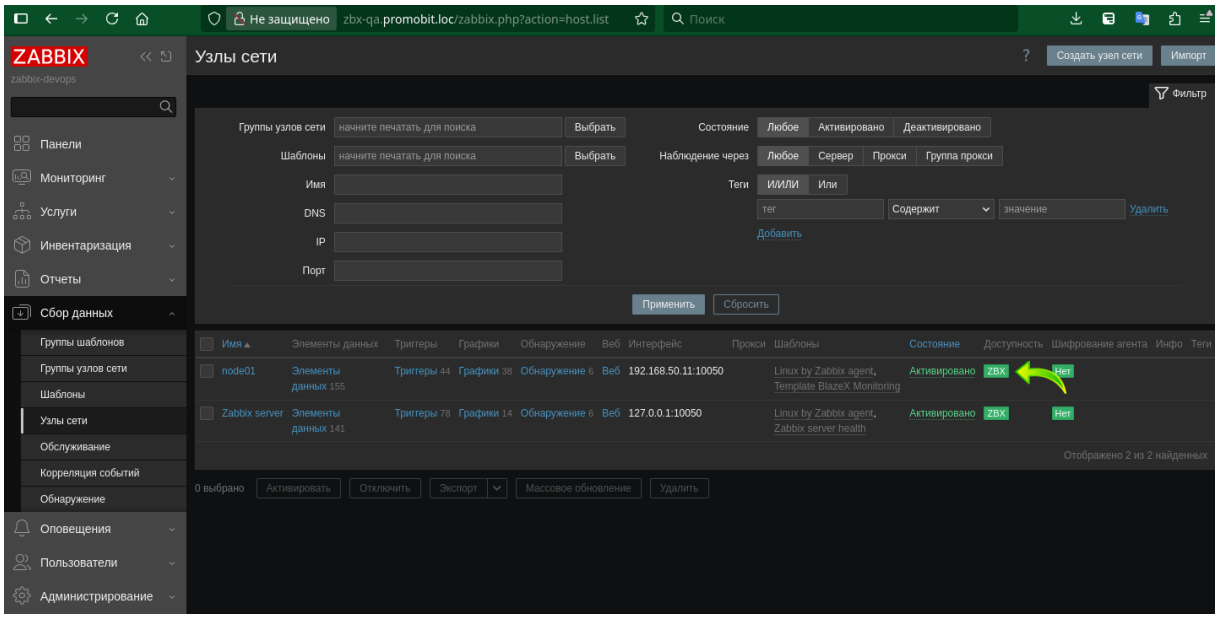


Рисунок 9.40 – blazex–install прошел без ошибок, узел сети настроен корректно

9. Если все предыдущие шаги прошли без ошибок, то можно переходить в «Мониторинг» «Последние данные». В фильтрах доступен выбор необходимых узлов и метрик. На рисунке 9.41 пример использования фильтра «Имя»

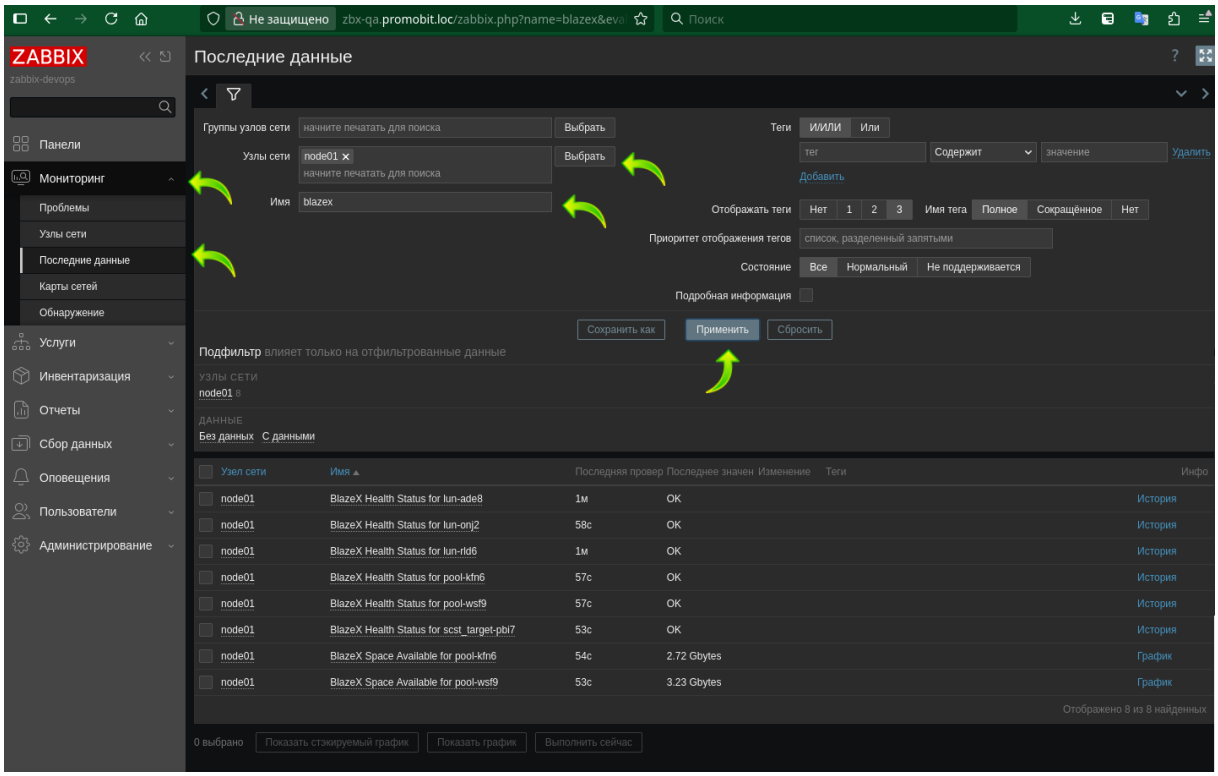


Рисунок 9.41 – Пример использования фильтра «Имя»

10 АППАРАТНАЯ ПЛАТФОРМА

Раздел «Аппаратная платформа» состоит из подразделов:

- Компоненты
- Сенсоры

10.1 КОМПОНЕНТЫ

Страница «Компоненты» предназначена для просмотра технического состояния и состава физического оборудования, установленного в системе хранения данных. Здесь можно получить информацию о дисках, контроллерах, дисковых полках, Fibre Channel и сетевых интерфейсах (рисунок 10.1).

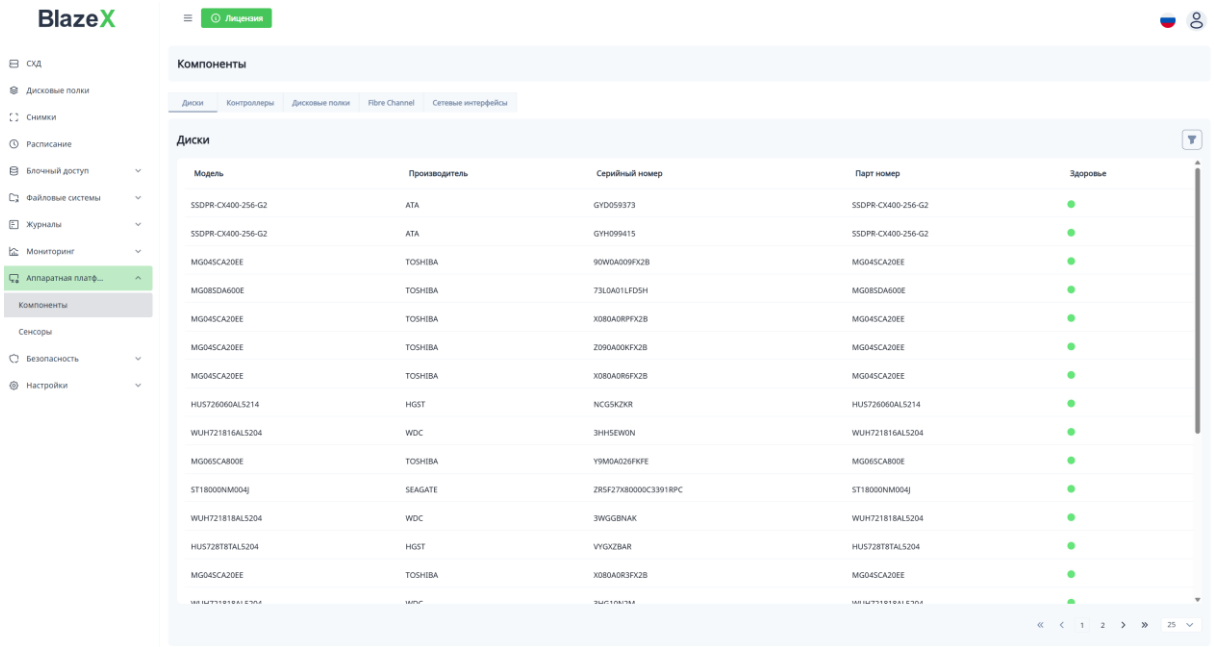


Рисунок 10.1 – Страница «Компоненты»

В верхней части страницы расположены переключатели (вкладки):

- Диски - отображает все установленные накопители (HDD, SSD).
- Контроллеры - информация о контроллерах СХД.
- Дисковые полки - сведения о подключённых внешних корзинах с дисками.
- Fibre Channel - параметры портов и адаптеров Fibre Channel.
- Сетевые интерфейсы - состояние сетевых адаптеров и их настройки

Во всех вкладах отображена следующая информация:

- Модель - Модель диска
- Производитель - Наименование производителя
- Серийный номер - Уникальный заводской номер
- Парт номер - Заводской артикул / Part Number
- Здоровье - Индикатор состояния

Вкладка «Диски» выглядит следующим образом (рисунок 10.2):

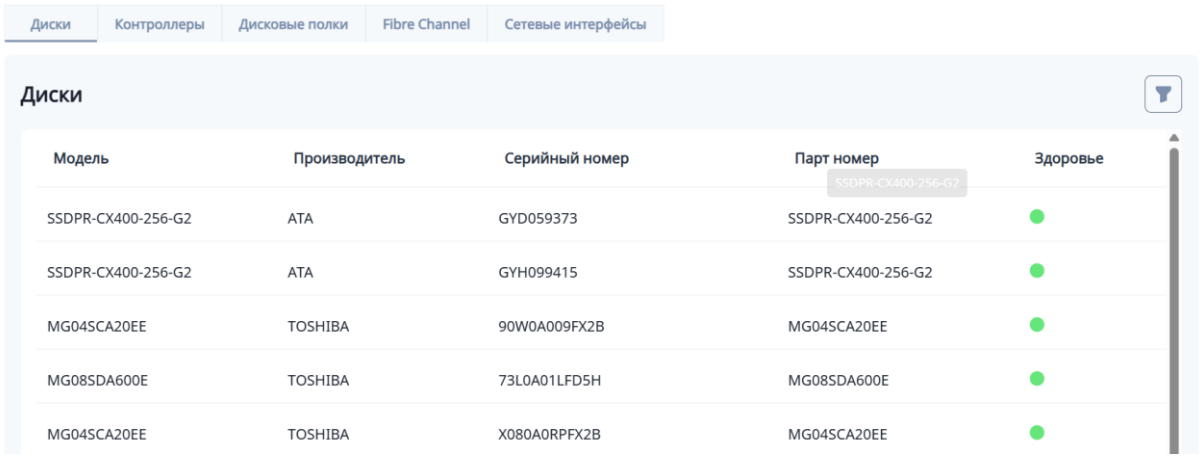


Рисунок 10.2 – Вкладка «Диски» страницы «Компоненты»

Вкладка «Контроллеры» выглядит следующим образом (рисунок 10.3):

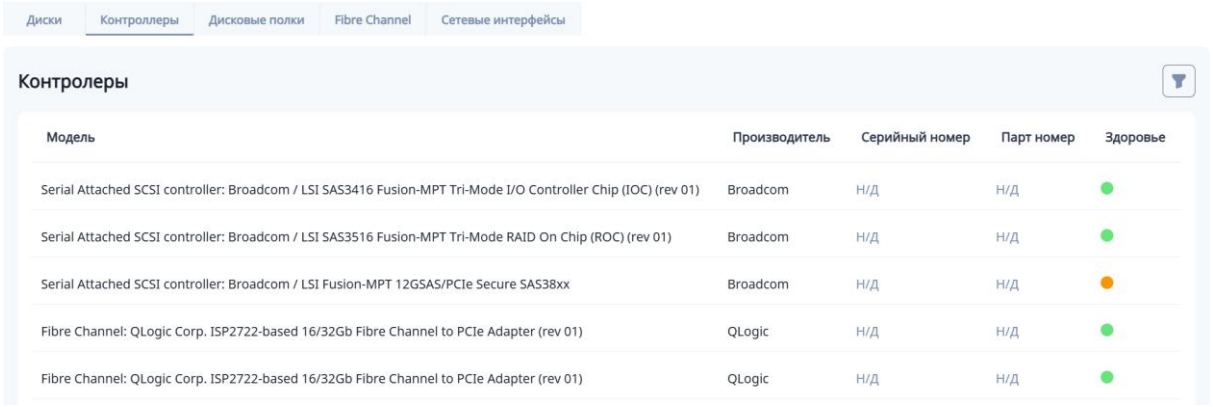


Рисунок 10.3 – Вкладка «Контроллеры» страницы «Компоненты»

Вкладка «Дисковые полки» выглядит следующим образом (рисунок 10.4):

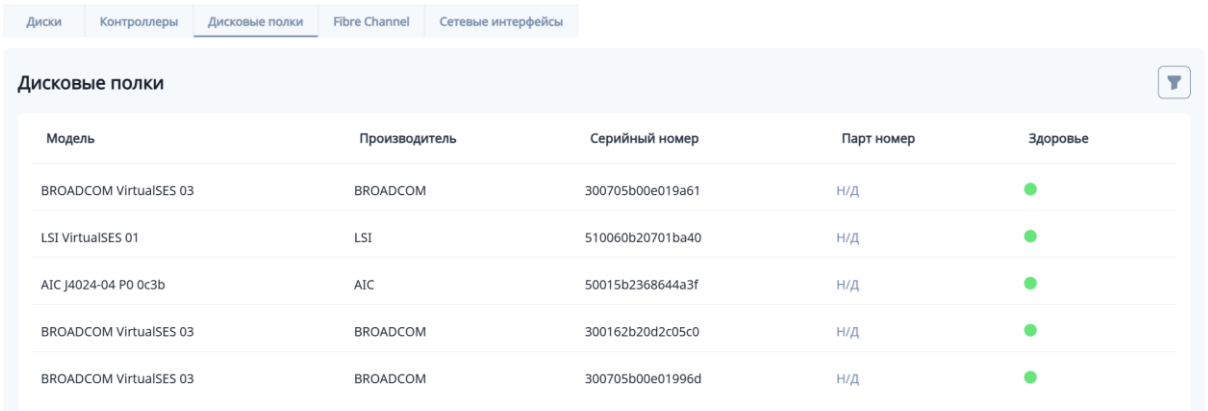


Рисунок 10.4 – Вкладка «Дисковые полки» страницы «Компоненты»

Вкладка «Fibre Channel» выглядит следующим образом (рисунок 10.5):

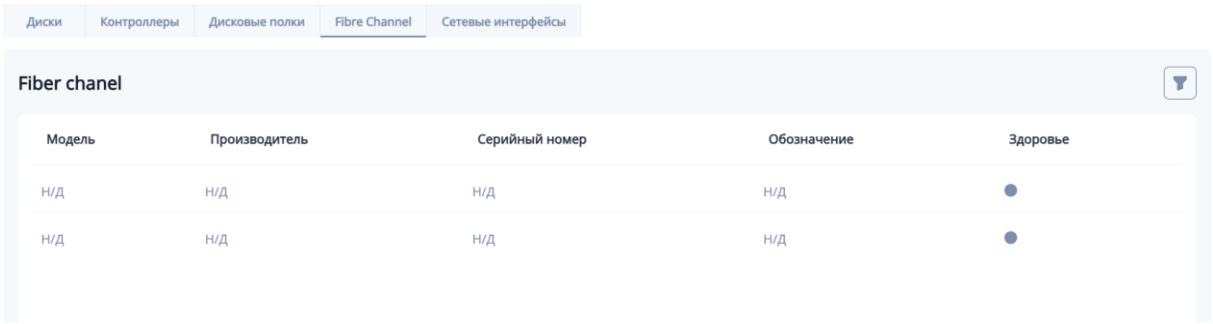


Рисунок 10.5 – Вкладка «Fibre Channel» страницы «Компоненты»

Вкладка «Сетевые интерфейсы» выглядит следующим образом (рисунок 10.6):

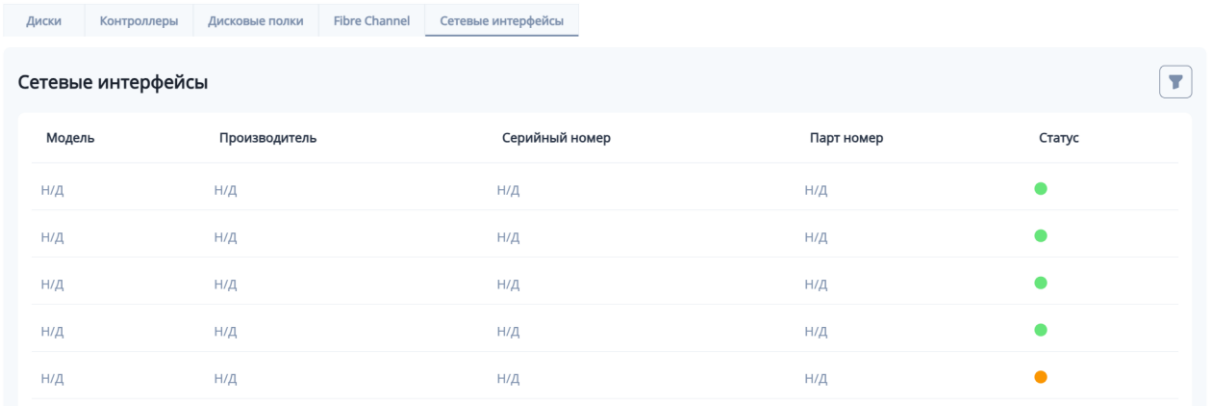


Рисунок 10.6 – Вкладка «Сетевые интерфейсы» страницы «Компоненты»

В разделе при нажатии на кнопку доступна фильтрация номеру узла (рисунок 10.7):

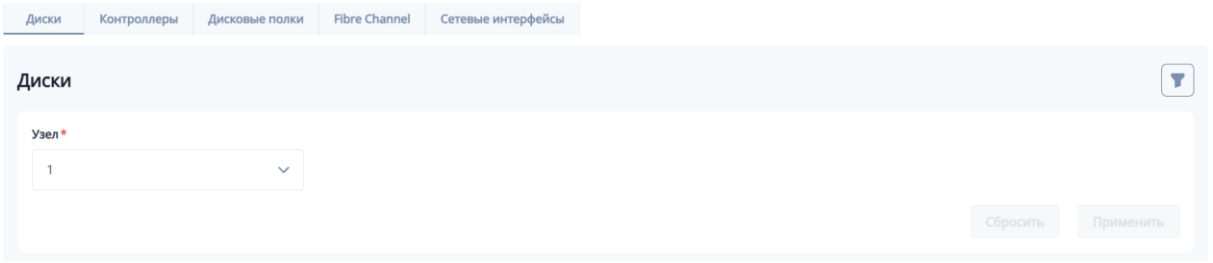


Рисунок 10.7 – Фильтрация по узлу страницы «Компоненты»

10.2 СЕНСОРЫ

Страница «Сенсоры» предназначена для мониторинга состояния аппаратного обеспечения в реальном времени. Здесь отображаются показания температурных датчиков, скорости вращения вентиляторов, напряжения на ключевых линиях питания и другие параметры, получаемые через интерфейс IPMI (Intelligent Platform Management Interface).

