softline® ПРЕМЬЕР СЕРВИСЫ

Подводные камни при переходе на ALD Pro

Александр Белозерцев

Премьер Сервисы Софтлайн

- Более 100 обследований инфраструктур заказчиков по различным технологиям
- Обследования по open source технологиям (Zabbix, PostgreSQL, Linux)
- Разработка стратегий резервного копирования и восстановления
- «Приземление» облачный сервисов, миграции между тенантами
- Проекты по импортозамещению
- Специализированные сервисы и кастомные работы
- Предоставление выделенного инженера
- Курсы с практической частью

Типичные вопросы

- Хотим сделать как в MS только на Linux
- А Exchange/SharePoint/etc будет работать с ALD Pro?
- Мы имеем много филиалов со своими доменами как поступить?
- У нас тут ERP система своей разработки она переживет переезд?
- У нас много legacy серверов с софтом работающим только не них
- Исторически так сложилось…

Точка входа – обследование текущей Active Directory у заказчика

Подводные камни. Дочерние домены AD

- ALD Pro как и FreeIPA не поддерживает иерархическую структуру доменов как MS AD
- Дочерний домен давно уже не считается границей безопасности. Компрометация дочернего домена легко ведёт к компрометации всего леса.
- Сценарии перехода
  - Отказаться от дочерних доменов – переезд в плоский лес (сложно и долго)
  - Создать несколько доменов ALD Pro и доверительные отношения с каждым доменом (сложно)
  - Создать один домен ALD Pro и использовать Pragmatic Tool для миграции (дорого)

Подводные камни. NTLM

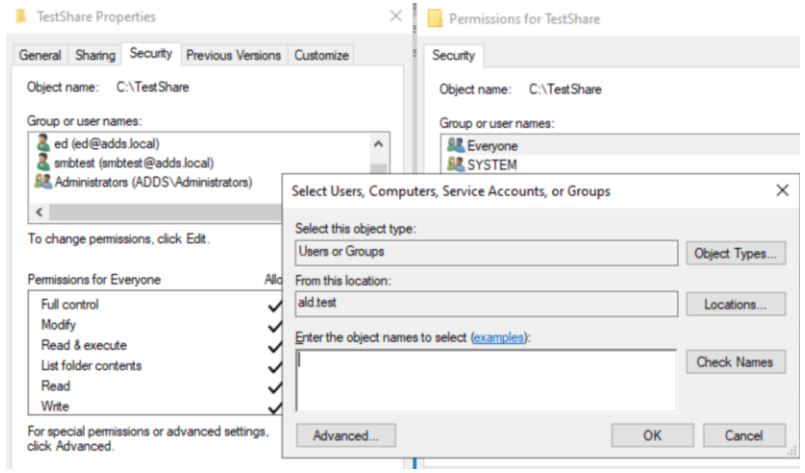
- ALD Pro как и FreeIPA не поддерживает NTLM
- Необходимо
  - Поиск и выявление систем которые используют слабые протоколы аутентификации
    - Транзитный NTLM (EventID 8004, 8006)
    - Входящий и исходящий NTLM (EventID 8001 - 8003)
  - Выявления возможных проблем в конфигурации Kerberos и в конфигурации сервисов
    - В основном проблемы с SPN
  - Керберизация сервисов, если это возможно

Подводные камни. LDAP Simple Bind

- ALD Pro поддерживает аутентификацию через LDAP Simple Bind
- Некоторые системы обращающиеся к конкретному контроллеру домена через LDAP и их нужно перенацелить на ALD Pro
- Существует проблема идентификации таких систем
- Как искать?
  - Высокая нагрузка на конкретный контроллер
  - Если LDAP Simple Bind не шифруется то можно определить источник по журналам событий (2886, 2887)
  - Если использует LDAPS определить можно только косвенно (неэффективные запросы)

Подводные камни. Авторизация

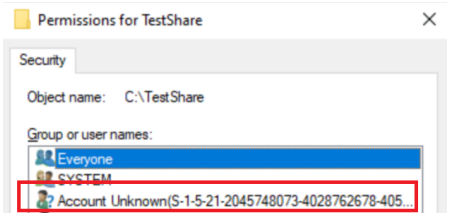
- В ALD Pro нет глобального каталога, то есть не работает поиск пользователей домена ALD Pro из стандартных форм в домене MS AD.



- Выход из ситуации
  - Получить SID пользователя с помощью утилиты wbinfo в домене ALD Pro
  - При помощи утилит subinacl или icacls в явном виде добавить пользователя в список доступа

```
PS C:\Program Files (x86)\Windows Resource Kits\Tools> ./subinacl /errorlog="c:\temp\errorlog.txt" /outputlog="c:\t
utputlog.txt" /file "c:\testshare" /grant="S-1-5-21-2045748073-4028762678-4055919142-1019"=F

Elapsed Time: 00 00:00:01
Done:         1, Modified         1, Failed         0, Syntax errors         0
Last Done   : c:\testshare
```



Подводные камни. Авторизация

- ALD Pro автоматически назначает идентификаторы SID для групп и пользователей
- Есть ограничение в 200 000 таких идентификаторов.
- При большом количестве объектов можно столкнуться с ситуацией когда этот диапазон закончится

- Выход из ситуации
  - Есть возможность обратиться в техподдержку ALD Pro для расширения диапазона, пока в ручном режиме

Подводные камни. Что еще

- FGPP (Fine-Grained Password Policy) в ALD Pro только на группу
- Нельзя назначить политики на группу или пользователя, только на OU (Security filtering)
- MSA/gMSA

Точки входа в Премьер Сервисы

- Если вы уже работаете с Софтлайном
  - Account Manager (AM)
  - Technical Account Manager (TAM)
- Если вы еще не работаете с Софтлайном
  - premier@softline.com