ОБНОВЛЕНО 16 МАР

Панель управления

Шаблоны

Шаблон — это готовый набор настроек, который помогает быстрее создавать профили и правила.

Шаблоны делятся на два типа:

- **Профили** – используются только при создании профилей.
- **Контрмеры** – добавляются в профили для формирования правил.

Шаблоны, связанные с базой вредоносных сигнатур, отображаются **фиолетовым цветом** и обновляются автоматически при каждом обновлении базы.

Локальные шаблоны, отображаются **белым цветом** и обновляются только вручную. Шаблоны с несохранёнными изменениями выделяются **желтым цветом**.

Профили, созданные из шаблонов, обновляются автоматически, пока связь с шаблоном не разорвана или автообновление не отключено.

Связь с шаблоном можно разорвать вручную с помощью кнопки «Разорвать связь». После этого профиль перестаёт получать обновления шаблона.

Пользователь может экспортировать, импортировать и редактировать шаблоны через соответствующие функции интерфейса.

Добавление нового шаблона

Добавление шаблона

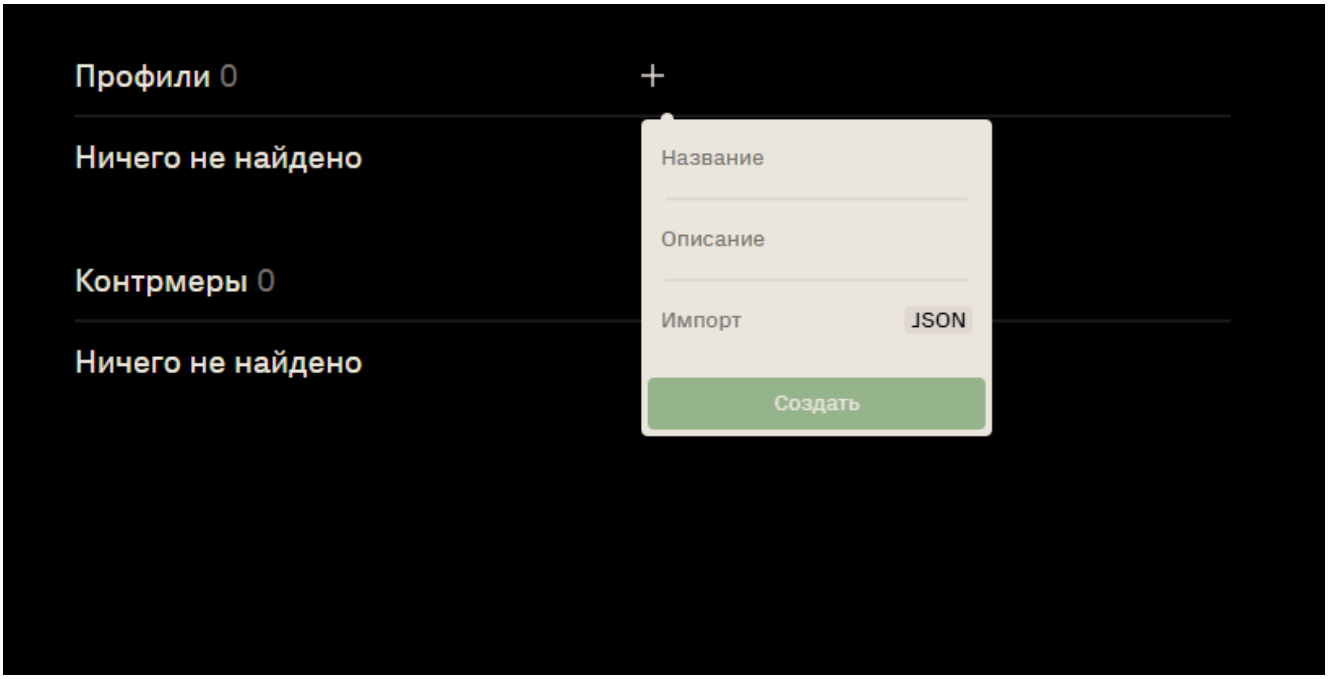
Чтобы создать шаблон, откройте раздел **Шаблоны**. В верхней части списка, рядом с заголовком **Профили**, нажать на значок серого плюса. Откроется окно для ввода параметров.

Укажите **Название**.

Примечание
Система не позволяет присваивать одинаковые названия профилям и контрмерам.

Добавьте **Описание**, указав назначение или параметры шаблона.

При наличии подготовленного JSON-файла загрузите его через кнопку **Импорт**.



Нажмите **Создать**. Новый шаблон появится в списке и будет доступен для редактирования.

Добавление контрмеры

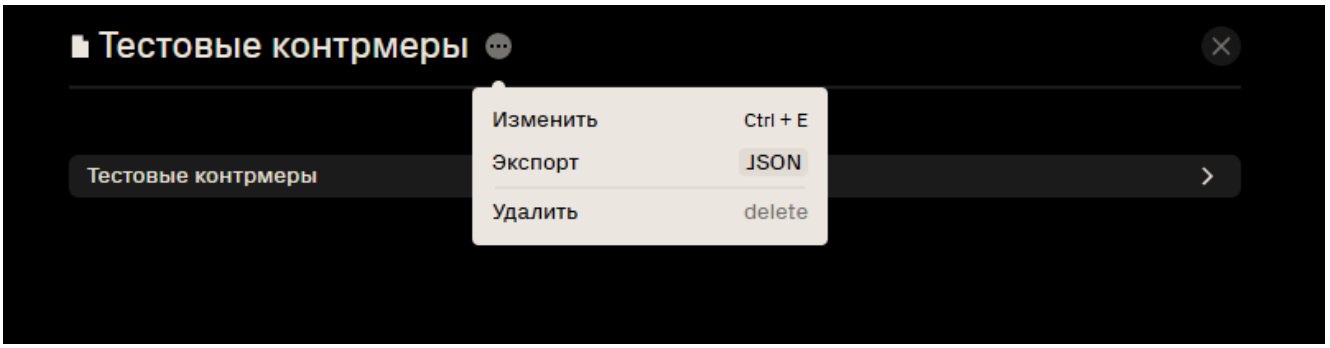
Добавление контрмер осуществляется аналогично добавлению профилей.

Редактирование шаблона

При открытии шаблона отображается интерфейс создания правил. Подробную информацию об этом процессе см. в разделе "Создать правило".

Экспорт шаблона

Чтобы экспортировать шаблон, выберите его в списке. В открывшемся меню редактирования нажмите на значок трёх точек для вызова дополнительных действий. Веберите **Экспорт**, шаблон сохранится в виде JSON-файла.