Регулярный просмотр этой страницы позволяет своевременно обнаружить перегрев, проблемы с охлаждением или отклонения в электропитании узла. (рисунок 10.8).

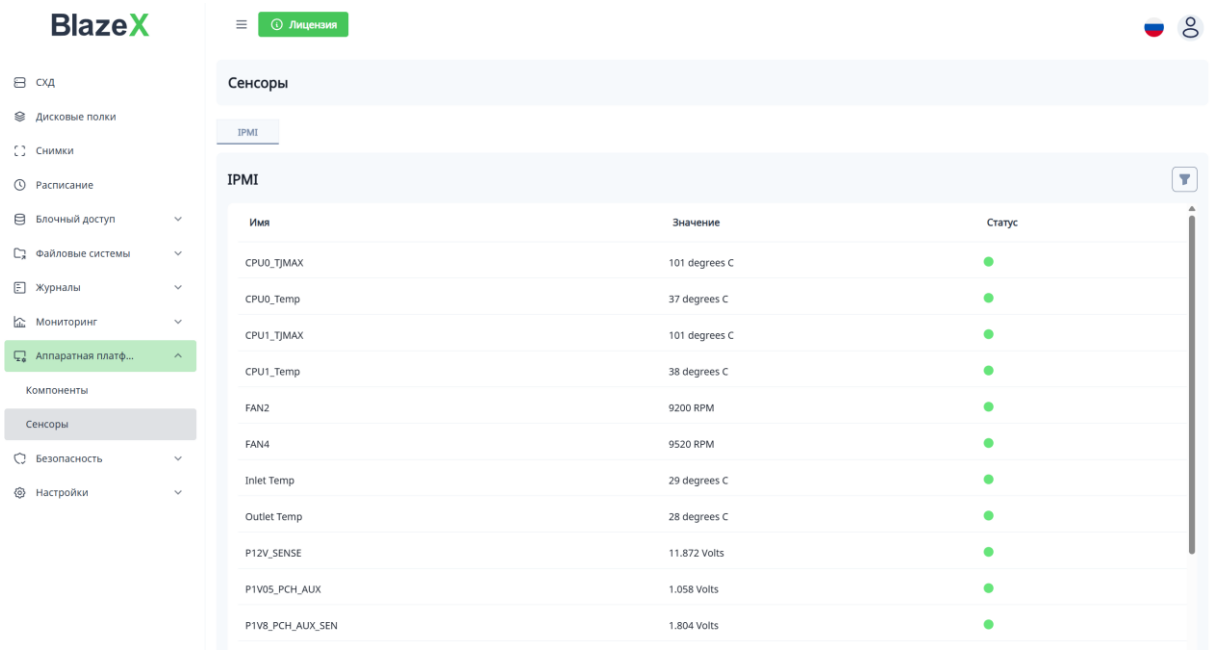


Рисунок 10.8 – Страница «Сенсоры»

Основная информация представлена в виде таблицы с тремя столбцами:

- Имя - Наименование сенсора (технический идентификатор)
- Значение - Текущее показание с указанием единиц измерения (градусы Цельсия, RPM, Вольты и т.д.)
- Статус - Индикатор состояния.

В разделе при нажатии на кнопку доступна фильтрация номеру узла (рисунок 10.9):

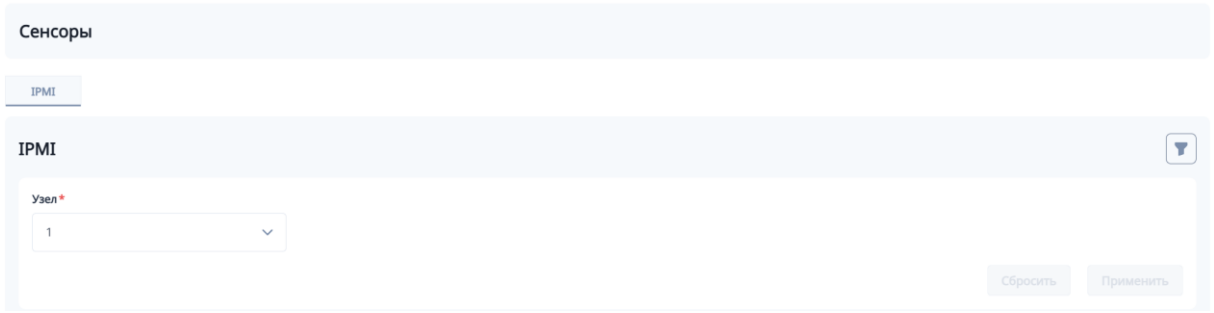


Рисунок 10.9 – Фильтрация по узлу страницы «Сенсоры»

11 БЕЗОПАСНОСТЬ

Раздел безопасность состоит из подразделов:

- Политики безопасности
- Подключение по AD/LDAP

11.1 ПОЛИТИКИ БЕЗОПАСНОСТИ

Раздел «Политики безопасности» предназначен для настройки правил аутентификации и управления доступом пользователей к системе. Здесь администратор задаёт требования к паролям, параметры сессий и правила блокировки при неудачных попытках входа (рисунок 11.1).

Раздел содержит три блока:

- Парольная политика
- Политика сессий
- Защита входа

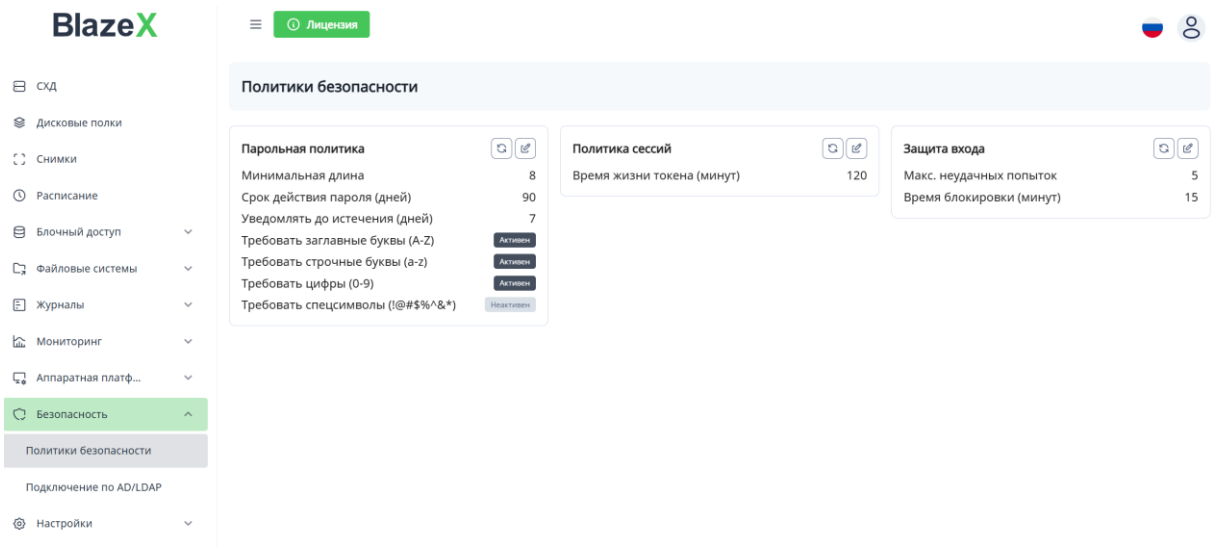


Рисунок 11.1 – Политики безопасности

11.1.1 ПАРОЛЬНАЯ ПОЛИТИКА

Этот блок определяет требования к паролям всех пользователей системы. Чем строже политика, тем выше устойчивость к подбору и компрометации. Для настройки доступны следующие параметры (рисунок 11.2):

- **Минимальная длина** - Наименьшее допустимое количество символов в пароле.
- **Срок действия пароля (дней)** - Период (в днях), через который пароль требуется сменить. По истечении срока система запросит новый пароль.

- **Уведомлять до истечения (дней)** - За сколько дней до окончания срока действия пользователю показывается предупреждение о необходимости смены пароля.
- **Требовать заглавные буквы (А-Я)** - Пароль должен содержать хотя бы одну заглавную латинскую или русскую букву.
- **Требовать строчные буквы (а-я)** - Пароль должен содержать хотя бы одну строчную букву.
- **Требовать цифры (0-9)** - Пароль должен содержать хотя бы одну цифру.
- **Требовать спецсимволы (!@#$%^&*)** - При включении этого параметра пароль обязан содержать хотя бы один специальный символ из предложенного набора.

Рисунок 11.2 – Парольная политика

Редактирование Парольной политики доступно при нажатии на кнопку «Редактирование»  . Откроется окно как показано на рисунке 11.3. Подтверждение по кнопке «Применить».

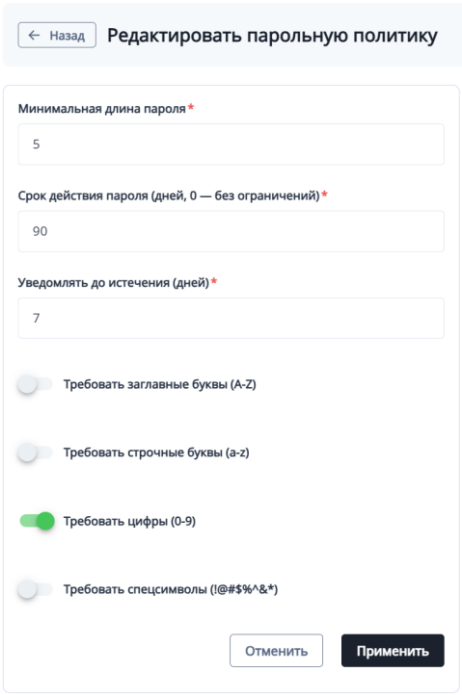


Рисунок 11.3 – Окно редактирования блока «Парольная политика»

Для сброса на настройки по умолчанию необходимо нажать на кнопку  . Система предупредит о сбросе следующим сообщением (рисунок 11.4)

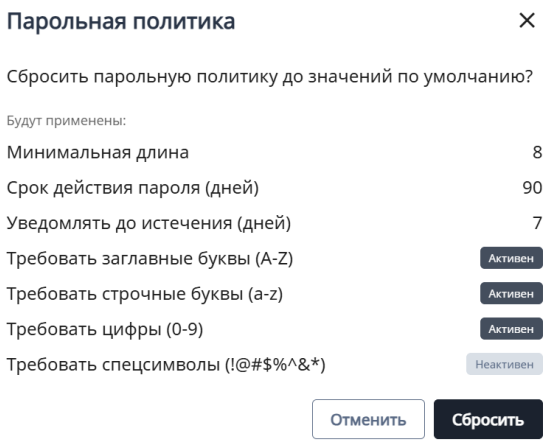
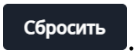


Рисунок 11.4 – Окно сброса настроек до значения по умолчанию блока «Парольная политика»

Для подтверждения необходимо нажать на кнопку «Спросить»  . Значения параметров примут вид (рисунок 11.5):

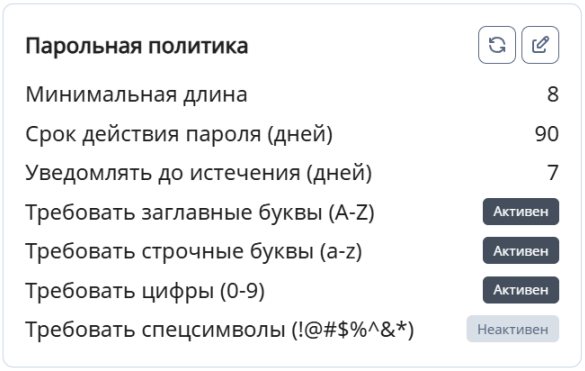


Рисунок 11.5 – Значения по умолчанию блока «Парольная политика»

11.1.2 ПОЛИТИКА СЕССИЙ

Этот блок управляет временем жизни пользовательской сессии (токена доступа). Для настройки доступен следующий параметр (рисунок 11.6):

Время жизни токена (минут) - Максимальное время (в минутах) с момента входа, после которого сессия автоматически завершается. Пользователю потребуется войти заново.

Значение 0 означает «без ограничений» (не рекомендуется).

После истечения этого времени любое действие в интерфейсе приведёт к перенаправлению на страницу входа.

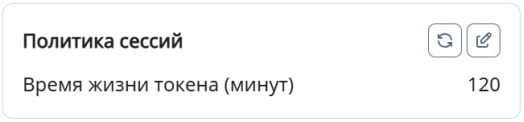


Рисунок 11.6 – Политика сессий

Редактирование Политики сессии доступно при нажатии на кнопку «Редактирование» . Откроется окно как показано на рисунке 11.7. Подтверждение по кнопке «Применить».

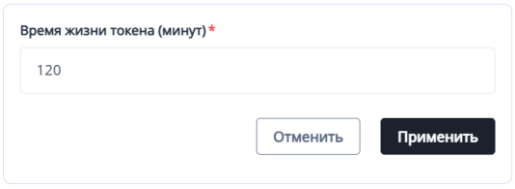


Рисунок 11.7 – Окно редактирования блока «Политики сессии»

Для сброса на настройки по умолчанию необходимо нажать на кнопку . Система предупредит о сбросе следующим сообщением (рисунок 11.8)

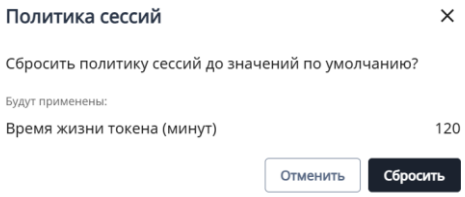


Рисунок 11.8 – Окно сброса настроек до значения по умолчанию блока «Политики сессии»

Для подтверждения необходимо нажать на кнопку «Спросить» . Значения параметров примут вид (рисунок 11.9):

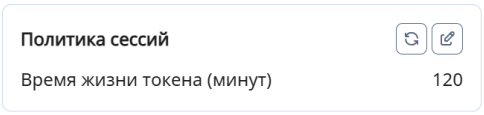


Рисунок 11.9 – Значения по умолчанию блока «Политики сессии»

11.1.3 ЗАЩИТА ВХОДА

Данный блок предотвращает автоматический подбор пароля (brute-force) путём временной блокировки учётной записи или IP-адреса. Для настройки доступны следующие параметры (рисунок 11.10):

- **Макс. неудачных попыток** - Количество неудачных попыток ввода пароля подряд, после которого срабатывает блокировка.

- **Время блокировки (минут) -** Продолжительность блокировки (в минутах). По истечении этого времени пользователь или IP-адрес снова может пытаться войти.

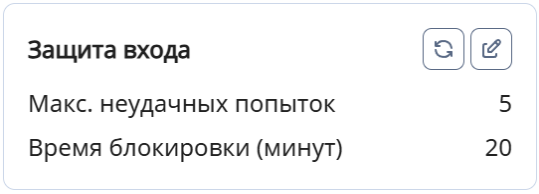


Рисунок 11.10 – Защита входа

Типовой сценарий срабатывания:

- Пользователь 5 раз подряд вводит неверный пароль.
- Учётная запись (или источник запроса) блокируется на 15 минут.
- В течение этого времени любые попытки входа с этого логина или адреса отклоняются.
- Через 15 минут блокировка автоматически снимается.

Редактирование Защиты входа доступно при нажатии на кнопку «Редактирование» . Откроется окно как показано на рисунке 11.11. Подтверждение по кнопке «Применить».

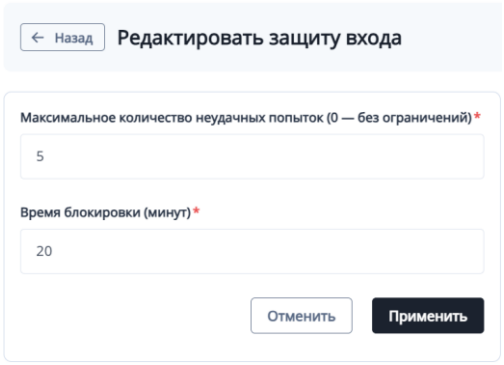


Рисунок 11.11 – Окно редактирования блока «Парольная политика»

Для сброса на настройки по умолчанию необходимо нажать на кнопку . Система предупредит о сбросе следующим сообщением (рисунок 11.12)

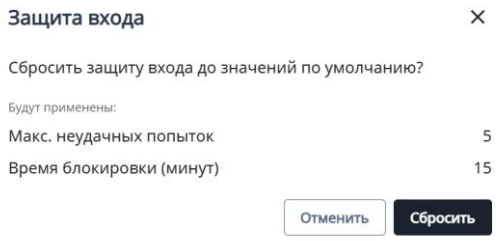


Рисунок 11.12 – Окно сброса настроек до значения по умолчанию блока «Защита входа»

Для подтверждения необходимо нажать на кнопку «Спросить» Сбросить. Значения параметров примут вид (рисунок 11.13):

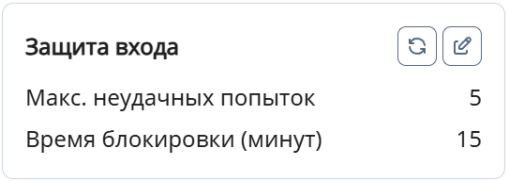


Рисунок 11.13 – Значения по умолчанию блока «Защита входа»

11.2 ПОДКЛЮЧЕНИЕ ПО AD/LDAP

Раздел AD/LDAP позволяет настроить интеграцию BlazeX с Active Directory или другими LDAP-совместимыми службами каталогов для централизованной аутентификации пользователей.

ПРИМЕЧАНИЕ.

Допустимые названия групп:
BlazexAdmins - администраторы,
BlazexUsers – операторы.

Для начала работы с AD/LDAP необходимо зайти в раздел «Безопасность» и выбрать подраздел «Подключение по AD/LDAP» (рисунок 11.14).

