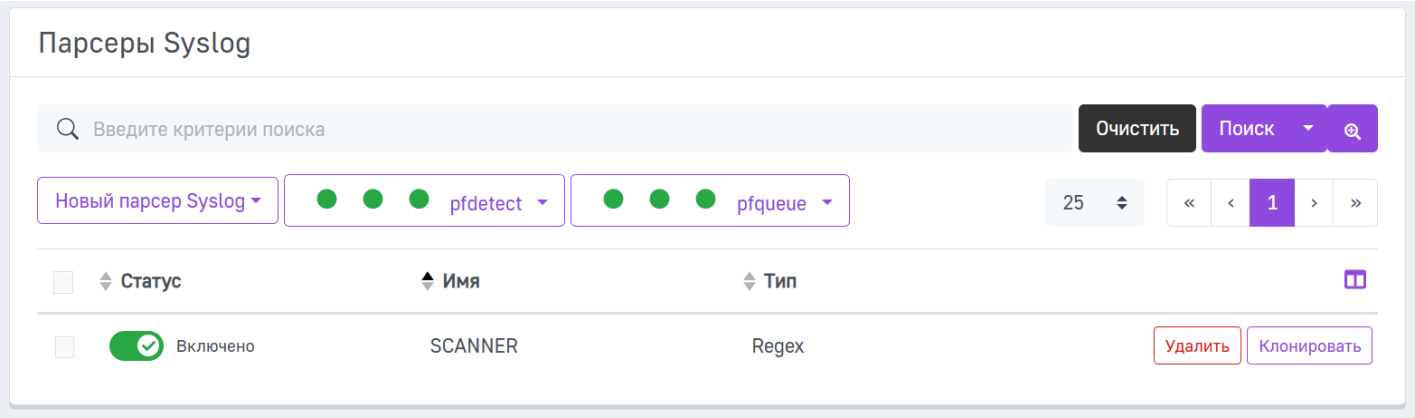
# Страница «Парсеры Syslog»

AxelNAC может получать информацию о событиях безопасности от нескольких решений одновременно, используя протокол Syslog.

На данной странице выполняется создание и изменение существующих парсеров Syslog.




По умолчанию в таблице отображаются 3 столбца:

- **Статус** — активность парсера Syslog. Нажмите на иконку, отображающую статус, чтобы изменить его доступность;
- **Имя** — имя парсера Syslog;
- **Тип** — тип парсера.

## Управление таблицей

Набор отображаемых столбцов в таблице может быть изменен, для этого нажмите на иконку . В выпадающем списке нажмите на название столбца, отображение которого в таблице необходимо изменить.

По умолчанию на странице отображается 25 записей, однако вы можете выбрать отображение 10, 50, 100, 200, 500 и 1000 записей на странице. Для этого нажмите на поле  в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Вы можете отсортировать таблицу в порядке возрастания или убывания с помощью иконки . По умолчанию все записи в таблице отображаются в порядке алфавитного возрастания по **Статусу**.

Для переключения между страницами используйте блок в правом верхнем углу списка.

## Служба pfdetect

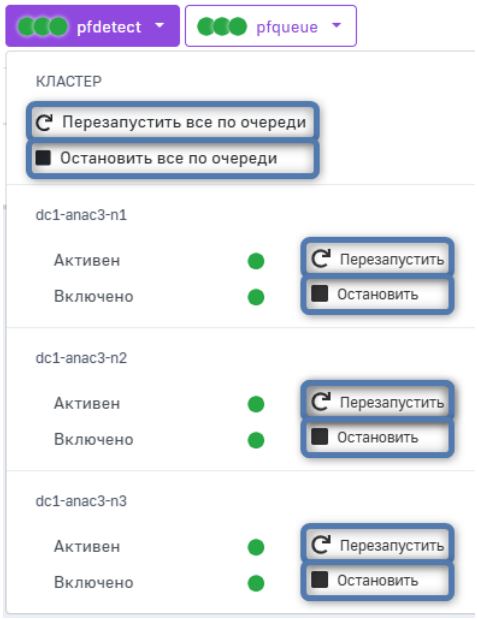
Служба **pfdetect** отвечает за обнаружение событий безопасности и сетевых инцидентов. Она анализирует входящие сообщения из разных источников, распознает события и запускает соответствующие действия.