Префикс-сет

Префикс-сет — это набор IP-адресов, который используют в правилах для формирования белых и чёрных списков.

Префикс-сеты делятся на:

- **Глобальные** – распространяются на всю арену и используются во всех профилях.
- **Локальные** – применяются только в рамках конкретного профиля.

Добавление префикс-сета

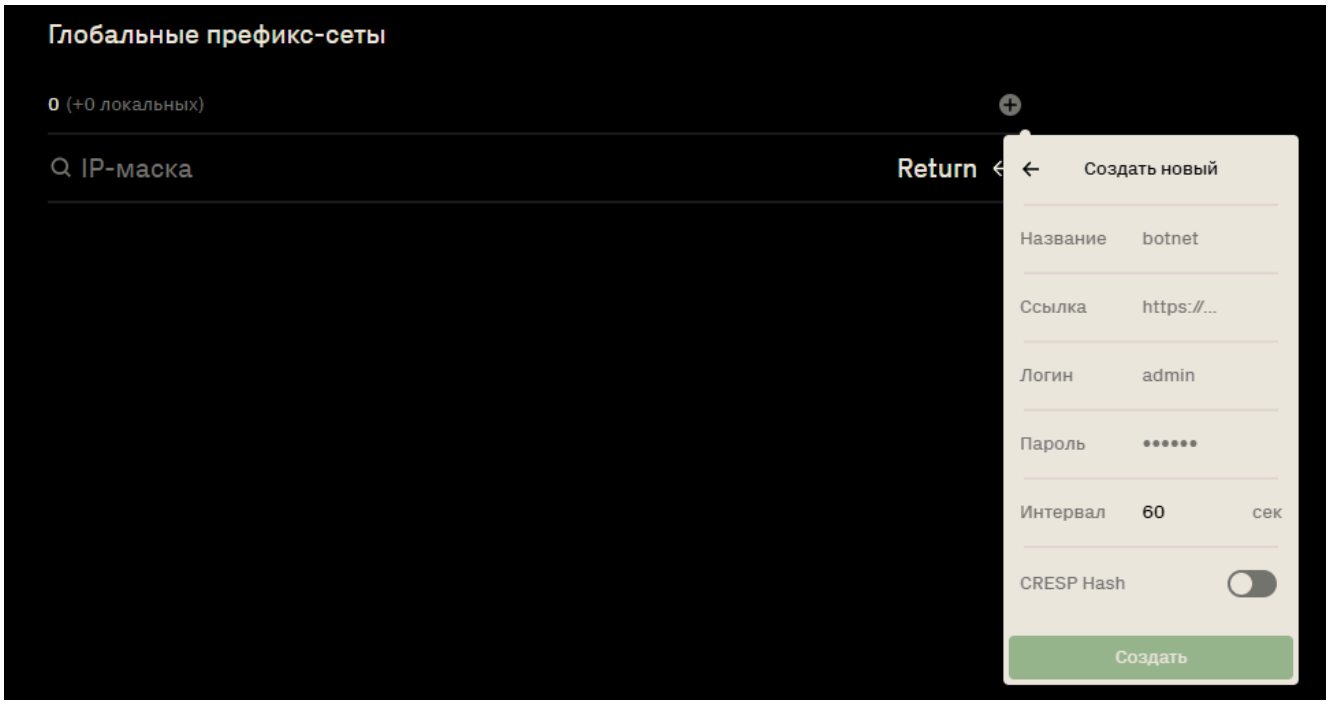
Для создания нового префикс-сета выполните следующие шаги:

- Для создания глобального префикс-сета: Перейдите в раздел **Глобальные префикс-сеты**.
- Для создания локального префикс-сета: Перейдите в раздел **Профиль** → **Префикс-сеты**.

В верхней части списка нажать значок плюса. В ниспадающем меню выбрать один из вариантов создания префикс-сета.

- **Создать новый**
  Указать имя создаваемого префикс-сета.
- **Создать по ссылке**

Префикс-сет может быть создан путем загрузки данных из внешнего источника по ссылке. Это позволяет автоматически обновлять записи в префикс-сете, используя актуальные данные, предоставленные по HTTP/HTTPS.



Для добавления префикс-сета по ссылке необходимо заполнить следующие поля:

Название – задать имя префикс-сета (например, whitelist).
Ссылка – указать URL-адрес источника списка (http/https).
Логин – ввести логин для аутентификации на удаленном ресурсе (если требуется).
Пароль – указать пароль для аутентификации (если требуется).
Интервал – задать периодичность обновления списка в секундах (например, 60).
CRESP Hash – включить обработку хешированного формата списка (используется в инсталяциях с модулем Антибот).

Нажать **Создать** для сохранения префикс-сета.

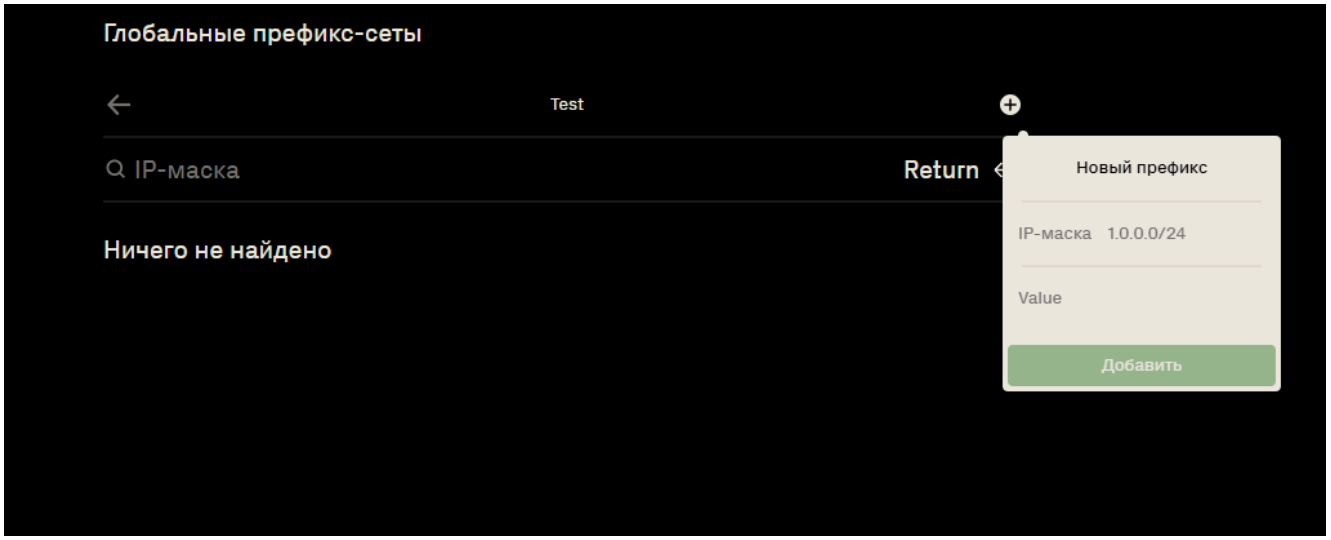
Добавление записи в префикс-сет

Префикс-сет представляет собой набор записей, каждая из которых содержит IP-префикс и value. Значение value служит идентификатором записи и используется для группировки записей при создании правил.

