

Regex

В AxelNAC реализовано создание синтаксического анализатора системного журнала (Syslog) с помощью регулярных выражений. Данный функционал позволяет создавать сложные фильтры и правила для работы с данными, получаемыми через журнал.

Для создания парсера перейдите в раздел **Конфигурация** → **Интеграция** → **Парсеры Syslog** → **Новый парсер Syslog** и выберите значение **Regex** в выпадающем списке.

Новый парсер Syslog

Regex



1

Имя

Требуется указать имя.

2

Статус



Включено

3

Канал уведомления

Требуется канал уведомления.

4

Правила

Добавить правило

5

Образцы строк журнала

Тест

Создать

Сбросить

Отмена

На открывшейся странице вы можете выполнить следующие настройки:

- Имя** — имя парсера, которое будет отображаться в таблице;
- Статус** — при активации данного параметра парсер будет принимать и обрабатывать сообщения Syslog;
- Канал уведомлений** — абсолютный путь до ранее созданного канала уведомлений;
- Правила** — список правил, определяющих, как сопоставлять записи в журнале и какие действия предпринимать при сопоставлении. Количество правил неограниченно и может изменяться с помощью нажатия на иконки . Доступные настройки:
 - Имя** — имя правила;
 - Regex** — регулярное выражение для сопоставления с записью журнала. Может иметь [именованные захваты](#) которые можно использовать для замены параметров, начинающихся с '\$'.
 - Действия** — список действий, которые необходимо выполнить при совпадении регулярного сообщения. Количество действий неограниченно и может изменяться с помощью нажатия на иконки . Каждое действие состоит из следующих элементов:
 - Метод** — имя действия, которое необходимо выполнить. Возможные значения:
 - Создать учетную запись для нового пользователя;
 - Остановить событие безопасности;
 - Снять узел с регистрации по IP;
 - Зарегистрировать узел по MAC;
 - Изменить узел по MAC;
 - Изменить существующего пользователя;
 - Реаутентификация устройства по MAC;
 - Зарегистрировать новый узел по PID;
 - Зарегистрировать узел по IP;
 - Завершить все события безопасности для узла по MAC;
 - Получить подробные данные о роли;
 - Запустить сканирование устройства;
 - Инициировать событие безопасности;
 - Снять узел с регистрации по PID;
 - Обновить ip4log по IP и MAC;
 - Обновить ip6log по IP и MAC;
 - Обновить конфигурацию ролей.
 - Список параметров** — список параметров, которые необходимо передать методу. Каждый параметр разделяется запятой. Параметры, которые должны быть заменены именованным захватом.
 - Остановить, если совпадает** — при активации данного параметра останавливается обработка других правил, если это правило совпадает;
 - IP ≠ MAC** — при активации данного параметра выполняется автоматическая трансляция IP-адресов в MAC-адреса и наоборот.
- Образцы строк журнала** — поле для тестирования корректности правил. Нажмите **Тест**, чтоб проверить правило на введенных примерах.

Для того чтобы добавить новый парсер, 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**.

ID статьи: 1503

Последнее обновление: 19 янв., 2026

Обновлено от: Михалева А.

Ревизия: 1

База знаний AxelNAS -> Документация -> Система контроля доступа к сети «AxelNAS». Версия 2.1.0 -> AxelNAS. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Интеграция» -> Страница «Парсеры Syslog» -> Regex <https://docs.axel.pro/entry/1503/>