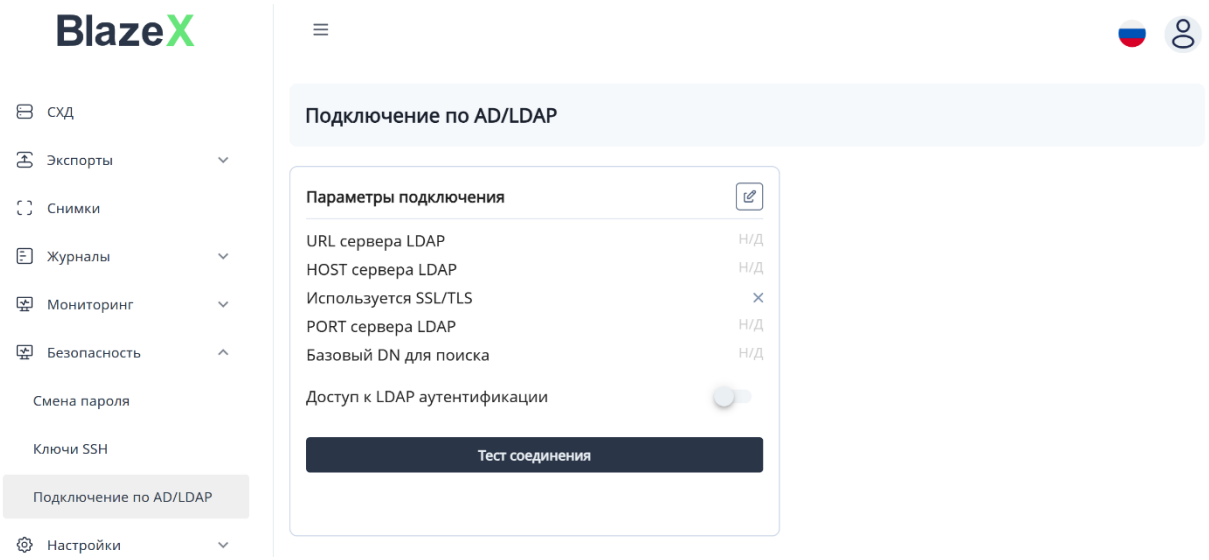


Рисунок 11.14 – Раздел «Подключение по AD/LDAP»

11.2.1 НАСТРОЙКА ПОДКЛЮЧЕНИЯ ПО AD/LDAP

Для настройки подключения по AD/LDAP необходимо нажать на кнопку «Настройки»  . Откроется окно настройки LDAP (рисунок 11.15)

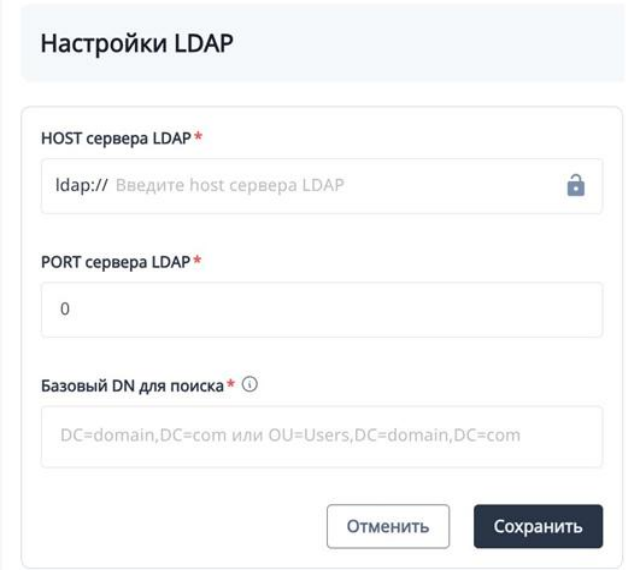


Рисунок 11.15 – Раздел «Подключение по AD/LDAP»

Для настройки LDAP необходимо:

1. Указать адрес сервера AD/LDAP в строке «HOST сервера LDAP» в формате ldap.example.com или 192.168.65.59
2. Указать порт для подключения к серверу в строке «PORT сервера LDAP». Стандартные порты:
   LDAP: 389 (без шифрования)
   LDAPS: 636 (с SSL/TLS)
3. Указать базовый путь в каталоге для поиска пользователей в строке «Базовый DN для поиска» в формате DC=promobit, DC=test
4. Нажать «Сохранить» 

Для **создания безопасного, зашифрованного соединения** необходимо указать порт 636, а в строке «HOST сервера LDAP» привести знак «замок» в состояние «secure»  , при этом адрес сервера будет начинаться с ldaps://… Заполненное окно будет выглядеть следующим образом (рисунок 11.16)

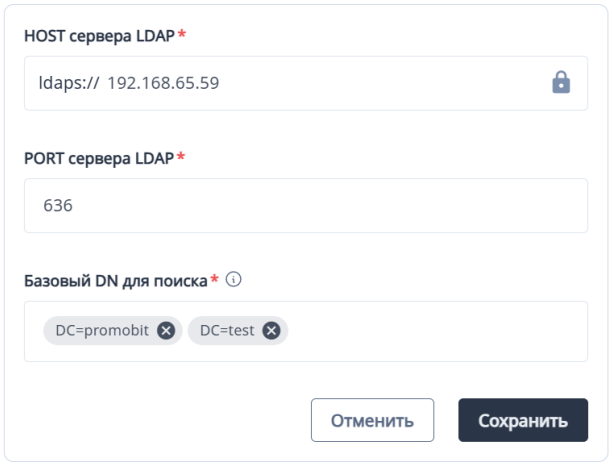


Рисунок 11.16 – Заполненное окно настроек LDAP для безопасного, зашифрованного соединения

Для создания **соединения без шифрования** необходимо указать порт 389, а в строке «HOST сервера LDAP» привести знак «замок» в состояние «insecure», при этом адрес сервера будет начинаться с ldap://… Заполненное окно будет выглядеть следующим образом (рисунок 11.17)

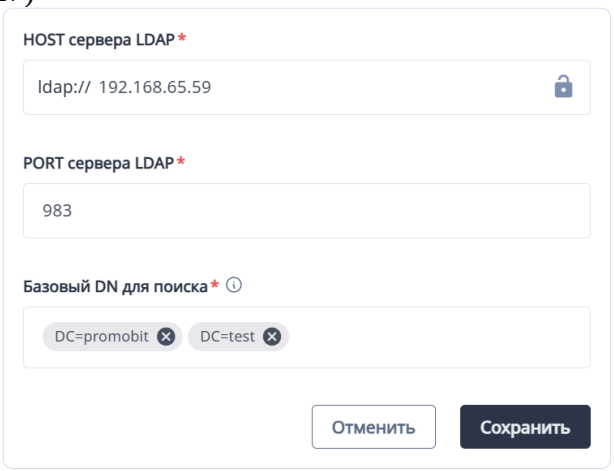


Рисунок 11.17 – Заполненное окно настроек LDAP для безопасного, зашифрованного соединения

В случае успешного выполнения команды сохранения окно «Параметра подключения LDAP» отобразится следующим образом (рисунок 11.18):

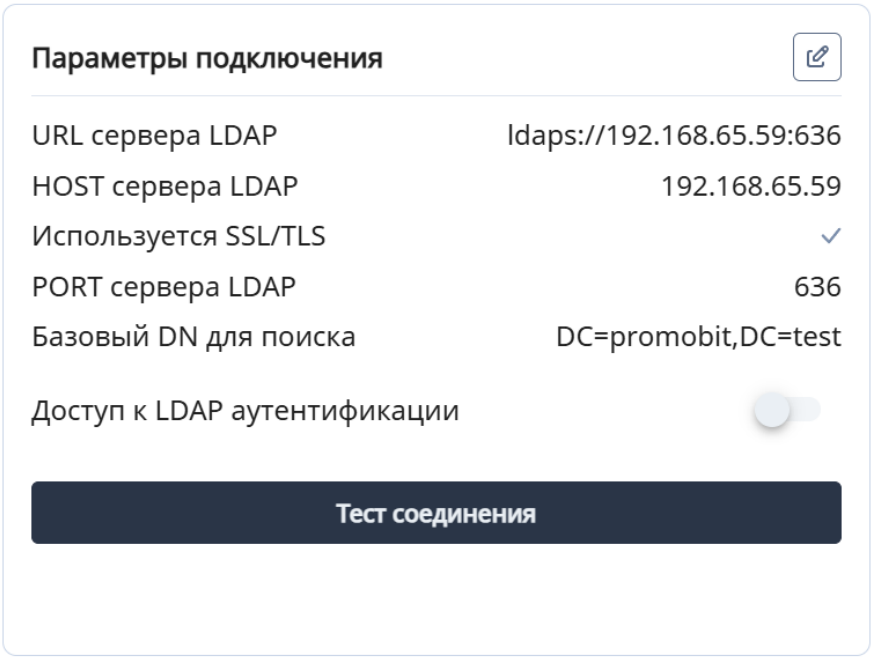


Рисунок 11.18 – Параметра подключения LDAP

11.2.2 ПРЕДОСТАВЛЕНИЕ ДОСТУПА К LDAP АУТЕНТИФИКАЦИИ

Для разрешения доступа к LDAP аутентификации необходимо привести состояние переключателя в состояние «Включено»  . После этого откроется модальное окно подтверждения (рисунок 11.19). Для подтверждения включения необходимо нажать «Включить» 

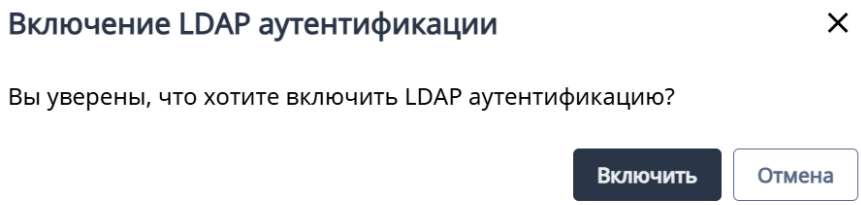


Рисунок 11.19 – Окно подтверждения включения LDAP аутентификации

В случае успешного выполнения команды Параметра подключения LDAP отобразятся следующим образом (рисунок 11.20):

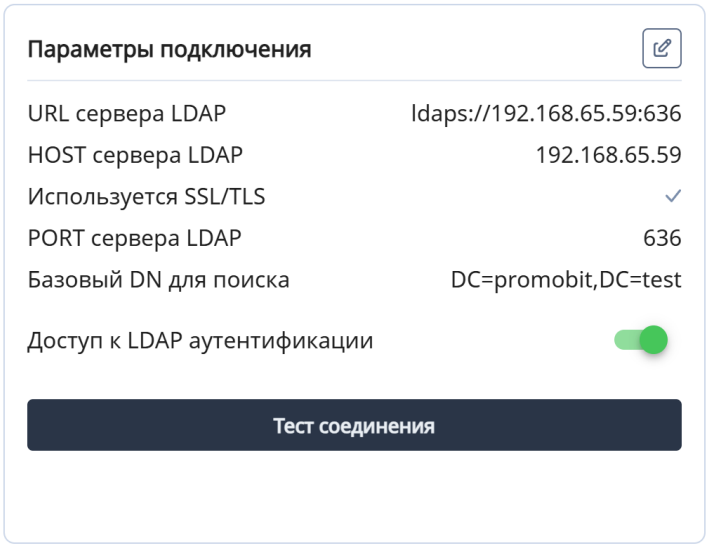


Рисунок 11.20 – Параметра подключения LDAP с включенной аутентификацией

11.2.3 ОТКЛЮЧЕНИЕ ДОСТУПА К LDAP АУТЕНТИФИКАЦИИ

Для отключения доступа к LDAP аутентификации необходимо привести состояние переключателя в состояние «Выключено» . После этого откроется модальное окно подтверждения (рисунок 11.21). Для подтверждения выключения необходимо нажать «Отключить» 

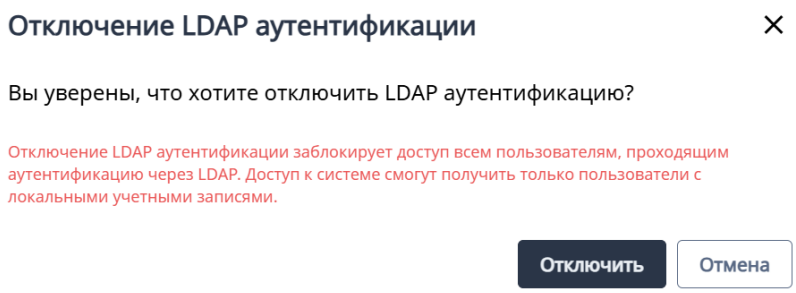


Рисунок 11.21 – Окно подтверждения отключения LDAP аутентификации

В случае успешного выполнения команды отключения окно «Параметра подключения LDAP» отобразится следующим образом (рисунок 8.11).

11.2.4 ТЕСТИРОВАНИЕ ПОДКЛЮЧЕНИЯ ПО AD/LDAP

Для проверки соединения по AD/LDAP необходимо нажать на кнопку «Тест соединения» 

.
В случае успешного выполнения команды в окне параметров подключения появится сообщение «LDAP connection successful» (рисунок 11.22)

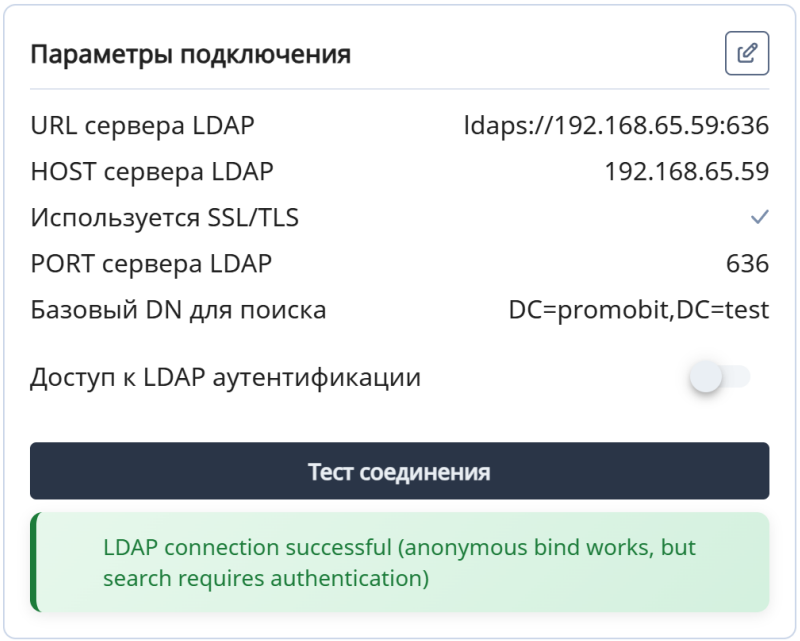


Рисунок 11.22 – Окно подтверждения успешного LDAP соединения.

12 НАСТРОЙКИ

Раздел настройки содержит:

- Сетевые интерфейсы
- Syslog
- Уведомления
- Время и дата

12.1 ПАРАМЕТРЫ СЕТЕВЫХ ИНТЕРФЕЙСОВ

Раздел предназначен для просмотра и настройки параметров сетевых интерфейсов устройства. Позволяет управлять сетевыми подключениями, включая настройку IP-адресации, включение/отключение DHCP, а также просмотр технических характеристик интерфейсов.

Окно параметры сетевых интерфейсов отображает перечень доступных сетевых интерфейсов для каждого узла с ключевой информацией (рисунок 12.1):

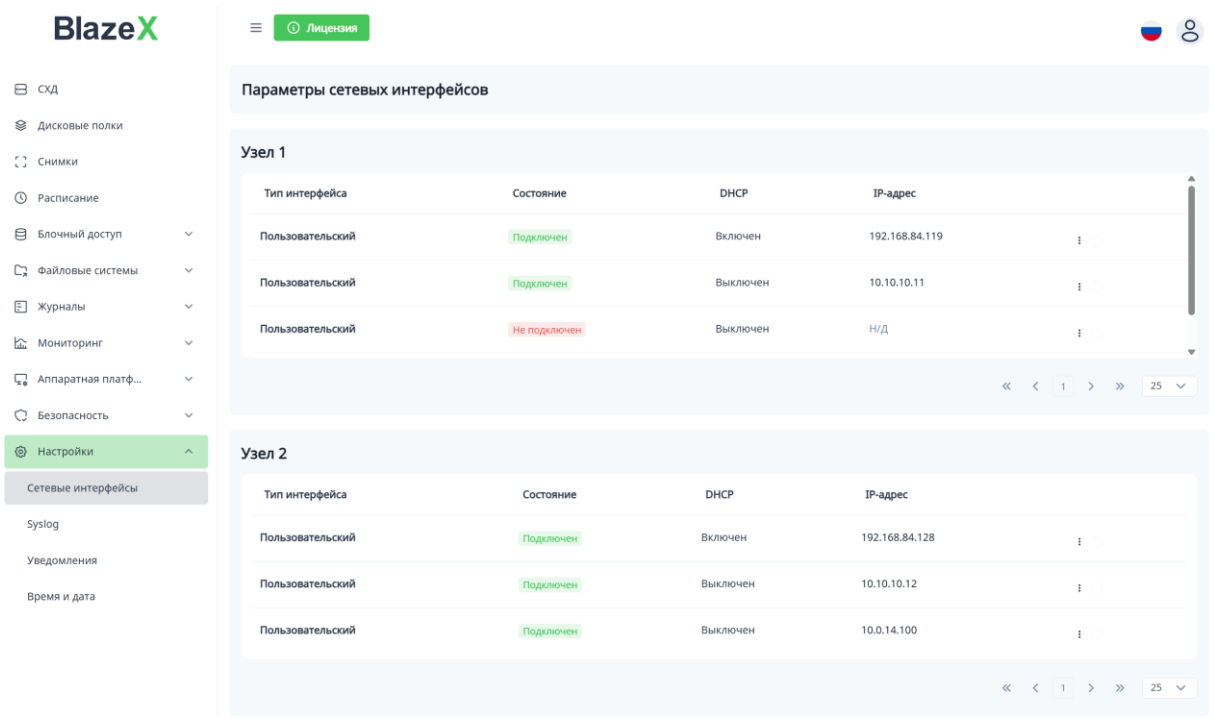


Рисунок 12.1 – Раздел Сетевые интерфейсы

Тип интерфейса - определяет категорию интерфейса:

- Управляющий (management)
- Пользовательский (data)

Состояние - индикатор активности:

- Подключен - интерфейс активен
- Отключен - интерфейс неактивен
- Неизвестно – состояние интерфейса неизвестно

DHCP - статус автоматической настройки:

- Включен - IP-адрес получается автоматически
- Выключен - используется статическая настройка

IP-адрес - текущий IPv4 адрес интерфейса
Для просмотра и редактирования параметров интерфейса необходимо выбрать его щелчком мыши или нажать на кнопку «Параметры» ⋮. Откроется окно редактирования (рисунок 12.2)

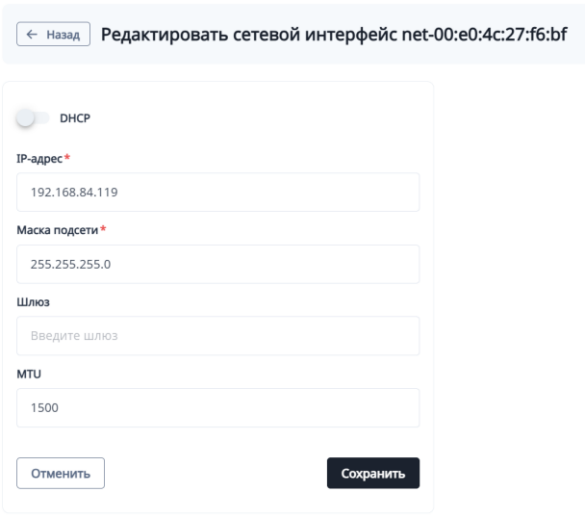


Рисунок 12.2 – Область просмотра и редактирования

12.1.1 НАСТРОЙКА ПАРАМЕТРОВ

Настраиваемые параметры (верхняя секция) содержит:
Переключатель DHCP - кнопка-переключатель «Включить/Выключить»  .