Value — это числовое значение, уникальное для каждой записи в префикс-сете. Оно не связано с самим префикс-сетом, а относится к конкретной записи.

В правилах фильтрации можно указывать конкретные значения value, чтобы применять правила только к соответствующим записям. Записи с одинаковым value могут быть объединены в группы для применения общих правил.

Для добавления записей в префикс-сет необходимо выбрать целевой префикс-сет и открыть его. В интерфейсе управления нажать значок плюса для добавления новой записи. В появившемся диалоговом окне указать **IP-адрес с маской** в формате `10.0.0.0/24` и задать числовое значение value, затем нажать "Добавить".



Примечание
Если при добавлении записи маска не указана, автоматически назначается маска /32.

Допустимо использовать альтернативный метод добавления записей путем перетаскивания файла формата TXT с префиксами в область таблицы, что позволит автоматически загрузить и обновить содержимое префикс-сета.

Файл должен содержать список IP-префиксов в следующем формате:

```
192.168.1.0/24
10.0.0.0/8
1.1.1.0/24
```

При отсутствии указанного value автоматически устанавливается значение 1.

Для назначения value каждой записи формат файла может быть расширен:

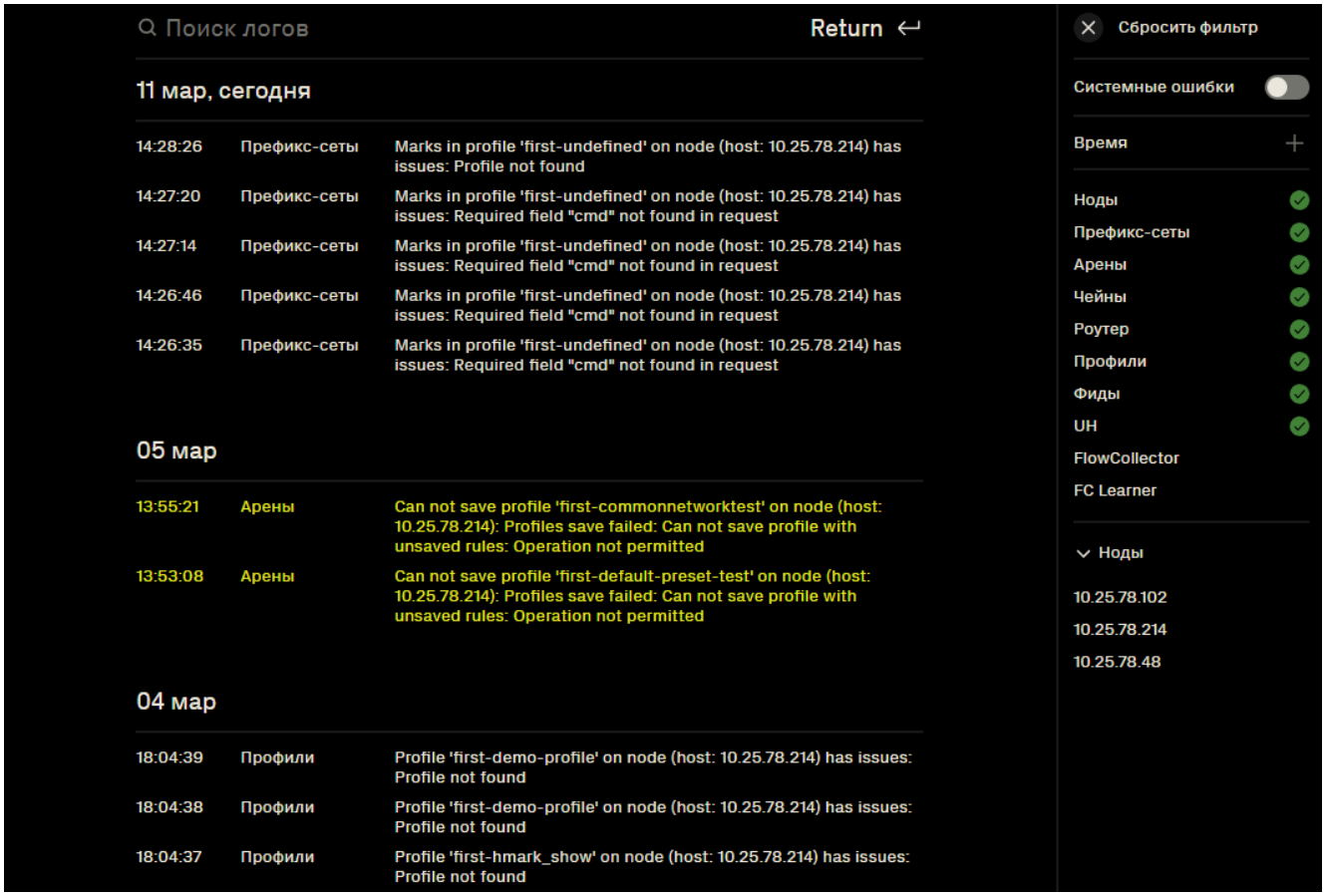
```
192.168.1.0/24  1
10.0.0.0/8      2
```

```
1.1.1.0/24      1
```

Логи и дампы

Логи

Логи предназначены для мониторинга событий, возникающих в системе, и позволяет пользователю анализировать ошибки, предупреждения и другие системные сообщения.



Поле ввода в верхней части экрана, позволяющее осуществлять поиск по записям журнала.

