Аутентификация с помощью LDAP-FreeIPA

В данной статье описано, как настроить аутентификацию пользователей и APM с помощью учетных данных, которые хранятся в доменном каталоге LDAP-FreeIPA. Данная аутентификация возможна как для APM под управлением ОС Windows так и для APM под управлением ОС Linux. При таком методе аутентификации, AxelNAC может взаимодействовать с контроллером домена для:

- проверки пользователей, подключенных по протоколу EAP-TLS на вхождение в группы домена, для последующей выдачи ролей и доступов;
- проверки учетных данных пользователей по протоколу MS-CHAPv2, для последующей аутентификации их в сети;
- осуществления входа администраторов по доменным УЗ.

Конфигурация источника аутентификации

Для того, чтобы реализовать доменную LDAP-аутентификацию на устройствах с поддержкой FreeIPA, необходимо создать источник аутентификации Active Directory. Для этого выполните следующие действия:

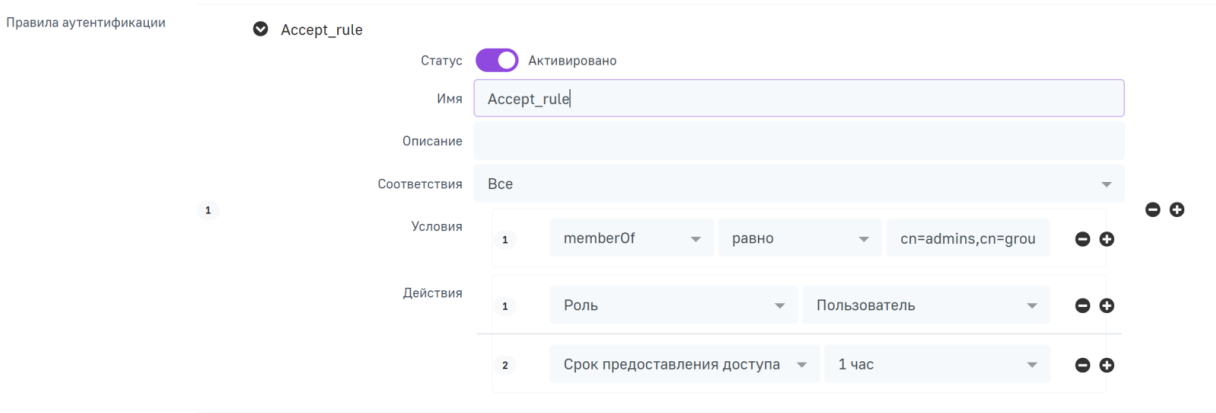
Шаг 1. Добавьте контроллер домена FreeIPA в качестве источника аутентификации в AxelNAC. Для этого в разделе **Конфигурация → Политики и контроль доступа → Источники аутентификации** нажмите кнопку **Новый внутренний источник** и выберите **Active Directory** из выпадающего списка.

Шаг 2. В открывшемся окне заполните все необходимые поля.

Чаще всего, поля CN и UID не ведут к уникальной записи, поэтому рекомендуется для поиска добавить дополнительный элемент вида **ObjectClass**, либо использовать конкретный **Base DN** (например, с использованием поля **Accounts**), либо использовать поле **Mail**.

Шаг 3. В созданном новом источнике аутентификации добавьте правила аутентификации. Нажмите **Добавить условия** и укажите атрибут, который будет использоваться для проверки уровня доступа. Затем нажмите **Добавить действие** и укажите следующие параметры:

- **Роль** — по умолчанию;
- **Срок предоставления доступа** — 5 дней.



В качестве атрибутов для проверки уровня доступа рекомендуется использовать **uid** или **memberOf**. Применение других полей (например, **sAMAccountName** или **UPN**) необходимо тщательно планировать и проверять в вашей сети, чтобы убедиться, что значения, возвращаемые при поиске по этим параметрам, будут уникальными.

Шаг 4. Убедитесь, что вся введенная информация верна. Для этого нажмите кнопку **Тест** справа от поля **Пароль**. Если появится сообщение с текстом "Успешно проведена валидация с IP-адрес_хоста", источник аутентификации FreeIPA настроен корректно.

Шаг 5. Сохраните новый источник аутентификации, нажав кнопку **Создать**.

Настройка профиля подключения

После того как создан источник аутентификации, необходимо настроить профиль подключения. Данная процедура необходима для того, чтобы AxelNAC знал, как обрабатывать подключение, которое поступает по проводной или беспроводной (Wi-Fi) сети.

В рассматриваемом примере будет создаваться новый профиль подключения для использования источника аутентификации FreeIPA, а также для того, чтобы AxelNAC знал, что нужно автоматически регистрировать все устройства, успешно прошедшие аутентификацию с помощью 802.1X в данном профиле подключения. Для этого необходимо произвести следующую настройку:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения** и нажмите кнопку **Новый профиль подключения**.

Шаг 2. На открывшейся странице заполните поля следующим образом:

- **Имя профиля:** 8021x;
- **Описание профиля:** Проводное соединение 802.1X;
- **Активировать профиль:** Включено;
- **Регистрировать устройства автоматически:** Включено;
- **Фильтры:** Все;
- **Тип подключения:** Ethernet-EAP;
- **Источники:** Выберите созданный ранее источник аутентификации LDAP.

Шаг 3. Сохраните изменения конфигурации, нажав **Создать**.

ID статьи: 554
Последнее обновление: 7 нояб., 2024
Обновлено от: Егоров В.
Ревизия: 5
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Источники аутентификации -> Аутентификация с помощью LDAP-FreeIPA
https://docs.axel.pro/entry/554/