Исследование проблемы поиска КД MS AD в доверительных отношениях с доменами FreeIPA и определение метода обнаружения КД MS AD через DNS и CLDAP

Крюков Иван Сергеевич, Дорохин Руслан Андреевич
Группа Астра, Москва, Огородный проезд, 16/1с5
ikriukov@astralinux.ru

История использования NetBIOS в службах каталога.

Active Directory (далее AD) – одна из самых распространненых служб каталога в настоящее время. С момента своего возникновения в рамках ОС Windows 2000 Server Edition, в ней используется протокол NetBIOS. Однако в начале 2000-х годов NetBIOS начинает активно замещаться целым набором технологий, таких как DNS, LDAP, Kerberos, в силу наличия уязвимостей и ограниченной масштабируемости NetBIOS.

В настоящее время протокол NetBIOS применяется как в Active Directory для поддержки обратной совместимости с более ранними версиями продукта, так и в Samba – программном пакете для Unix-подобных систем, обеспечивающем взаимодействие с доменами AD.

В реализации службы каталога ALD Pro (сокр. AstraLinux Directory Pro) для взаимодействия с контроллерами домена (далее КД) AD также применяются компоненты Samba, и, как следствие, используются те же зависимости.

Проблема поиска КД в доменах ALD Pro

Одним из ключевых компонентов Samba, обеспечивающим взаимодействие с КД AD, является служба *winbindd*. Эта служба выполняет следующие функции: разрешение NetBIOS-имен, преобразование идентификаторов SID в Unix-идентификаторы (и обратно), а также интеграцию модуля PAM (Pluggable Authentication Module) с различными механизмами аутентификации в домене, включая NTLM и Kerberos. Winbindd позволяет Unix-системам полноценно работать в домене как в роли клиента, так и в роли контроллера домена.

При использовании базовых настроек NetBIOS не отключен и поиск КД происходит по NetBIOS-имени КД. Однако возникает проблема зацикливания поиска и выдача ошибки ненахождения искомых КД.

Описание стенда

В проведимых исследованиях использовался следующий стенд:

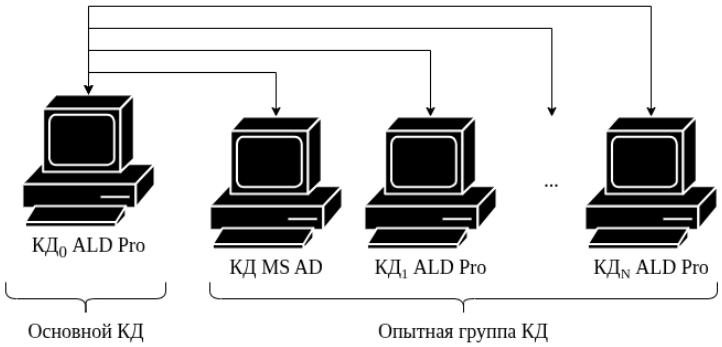

Рис. 1 – Схема подключения КД в стенде, где N = 3.

Согласно приведенной на рис. 1 схеме, двусторонние доверительные отношения (далее ДДО) установлены между основным КД ALD Pro и поочередно с каждым КД ALD Pro и КД MS AD. Внутри опытной группы КД установка ДДО не производилась.

Решение проблемы поиска КД и его эффективности

Решением проблемы стало блокирование протокола NetBIOS на уровне конфигурации Samba и его замена на алгоритм поиска по DNS SRV-записей КД в рамках заданного домена (*поиск КД по DNS*):

1. Получение полного имени домена через DNS-запрос res_query;
2. Обработка результатов запроса и вычленение имен КД;
3. Обращение к КД с использованием протокола CLDAP для определения его досягаемости.

Использование CLDAP вместо LDAP обусловлено тем, что CLDAP использует анонимный запрос только к RootDSE записи верхнего уровня, который не требует авторизации запрашивающей стороны.

Однако возникла дополнительная проблема – возникают ситуации, когда в рамках одного домена некоторое подмножество КД доверенного домена в силу некоторых причин может находиться вне зоны досягаемости. Это заставляет winbindd бесконечно искать такие утерянные КД, с которыми ранее уже было установлено соединение, что тратит ресурсы КД и значительно засоряет трафик.

Решением такой проблемы является создание в Samba отдельного параметра, который включает в себя список КД различных доменов, которые с высокой вероятностью доступны в сети постоянно:

1. Считывание списка КД из параметра: формирование иерархического списка “список доменов – подсписок КД”;
2. Обращение к домену из базы данных доверенных доменов;
3. Поиск доступных КД:
   - Если для домена существует список доступных КД – ищем только их, используя описанный ранее “*поиск КД по DNS”*;
   - Иначе используем описанный ранее “*поиск КД по DNS”* для всех КД, которые можем найти.

Вывод

Изоляция между доменами при установлении ДДО обеспечивается за счет механизмов аутентификации и авторизации (например Kerberos), групповых политик и списков контроля доступа ACL (*англ. Access Control List*). В случае некорректной работы методов и алгоритмов поиска КД доверенных доменов механизмы изоляции могут сообщать о недоступности некоторых пользователей и служб к различным ресурсам доверенных доменов.

Таким образом, работа механизмов изоляции становится некорректной, так как потеряна связь с уже имеющимися доверенными доменами, и, следовательно, информация об имеющихся ресурсах и доступах между доменами не поступает.

Найденное в исследовании решение позволяет обойти недостатки протокола NetBIOS, освобождает ресурсы КД при обращении к КД доверенных доменов, находящихся вне зоны досягаемости и позволяет сохранить корректную работу механизмов изоляции.