Кэширование NTLM-аутентификации

• В данном примере предполагается, что источник аутентификации Active Directory уже настроен, а AxelNAC уже введен в домен. Подробная информация о настройке этих двух компонентов приведены в соответствующих разделах руководства.
• Для работы кэширования требуется как минимум Windows Server 2008. Кэширование NTLM-аутентификации не поддерживается на более старых версиях Windows Server.

Использование NTLM-аутентификации в Active Directory для 802.1X EAP-PEAP соединений может стать узким местом при обработке десятков аутентификаций в секунду.

Для преодоления этого ограничения можно использовать кэш внутри AxelNAC, чтобы уменьшить количество аутентификаций, требующих внешнего вызова NTLM-аутентификации. Если пользователь находится в кэше, AxelNAC попытается сравнить с ним учетные данные 802.1X. В случае неудачи проверки выполняется вызов запроса к домену Active Directory на валидацию данных пользователя **ntlm_auth**. В случае потери кэша также выполняется вызов запроса **ntlm_auth**. Таким образом, даже если пользователь меняет пароль, его новый пароль сразу же становится действительным для соединений 802.1X EAP-PEAP, даже если кэш содержит устаревшую запись.

Кэш NTLM не кэширует пароли в открытом виде. Кэшируется только NT-хэш пароля.

Конфигурация AxelNAC

Для того, чтобы настроить кэширование NTLM, выполните следующие действия:

Шаг 1. Включите глобальное кэширование NTLM. Для этого активируйте параметр **Кэширование NTLM Redis** в разделе **Конфигурация → Настройки системы → RADIUS → Основное** , затем перезапустите службу **radiusd-auth**.

Шаг 2. Настройте AxelNAC для запуска кеширования учетных данных. Для этого перейдите в раздел **Конфигурация → Политики и контроль доступа → Домены → Домен Active Directory** и выберите домен, для которого необходимо кешировать учетные данные.

Шаг 3. Перейдите на вкладку **Кэширование NTLM** и настройте следующие параметры:

- активируйте параметр **Кэширование NTLM**;
- выберите источник аутентификации Active Directory, привязанный к этому домену;
- настройте параметр **Срок хранения записи**.

Нажмите кнопку **Сохранить**, чтобы применить изменения.

Шаг 4. Активируйте службу **redis_ntlm_cache**, которая используется AxelNAC для хранения кэшированных учетных данных. Перейдите в раздел **Конфигурация → Настройки системы → Основные настройки → Службы** и активируйте **redis_ntlm_cache**, после чего сохраните изменения.

Шаг 5. Перейдите в раздел **Статус → Службы** и запустите работу службы.

Конфигурация Active Directory

Чтобы AxelNAC мог получать учетные данные NTLM из Active Directory, ему необходим пользователь, обладающий правами на репликацию. Пользователь, которому нужно предоставить эти права, является пользователем, учетная запись которого настроена в источнике аутентификации.

Настройка прав репликации (**Replicating Directory Changes** и **Replicating Directory Changes All**) описана в официальной документации Microsoft.

ID статьи: 99
Последнее обновление: 3 февр., 2025
Обновлено от: Егоров В.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство администратора -> Оптимизация производительности -> Кэширование NTLM-аутентификации
https://docs.axel.pro/entry/99/