Список логов отображает хронологический перечень событий, включающий:

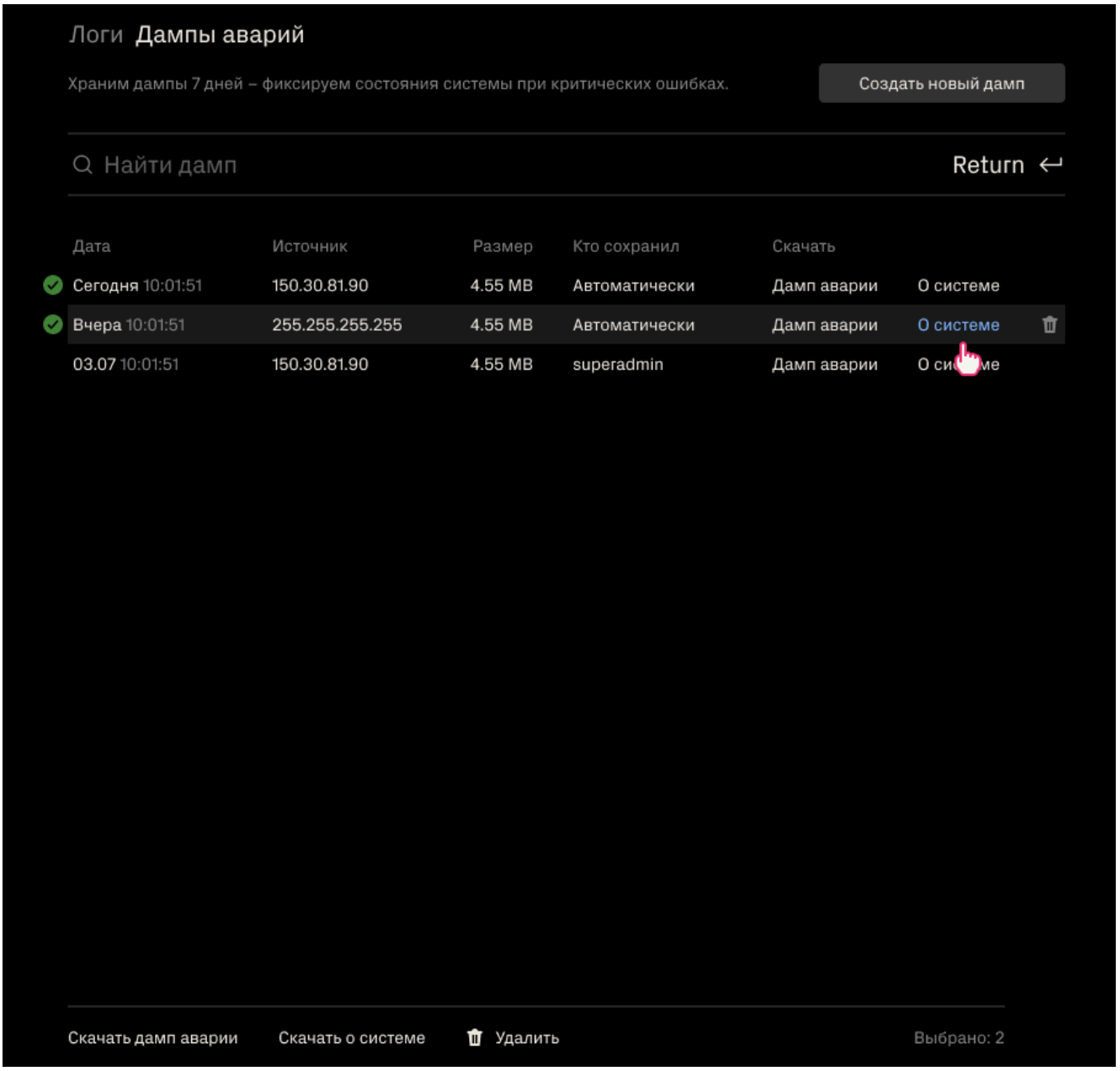
- Время события.
- Источник (Префикс-сеты, Профили, Арены и т.д).
- Описание события

Фильтр логов содержит следующие параметры:

- Системные ошибки – переключатель, позволяющий фильтровать критические ошибки.
- Время – настройка для ограничения выборки логов по дате и времени.
- Категории событий – возможность выбрать источники логов, такие как Ноды, Префикс-сеты, Роутеры, UH и другие.
- Ноды – меню для выбора ноды, логи которой отображаются.

Дампы аварий

Дампы аварий — это механизм быстрой диагностики. При сбое любого сервиса платформы система автоматически формирует архив с технической информацией за последние 5 минут.



Поиск дампов позволяет находить нужные записи журнала через поле ввода в верхней части экрана.

В верхней части интерфейса расположена кнопка **Создать новый дамп**. Она запускает ручное создание аварийного дампа. Система собирает данные и формирует архив.

Готовый дамп появляется в таблице. Его можно скачать или удалить.

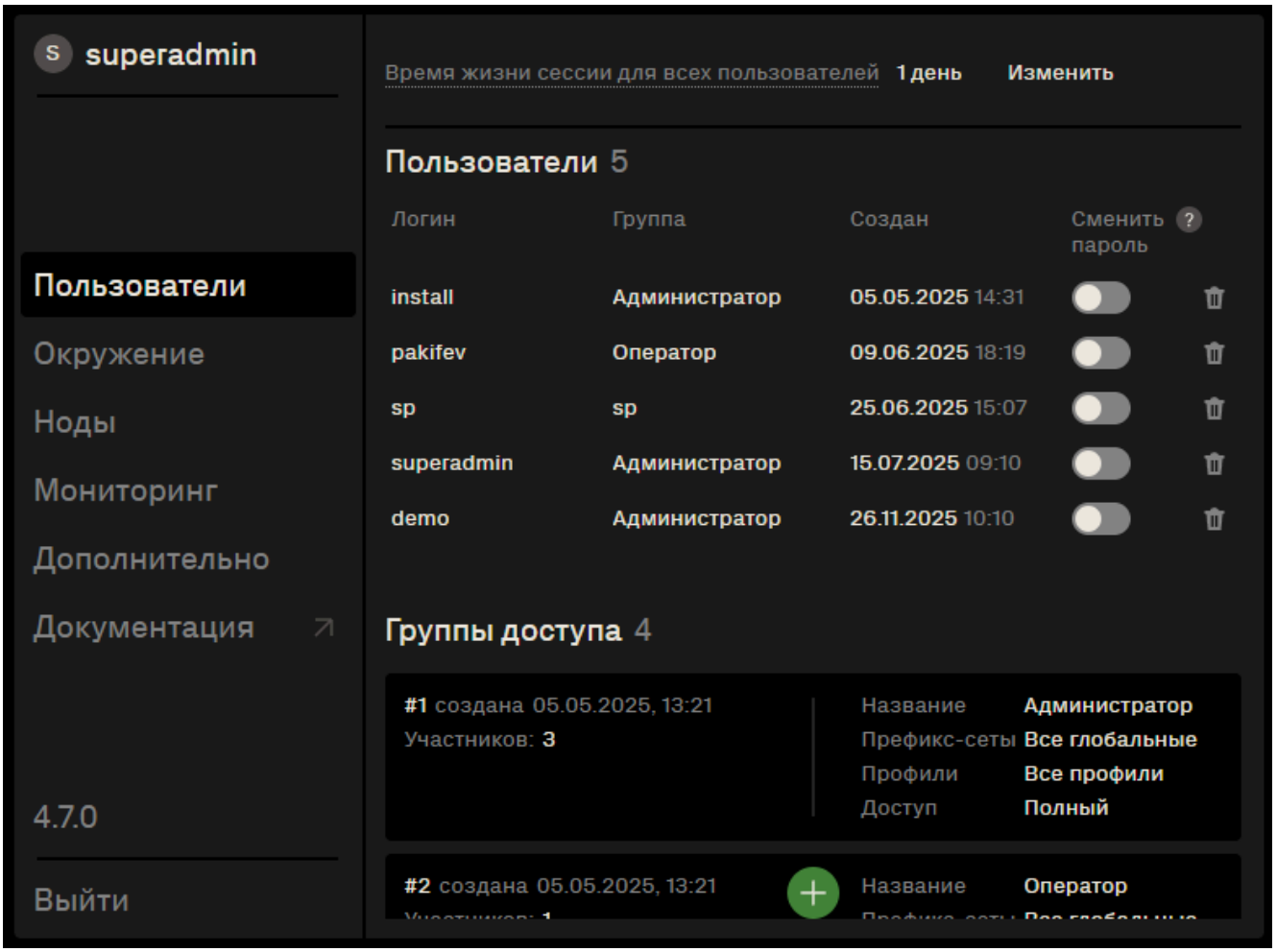
- **Дамп аварии** — полный архив с логами и служебными данными, собранными при сбое.
- **О системе** — краткая сводка о текущем состоянии сервера. Она включает информацию о оборудовании: сетевые интерфейсы, версию ядра, версию операционной системы и другие базовые параметры.