- При включении IP-адрес, маска и шлюз получаются автоматически от DHCP-сервера
- При выключении: требуется ручная настройка сетевых параметров

IP-адрес - текстовое поле в формате IPv4 (XXX.XXX.XXX.XXX)

- Доступно для редактирования только при выключенном DHCP).
- Автоматически блокируется при включении DHCP

Маска подсети - текстовое поле в формате IPv4 (XXX.XXX.XXX.XXX) или в формате CIDR (/24)

- Доступно для редактирования только при выключенном DHCP
- Автоматически блокируется при включении DHCP

Шлюз - текстовое поле в формате IPv4 (XXX.XXX.XXX.XXX)

- Доступно для редактирования только при выключенном DHCP
- Автоматически блокируется при включении DHCP

MTU - максимальный размер передаваемого пакета в байтах

- Доступно для редактирования только при выключенном DHCP
- Автоматически блокируется при включении DHCP

Детали интерфейса (нижняя секция, только для чтения)

- Тип интерфейса - технология подключения

- MAC-адрес - физический адрес сетевого адаптера
- Скорость интерфейса - текущая скорость соединения (1 Gb/s, 10 Gb/s и т.д.)
- MTU - максимальный размер передаваемого пакета

Процедура настройки интерфейса:
Включение DHCP (автоматическая настройка)
Для включения DHCP необходимо:

- Установить переключатель DHCP в положение «Включен»  . Поля IP-адрес, маска и шлюз станут недоступными для редактирования.
- Нажать кнопку «Сохранить» 

. Интерфейс получит настройки автоматически от DHCP-сервера

Настройка статического IP-адреса
Для настройки статического IP-адреса необходимо:

- Установить переключатель DHCP в положение «Выключен» . Поля IP-адрес, маска, шлюз станут доступными для редактирования и значение в поле шлюз обнулится.

Заполнить поля:

- IP-адрес - ввести статический IPv4 адрес
- Маска подсети - ввести соответствующую маску подсети
- Шлюз - ввести адрес шлюза по умолчанию (не обязательно).
- Нажать кнопку «Сохранить» 

.

Система выполнит проверку корректности введенных данных. В случае успеха область просмотра и редактирования закроется и отобразится окно параметры сетевых интерфейсов (рисунок 12.1)

12.2 SYSLOG

Syslog (System Logging Protocol) - это стандарт для отправки логов системы хранения данных на внешний сервер для централизованного сбора и анализа. В системе реализован интерфейс для настройки параметров отправки системных журналов.

12.2.1 НАСТРОЙКИ ПАРАМЕТРОВ SYSLOG

Для настройки Syslog необходимо зайти в раздел «Настройки» и выбрать подраздел «Syslog» (рисунок 12.3).

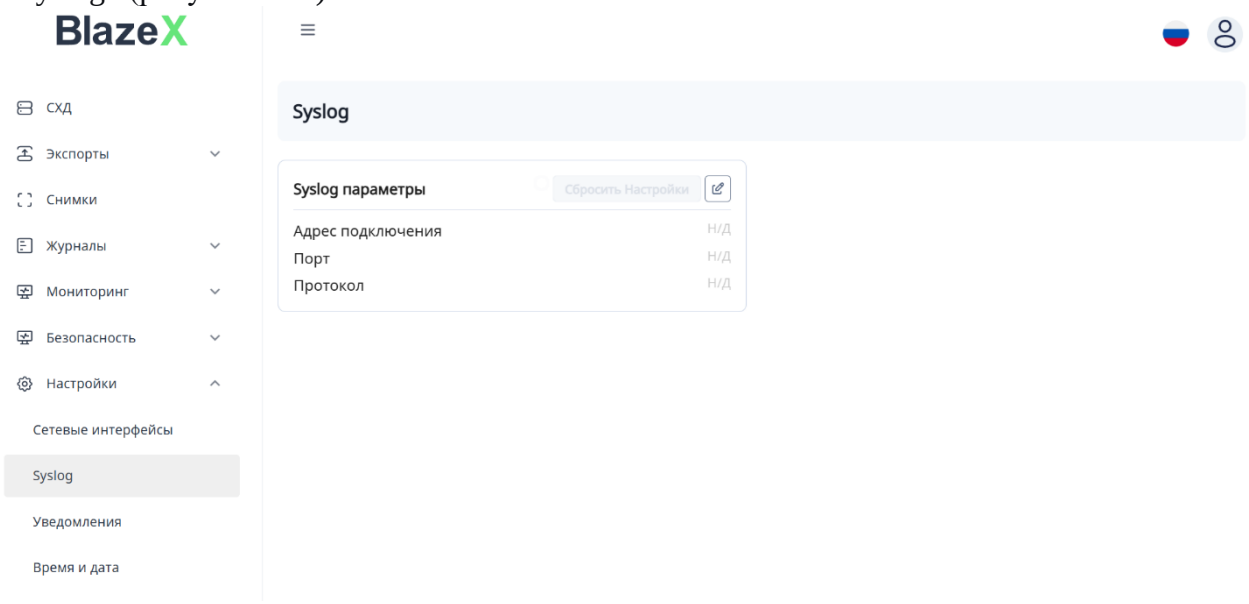


Рисунок 12.3 – Раздел «Syslog»

Для настройки параметров Syslog необходимо нажать на кнопку «Настройки»  .
Откроется окно настройки LDAP (рисунок 12.4)

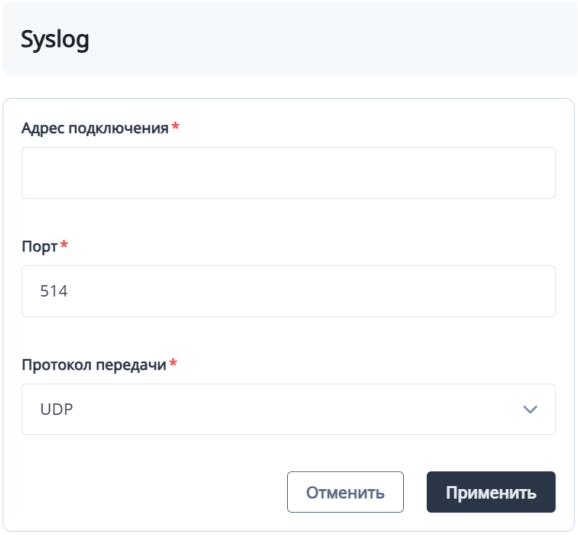


Рисунок 12.4 – Параметры Syslog

Для настройки Syslog необходимо:

1. Указать адрес сервера Syslog - текстовое поле для ввода IP-адреса или доменного имени сервера (например, allow.com или 192.168.1.100)
2. Указать порт в диапазоне 1-65535. Значение по умолчанию: 514
3. Выбрать протокол передачи:
    a. UDP (User Datagram Protocol) - протокол без установления соединения
    b. TCP (Transmission Control Protocol) - протокол с гарантированной доставкой

ПРИМЕЧАНИЕ.

Порт: 514 и протокол: UDP установлены по умолчанию

4. Нажать «Применить» 

В случае успешного выполнения команды сохранения окно раздела «Syslog» отобразится следующим образом (рисунок 12.5):

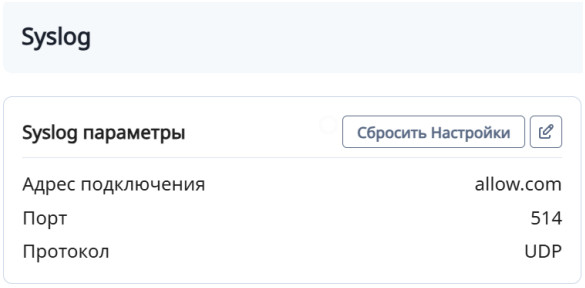


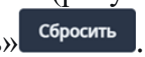
Рисунок 12.5 – Раздел «Syslog» с установленными параметрами

ПРИМЕЧАНИЕ.

На стороне Syslog-сервера должны быть настроены соответствующие права для доступа к директории хранения журнала

12.2.2 СБРОС НАСТРОЕК SYSLOG

Для сброса настроек необходимо нажать на кнопку «Сбросить настройки» 

.Откроется окно подтверждения (рисунок 12.6). Для подтверждения сброса настроек необходимо нажать «Сбросить» 

.

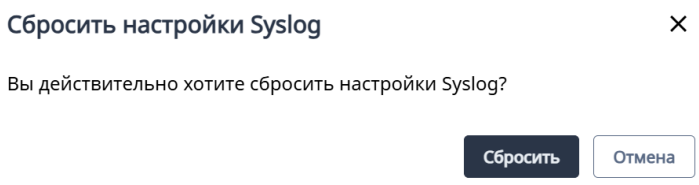


Рисунок 12.6 – Окно подтверждения сброса настроек Syslog

В случае успешного выполнения команды сохранения окно раздела «Syslog» отобразится следующим образом (рисунок 12.3).

Рекомендации по настройке

Выбор протокола:

- UDP - рекомендуется для локальных сетей с высокой стабильностью
- TCP - рекомендуется для ненадёжных сетей или когда требуется гарантированная доставка логов

12.3 УВЕДОМЛЕНИЯ (SMTP)

Раздел SMTP предназначен для настройки отправки уведомлений по электронной почте. Здесь пользователь может:

- Настроить параметры почтового сервера
- Указать список получателей уведомлений
- Управлять группами получателей

Для начал работы с уведомлениями необходимо зайти в раздел «Настройки» и выбрать подраздел «Уведомления» (рисунок 12.7).

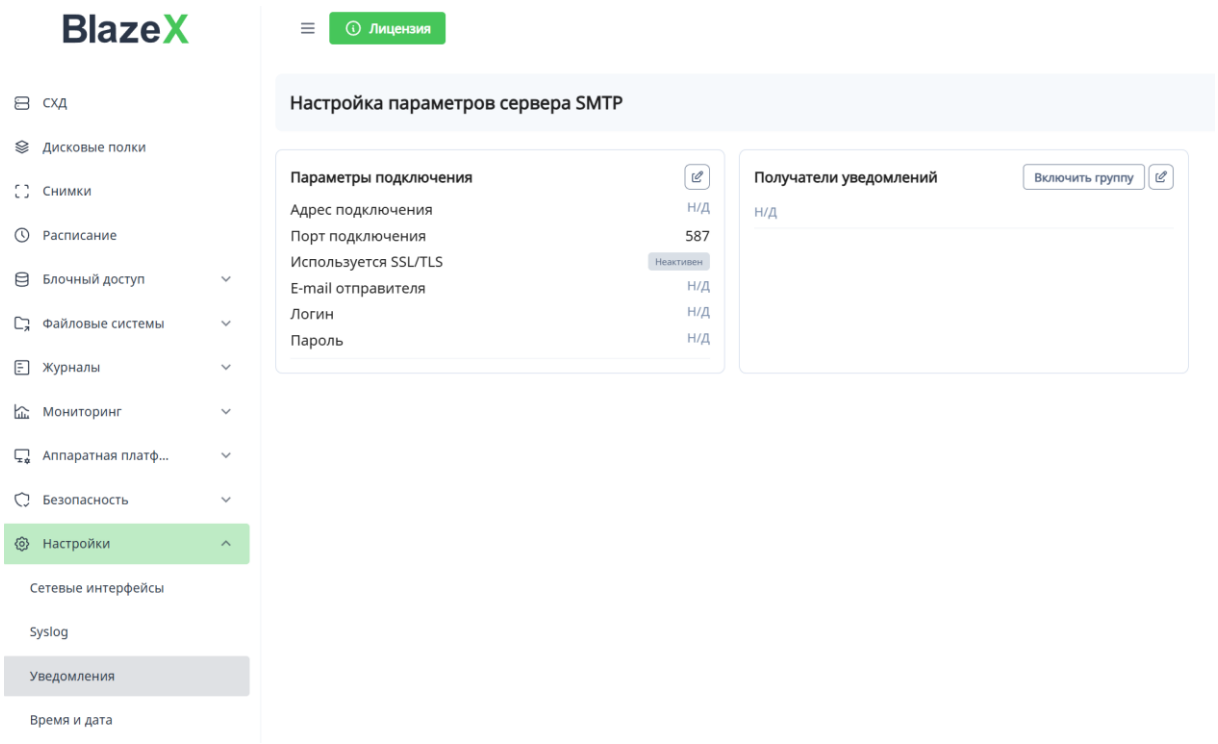


Рисунок 12.7 – Раздел «Уведомления»

9.3.1 НАСТРОЙКА ПАРАМЕТРОВ СЕРВЕРА SMTP

Для настройки параметров почтового сервера необходимо в области «Параметры подключения» нажать на значок «Настройки»  . Откроется окно «Редактирование параметров сервера SMTP» (рисунок 12.8).

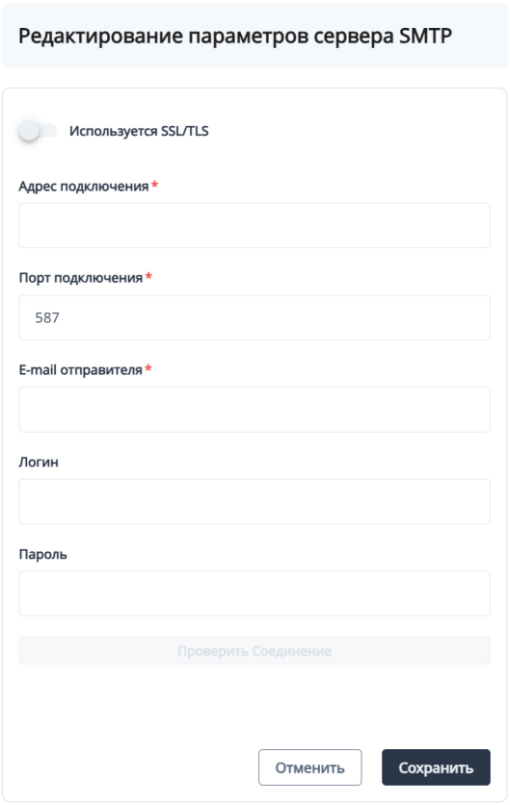


Рисунок 12.8 – Редактирование параметров сервера SMTP

Для настройки параметров почтового сервера необходимо:

1. Выбрать вариант использования шифрования в строке «Используется SSL/TLS»:

   Отключено - используется соединение без постоянного SSL-шифрования. При указании порта **587** применяется **STARTTLS (TLS)** - шифрование начинается после установки соединения.

   Включено - используется **SSL/TLS** с шифрованием с момента подключения *(порт 465)*
2. Указать адрес подключения - доменное имя или IP-адрес SMTP-сервера (например, smtp.ethereal.email, smtp.gmail.com, 192.168.1.100)
3. Указать порт. Стандартные порты:
   - 25 - без шифрования (не рекомендуется)
   - 465 - SSL/TLS
   - 587 - TLS (STARTTLS)

ПРИМЕЧАНИЕ.

Порт **587** установлен по умолчанию и используется с **STARTTLS (TLS)**.

4. Указать email отправителя (в примере jarred.hodkiewicz@ethereal.email)
5. Указать логин (в примере jarred.hodkiewicz@ethereal.email)
6. Указать пароль

После заполнения всех полей необходимо проверить соединение, для этого нужно нажать на кнопку Проверить Соединение. В случае успешного выполнения команды появится сообщение «Соединение успешно установлено» (рисунок 12.9)

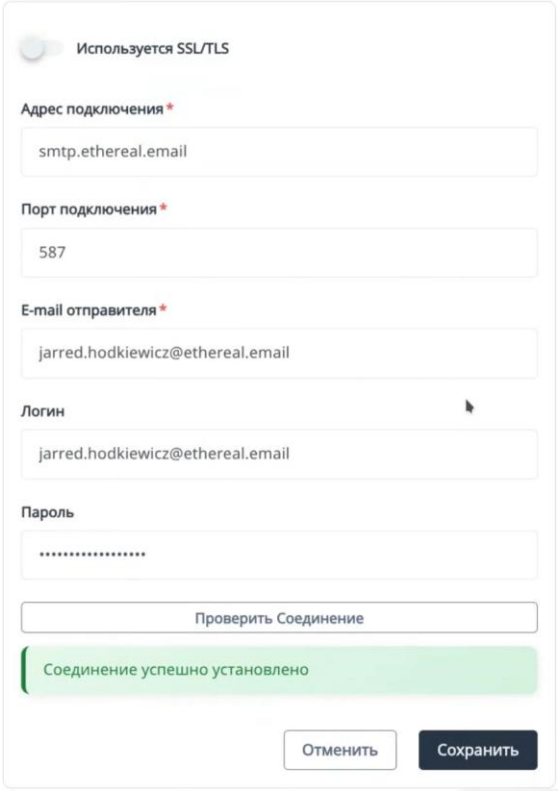


Рисунок 12.9 – Заполненное окно редактирования параметров сервера SMTP с успешной проверкой соединения

7. Нажать «Сохранить» Сохранить.

ПРИМЕЧАНИЕ

Дополнительные параметры SMTP доступны для изменения в конфигурации YAML:

Пул соединений

- pool - использовать пул соединений (true)
- maxConnections - макс. количество соединений (2)
- maxMessages - писем на одно соединение (50)

Таймауты (мс)

- connectionTimeout - таймаут подключения (10000)
- socketTimeout - таймаут сокета (30000)
- greetingTimeout - ожидание приветствия (10000)

Очередь писем

- intervalMs - интервал обработки очереди (5000)
- maxAttempts - количество попыток (5)

- backoffMs - задержка между попытками (3000)
- maxQueueSize - размер очереди (100)
- concurrency - параллельная отправка (2)
- • logging - логирование (false)

9.3.2 НАСТРОЙКА ПОЛУЧАТЕЛЕЙ УВЕДОМЛЕНИЙ

Для настройки получателей уведомлений необходимо в области «Получатели уведомлений» нажать на значок «Настройки»  . Откроется окно «Редактирование получателей SMTP уведомлений» (рисунок 12.10).

