

Страница «Регистраторы событий»

Функционал AxelNAC позволяет использовать **Event Logger (Регистраторы событий)** для переадресации журналов, записанных в БД AxelNAC и TACACS, на другие серверы в формате **CEF** с использованием протокола Syslog.

Вкладка «Регистраторы событий»

На данной странице описан процесс конфигурации регистратора событий.

Регистраторы событий

Создание, изменение или удаление записи в журнале событий требует перезапуска службы packetfence-mariadb с помощью следующей команды: `systemctl restart packetfence-mariadb`

Введите критерии поиска Очистить Поиск

[Новый регистратор событий](#) 25 « < 1 > »

<input type="checkbox"/>	Идентификатор	Тип	Описание	Хост	Порт	Категория	Журналы для отправки	Приоритет	
<input type="checkbox"/>	1312	Syslog	test	10.31.219.12	514	daemon		notice	Удалить Клонировать

По умолчанию в таблице отображаются 8 столбцов:

- **Идентификатор** — имя регистратора событий;
- **Тип** — тип используемого протокола;
- **Описание** — описание регистратора событий;
- **Хост** — IP-адрес или имя хоста для получения журналов;
- **Порт** — порт, который используется для отправки журналов;
- **Категория** — категория отправителя;
- **Журналы для отправки** — имя журнала для отправки;
- **Приоритет** — тип отправляемых уведомлений.

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 **Идентификатору**.

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

Создание нового регистратора событий

Для того чтобы настроить конфигурацию регистратора событий, нажмите **Новый регистратор событий** в левом верхнем углу страницы.

1	Идентификатор	<input type="text"/>	ⓘ
Требуется указать идентификатор.			
2	Описание	<input type="text"/>	ⓘ
Требуется указать описание.			
3	Хост	<input type="text"/>	ⓘ
Требуется указать хост.			
4	Порт	514	
5	Категория	<input type="text"/>	▼
Требуется указать категорию.			
6	Журналы для отправки	<input type="text"/>	▼
7	Приоритет	notice	▼

В данном меню доступны следующие настройки:

1. **Идентификатор** — имя регистратора событий, которое будет отображаться в таблице;
2. **Описание** — описание регистратора событий, которое будет отображаться в таблице;
3. **Хост** — IP-адрес или имя хоста для получения журналов;
4. **Порт** — порт, который используется для отправки журналов (по умолчанию 514);
5. **Категория** — категория отправителя. Рекомендуемое значение — **auth**;
6. **Журналы для отправки** — имя журнала для отправки:
 - **admin_api_audit_log** — журнал аудита API администратора;
 - **auth_log** — журнал аудита авторизации;
 - **dns_audit_log** — журнал аудита DNS;
 - **dhcp_option82** — журнал аудита опции 82 DHCP;
 - **radius_audit_log** — журнал аудита RADIUS;
 - **tacacs_authentication_log** — журнал аудита аутентификации TACACS+;
 - **tacacs_authorization_log** — журнал аудита авторизации TACACS+;
 - **tacacs_accounting_log** — журнал аудита аккаунтинга TACACS+;
 - **tacacs_event_log** — журнал аудита событий API TACACS+.
7. **Приоритет** — тип отправляемых уведомлений:
 - **emergency** — аварийное уведомление;
 - **alert** — оповещение;
 - **critical** — критическая ошибка;
 - **error** — ошибка;
 - **warning** — предупреждение;
 - **notice** — уведомление;
 - **informational** — информационное сообщение (рекомендуемое значение);
 - **debug** — отладочное сообщение.

Для того чтобы создать новый регистратор событий, заполните параметры конфигурации и нажмите **Создать**. Чтобы сбросить введенные параметры на стандартные значения, нажмите **Сбросить**. Для возвращения на предыдущую страницу без сохранения выполненных на странице действий, нажмите **Отменить**.

Для создания, изменения или удаления записи в регистраторе событий требуется перезагрузка сервера AxiInAC.

Поиск регистратора событий

Для того чтобы найти определенный регистратор событий, можно выполнить поиск по критериям: **Идентификатор**, **Описание**, **Хост**, **Порт**, **Категория**, **Журналы для отправки**, **Приоритет**. 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:


- **Идентификатор** — поиск по имени регистратора событий;
- **Описание** — поиск по описанию регистратора событий;

- **Хост** — поиск по IP-адресу или имени хоста для получения журналов;
- **Порт** — поиск по порту, который используется для отправки журналов;
- **Категория** — поиск по категории отправителя;
- **Журналы для отправки** — поиск по имени журнала для отправки;
- **Приоритет** — поиск по типу отправляемых уведомлений.

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 регистратора событий

Для того чтобы отредактировать конфигурацию регистратора событий, нажмите на строку в таблице с названием нужного регистратора событий. На открывшейся странице можно изменить все параметры регистратора событий, кроме **Идентификатора**.

Клонирование регистратора событий

Для того чтобы создать копию определенного регистратора событий, нажмите **Клонировать**. После этого вам будет предложено отредактировать скопированный регистратор событий.

<input type="checkbox"/>	Идентификатор	Тип	Описание	Хост	Порт	Категория	Журналы для отправки	Приоритет	
<input type="checkbox"/>	1312	Syslog	test	10.31.219.12	514	daemon		notice	<input type="button" value="Удалить"/> <input type="button" value="Клонировать"/>

Также в режиме редактирования регистратора событий вы можете в конце страницы нажать кнопку **Клонировать**.

Удаление регистратора событий

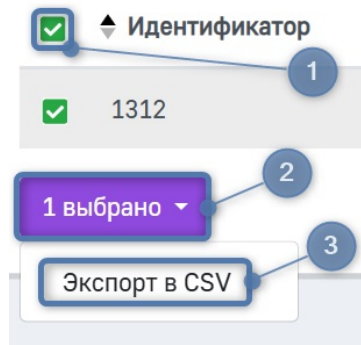
Для того чтобы удалить регистратор событий, нажмите **Удалить**. После этого подтвердите удаление.

<input type="checkbox"/>	Идентификатор	Тип	Описание	Хост	Порт	Категория	Журналы для отправки	Приоритет	
<input type="checkbox"/>	1312	Syslog	test	10.31.219.12	514	daemon		notice	<input type="button" value="Удалить"/> <input type="button" value="Клонировать"/>

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

Групповые действия

Для того чтобы выполнить действия с несколькими регистраторами событий, отметьте необходимые регистраторы событий. Чтобы выполнить действия со всеми регистраторами событий 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: 1500

Последнее обновление: 19 янв., 2026

Обновлено от: Михалева А.

Ревизия: 1

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Интеграция» -> Страница «Регистраторы событий» -> Страница «Регистраторы событий»

<https://docs.axel.pro/entry/1500/>