Чтобы поочередно перезапустить службу **pfdetect** на всех узлах, нажмите на поле  и выберите из выпадающего списка .

Для проверки работоспособности новых настроек примените их только на одном узле, для этого нажмите на поле  и выберите из выпадающего списка .

Чтобы отключить службу , нажмите . Это приведет к тому, что работа службы на всех узлах кластера AxelNAC будет остановлена.

Чтобы на один из улов кластера не приходил трафик (например, для выявления возможных проблем) — нажмите .




## Служба pfqueue

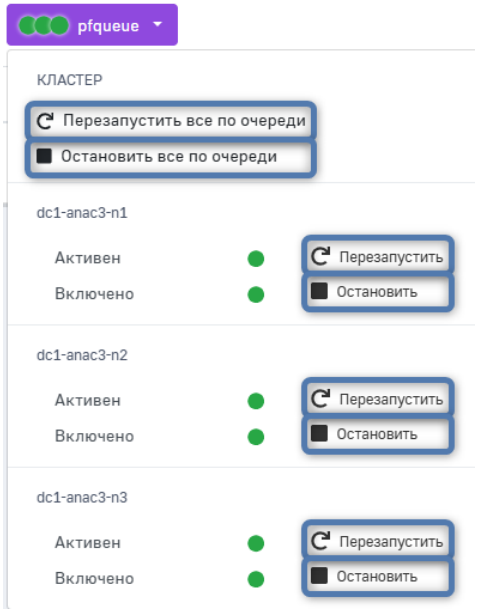
Служба **pfqueue** отвечает за очередь обработки событий и заданий внутри AxelNAC.

Чтобы поочередно перезапустить службу **pfqueue** на всех узлах, нажмите на поле pfqueue и выберите из выпадающего списка .

Для проверки работоспособности новых настроек примените их только на одном узле, для этого нажмите на поле pfqueue и выберите из выпадающего списка .

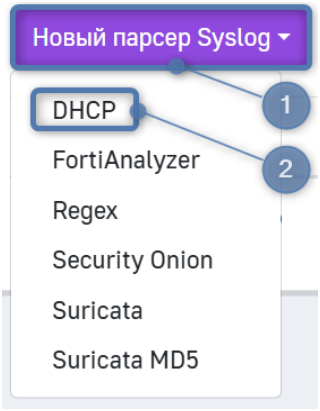
Чтобы отключить службу , нажмите . Это приведет к тому, что работа службы на всех узлах кластера AxelNAC будет остановлена.

Чтобы на один из улов кластера не приходил трафик (например, для выявления возможных проблем) — нажмите .




## Создание нового парсера Syslog

Для того чтобы создать новый парсер Syslog, нажмите **Новый парсер Syslog** в левом верхнем углу страницы и выберите желаемый внешний источник из выпадающего списка. После этого откроется меню конфигурации нового парсера Syslog.




Подробное описание каждого внешнего источника приведено в следующих статьях:

- DHCP;
- FortiAnalyzer;
- Regex;
- Security Onion;
- Suricata;
- Suricata MD5.

## Поиск парсера Syslog

Для того чтобы найти определенный парсер Syslog, можно выполнить поиск по критериям: **Имя**, **Тип**. Введите интересующий критерий в поле поиска и нажмите **Поиск**. Нажмите **Очистить**, чтобы сбросить критерии поиска.

Также можно выполнять поиск по нескольким критериям. Для этого нажмите на иконку лупы справа от кнопки **Поиск**.

В меню расширенного поиска вы можете выбрать операторы **И** и **ИЛИ** и указать несколько критериев для поиска. Поиск можно вести по критериям:

- **Имя** — поиск по имени парсера Syslog;
- **Тип** — поиск по типу парсера.