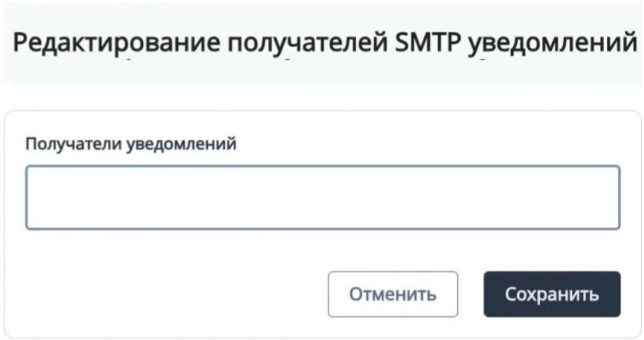


Рисунок 12.10 – Редактирование получателей SMTP уведомлений

ПРИМЕЧАНИЕ.

Ввод email адресов получателей доступен через запятую, пробел и по нажатию на «Enter»

Список получателей отображается в строке следующим образом (Рисунок 12.11):

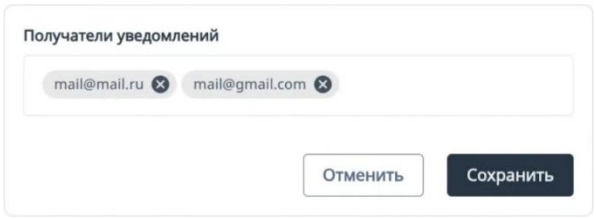


Рисунок 12.11 – Отображение списка получателей

Для сохранения списка получателей уведомлений необходимо нажать на кнопку «Сохранить»  .

12.3.3 ВКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ УВЕДОМЛЕНИЙ ДЛЯ ГРУПП ПОЛУЧАТЕЛЕЙ

Для включения уведомлений для группы получателей необходимо в области «Получатели уведомлений» нажать на кнопку «Включить группу» 

. В итоге окно с включенной отправкой уведомлений примет вид (рисунок 12.12):

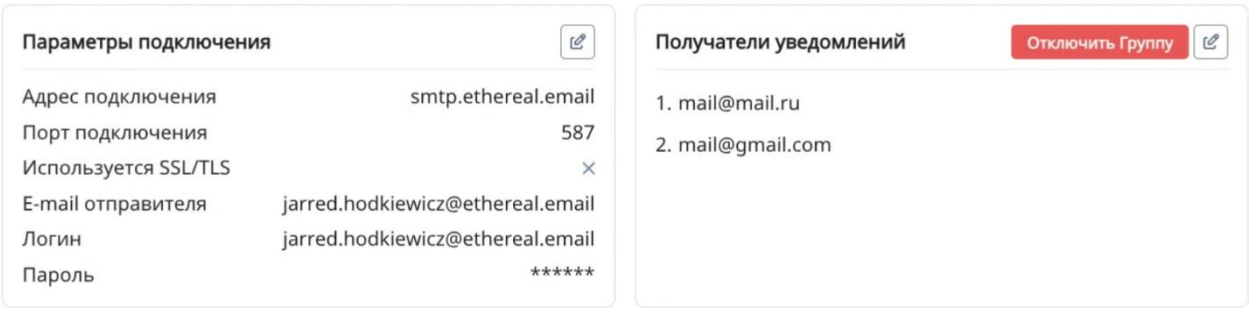


Рисунок 12.12 – Окно уведомлений с включенной отправкой уведомлений

Для выключения уведомлений для группы получателей необходимо в области «Получатели уведомлений» нажать на кнопку «Отключить группу» 

.

12.4 ВРЕМЯ И ДАТА

Раздел предназначен для выбора часового пояса и и настройки NTP серверов
Для начал работы с настройкой времени и даты необходимо зайти в раздел «Настройки» и выбрать подраздел «Время и дата» (рисунок 9.13).

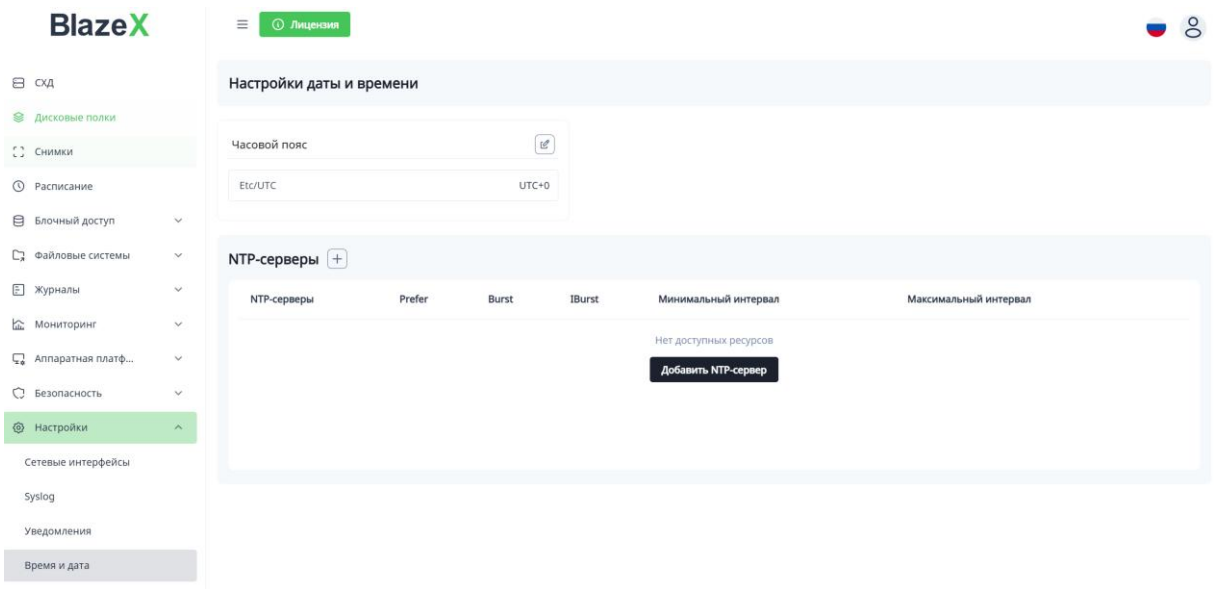


Рисунок 12.13– Раздел «Время и дата»

12.4.1 ВЫБОР ЧАСОВОГО ПОЯСА

Для выбора часового пояса необходимо в разделе «Часовой пояс» нажать на значок «Настройки»  , выбрать в строке ниже необходимый часовой пояс, например Asia/Omsk, и подтвердить выбор нажав на «Применить»  для сохранения настроек. Изменение часового пояса применяется ко всем системным часам и логам.

12.4.2 НАСТРОЙКА СИНХРОНИЗАЦИИ ВРЕМЕНИ ЧЕРЕЗ NTP

Для настройки NTP сервера необходимо нажать на «плюс»  в заголовке раздела «NTP-серверы». Откроется окно добавления NTP сервера (рисунок 12.14)

Рисунок 12.14 – Окно добавления NTP сервера

Необходимо ввести параметры NTP-сервера:
Адрес подключения:
В поле "Адрес NTP-сервера" вводится доменное имя или IP-адрес сервера времени, (например, pool.ntp.org, ntp1.stratum1.ru, 192.168.1.100)

Параметры опроса:
Минимальный интервал (minpoll):

- Определяет минимальный интервал между запросами к серверу
- Значение указывается в виде степени двойки (например, 6 = 2^6 = 64 секунды)
- Допустимый диапазон: от 4 (16 сек) до 17 (≈36 часов)

- Рекомендуемое значение: 6 (64 секунды)

Максимальный интервал (maxpoll):

- Определяет максимальный интервал между запросами
- Также указывается как степень двойки
- Должен быть больше или равен минимальному интервалу
- Рекомендуемое значение: 10 (≈17 минут)

Дополнительные параметры:

Burst (burst):

- При включенной опции клиент отправляет серию из 8 запросов вместо одного
- Ускоряет первоначальную синхронизацию
- Использует больше сетевых ресурсов
- Рекомендация: Включать для нестабильных соединений

Iburst (iburst):

- Улучшенная версия burst - отправляет 8 запросов с интервалом 2 секунды
- Обеспечивает быструю первоначальную синхронизацию при старте системы
- Рекомендация: Включать для всех серверов

Prefer (prefer):

- Отмечает основной (предпочтительный) NTP-сервер из списка
- Система будет использовать его как основной источник времени
- Рекомендация: Установить флажок для наиболее надежного сервера

Пример типовой конфигурации

Для корпоративной сети:

- Адрес NTP-сервера: ntp.local.company.com
- Минимальный интервал: 6
- Максимальный интервал: 10
- ☑ Iburst
- ☐ Burst
- ☑ Prefer

Для работы с публичными серверами:

- Адрес NTP-сервера: time.google.com
- Минимальный интервал: 6
- Максимальный интервал: 10
- ☑ Iburst
- ☐ Burst
- ☐ Prefer

После ввода параметров настройки необходимо нажать на кнопку «Сохранить» 

. В случае успешного выполнения команды созданный NTP-сервер отобразится в итоговой таблице (рисунок 12.15)

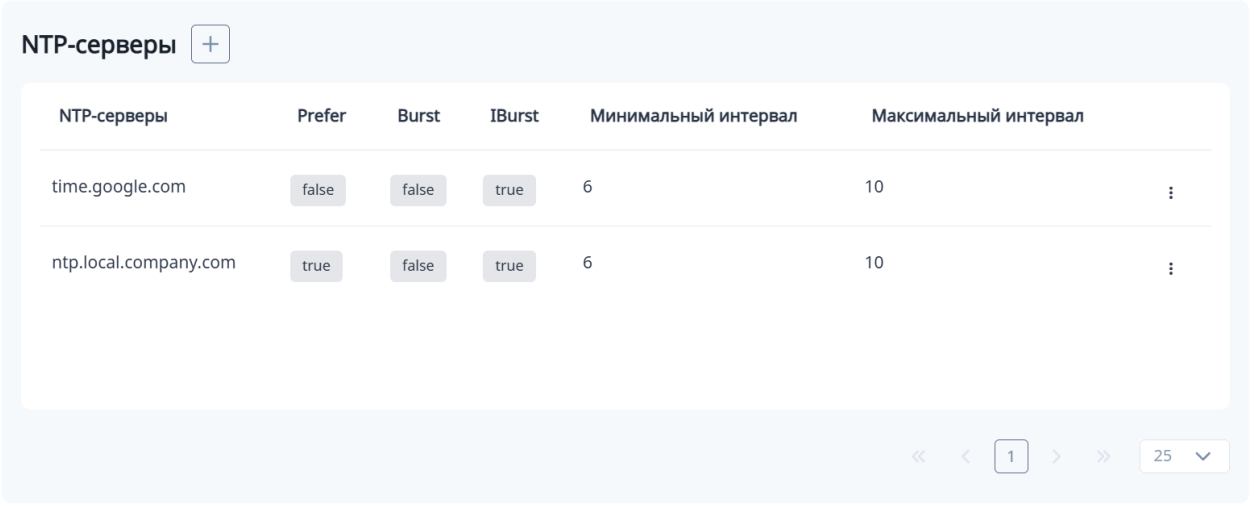


Рисунок 12.15 – Подраздел «NTP-серверы»

12.4.3 РЕДАКТИРОВАНИЕ ПАРАМЕТРОВ NTP-СЕРВЕРА

Для редактирования параметров NTP-сервера необходимо нажать на значок «Параметры» и выбрать строку «Редактировать» Редактировать (рисунок 12.16). Для сохранения измененных параметров настройки необходимо нажать на кнопку «Сохранить» Сохранить. В случае успешного выполнения команды скорректированный NTP-сервер отобразится в итоговой таблице (рисунок 12.15)

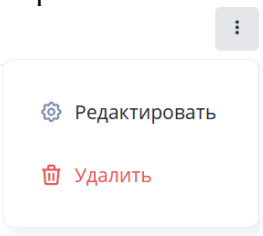


Рисунок 12.16 – Всплывающее окно параметров NTP-сервера

12.4.4 УДАЛЕНИЕ NTP-СЕРВЕРА

Для удаления NTP-сервера необходимо нажать на значок «Параметры» и выбрать строку «Удалить» Удалить (рисунок 12.16). В случае успешного выполнения команды скорректированный NTP-сервер отобразится в итоговой таблице (рисунок 12.15).

12.5 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI)

Командный интерфейс (CLI) системы хранения данных предоставляет инструменты для управления пулами хранения и логическими томами.
Чтобы подключиться к серверу CLI по SSH, понадобится SSH-клиент (например, встроенный в Linux/macOS Терминал или PuTTY для Windows). Получение ключа SSH описано в пункте 1.7 данной документации. Получение доступа к CLI описано в пункте 12.5.4.

12.5.1 ПОДКЛЮЧЕНИЕ К СИСТЕМЕ

Шаг 1: Подключение по SSH

1. Определите IP-адрес управления (используйте значение blazex_mgmt от одного из узлов):

```
ssh ivan@192.168.0.10
```

Примечание: Замените 192.168.0.10 на реальный IP-адрес из параметра blazex_mgmt

2. Система запросит учетные данные:

```
Username: ivan
Password:
```

3. При успешной аутентификации вы увидите:

```
✓ LOGIN SUCCESS
Storage Management Shell
[https://localhost/] storage>
```

Шаг 2: Начало работы
После успешного входа вы находитесь в командной строке управления хранилищем. Приглашение [https://localhost/] storage> указывает на готовность системы к приему команд.

12.5.2 СПИСОК КОМАНД

Команды взаимодействия с СХД
1. Управление дисками в пулах
   - **add-drive** - Добавить диск в пул
   - **remove-drive** - Удалить диск из пула
2. Управление пулами хранения
   - **create-pool** - Создать новый пул
   - **create-pool-saa** - Создать Symmetric Active-Active пул
   - **merge-pool** - Объединить пулы
   - **delete-pool** - Удалить пул

- **get-pool** - Получить информацию о пуле
- **get-pool-list** - Получить список пулов

3. Управление логическими томами (LUN)
   - **create-lun** - Создать том
   - **delete-lun** - Удалить том
   - **update-lun-size** - Расширение тома с блочным доступом
   - **get-lun** - Получить информацию о томе
   - **get-lun-list** - Получить список томов
4. Управление снапшотами
   - **create-snapshot** - Создать снапшот
   - **clone-snapshot** - Клонировать снапшот в новый том
   - **delete-snapshot** - Удалить снапшот
   - **get-snapshot** - Получить информацию о снапшоте
   - **get-snapshot-list** - Получить список снапшотов
5. Управление NFS экспортами
   - **create-nfs** - Создать NFS экспорт
   - **update-nfs** - Обновить параметры NFS экспорта
   - **delete-nfs** - Удалить NFS экспорт
   - **get-nfs** - Получить информацию об NFS экспорте
   - **get-nfs-list** - Получить список NFS экспортов
6. Управление пользователями
   - **create-user** - Создать пользователя
   - **update-user** - Обновить данные пользователя
   - **update-user-password** - Обновить пароль пользователя
   - **delete-user** - Удалить пользователя
   - **get-user** - Получить информацию о пользователе
   - **get-user-list** - Получить список пользователей
7. Информационные команды
   - **get-drive-list** - Получить список дисков
   - **get-system** - Получить информацию о системе
   - **get-net-list** - Получить список сетевых интерфейсов
   - **get-net** - Получить информацию о сетевом интерфейсе
8. Служебные команды
   - **exit** - Выход из интерфейса
   - **help** - Вывод справки
   - **quit** - Выход из интерфейса
9. Политика безопасности
   - **get-auth-security-config** - Получение конфигурации политики безопасности
   - **update-auth-security-config** - Обновление конфигурации политики безопасности

Подробное описание команд

1. add-drive - Добавление диска в пул

Назначение: Добавляет физический диск в существующий пул хранения.

Синтаксис:

```
add-drive -i <pool_id> -d <disk_id>
```

Параметры:

- -i, --id TEXT - ID пула (обязательный)
- -d, --disk TEXT - ID диска для добавления (обязательный)

Пример:

```
[https://localhost/] storage> add-drive -i pool-Cvy3 -d drive-0e925b72-a593-4236-9
```

Результат: Диск добавлен в пул; в get-pool отображается новый диск, в get-drive-list меняется привязка/статус.

2. remove-drive - Удаление диска из пула

Назначение: Удаляет физический диск из пула хранения.

Синтаксис:

```
remove-drive -i <pool_id> -d <disk_id>
```

Параметры:

- -i, --id TEXT - ID пула (обязательный)
- -d, --disk TEXT - ID диска для удаления (обязательный)

Пример:

```
[https://localhost/] storage> remove-drive -i pool-Cvy3 -d drive-0e925b72-a593-4236-9
```

Результат: Диск исключён из пула; изменения видны в get-pool и get-drive-list.

3. create-pool - Создание пула хранения

Назначение: Создает новый пул хранения с заданными параметрами RAID.

Синтаксис:

```
create-pool -e <engine> --node-id <node_id> -l <level> -d <disk_ids>
[дополнительные_параметры]
```

Обязательные параметры:

- -e, --engine [mdraid|blazeio] - RAID-контроллер (обязательный)

- --node-id TEXT - ID узла (обязательный)
- -l, --level [0|1|5|6|n+m] - Уровень RAID (обязательный)
- -d, --disk TEXT - ID дисков (повторяемый, обязательный)

Дополнительные параметры:

- -n, --name TEXT - Имя пула
- -s, --schema [2+1|4+1|4+2|8+1|8+2|8+3|8+4|16+1|16+2|16+3|16+4] - Схема RAID
- --strip-size [4|8|16|32|64|128|256|512|1024] - Размер полосы в КБ (степень двойки, 4-1024). Настройка параметра «Размер блока (Strip size)» зависит от драйвера и уровня RAID группы (подробнее смотри в 2.4.1 «Создание групп накопителей»)
- --thin / --no-thin - Включить тонкое провизионирование
- --vdo / --no-vdo - Включить VDO-сжатие

Пример:

```
[https://localhost/] storage> create-pool --engine blazeio -d drive-6a939b47-458a-4796-b -d drive-0e925b72-a593-4236-9 -d drive-b0701b7a-6f16-4d93-9 --level n+m --schema 2+1 --node-id 1
```

Результат: Создан пул; появляется pool-<id> в get-pool-list; детали доступны через get-pool -i pool-<id>.

После создания пула на экране отобразится таблица с параметрами (рисунок 8.18).