Дампы хранятся 7 дней и удаляются автоматически.

Настройки

Пользователи

Раздел **Пользователи** предназначен для управления пользователями системы и их принадлежностью к группам доступа.



Время жизни сессии для всех пользователей задаёт период, после которого пользователи должны заново войти в систему. При необходимости может быть изменено.

Пользователи - отображает учётные записи и их группы доступа. В списке можно удалить пользователя или включить переключатель **Сменить пароль** — в этом случае система завершит его сессию и попросит установить новый пароль при следующем входе.

Группы доступа - список доступных групп с детализацией параметров.

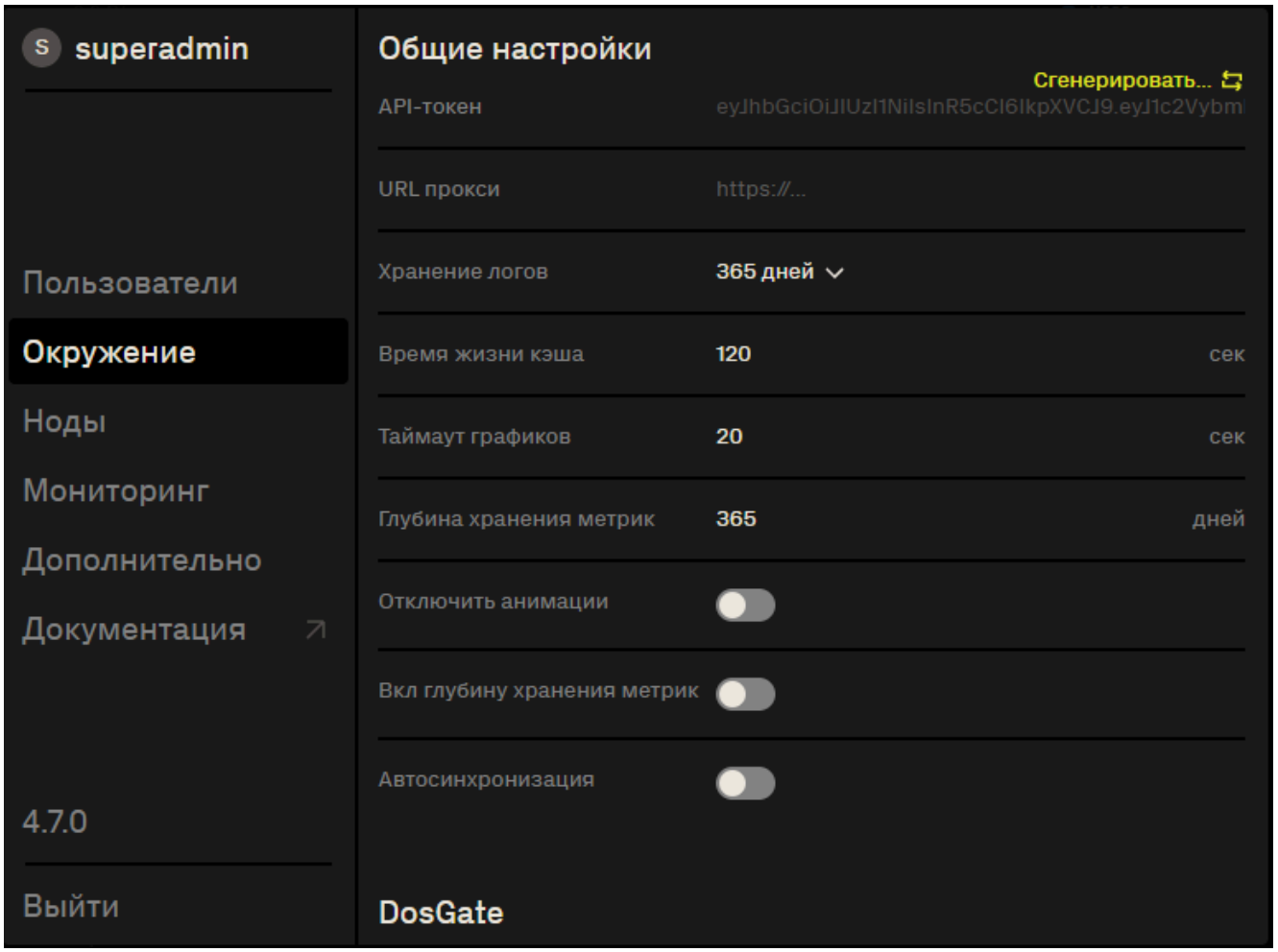
Группы доступа определяют права пользователей на доступ к профилям и префикс-сетам. По умолчанию в системе существуют три роли:

- Администратор
- Оператор
- Пользователь

Каждой группе можно назначить доступ ко всем или только определенным профилям и префикс-сетам. В системе есть возможность создавать собственные группы пользователей с индивидуальными правами доступа. Администратор может настраивать новые группы или изменять права существующих.
В нижней части интерфейса расположена кнопка "+", которая позволяет добавлять как новых пользователей, так и создавать новые группы доступа.