Также вам доступны следующие операторы**:**

- **равно;**
- **не равно**;
- **начинается с**;
- **заканчивается на**;
- **содержит**.

Для того чтобы изменить порядок выражений, нажмите и удерживайте иконку и перетащите выражение. Чтобы удалить выражение, нажмите на иконку .

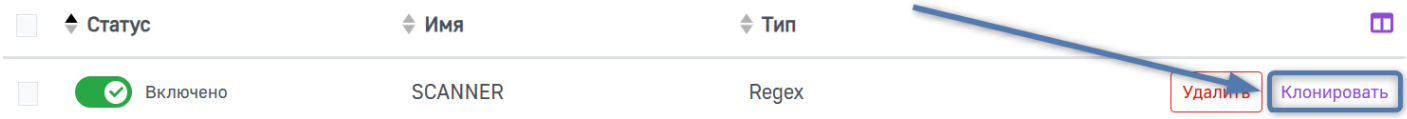
Вы можете сохранить и экспортировать существующий запрос, чтобы воспользоваться им позднее или импортировать уже существующий запрос. Все эти действия можно выбрать из выпадающего списка, нажав на иконку .

## Редактирование настроек парсера Syslog

Для того чтобы отредактировать парсер Syslog, нажмите на строку в таблице с названием нужного парсера Syslog. На открывшейся странице можно изменить все параметры парсера Syslog, кроме **Имени**.

## Клонирование парсера Syslog

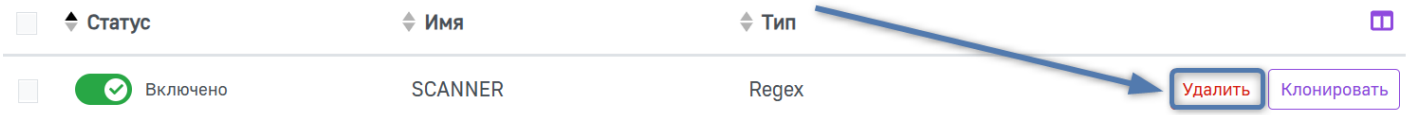
Для того чтобы создать копию определенного парсера Syslog, нажмите **Клонировать**. После этого вам будет предложено отредактировать скопированный парсер Syslog.




Также в режиме редактирования парсера Syslog вы можете в конце страницы нажать кнопку **Клонировать**.

## Удаление парсера Syslog

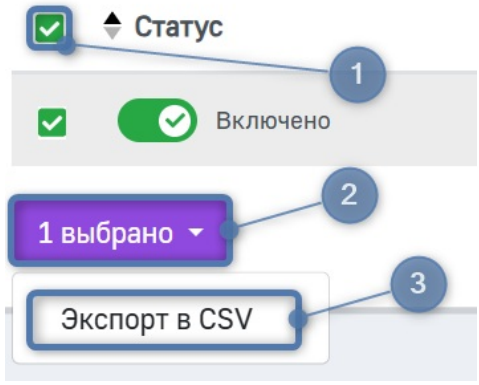
Для того чтобы удалить парсер Syslog, нажмите **Удалить**. После этого подтвердите удаление.




Также в режиме редактирования парсера Syslog вы можете в конце страницы нажать кнопку **Удалить**. После этого подтвердите удаление.

## Групповые действия

Для того чтобы выполнить действия с несколькими парсерами Syslog, отметьте необходимые парсеры. Чтобы выполнить действия со всеми парсерами Syslog в списке, нажмите на селектор в шапке таблицы.




На данный момент единственное доступное групповое действие в системе — **Экспорт в CSV**. При его выборе, файл в формате **.csv**, содержащий записи таблицы, попадает в менеджер загрузки вашего браузера.

---

ID статьи: 1341
Последнее обновление: 2 окт., 2025
Обновлено от: Михалева А.
Ревизия: 1
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Интеграция» -> Страница «Парсеры Syslog» -> Страница «Парсеры Syslog»
https://docs.axel.pro/entry/1341/