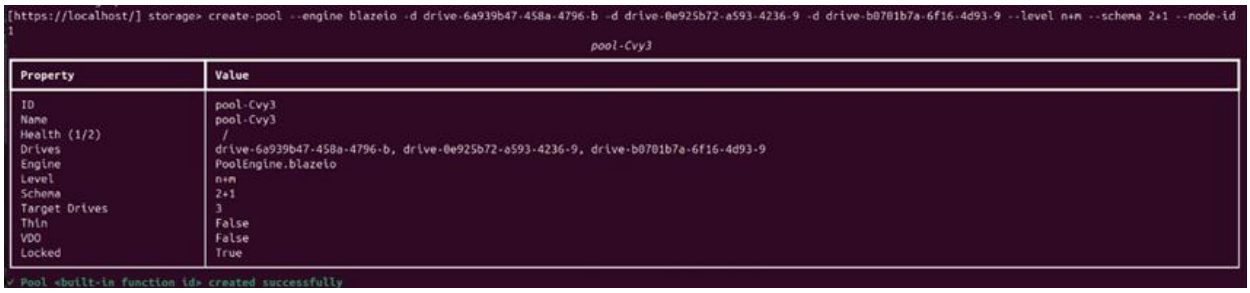


Рисунок 8.18 – отображение созданного пула

4. create-pool-saa - Создание Symmetric Active-Active пула

Назначение: Создает Symmetric Active-Active пул хранения.

Синтаксис:

```
create-pool-saa -n "SAA_Pool_1" -l 5 -s 4+1 --strip-size 64 -d <id1> -d <id2> -d <id3> -d <id4> -d <id5>
```

Параметры:

- -n, --name TEXT - Имя пула
- -l, --level INTEGER - Уровень RAID
- -s, --schema TEXT - Схема RAID (например, "4+1")
- --strip-size INTEGER - Размер полосы в КБ
- -d, --disk TEXT - ID дисков (повторяемый, обязательный)

Пример:

```
[https://localhost/] storage> create-pool-saa -n "SAA_Pool_1" -l 5 -s 4+1 --strip-size 64 -d drive-123 -d drive-456 -d drive-789 -d drive-abc -d drive-def
```

Результат: Создан Symmetric Active-Active пул; появляется pool-<id> в get-pool-list; параметры соответствуют level/schema/strip-size.

5. merge-pool - Объединение пулов

Назначение: Объединяет два пула с одинаковым engine.

Синтаксис:

```
merge-pool -p <parent_id> -c <child_id>
```

Параметры:

- -p, --parent TEXT - ID родительского пула (обязательный)
- -c, --child TEXT - ID дочернего пула (обязательный)

Пример:

```
https://localhost/] storage> merge-pool -p pool-123 -c pool-456
```

Результат: Пулы с одинаковым engine объединены; изменения видны в get-pool-list и get-pool.

6. delete-pool - Удаление пула

Назначение: Удаляет пул хранения по его ID.

Синтаксис:

```
delete-pool -i <pool_id>
```

Параметры:

- -i, --id TEXT - ID пула для удаления (обязательный)

Пример:

```
[https://localhost/] storage> delete-pool -i pool-Cvy3
```

Результат: Пул удалён; пропадает из get-pool-list; get-pool по id возвращает ошибку/не найден.

7. get-pool - Получение информации о пуле

Назначение: Получает детальную информацию о конкретном пуле хранения.
Синтаксис:

```
get-pool -i <pool_id>
```

Параметры:
- -i, --id TEXT - ID пула для получения информации (обязательный)

Пример:
```
[https://localhost/] storage> get-pool -i pool-Cvy3
```

Результат: Детальная информация по пулу: диски, RAID/engine, состояние.

8. get-pool-list - Список пулов

Назначение: Выводит список всех пулов хранения в системе.

Синтаксис:
```
get-pool-list
```

Пример:
```
[https://localhost/] storage> get-pool-list
```

Результат: Вывод списка пулов (pool-<id>) со статусом/типом/именем.

9. create-lun - Создание логического тома

Назначение: Создает новый логический том (LUN) в указанном пуле.

Синтаксис:
```
create-lun -p <pool_id> -a <access_type> [дополнительные_параметры]
```

Обязательные параметры:
- -p, --pool-id TEXT - ID пула (обязательный)
- -a, --access [Block|File] - Тип доступа к тому (обязательный)

Дополнительные параметры:
- -n, --name TEXT - Имя тома
- -t, --lun-type [vdo|thin|regular|striped|snapshot] - Тип тома
- -b, --scst-block-size INTEGER - Размер блока SCST в КБ
- -s, --size INTEGER - Размер тома в Байтах

Пример:
```
[https://localhost/] storage> create-lun -p pool-Cvy3 -a File -t regular -s 1000000000
```

Результат: Создан том (lun-<id>); появляется в get-lun-list; детали доступны через get-lun.

После создания тома на экране отобразится таблица с параметрами (рисунок 8.19):

Рисунок 8.19 – Отображение созданного тома

10. delete-lun - Удаление логического тома

Назначение: Удаляет логический том по его ID.

Синтаксис:

```
delete-lun -i <lun_id>
```

Параметры:

- -i, --id TEXT - ID тома для удаления (обязательный)

Пример:

```
[https://localhost/] storage> delete-lun -i lun-001
```

Результат: Том удалён; пропадает из get-lun-list; get-lun по id возвращает ошибку/не найден.

11. update-lun-size - Расширение тома с блочным доступом

Назначение: Обновляет размер тома с блочным доступом (LUN).

Синтаксис:

```
update-lun-size -i <ID> [-s <размер в байтах>]
```

Параметры:

- -i, --id - ID тома (обязательный)
- -s, --size - Новый размер в байтах

Пример:

```
[https://localhost/] storage> update-lun-size -i lun-ifz4 -s 2001000000
```

Результат: Сообщение об успешном обновлении размера тома.

12. get-lun - Получение информации о томе

Назначение: Получает детальную информацию о конкретном логическом томе.
Синтаксис:

```
get-lun -i <lun_id>
```

Параметры:
- -i, --id TEXT - ID тома для получения информации (обязательный)

Пример:
```
[https://localhost/] storage> get-lun -i lun-001
```

Результат: Детальная информация по тому: размер, тип (thin/regular), access (Block/File), статус.

13. get-lun-list - Список томов

Назначение: Выводит список всех логических томов в системе.

Синтаксис:
```
get-lun-list
```

Пример:
```
[https://localhost/] storage> get-lun-list
```

Результат: Вывод списка томов (lun-<id>) с основными параметрами.

14. create-snapshot - Создание снапшота

Назначение: Создает снапшот указанного тома.

Синтаксис:
```
create-snapshot -l <lunId> -n "snap1"
```

Параметры:
- -l, --lun-id TEXT - ID тома (обязательный)
- -n, --name TEXT - Имя снапшота (обязательный)

Пример:
```
[https://localhost/] storage> create-snapshot -l lun-123 -n "snap1"
```

Результат: Создан снапшот; появляется в get-snapshot-list; привязан к указанному lun-id.

15. get-snapshot-list - Список снапшотов

Назначение: Выводит список всех снапшотов в системе.

Синтаксис:

```
get-snapshot-list
```

Пример:

```
[https://localhost/] storage> get-snapshot-list
```

Результат: Вывод списка снапшотов (snapshot-<id>) с привязкой к томам.

16. get-snapshot - Информация о снапшоте

Назначение: Получает детальную информацию о конкретном снапшоте.

Синтаксис:

```
get-snapshot -i <snapshotId>
```

Параметры:

- -i, --id TEXT - ID снапшота (обязательный)

Пример:

```
[https://localhost/] storage> get-snapshot -i snapshot-001
```

Результат: Детальная информация по снапшоту.

17. clone-snapshot - Клонирование снапшота

Назначение: Создает новый том из снапшота.

Синтаксис:

```
clone-snapshot -s <snapshotId> -n "clone1"
```

Параметры:

- -s, --snapshot-id TEXT - ID снапшота (обязательный)
- -n, --name TEXT - Имя нового тома (обязательный)

Пример:

```
[https://localhost/] storage> clone-snapshot -s snapshot-001 -n "clone1"
```

Результат: Создан новый том из снапшота (для THIN); появляется новый lun-<id> в get-lun-list.

18. delete-snapshot - Удаление снапшота

Назначение: Удаляет снапшот по его ID.

Синтаксис:

```
delete-snapshot -i <snapshotId>
```

Параметры:
- -i, --id TEXT - ID снапшота (обязательный)

Пример:
```
[https://localhost/] storage> delete-snapshot -i snapshot-001
```

Результат: Снапшот удалён; пропадает из get-snapshot-list.

19. create-nfs - Создание NFS экспорта

Назначение: Создает NFS экспорт для FILE-тома.

Синтаксис:
```
create-nfs -l <lunId> -n "nfs_export_1" -f "rw/ro,sync/async,secure/insecure"
```

Параметры:
- -l, --lun-id TEXT - ID тома (обязательный)
- -n, --name TEXT - Имя экспорта (обязательный)
- -f, --flags TEXT - Флаги доступа (обязательный)

Пример:
```
[https://localhost/] storage> create-nfs -l lun-123 -n "nfs_export_1" -f "rw,sync,secure"
```

Результат: Создан NFS экспорт; появляется в get-nfs-list; связан с FILE-томом. Для Block-тома ожидается ошибка.

20. get-nfs-list - Список NFS экспортов

Назначение: Выводит список всех NFS экспортов в системе.

Синтаксис:
```
get-nfs-list
```

Пример:
```
[https://localhost/] storage> get-nfs-list
```

Результат: Вывод списка NFS экспортов (<nfsId>).

21. get-nfs - Информация об NFS экспорте

Назначение: Получает детальную информацию о конкретном NFS экспорте.

Синтаксис:

```
get-nfs -i <nfsId>
```

Параметры:

- -i, --id TEXT - ID NFS экспорта (обязательный)

Пример:

```
[https://localhost/] storage> get-nfs -i nfs-001
```

Результат: Детальная информация по NFS экспорту (lun-id/имя/флаги и др.).

22. update-nfs - Обновление NFS экспорта

Назначение: Обновляет параметры NFS экспорта.

Синтаксис:

```
update-nfs -i <nfsId>
```

Параметры:

- -i, --id TEXT - ID NFS экспорта (обязательный)

Результат: Предлагается контекстное меню с выбором default_flags/groups и далее можно поменять поля.

23. delete-nfs - Удаление NFS экспорта

Назначение: Удаляет NFS экспорт по его ID.

Синтаксис:

```
delete-nfs -i <nfsId>
```

Параметры:

- -i, --id TEXT - ID NFS экспорта (обязательный)

Пример:

```
[https://localhost/] storage> delete-nfs -i nfs-001
```

Результат: Экспорт удалён; пропадает из get-nfs-list.

24. get-net-list - Список сетевых интерфейсов

Назначение: Выводит список всех сетевых интерфейсов в системе.

Синтаксис:

```
get-net-list
```

Пример:

```
[https://localhost/] storage> get-net-list
```

Результат: Вывод списка сетевых интерфейсов (<netId>) с адресацией/статусом.

25. get-net - Информация о сетевом интерфейсе

Назначение: Получает детальную информацию о конкретном сетевом интерфейсе.

Синтаксис:

```
get-net -i <netId>
```

Параметры:

- -i, --id TEXT - ID сетевого интерфейса (обязательный)

Пример:

```
[https://localhost/] storage> get-net -i net-001
```

Результат: Детальная информация по конкретному интерфейсу.

26. create-user - Создание пользователя

Назначение: Создает нового пользователя системы.

Синтаксис:

```
create-user -n <имя> -l <логин> -r [admin|operator|readonly] [-p [CLI]]
```

Параметры:

- -n, --name TEXT - Имя пользователя (обязательный)
- -l, --login - Логин (ID) пользователя (обязательный)
- -p, --permission TEXT - Права доступа (обязательный)
- -r, --role TEXT - Роль пользователя (обязательный)

Пример:

```
[https://localhost/] storage> create-user -l ivanovi -n 'Ivan' -r 'readonly' -p CLI
```

Результат: Создан пользователь; появляется в get-user-list с указанными permission/role.

27. get-user-list - Список пользователей

Назначение: Выводит список всех пользователей системы.

Синтаксис:

```
get-user-list
```

Пример:

```
[https://localhost/] storage> get-user-list
```

Результат: Вывод списка пользователей (<userId>) с ролями/правами.

28. get-user - Информация о пользователе

Назначение: Получает детальную информацию о конкретном пользователе.

Синтаксис:

```
get-user -i <userId>
```

Параметры:

- -i, --id TEXT - ID пользователя (обязательный)

Пример:

```
[https://localhost/] storage> get-user -i user-001
```

Результат: Детальная информация по пользователю.

29. update-user - Обновление пользователя

Назначение: Обновляет данные пользователя.

Синтаксис:

```
update-user -i <ID> [-n <имя>] [-p [CLI]] [-r [admin|operator|readonly]] [-l <true|false>]
```

Параметры:

- -i, --id TEXT - ID пользователя (обязательный)
- -n, --name TEXT - Новое имя пользователя
- -r, --role TEXT - Новая роль
- -p, --permission TEXT - Новые права доступа
- -l, --locked - Блокировка пользователя (true/false)

Пример:

```
https://localhost/] storage> update-user -i user -l true
```

Результат: Поля пользователя обновлены; изменения видны в get-user.

30. update-user-password - Обновление пароля пользователя

Назначение: Обновляет пароль пользователя.

Синтаксис:

```
update-user-password -i <userId>
```

Параметры:

- -i, --id TEXT - ID пользователя (обязательный)

Пример:

```
[https://localhost/] storage> update-user-password -i user-001
```

Результат: Пароль пользователя обновлён (обычно через интерактивный ввод); вход с новым паролем успешен, со старым - нет.

31. delete-user - Удаление пользователя

Назначение: Удаляет пользователя по его ID.
Синтаксис:

```
delete-user -i user-<id>
```

Параметры:

- -i, --id TEXT - ID пользователя (обязательный)

Пример:

```
[https://localhost/] storage> delete-user -i user-001
```

Результат: Пользователь удалён; пропадает из get-user-list.

32. get-drive-list - Список дисков

Назначение: Выводит список всех физических дисков в системе.

Синтаксис:

```
get-drive-list
```

Пример:

```
[https://localhost/] storage> get-drive-list
```

Результат: Вывод списка дисков (drive-<id>) с состоянием/ёмкостью/привязкой.

33. get-system - Информация о системе

Назначение: Выводит общую информацию о системе хранения данных.

Синтаксис:

```
get-system
```

Пример:

```
[https://localhost/] storage> get-system
```

Результат: Вывод health узлов системы.

34. get-auth-security-config - Получение конфигурации политики безопасности

Назначение: Выводит текущую конфигурацию политики безопасности системы аутентификации.

Синтаксис:

```
get-auth-security-config
```

Пример:

```
[https://localhost/] storage> get-auth-security-config
```

Результат: Вывод текущей конфигурации политики безопасности аутентификации.

35. update-auth-security-config - Обновление конфигурации политики безопасности

Назначение: Частично обновляет конфигурацию политики безопасности системы аутентификации. Указываются только изменяемые параметры.

Синтаксис:

```
update-auth-security-config [--max-failed-attempts <0-10>] [--login-throttle-ttl-minutes <1-1440>] [--jwt-expiration-time-minutes <1-43200>] [--password-policy-min-length <1-64>] [--password-policy-require-uppercase <true|false>] [--password-policy-require-lowercase <true|false>] [--password-policy-require-numbers <true|false>] [--password-policy-require-special-chars <true|false>] [--password-policy-expiry-days <0-365>] [--password-policy-notification-days <0-30>]
```

Параметры:

- max-failed-attempts - Максимальное количество неудачных попыток входа (0-10)
- login-throttle-ttl-minutes - Время блокировки при переборе в минутах (1-1440)
- jwt-expiration-time-minutes - Время жизни JWT токена в минутах (1-43200)
- password-policy-min-length - Минимальная длина пароля (1-64)
- password-policy-require-uppercase - Требовать заглавные буквы (true/false)
- password-policy-require-lowercase - Требовать строчные буквы (true/false)
- password-policy-require-numbers - Требовать цифры (true/false)

- password-policy-require-special-chars - Требовать спецсимволы (true/false)
- password-policy-expiry-days - Срок действия пароля в днях (0-365)
- password-policy-notification-days - Уведомление до истечения в днях (0-30)

Пример:

```
[https://localhost/] storage> update-auth-security-config --jwt-expiration-time-minutes 120
```

Результат: Вывод обновлённой конфигурации политики безопасности аутентификации.

12.5.3 СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

Сценарий 1: Создание пула и тома

1. Получить список доступных дисков:

```
[https://localhost/] storage> get-drive-list
```

2. Создать пул RAID 5:

```
[https://localhost/] storage> create-pool -e mdraid --node-id 1 -l 5 \
  -d drive-<id1> -d drive-<id2> -d drive-<id3> -d drive-<id4> \
  --strip-size 64 --no-thin --no-vdo -n "PrimaryPool"
```

3. Создать тонкий том в пуле:

```
[https://localhost/] storage> create-lun -p pool-<id> -a Block -n "VMStorage" -t thin -s
100000000000
```

Сценарий 2: Расширение пула

1. Проверить текущее состояние пула:

```
[https://localhost/] storage> get-pool -i pool-001
```

2. Добавить новый диск:

```
[https://localhost/] storage> add-drive -i pool-001 -d disk-005
```

Сценарий 3: Управление томами

1. Просмотреть все тома:

```
  [https://localhost/] storage> get-lun-list
```

2. Получить детали тома:

```
[https://localhost/] storage> get-lun -i lun-001
```

3. Удалить неиспользуемый том:

```
[https://localhost/] storage> delete-lun -i lun-002
```

ПРИМЕЧАНИЕ.

1. Обязательные параметры: Все команды, требующие ID, имеют обязательный параметр -i или --id

2. Повторяемые параметры: В команде create-pool параметр -d можно указывать несколько раз для добавления нескольких дисков

3. Флаги: Параметры типа --thin / --no-thin являются переключателями (используйте --thin для включения, --no-thin для выключения)

4. Единицы измерения:

- Размер полосы: указывается в КБ
- Размер тома: указывается в байтах

5. Типы доступа: Для томов доступны два типа доступа - Block (блочный) и File (файловый)

Справка (помощь в работе с командами):

Для любой команды можно получить подробную справку с помощью параметра --help:

```
[https://localhost/] storage> <command_name> --help
```

Для вывода общего списка команд используйте:

```
[https://localhost/] storage> help
```

12.5.4 ДОСТУП К «CLI»

Доступ к CLI выдаётся оператором или администратором (см раздел 1.5 Ролевой доступ) себе, другому оператору или гостю. Доступ выставляется в окне «Пользовательские настройки» выбранного пользователя в разделе «Ролевой доступ». (рисунок 12.20)

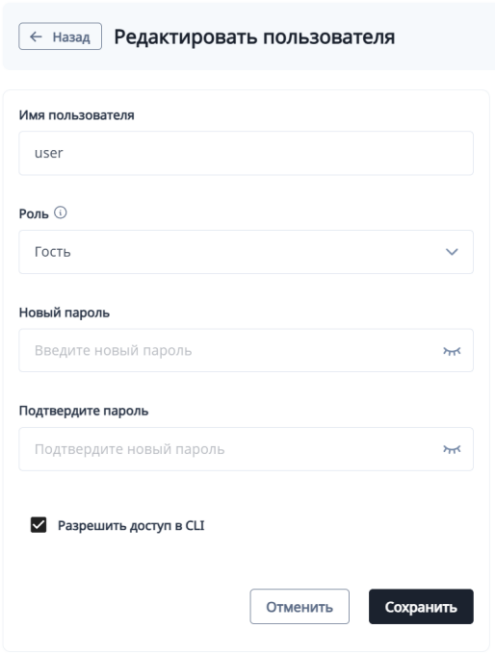


Рисунок 12.20 – Предоставление доступа к CLI в разделе «Ролевой доступ»

Чтобы разрешить доступ необходимо поставить галочку около строки «Разрешить доступ к CLI»☑. Для отключения галочку нужно снять.