Окружение

Раздел **Окружение** содержит общие настройки системы, включая параметры API, прокси, кэширование, логи и интеграцию с внешними сервисами для работы с метриками и данными.



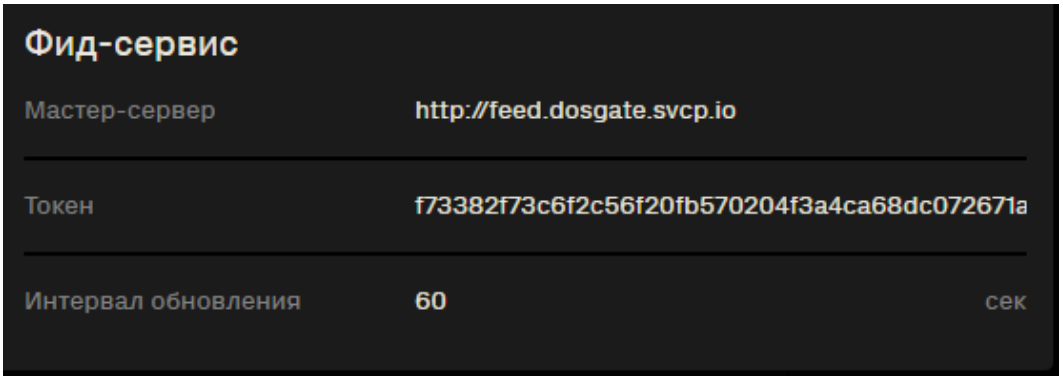
Общие настройки

- **API-токен** – позволяет сгенерировать уникальный ключ доступа к API.
- **URL прокси** – адрес прокси-сервера. Используется для доступа к фид-сервису Servicepipe через прокси-сервер
- **Хранение логов** – задает срок хранения логов в днях (по умолчанию 365 дней).
- **Время жизни кэша** – Хранит данные о профилях и их содержимом для ускорения работы системы. Чем больше значение кэша, тем реже он обновляется, что повышает производительность в крупных инсталляциях.
- **Отключить анимации** – переключатель, отключающий анимационные эффекты интерфейса. Рекомендуется отключать анимацию при подключении к веб-интерфейсу по RDP.
- **Автосинхронизация** – обеспечивает автоматическое приведение конфигурации узлов в соответствие с мастер-сервером при добавлении новых серверов или обнаружении расхождений в политиках.

DosGate

- **Graphite URL** – адрес сервера Graphite для сбора и отображения метрик.
- **Арена по умолчанию** – название арены, используемой в системе по умолчанию.
- **Обновление графиков** – интервал обновления графиков в секундах.

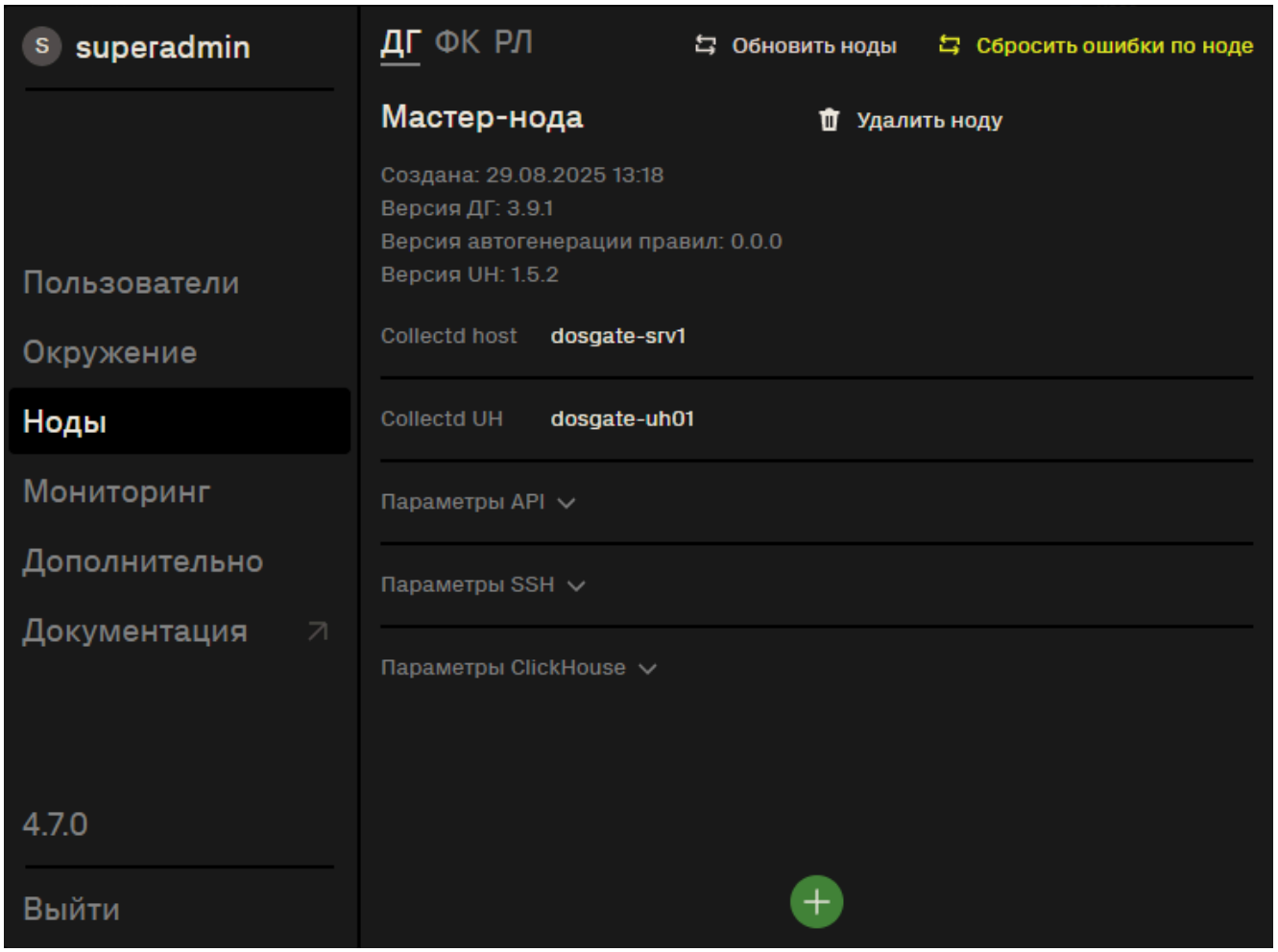
Фид-сервис



- **Мастер-сервер** – URL основного сервера фид-сервиса.
- **Токен** – ключ аутентификации, предоставленный вендором.
- **Интервал обновления**– частота обновления данных фид-сервиса в секундах.

