Настройка интеграции с доменом

В рамках данной лабораторной работы мы изучим как наш продукт может взаимодействовать с доменом, рассмотрим сценарий с интеграцией AxelNAC с доменом (Active Directory) и вводом AxelNAC в домен, изучим процесс настройки политик аутентификации и авторизации, настройку супликанта для работы по протоколу PEAP-MSCHAPv2, приведем пример сценария аутентификации для проверки результата, рассмотрим сценарий аутентификации с проверкой атрибутов LDAP и разберем самые часто встречающиеся проблемы. Длительность выполнения лабораторной работы — 2 часа.

Доменная аутентификация

При обслуживании больших сетей системные администраторы часто сталкиваются с проблемами аутентификации и авторизации на сетевом оборудовании. В частности, довольно сложно организовать нормальную работу нескольких сетевых администраторов под индивидуальными учетными записями на большом количестве оборудования (приходится вести и поддерживать в актуальном состоянии базу локальных учетных записей на каждом устройстве). Логичным решением является использование для авторизации уже существующего каталога учетных записей — LDAP. На текущий момент самым популярным каталогом LDAP является Active Directory. В данной лабораторной работе мы разберемся, как настроить в AxelNAC **интеграцию с Active Directory для аутентификации и\или авторизации** пользователей.

AxelNAC может взаимодействовать с доменом 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.

Принцип работы AxelNAC при аутентификации по протоколу MS-CHAPv2:

1. Пользователь авторизуется в системе, вводя логин/пароль.
2. Супликант системы принимает логин/пароль и отправляет их на проверку контроллеру домена.
3. Контроллер домена, когда логин/пароль верны, возвращает данные об успешной аутентификации пользователя.
4. При необходимости AxelNAC осуществляет запрос дополнительных данных по клиенту (принадлежность доменным группам или другие поля из каталога LDAP).
5. AxelNAC авторизует пользователя в сети на основании полученной информации.

Интеграция AxelNAC с доменом

Для того чтобы настроить процесс аутентификации пользователя в сети при помощи супликанта, необходимо интегрировать AxelNAC в домен. Данный процесс состоит из двух этапов:

1. Добавление AxelNAC в домен.
2. Добавление домена в соединение.

Интеграция необходима для аутентификации пользователя в сети с использованием учетных данных пользователя, заведенного в домен. Если вам не требуется аутентифицировать пользователя по протоколу MS-CHAPv2, и необходимо настроить только процесс авторизации пользователя с распределением ролей, вы можете пропустить данный раздел и перейти сразу к настройке политик авторизации.

Добавление AxelNAC в домен

Для того чтобы ввести AxelNAC в домен, выполните следующие шаги:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Домены → Домены Active Directory** и нажмите кнопку **Новый домен**.

Шаг 2. В поле **Идентификатор** задайте уникальное имя для домена в AxelNAC. Оно может отличаться от имени домена и будет отображаться в списке на странице **Домены Active Directory**.

Шаг 3. В поле **Рабочая группа** укажите рабочую группу к которой будет принадлежать AxelNAC в домене. Рекомендуется выбирать верхнеуровневую рабочую группу для доступа ко всем доменным пользователям и авторизации.

Шаг 4. В поле **DNS-имя домена** введите DNS-имя домена, в который вы интегрируете AxelNAC.

Шаг 5. В поле **Имя AxelNAC в домене** укажите имя AxelNAC в домене. Рекомендуется оставить стандартное значение **%h**.

Шаг 6. В поле **Sticky DC** задайте контроллеры домена, к которым будет подключаться AxelNAC. Для упрощения, можно указать "*" для использования всех возможных контроллеров домена.

Шаг 7. В поля **Сервер активного каталога** и **DNS-сервер(ы)** укажите IP-адрес сервера Active Directory. Если DNS-серверов несколько, используйте запятую в качестве разделителя.

Шаг 8. В поле **Структурное подразделение (OU)** введите каталог AD, в который будет помещена запись AxelNAC и нажмите **Создать**.

Если в пути содержится пробел, его необходимо экранировать обратной косой чертой \ (пример: Computers/Servers/ Unix\ systems). В ином случае, система не сможет найти указанный объект.

Шаг 9. На странице **Домены Active Directory** в столбце **Присоединение к домену** нажмите на кнопку **Подключение не удалось** и выберите в выпадающем списке **Подключиться**.

Шаг 10. В открывшемся окне введите логин и пароль от учетной записи администратора домена. Учетные данные не хранятся в AxelNAC, они нужны только для подключения к домену.

Добавление домена в соединение

После того как AxelNAC введен в домен можно добавить этот домен в настройку соединения.

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Домены → Области** и выберите область, которую вы настроили в рамках лабораторной работы №1.

Шаг 2. На вкладке **NTLM-аутентификация** выберите добавленный домен в поле **Домен**.

Таким образом, учетные данные которые AxelNAC получит от супликанта будут отправляться в домен для проверки соответствия. В случае успешной аутентификации пользователь будет авторизован в сети.

Настройка политик авторизации

После успешной интеграции AxelNAC с доменом можно настраивать политики авторизации. Данный раздел состоит из двух этапов:

- Добавление источника аутентификации.
- Настройка политик авторизации.