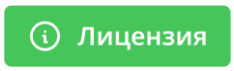
13 ЛИЦЕНЗИРОВАНИЕ

ПРИМЕЧАНИЕ

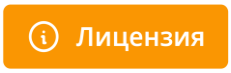
В случае приобретения ПО BlazeX в составе ПАК, лицензия должна быть активирована на период, определенный договором.

В случае, если система требует активации лицензии для полноценной работы. Лицензия генерируется с учетом характеристик оборудования и сроком действия, и должна быть получена у службы поддержки производителя.

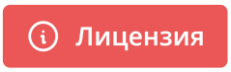
В интерфейсе состояние лицензии отображается цветом специальной кнопки:



Зеленый - лицензия действительна, все функции системы доступны.



Оранжевый - срок действия подходит к концу, требуется продление;



Красный - лицензия отсутствует или недействительна, система работает в режиме "Только чтение".

Для активации лицензии, необходимо выполнить следующее:

1. Нажмите на кнопку «Лицензия», расположенную рядом с логотипом ПО.

Рисунок 13.1 – Отображение состояния лицензии до активации

2. В открывшемся окне, во вкладке «Активация» скопируйте содержимое области «Спецификация СХД» с помощью кнопки с иконкой «копировать», как показано на рисунке 13.2.

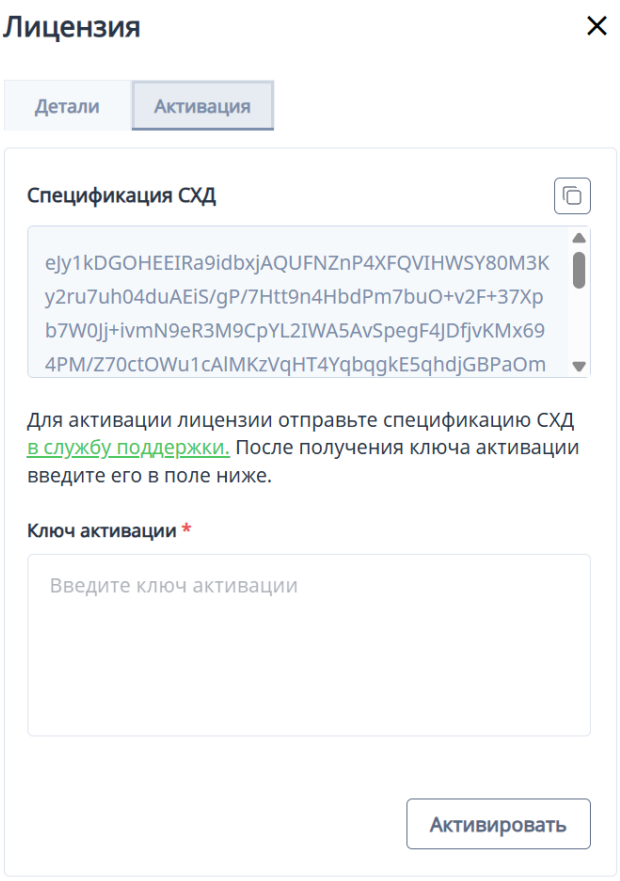


Рисунок 13.2 – Вкладка «Активация» в окне «Лицензия»

3. Передайте эту строку в службу поддержки для генерации лицензионного ключа. В разделе «Управление заявками» и создайте новую, выбрав категорию «Лицензия», темой обращения укажите, например: «Сгенерировать ключ лицензии BlazeX для активации», как показано на рисунке 13.3.

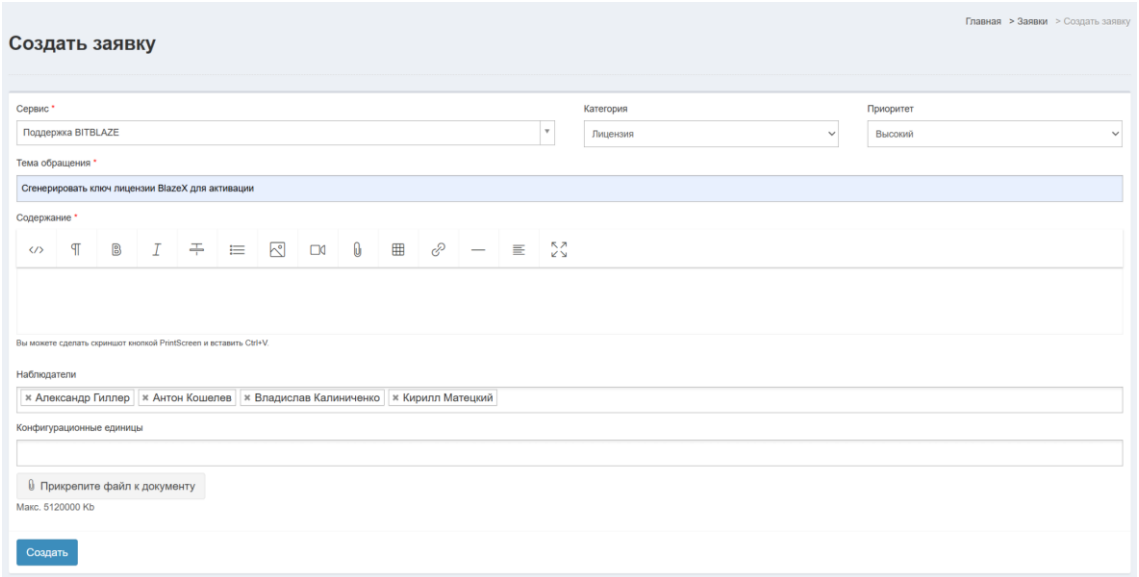


Рисунок 13.3 – Отображение состояния лицензии до активации

4. Полученный ключ введите на вкладке «Активация» в поле «Ключ активации».

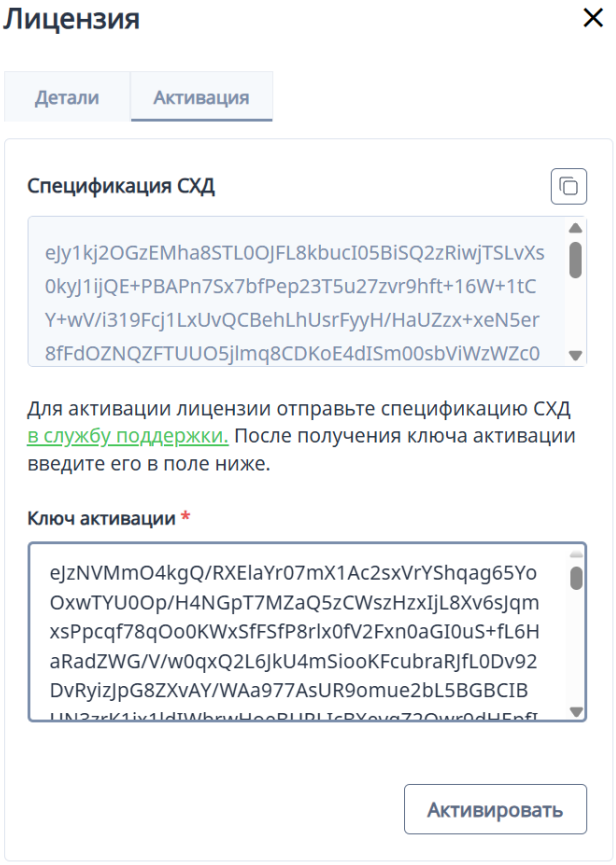


Рисунок 13.4 – Отображение состояния лицензии до активации

5. Нажмите кнопку «Активировать».

Рисунок 13.5 – Отображение состояния лицензии до активации

6. В случае успешной активации лицензии цвет кнопки должен измениться на зеленый, в разделе «Детали» должна появиться следующая информация:
   - Дата окончания действия лицензии
   - Оставшийся период
   - Статус лицензии на каждом из узлов «Лицензия активна»

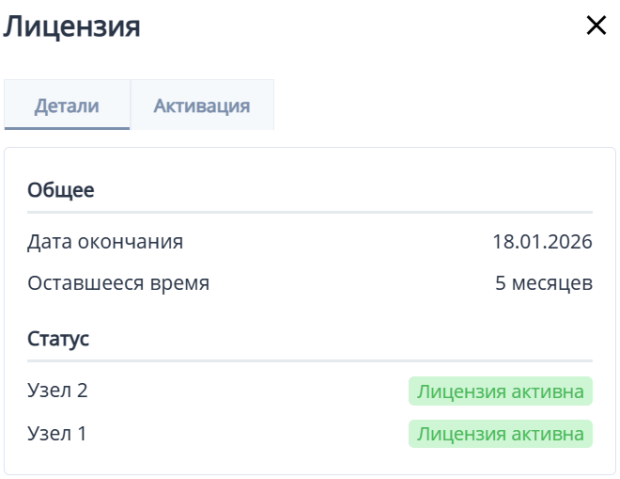


Рисунок 13.6 – Раздел «Детали» при успешной активации лицензии

Если лицензия не активирована:

- Система автоматически переходит в режим «Только чтение» - создание новых групп будет недоступно;
- Доступ к страницам интерфейса сохраняется для просмотра информации.

Для продления необходимо повторить процедуру получения лицензии.

14 ПАНЕЛЬ СТАТУСОВ СИСТЕМЫ

В верхней части страницы располагается панель глобального состояния, которая отображает текущий статус работы СХД и синхронизации между узлами, отображение которой в рабочем состоянии отсутствует. При возникновении проблем с синхронизацией система может автоматически переключить оба узла в режим «Только чтение» (Read-Only), чтобы предотвратить повреждение данных. Отображаются сообщения следующим образом (рисунок 14.1)

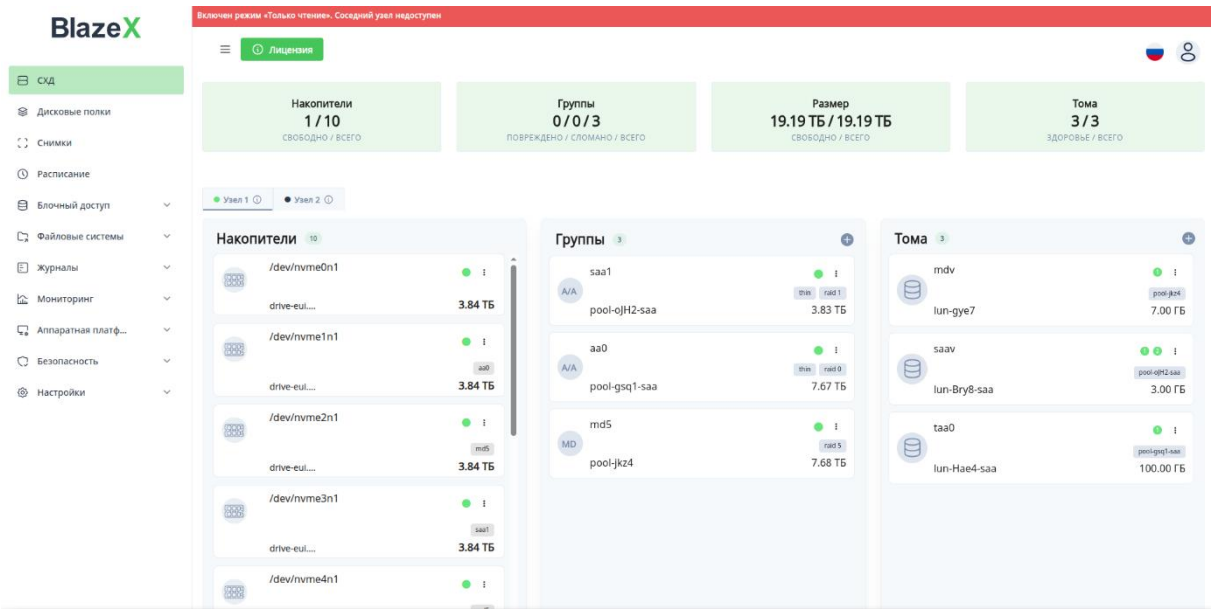


Рисунок 14.1 – Отображение состояния системы

Режим «Только чтение»
Когда нарушается связь или синхронизация между узлами, система переходит в безопасный режим «Только чтение». В этом режиме все операции записи, изменения конфигурации и удаление данных блокируются. Можно только просматривать данные и текущие настройки.

Система отображает один из трех вариантов сообщения, поясняющих причину перехода в режим «Только чтение».

1. Ожидание синхронизации

Сообщение	Включен режим «Только чтение». Дождитесь синхронизации узлов
Значение	Система находится в процессе автоматического восстановления и сверки конфигураций (хэшей). Это временное состояние.
Цветовая индикация	Включен режим «Только чтение». Дождитесь синхронизации узлов
Действия администратора	**Никаких действий не требуется.** Необходимо просто дождаться окончания процесса синхронизации. После

успешного завершения система автоматически вернется в полнофункциональный режим.

2. Потеря связи с соседним узлом

Сообщение	Включен режим «Только чтение». Соседний узел недоступен
Значение	Связь между узлами потеряна (статус **LostRemote**). Второй узел не отвечает, поэтому синхронизация невозможна.
Цветовая индикация	Включен режим «Только чтение». Соседний узел недоступен
Действия администратора	1. Проверить, включен ли соседний узел. 2. Проверить сетевое соединение между узлами (кабели, коммутаторы, IP-адреса). 3. После восстановления связи процесс синхронизации должен запуститься автоматически.

3. Ошибка синхронизации

Сообщение	Включен режим «Только чтение». Ошибка синхронизации узлов. Обратитесь в техническую поддержку.
Значение	Связь между узлами есть, но их конфигурации разошлись (статус **ManualFix**), и автоматическая синхронизация невозможна. Это нештатная ситуация.
Цветовая индикация	Включен режим «Только чтение». Ошибка синхронизации узлов. Обратитесь в техническую поддержку.
Действия администратора	**Самостоятельное исправление невозможно.** Не пытайтесь вручную изменять конфигурацию, чтобы не усугубить проблему. **Необходимо:** 1. Немедленно обратиться в **техническую поддержку**, предоставив это сообщение об ошибке. 2. Специалисты поддержки помогут вручную определить эталонную конфигурацию и восстановить работоспособность системы.

15 ПОДКЛЮЧЕНИЕ К СХД

Для подключения к ресурсам, предоставляемым СХД, можно использовать любое пользовательское ПО, корректно поддерживающее клиентские интерфейсы инициаторов iSCSI.

В случае использования ОС Linux можно использовать следующие примеры команд для подключения.

15.1 ПОДКЛЮЧЕНИЕ К ISCSI–ТАРГЕТУ

ВНИМАНИЕ! Особенности работы с двухконтроллерной версией.

Подключение к таргетам необходимо выполнять для обоих узлов.

ПРИМЕЧАНИЕ

Для подключения инициаторов к iSCSI-таргетам СХД настоятельно рекомендуется использовать статическую адресацию на обеих сторонах (как на СХД, так и на сервере-инициаторе). Применение DHCP для адресации интерфейсов, задействованных в передаче данных (Data-сеть), не рекомендуется, так как это может привести к потере связи хранилищем при смене IP-адреса и, как следствие, к сбоям в работе сервисов.

Для подключения к данному виду таргетов со стороны iSCSI–инициатора можно применять ПО «Open iSCSI». В современных дистрибутивах ОС Linux данное ПО обычно бывает предустановлено, а в случае отсутствия может быть дополнительно установлено в систему. Название установочного пакета можно уточнить в каталоге ПО репозитория ОС.

Поиск iSCSI–таргета в ЛВС выполняется следующей командой в эмуляторе терминала (команды поиска и подключения выполняется на хосте iSCSI–инициатора):

```
sudo iscsiadm –m discovery –t sendtargets –p <IP–адрес_узла>
```

Здесь и далее <IP–адрес_узла> - адрес сетевого интерфейса узла СХД в высокоскоростной ЛВС ввода–вывода.

ПРИМЕЧАНИЕ

В частном случае IP–адреса сетевых интерфейсов узла СХД в сети управления и в ЛВС ввода–вывода могут совпадать.

Отклик на вышеприведенную команду содержит название iSCSI–таргетов, к которым можно подключиться. Пример такого отклика:

```
<IP–адрес_узла>:3260,1 <название_iSCSI–таргета>
```

ПРИМЕЧАНИЕ

Вывод команды «iscsiadm –m discovery...» может включать несколько таргетов. Необходимо уточнить название нужного таргета, сравнив строки вывода с отображением таргетов в ГИП.

Пример команды для подключения к выбранному iSCSI–таргету:

```
sudo iscsiadm —mode node —targetname <название_iSCSI–таргета> \
-- portal <IP–адрес_узла> --login
```

В случае удачного подключения, в отклике на данную команду будет содержаться слово «successful», а в системе добавится новое блочное устройство.

Пример вывода в эмуляторе терминала при успешном подключении:

```
Logging in to [iface: default, target: <название_iSCSI–таргета>, portal: 192.168.84.148,3260]
Login to [iface: default, target: <название_iSCSI–таргета>, portal: 192.168.84.148,3260] successful.
```

Затем необходимо перейти на машине–инициаторе в каталог /etc/iscsi и открыть файл iscsid.conf. Найти и раскомментировать опцию:

```
node.startup = automatic
```

После этого необходимо закомментировать следующий пункт и сохранить изменения:

```
node.startup = manual
```

Более подробное описание ПО «Open iSCSI» и другие примеры команд можно найти в документации. Для вызова man–страниц в эмуляторе терминала необходимо использовать следующую команду:

```
man iscsiadm
```

В случае переустановки ПО на СХД могут быть удалены таргеты. Повторное отображение будет выдавать ошибку. В случае если в базе данных инициатора осталась запись о несуществующем (удаленном) таргете, можно удалить его из базы данных при помощи следующей команды:

```
iscsiadm –m discoverydb –t sendtargets –p <IP>:<порт> –o delete
```

После этого необходимо будет проверить файловую систему, чтобы убедиться, что Linux не попытается восстановить соединение при будущих операциях загрузки:

```
ls /var/lib/iscsi/nodes/<iqn>
```

15.2 ПОДКЛЮЧЕНИЕ К ЭКСПОРТУ NFS

Для подключения к экспорту необходимо выполнить следующие действия:

1. Создать экспорт NFS и группы клиентов в ГИП ПО BlazeX.
2. Установить пакет NFS версии 3 и выше, на стороне инициатора:

```
sudo apt install nfs-common
```

3. Подключить файловый том на стороне инициатора выполнив команду:

```
mount -t nfs <IP–адрес_узла>:<Путь экспорта> <Папка монтирования>
```

ПРИМЕЧАНИЕ

- IP–адрес_узла отображен в ГИП, в разделе «СХД», в окне «Информация» на вкладке «Узел», на котором расположен экспортируемый том;
- Путь экспорта отображен в ГИП в разделе «Экспорты NFS», далее « NFS», таблица «Экспорты NFS» в строке подключаемого экспорта, в колонке «Путь экспорта».