Ноды

Раздел **Ноды** предназначен для управления узлами системы. Здесь отображается список доступных узлов, их статус и параметры.



Основные элементы:

- **Мастер-нода** — узел системы, на котором формируется бэкап настроек.
- **Collectd host** — имя хоста, с которого собираются системные и сервисные метрики.
- **Collectd UH** — имя хоста, с которого собираются системные и сервисные метрики для сессионой защиты.
- **Параметры API** — настройки доступа к API ноды.
- **Параметры SSH** — настройки SSH-доступа к ноде.
- **Параметры ClickHouse** — параметры подключения к базе данных ClickHouse для хранения и обработки аналитических данных.

Доступные действия:

- **Обновить ноды** – инициирует обновление данных о текущих узлах.
- **Синхронизировать** – выполняет принудительную синхронизацию конфигурации узлов с мастер-нодой.

Добавление новой ноды

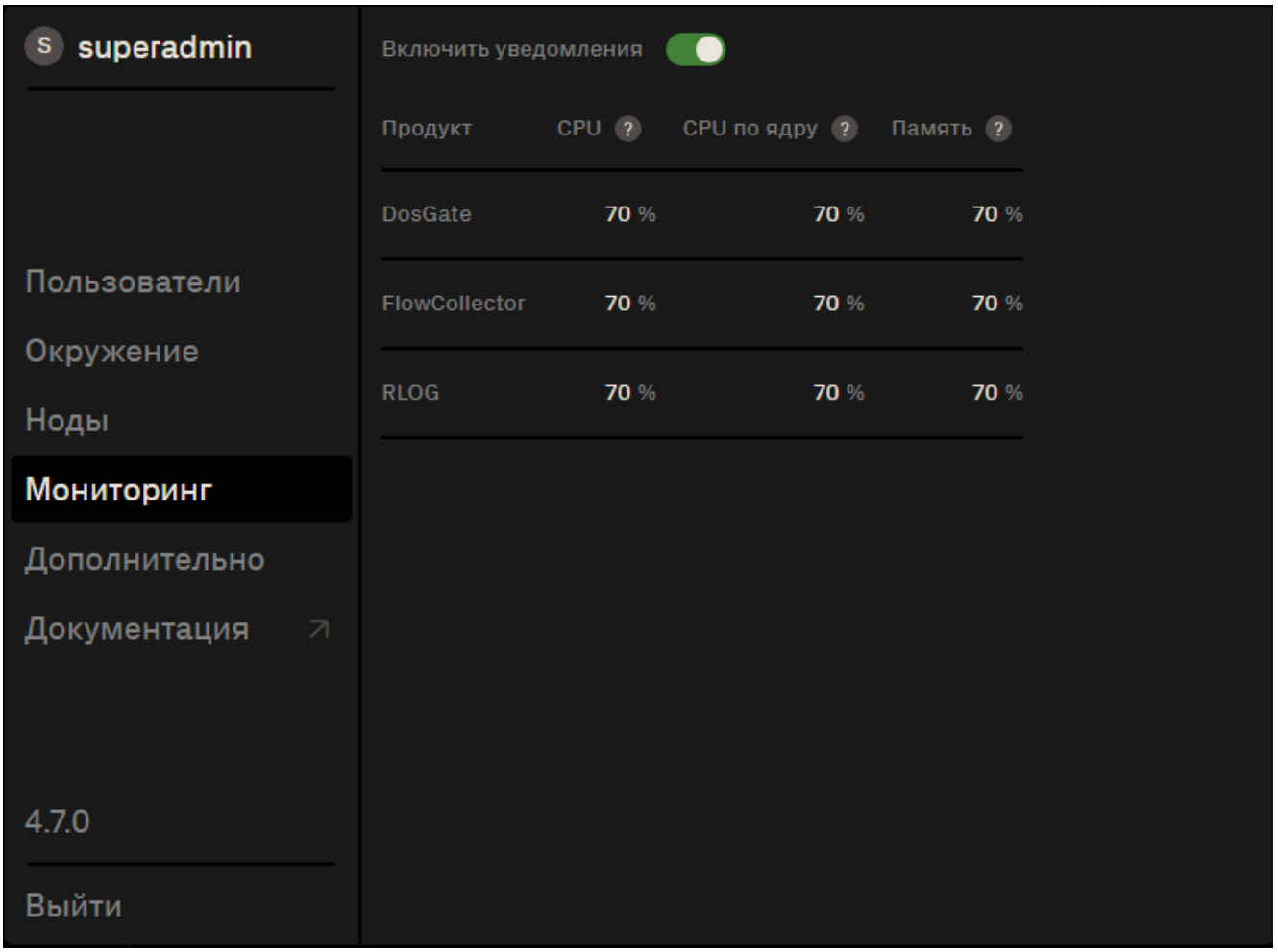
Для добавления нового узла в систему выполните следующие шаги:

1. Открыть раздел "Ноды" в интерфейсе.
2. Нажать кнопку "+" для создания новой ноды.
3. Заполнить параметры узла:
   - **Операционная система** – выбрать ОС из списка (Ubuntu 18, Альт 8 СП, Alma Linux).
   - **Модуль** – выбрать необходимый модуль (DosGate/FlowCollector).
   - **Collectd host** – указать имя хоста.
   - **Collectd UH** – указать имя сетевого модуля.
   - **HW Bypass** – функция управления сетевыми картами с поддержкой аппаратного байпаса, позволяющая включать или отключать режим прямой передачи трафика между портами на физическом уровне.
4. Нажать **Подключение**.
   - Доступны два способа соединения – API и SSH, выберите любой из них и настройте соответствующие параметры.
5. Нажать кнопку **Применить**.
6. Завершить добавление узла, нажав **Добавить ноду**.

После этого узел будет добавлен и отображён в общем списке нод.

