RADIUS

В данной статье описано, как настроить источник аутентификации, использующий протокол RADIUS для централизованного управления доступом к сетевым ресурсам. Этот метод аутентификации обеспечивает аутентификацию пользователей через внешний или сторонний сервер RADIUS.

Создание нового источника аутентификации RADIUS

Для того чтобы создать новый источник аутентификации RADIUS, нажмите **Новый внутренний источник** в левом верхнем углу таблицы. После этого откроется меню конфигурации нового источника.

В данном меню доступны следующие настройки:

1. **Имя** — имя источника аутентификации, которое будет отображаться в таблице со списком всех источников аутентификации. Задается при создании источника и не может быть изменено в дальнейшем;
2. **Описание** — описание источника аутентификации, которое будет отображаться в таблице со списком всех источников аутентификации;
3. **Хост** — адрес сервера RADIUS, который обрабатывает запросы на аутентификацию;
4. **Порт** — порт для подключения к серверу RADIUS. Если вы используете этот источник аутентификации в конфигурации области, порт для аккаунтинга будет иметь значение **номер этого порта + 1**;
5. **Секретная фраза** — укажите секретную фразу, которую вы настроили на сервере RADIUS;

6. **Таймаут** — время ожидания ответа от сервера RADIUS;
7. **Отслеживать** — включает логирование событий аутентификации и диагностику работы источника;
8. **Использовать коннектор** — использовать доступные коннекторы AxelNAC для подключения к данному источнику аутентификации. По умолчанию на данном сервере размещается локальный коннектор. Использование удаленных коннекторов в настоящее время поддерживается только на автономном исполнении;
9. **IP-адрес сервера сетевого доступа (NAS)** — данный параметр определяет, какой IP-адрес NAS использовать при взаимодействии с RADIUS-сервером. Если оставить значение пустым, источник будет использовать управляющий IP-адрес сервера (управляющий VIP в кластере);
10. **Опции** — задайте опции для определения FreeRADIUS home_server (если вы используете источник в конфигурации области). Для применения изменений необходим перезапуск службы **radiusd**;
11. **Связанные области** — области, которые будут связаны с данным источником (для портальной/администраторской пост-аутентификации GUI/RADIUS, но не для проксирования FreeRADIUS);
12. **Правила аутентификации** — набор условий, определяющих, каким образом клиент или устройство должно быть проверено перед предоставлением доступа к сети. Нажмите **Добавить правило**, чтобы добавить правило аутентификации. Заполните следующие поля:
    - **Статус** — активно ли правило;
    - **Имя** — имя правила;
    - **Описание** — описание правила;
    - **Оператор** — принцип проверки условий. Значение **ALL** указывает, что должны быть выполнены все перечисленные условия. Значение **ANY** указывает, что должно быть выполнено хотя бы одно правило;
    - **Условия** — набор критериев, используемых для проверки клиента. Количество условий неограниченно и может изменяться с помощью нажатия на иконки ⛔ ✪. Каждое условие состоит из следующих элементов:
        - **Атрибут** — параметр, который будет проверяться;
        - **Оператор** — тип сравнения или проверки;
        - **Значение** — ожидаемое значение атрибута для выполнения условия.
    - **Действия** — определяют, что произойдет после успешного выполнения условия правила. Количество действий неограниченно и может изменяться с помощью нажатия на иконки ⛔ ✪. Каждое действие состоит из следующих элементов:
        - **Тип** — вид результата. Возможные значения:
            - **Роль**;
            - **Период доступа без реавторизации**;
            - **Дата снятия с регистрации**;
            - **Баланс времени**;
            - **Баланс трафика**;
            - **Роль из источника**;
            - **Инициировать RADIUS MFA**;
            - **Инициировать портальную MFA**.
        - **Значение** — значение, соответствующее указанному типу.
13. **Правила администрирования** — набор условий, использующиеся для управления доступом администратора к системе на основе различных критериев. Позволяют настроить уровни доступа пользователей в зависимости от ролей, источников аутентификации и других параметров. Нажмите **Добавить правило**, чтобы добавить правило администрирования. Заполните следующие поля:
    - **Статус** — активно ли правило;
    - **Имя** — имя правила;
    - **Описание** — описание правила;
    - **Оператор** — принцип проверки условий. Значение **ALL** указывает, что должны быть выполнены все перечисленные условия. Значение **ANY** указывает, что должно быть выполнено хотя бы одно правило;
    - **Условия** — набор критериев, используемых для проверки клиента. Количество условий неограниченно и может изменяться с помощью нажатия на иконки ⛔ ✪. Каждое условие состоит из следующих элементов:
        - **Атрибут** — параметр, который будет проверяться;
        - **Оператор** — тип сравнения или проверки;
        - **Значение** — ожидаемое значение атрибута для выполнения условия.
    - **Действия** — определяют, что произойдет после успешного выполнения условия правила. Количество действий неограниченно и может изменяться с помощью нажатия на иконки ⛔ ✪. Каждое действие состоит из следующих элементов:
        - **Тип** — вид результата. Возможные значения:
            - **Уровень доступа.**
        - **Значение** — значение, соответствующее указанному типу.

Для того чтобы создать новый источник, 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: 249
Последнее обновление: 29 мая, 2025
Обновлено от: Ильина В.
Ревизия: 18
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Страница «Источники аутентификации» -> Вкладка «Внутренние источники» -> RADIUS
https://docs.axel.pro/entry/249/