ВНИМАНИЕ!
Папка монтирования должна обладать правами на чтение-запись.

Для проверки подключения необходимо следующее:

1. Выполнить команду:

```
df -h
```

2. Проверить вывод. В выводе команды должны отобразиться данные в следующем формате:

```
Filesystem                              Size  Used Avail Use% Mounted on
<IP–адрес_узла>:<Путь экспорта>  000M  00M 000M  0%  <Папка монтирования>
```

15.3 УПРАВЛЕНИЕ ЧЕРЕЗ REST API

ПО «BlazeX» поддерживает интерфейс внешнего управления API (*англ*. Application Programming Interface, API) по типу HTTP REST.

Назначение API: обработка команд управления СХД, формируемых внешним ПО.

Для получения описания API требуется выполнить следующие действия:

1. Открыть в браузере страницу:

```
https://<IP–адрес_узла>/api/
```

На данной странице отображается интерактивная документация BlazeX API (см. рисунок 15.1), содержащая описание типов и компонентов HTTP–запросов. Встроенная функциональность позволяет отправлять пробные запросы к API (кнопка «Try it out») и анализировать возвращаемые ответы.

ПРИМЕЧАНИЕ

Чтобы отправлять пробные запросы, необходимо авторизоваться в «Swagger»:

1. Отправить пост запрос в разделе auth - POST: /api/v2/auth/login;
2. В теле запроса указать актуальный логин и пароль в кавычках;
3. Затем в ответе запроса скопировать токен (без кавычек);
4. Кликнуть по кнопке "Authorize";
5. В открывшемся окне "Available authorizations" ввести скопированный токе в поле "Value:";
6. Нажать на кнопку "Authorize".

Если пропустить этап авторизации, на все отправленные запросы будет приходить 401 код ошибки (неавторизован).

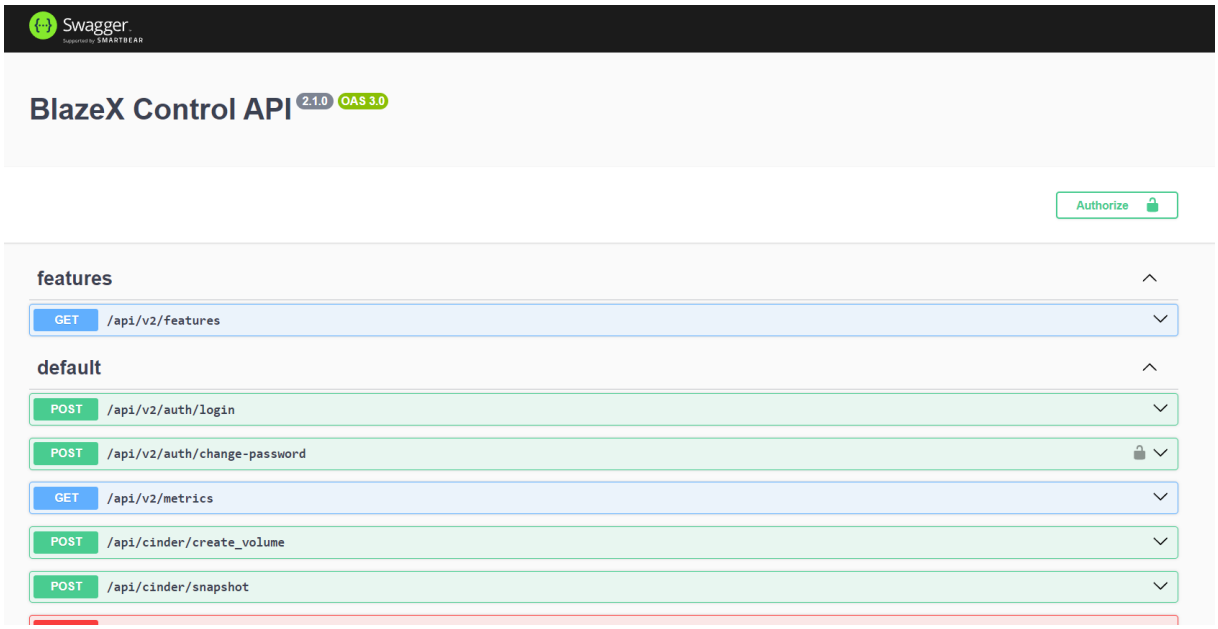


Рисунок 15.1 – Интерактивная документация BlazeX API

СОКРАЩЕНИЯ

ВМ - виртуальная машина.

ГИП - графический пользовательский интерфейс.

ОС - операционная система.

ПАК - программно–аппаратный комплекс.

ПК - персональный компьютер.

ПО - программное обеспечение.

СХД - система хранения данных.

ALUA - Asymmetric Logical Units Access.

API - Application Programming Interface.

e2k - архитектура Эльбрус 8СВ.

FC - Fibre Channel.

FTP - File Transfer Protocol.

GiB - Гибибайт.

HDD - Hard Disk Drive.

IP - Internet Protocol.

iSCSI - Internet Small Computer System Interface.

IQN - ISCSI Qualified Name

KiB - Кибибайт.

LUN - Logical Unit Number.

MiB - Мибибайт.

NAS - Network Attached Storage.

NFS - Network File System.

NVMe - Non–Volatile Memory Host Controller Interface Specification.

NVMe–oF - NVMe over Fabric.

PCI Express - Peripheral Component Interconnect Express.

RAID - Redundant Array of Independent Disks.

RDMA - Remote Direct Memory Access.

REST API - Representational State Transfer API.

SAN - Storage Area Network.

SSD - Solid State Drive.

SSL - Secure Sockets Layer.

TCP - Transmission Control Protocol.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Asymmetric Logical Units Access (ALUA) - технология управления путями доступа к томам (LUN), при которой все контроллеры системы хранения видимы, но могут иметь разный приоритет и производительность. Один их путей является оптимальным (active optimized), второй - неоптимальным (active non-optimized) и используется только в случае отказа или перегрузки оптимального пути.

Active/Active - Режим, в котором все контроллеры системы хранения могут одновременно обслуживать ввод-вывод к одному и тому же тому (LUN) с одинаковой производительностью и приоритетом. Обеспечивает постоянную балансировку нагрузки между контроллерами, что повышает общую пропускную способность. При отказе любого контроллера оставшиеся продолжают обслуживать запросы без переключений и деградаций.

BlazeX OpenStack Cinder API - программный интерфейс для предоставления возможности взаимодействия с компонентом управления блочными устройствами Cinder в ПО виртуализации OpenStack.

BlazeIO - драйвер под управлением утилиты "blazeio–ctl", с повышенной производительностью при записи, и поддержкой отказов до 4 накопителей одновременно

Fibre Channel (FC) - протокол подключения блочного устройства (диска) по оптоволоконному каналу.

GiB (Гибибайт), MiB (Мибибайт), KiB (Кибибайт) - единицы измерения емкости в вычислительной технике, основанные на двоичной системе счисления.

Hard Disk Drive (HDD) - устройство для хранения данных, использующее магнитный метод записи.

IP–адрес - уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP.

Internet Small Computer System Interface (iSCSI) - протокол подключения блочного устройства (диска) по сети передачи данных TCP\IP.

ISCSI Qualified Name (IQN) - iSCSI–типизированные имена. Полное имя участников взаимодействия - инициатора и таргета.

Logical Unit Number (LUN) - уникальный идентификатор, используемый для обозначения логического устройства в системах хранения данных, работающих по протоколу SCSI (Small Computer System Interface) или других протоколах, которые инкапсулируют SCSI, таких как Fibre Channel или iSCSI.

MDRAID - драйвер под управлением утилиты «mdadm».

Network File System (NFS) - протокол удаленного файлового доступа к данным.

Non–Volatile Memory Host Controller Interface Specification (NVMe) - интерфейс доступа к твердотельным накопителям, подключённым по шине PCI Express. «NVM» в названии спецификации обозначает энергонезависимую память, в качестве которой в SSD повсеместно используется флеш–память типа NAND. Основные цели создания NVMe - получение низких задержек и эффективное использование высокого параллелизма твердотельных накопителей за счет применения нового набора команд и механизма обработки очередей, оптимизированного для работы с современными многоядерными процессорами.

NVMe over Fabric (NVMe–oF) - стандарт, который позволяет использовать преимущества NVMe накопителей в масштабе сети дата–центра. Он использует технологии Ethernet, Fiber Channel, RoCE и InfiniBand для передачи данных между накопителями и приложениями на серверах.

OpenStack Cinder API - программный интерфейс для взаимодействия с сервисом хранения блоков (Block Storage) в OpenStack. Этот API позволяет создавать, управлять и использовать тома (volumes) для различных виртуальных машин, физических серверов и контейнеров.

Peripheral Component Interconnect Express (PCI Express) - компьютерная шина, использующая программную модель шины PCI и высокопроизводительный физический протокол, основанный на последовательной передаче данных.

Redundant Array of Independent Disks (RAID) - технология виртуализации хранения данных, которая объединяет несколько физических дисковых устройств в одну или несколько логических единиц для повышения надежности, производительности или обоих этих показателей одновременно.

Remote Direct Memory Access (удалённый прямой доступ к памяти, RDMA) - аппаратное решение для обеспечения прямого доступа к оперативной памяти другого компьютера при помощи высокоскоростной сети.

Representational State Transfer API (REST API) - архитектурный стиль для создания веб–интерфейсов, который позволяет различным приложениям обмениваться данными через Интернет.

SCSI Target Subsystem (SCST) - набор драйверов ядра Linux, реализующих функциональность SCSI–таргета.

Solid State Drive (SSD) - компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти, альтернатива жёстким дискам (HDD).

Размер блока (Strip size) - объем данных, записываемый RAID контроллером на один диск в рамках одной полосы.

Transmission Control Protocol (TCP) - протокол управления передачей, один из основных протоколов передачи данных интернета. Пакеты в TCP называются сегментами.

Thin provisioning - метод динамического распределения дискового пространства, технология виртуализации систем хранения данных, которая позволяет увеличить

эффективность использования ресурсов системы хранения. Эта технология необходима для уменьшения использования дискового пространства, которое непосредственно не используется для хранения данных приложений.

Виртуальная машина (ВМ) - это виртуальный компьютер, который использует выделенные ресурсы реального компьютера (процессор, диск, адаптер). Эти ресурсы хранятся в облаке и позволяют ВМ работать автономно.

Графический пользовательский интерфейс (ГИП, англ. GUI) - система интерактивных визуальных компонентов для компьютерного программного обеспечения, позволяющая пользователям взаимодействовать с электронными устройствами через визуальные индикаторы и метафоры.

Группа инициаторов - логическое объединение инициаторов (хостов или серверов) для централизованного управления доступом к томам хранилища. Позволяет назначать права доступа группам серверов одновременно, упрощая администрирование и повышая безопасность.

Гипервизор - программное обеспечение, которое позволяет запускать несколько виртуальных машин (ВМ) на одном физическом сервере, обеспечивая совместное использование физических ресурсов.

Дедупликация - технология устранения избыточных дублирующихся данных. Позволяет существенно сократить требуемый объем хранилища для повторяющихся данных.

Дистрибутив - комплект программного обеспечения, который содержит все необходимые файлы, архивы и другие компоненты для установки и запуска программы или операционной системы.

Инициатор - клиентский компонент, который инициирует подключение к системе хранения. Устанавливает соединение с таргетом.

Клон (англ. snapclone) - технология создания снимков данных с возможностью их использования в качестве полноценных клонов. Сочетает преимущества снапшотов (моментальное создание) и клонов (независимость от оригинала). Используется для тестирования, разработки и быстрого развертывания сред.

Композитная группа - логическое объединение нескольких RAID–групп для создания единой группы хранения и расширения емкости. Позволяет более гибко управлять емкостью системы хранения и эффективнее использовать доступное дисковое пространство.

Логическая группа (англ. pool) - пул устройств хранения, в состав которого входит один или несколько физических томов.

Логический том (англ. volume) - логический раздел в группе томов, аналогичен обычном разделу, представляет из себя блочное устройство и может содержать файловую систему.

Операционная система (ОС) - программное обеспечение, управляющее компьютерами (включая микроконтроллеры) и позволяющее запускать на них прикладные программы.

Программно–аппаратный комплекс (ПАК) - интегрированная система, состоящая из технических и программных средств, работающих совместно для выполнения одной или нескольких специальных задач.

Пакет (программный пакет) - это архивный файл, содержащий все необходимые файлы и метаданные для установки и управления конкретным программным обеспечением.

Программное обеспечение (ПО) - совокупность программ, данных и связанных с ними документов, используемых для управления информационной системой (компьютером).

Сервер - выделенный вычислительный комплекс, обрабатывающий запросы от других ПК и предоставляющий им необходимую информацию и/или услуги.

Снимок (англ. snapshot) - снимок состояния блочного устройства или файловой системы в определенный момент времени. Позволяет быстро создавать точки восстановления без дублирования всех данных.

Система хранения данных (СХД) - комплекс аппаратного и программного обеспечения, предназначенный для хранения и оперативной обработки информации.

Таргет - часть системы хранения данных, предоставляющая доступ к своим ресурсам. Экспортируемый объект или целиком экспортирующий узел.

Терминал (или командная строка) - программный интерфейс, который позволяет взаимодействовать с операционной системой путем ввода текстовых команд.

Узел (англ. node) - сервер в многосерверной конфигурации, обеспечивающий доступ к ресурсам СХД.

Экспорт - доступ к файловым и блочным ресурсам. Обеспечивает передачу данных из СХД в другую систему, например, для резервного копирования, восстановления, анализа или предоставления данных другим приложениям.

Эльбрус 8СВ - процессор серверного класса с усовершенствованным набором векторных команд. Реализует аппаратную архитектуру e2k.

КОНФИГУРАЦИОННЫЙ ФАЙЛ MULTIPATH-TOOLS

Конфигурационный файл multipath-tools (multipath.conf) используется для настройки Device Mapper Multipath (DM-Multipath) механизма, который объединяет несколько физических путей (каналов) доступа к устройству хранения данных (SAN, iSCSI…) в один виртуальный диск для отказоустойчивости и повышения производительности. Один их путей является оптимальным (active optimized), второй - неоптимальным (active non-optimized) и используется только в случае отказа или перегрузки оптимального пути.

```
defaults {
	detect_prio		no
	polling_interval	5
	path_selector		"round-robin 0"
	path_checker		tur
	rr_min_io		100
	rr_weight		priorities
	failback		180
	no_path_retry		30
	user_friendly_names	yes
	checker_timeout		5
	#enable_foreign		"nvme"
}
devices {
	device {
		vendor			"BITBLAZE"
		product			"BLAZEX"
		path_grouping_policy	group_by_prio
		prio			alua
		hardware_handler	"1 alua"
		uid_attribute		ID_SERIAL
	}
	device {
		vendor			"BITBLAZE"
		product			"BLAZEX-SAA"
		path_grouping_policy	multibus
		prio			const
	}
}
#blacklist_exceptions {
#	property "(ID_SERIAL)"
#}
```

СТРУКТУРА

Секция defaults (глобальные настройки по умолчанию)

Устанавливает поведение для всех устройств, если не указано иное:

- detect_prio no - не пытаться автоматически определять приоритет путей (будет использовано ручное задание).

- polling_interval 5 - интервал проверки состояния путей (в секундах).
- path_selector "round-robin 0" - алгоритм выбора пути для ввода-вывода (Round-Robin, 0 = версия алгоритма).
- path_checker tur - метод проверки доступности пути (Test Unit Ready).
- rr_min_io 100 - количество операций ввода-вывода на один путь перед переключением (при round-robin).
- rr_weight priorities - приоритеты учитываются при распределении нагрузки.
- failback 180 - через 180 секунд после восстановления основного пути выполнить обратное переключение (failback).
- no_path_retry 30 - количество попыток повтора при отсутствии путей (30), после чего операции ввода-вывода завершаются с ошибкой.
- user_friendly_names yes - вместо WWID использовать понятные имена (например, mpathb вместо длинного идентификатора).
- checker_timeout 5 - таймаут выполнения проверки состояния (в секундах).
- #enable_foreign "nvme" - закомментированная опция для управления сторонними (foreign) устройствами, например NVMe.

Секция devices (параметры для конкретных моделей устройств)

Здесь задаются правила для определенных вендоров и продуктов.

Первый блок device (для BITBLAZE BLAZEX):

- path_grouping_policy group_by_prio - пути группируются по приоритетам (ALUA - Active/Active или Active/Passive).
- prio alua - приоритет путей определяется по стандарту ALUA (Asymmetric Logical Unit Access).
- hardware_handler "1 alua" - специальный обработчик для корректной работы с ALUA.
- uid_attribute ID_SERIAL - использовать серийный номер устройства в качестве уникального идентификатора.

Второй блок device (для BITBLAZE BLAZEX-SAA):

- path_grouping_policy multibus - все пути в одной группе (без разделения на приоритеты, просто балансировка).
- prio const - все пути имеют одинаковый (константный) приоритет.

Закомментированная секция blacklist_exceptions

Если после подключения нашей СХД диски не отобразятся, а в логах появятся ошибки вроде "sdb: blacklisted, udev property missing", и при выполнении команды multipath -v4 устройства не будут видны следует раскомментировать указанный параметр. После этого диски станут доступны.

Типичное расположение файла:

/etc/multipath.conf

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка ПО «BlazeX» включает следующий набор услуг:

- предоставление обновлений программного обеспечения по мере выхода новых релизов;
- консультация ИТ–специалистов заказчика по работе управляющего ПО;
- помощь в устранении сбоев, вызванных некорректной работой управляющего ПО
- помощь в обновлении программного продукта в удаленном режиме.

Контакты службы поддержки и сервиса:

Адрес электронной почты: help@bitblaze.ru

Интернет–сайт: https://bitblaze.tech/

Телефон компании: (3812)–36–11–11

ПРИМЕЧАНИЕ

Техническая поддержка осуществляется в рамках Соглашения об уровне сервиса (SLA).

Все гарантии, касающиеся товаров и услуг, реализуемых ООО «БитТех», изложены в формулировках прямых гарантий, сопровождающих соответствующие товары и услуги.

Никакая информация, приведенная в данном документе, не должна рассматриваться как дополнительная гарантия.