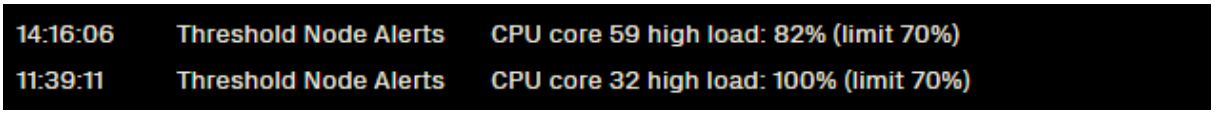
Мониторинг

Мониторинг отображает состояние ресурсов, используемых сервисами платформы. Интерфейс позволяет контролировать загрузку CPU, загрузку CPU по ядрам и объём используемой памяти для каждого продукта.

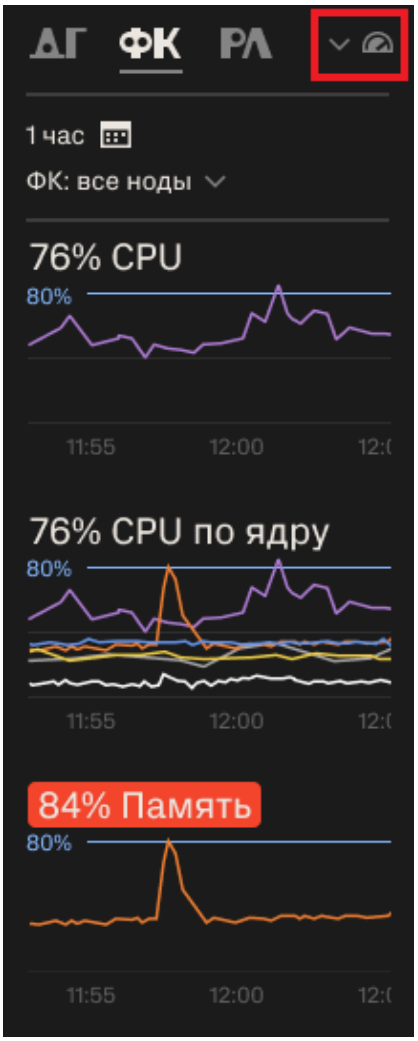


В верхней части расположен переключатель **Включить уведомления**, который активирует отправку предупреждений при превышении заданных порогов нагрузки.

Уведомления мониторинга отображаются в общем списке событий раздела **Логи**.



Для быстрого перехода к данным мониторинга в панели быстрого доступа доступна иконка мониторинга. Показатели, превышающие пороговые значения отображаются красным.

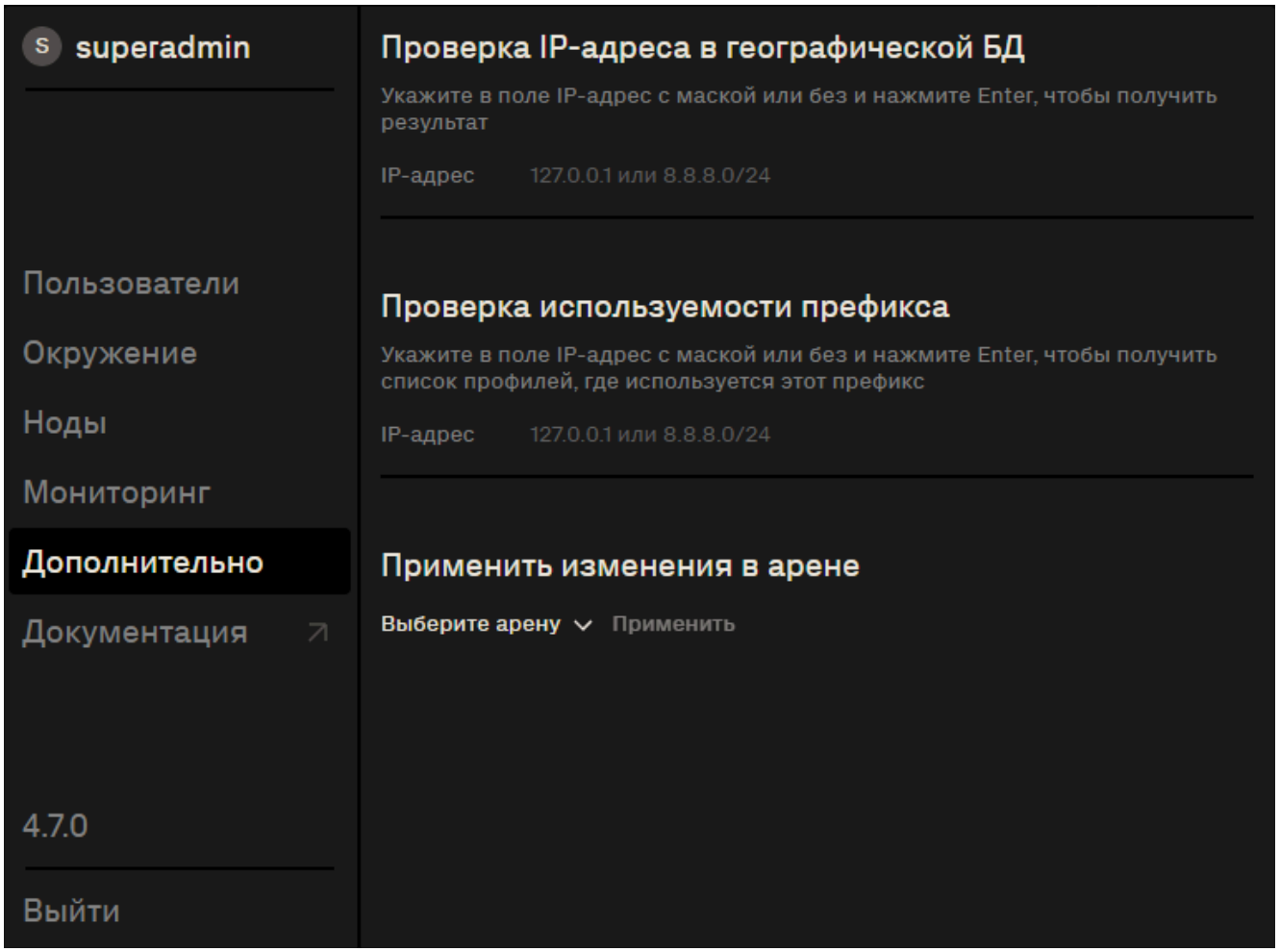


Дополнительно

Проверка IP-адреса в географической БД – позволяет определить географическую принадлежность IP-адреса.

Проверка используемости префикса – отображает список профилей, в которых используется заданный IP-адрес или префикс.

Применение изменений в арене – предоставляет возможность выбора арены из выпадающего списка и применения внесённых изменений с помощью кнопки **Применить**.



Документация

Раздел **Документация** в боковом меню является ссылкой, которая открывает справочные материалы по системе.