Планы развития Samba: upstream и downstream (Fedora)

Александр Боковой

October 17, 2015

Red Hat Ltd

О себе

Александр Боковой:

- Principal Software Engineer, Red Hat
- Член Samba Team с 2003
- Разработчик FreeIPA и SSSD с 2011

Введение

История (удаленной) любви

В основе Active Directory — технологии, пришедшие из UNIX: LDAP, Kerberos, DNS, DHCP, сертификаты x.509...

Системы под управлением Linux могут работать с Active Directory на разных уровнях, но в большинстве случаев заказчики заинтересованы в:

- запуск процессов, используя учетные записи пользователей Active Directory
  - Аутентификация средствами LDAP, SMB или Kerberos
  - Авторизация централизованным образом с использоанием групповых политик AD или похожих механизмов допуска
  - Аудит
- Интеграция систем под управлением Linux в среду под контролем Active Directory

История (удаленной) любви

Существует два способа развертывания систем в среде под контролем Active Directory

- Прямой: сделать систему частью домена в лесу Active Directory
- Непрямой: сделать систему частью другого домена в другом лесу Active Directory

Прямой флирт

Прямая интеграция систем под управлением Linux в домен в лесу Active Directory достигается двумя способами:

- Samba, используя winbindd
- SSSD

Оба подхода имеют свои достоинства и недостатки. Так, SSSD не поддерживает сложные топологии внутри леса Active Directory без помощи FreeIPA, а системы под контролем winbindd не всегда работают стабильно.

Благодаря Стефу Уолтеру и проектам adcli и realmd, интеграция систем Linux в существующий домен в лесу Active Directory стала очень простой, начиная с Fedora 19.

Но прямая интеграция не устраняет проблему наличия лицензий CAL.

Любовь по переписке

Непрямая интеграция означает использование леса Active Directory, но необязательно от Microsoft.

Существуют по меньшей мере две реализации, которые не требует CAL:

- Samba AD не требует CAL
- FreeIPA не требует CAL

* FreeIPA не является реализацией Active Directory, но об этом позже

Технические основы любви

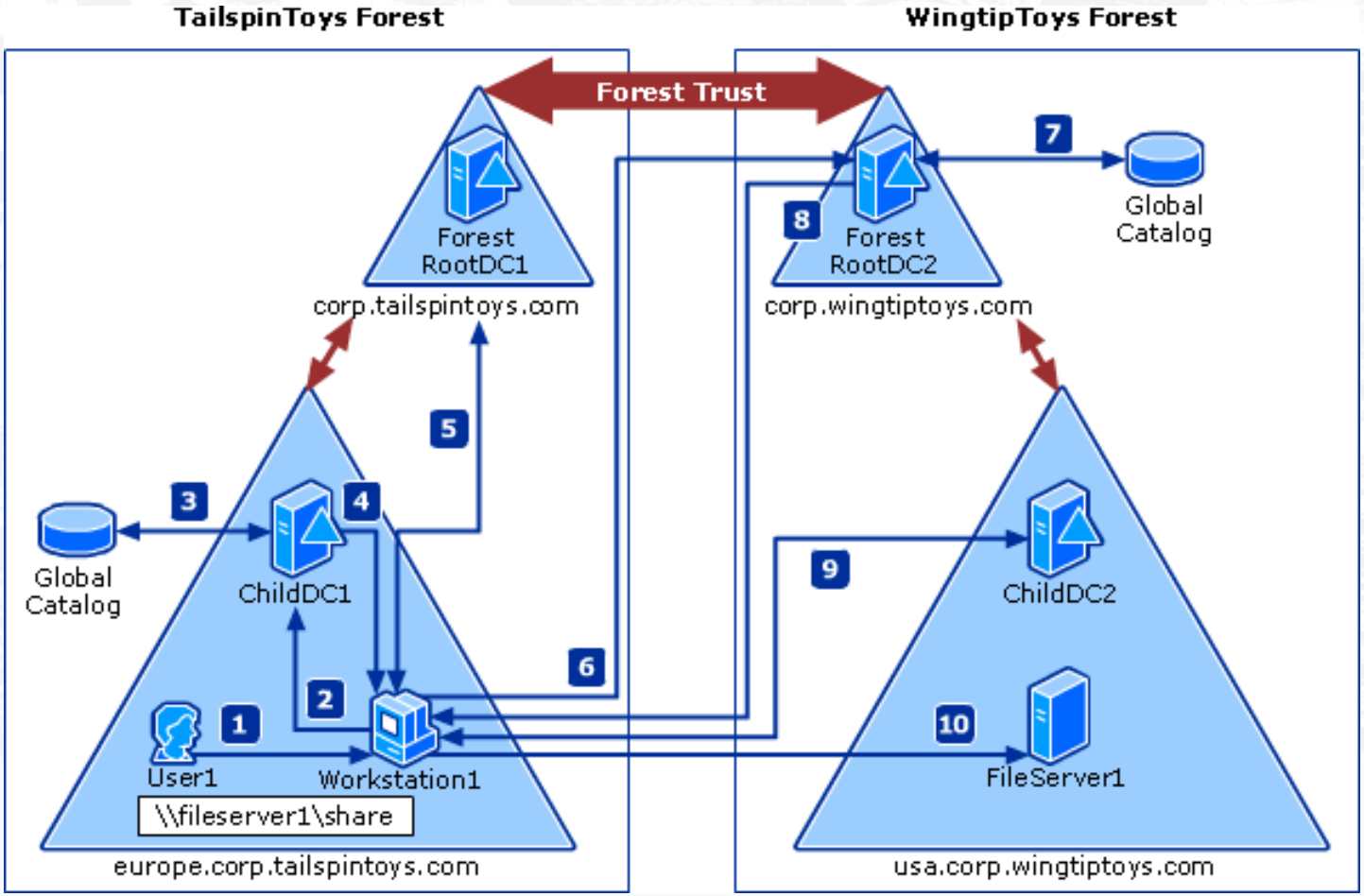
Доверительные отношения: случай Active Directory