Добавление источника аутентификации

Перед настройкой политик авторизации необходимо добавить источник аутентификации.

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Источники аутентификации** , нажмите **Новый внутренний источник** и выберите **Active Directory** в выпадающем меню.

Шаг 2. Заполните поля **Имя** и **Описание**. Эти значения будут отображаться в списке на странице **Источники аутентификации**.

Шаг 3. Введите IP-адрес домена в поле **Хост**. Поле Режим верификации SSL оставьте без изменений, т.к. данная проверка необходима для подключений в которых применяются протоколы Start TLS и LDAPS.

Шаг 4. В поле **Базовое DN** укажите контроллеры домена использую запятую как разделитель. **Пример:** для домена **axel.pro** контроллеры домена указываются в виде **DC=axel, DC=pro**.

Шаг 5. В поле **Область применения** выберите значение **Subtree**.

Шаг 6. В поле **Атрибут имени пользователя** вы можете выбрать одно из этих значений:

- **sAMAccountName** — при выборе этого значения пользователь будет аутентифицироваться с логином вида **имя_домена\имя_пользователя**;
- **UserPrincipalName** — при выборе этого значения пользователь будет аутентифицироваться с логином вида **имя_пользователя@имя_домена**.

Шаг 7. В поле **Прочие поиска** укажите атрибуты, которые также могут использоваться для аутентификации:

- **sAMAccountName** — поиск пользователя по короткому имени входа (**пример:** AxelNACAdmin);
- **UserPrincipalName** — поиск пользователя по полному имени входа с указанием домена (**пример:** AxelNACAdmin@axeldemo.pro);
- **cn** — поиск пользователя по имени в AD (**пример:** AxelDemo. Admin);
- **dNSHostName** — поиск пользователя по доменному имени (**пример:** axeltest.axeldemo.pro).

Шаг 8. Заполните поле **Привязать DN** данными пользователя, через которого AxelNAC будет выполнять проверку учетных данных в домене (**пример корректного DN:** CN=Axel SA. Admin,OU=admin_nac,OU=admins,DC=axeldemo,DC=pro). Точный DN необходимо запрашивать у **доменного администратора**.

Шаг 9. Введите пароль для данного пользователя в поле **Пароль**.

Данный пользователь должен быть предварительно создан в домене с правами просмотра всего домена.

Шаг 10. В поле **Связанные области** выберите область, которую вы настроили в предыдущем разделе.

После этого можно создать источник аутентификации, либо можно продолжить его настройку, обогащая его определенными правилами авторизации.

Настройка политик авторизации

Для того, чтобы настроить политики (правила) авторизации, необходимо вернуться в окно настройки источника аутентификации и выполнить следующие шаги:

Шаг 1. В строке **Правила аутентификации** нажмите **Добавить правило**.

Шаг 2. Введите имя для правила и нажмите **Добавить условие**.

Шаг 3. В выпадающем списке выберите значение **radius_request.User-Name** и оператор **содержит**. В качестве искомого значения укажите ваш домен в следующем виде: **@имя_домена**.

Шаг 4 (опционально). Также вы можете добавить условие **memberOf** для поиска пользователя в конкретной группе домена для разграничения прав доступа.

Шаг 5. Нажмите **Добавить действие** и выдайте такому пользователю роль **User** продолжительностью 3 часа (добавление действий более подробно рассмотрено в лабораторной работе №2).

Настройка супликанта для работы по протоколу PEAP-MSCHAPv2

Для того, чтобы клиентское устройство могло быть подключено к серверу с аутентификацией по протоколу PEAP-MSCHAPv2 необходимо настроить соединение на устройстве.

Шаг 1. Запустите в Windows сервис **Проводная автонастройка** (dot3svc) и добавьте его в автозагрузку.

Шаг 2. Откройте меню **Сетевые подключения**, затем откройте свойства сетевого интерфейса, по которому организовано подключение.

Шаг 3. На вкладке **Проверка подлинности** установите флажки для всех параметров.

Шаг 4. В поле **Метод проверки подлинности в сети** выберите значение **Microsoft: Protected EAP (PEAP)**.

Шаг 4. Нажмите на кнопку **Параметры** справа от поля выбора метода и снимите флажок с параметра **Подтверждать удостоверение сервера с помощью проверки сертификата**.

Шаг 6. Перейдите в раздел **Настроить** и установите галочку на все параметры. Затем нажмите **ОК** дважды.

Шаг 7. На вкладке **Проверка подлинности** нажмите **Дополнительные параметры**, и в поле **Указать режим проверки подлинности** установите **Проверка подлинности пользователя или компьютера**. Затем нажмите **ОК**.

После этого супликант на клиентском устройстве настроен.

Решение самых часто встречающихся проблем

Данный раздел находится в разработке и будет добавлен в следующих версиях лабораторной работы.

ID статьи: 11
Последнее обновление: 10 июн., 2025
Обновлено от: Егоров В.
Ревизия: 9
База знаний AxelNAC -> Обучающие материалы -> Лабораторные работы -> Настройка интеграции с доменом
https://docs.axel.pro/entry/11/