Доверительные отношения (*trust relationship*) позволяют пользователям из одной системы управления ресурсами выполнять действия над службами другой системы управления ресурсами. Сами системы между собой никаким иным образом не связаны.

FreeIPA поддерживает установление доверительных отношений с Active Directory. На стороне AD эти отношения видны как *cross-forest trust* к другому лесу Active Directory.

Доверительные отношения типа cross-forest trust устанавливаются между корневыми доменами обоих лесов. Каждый корневой домен Active Directory может доверять другим доменам в своем лесу. Домен внутри леса доверяет транзитивно другому лесу через свой путь доверия корневому домену своего леса.

Доверительные отношения: случай Active Directory



Подробнее: “How domains and forest trusts work in Active Directory”

Основы доверия

Домены в лесу Active Directory – это realm Kerberos. *Контроллеры домена* обеспечивают работу служб KDC, LDAP, SMB, DNS (и многих других). Для каждого пользователя в домене существует объект в LDAP и соответствующая учетная запись (principal) Kerberos.

Каждая машина в домене AD имеет объект в LDAP (account) с именем `MACHINE$`. Этому объекту в терминах Kerberos соответствует учетная запись `host/f.q.d.n@REALM`. Каждая служба Kerberos на машине в Active Directory представляет собой ссылку на объект `MACHINE$`. Все эти службы используют один и тот же ключ Kerberos, но могут быть предназначены для разных задач. Клиенты могут запрашивать билеты Kerberos к соответствующим службам, а не напрямую по имени машины.

Адресация объектов и доступ к ним

Когда установлены доверительные отношения между двумя доменами Active Directory, в LDAP каждого домена существует специальный объект, представляющий доверяемый домен. Также в LDAP существует учетная запись, представляющая доверяемый домен как NetBIOS-имя доверяемого домена *плюс знак $*. Таким образом, доверяемый домен представляет собой специальный случай машинной учетной записи.

Учетная запись доверяемого домена является полным эквивалентом учтеной записи Kerberos `krbtgt/TRUSTED.REALM@TRUSTING.REALM`. Если в области Kerberos есть такая учетная запись, то учетная запись в `TRUSTED.REALM` может быть использована для получения *cross-realm TGT* и полученный билет может быть использован для доступа к ресурсам в `TRUSTING.REALM`.

Адресация объектов и доступ к ним

Доверяющий домен в Active Directory может ограничить доступ к своим ресурсам. Каждая учетная запись в Active Directory имеет связанный с ней идентификатор безопасности (*security identifier*, *SID*). SID имеет универсальную структуру: *S-1-2-3-4-56789-0123*, где первые несколько чисел представляют контекст предназначения SID, а остальное кодирует домен и учетную запись внутри домена.

Преобразование SID в имя учетной записи осуществляет контроллер домена. Доступ к соответствующей службе требует аутентификацию. Контроллер домена из доверяемого домена может преобразовать SID в имя из доверяющего домена, основываясь на аутентификации средствами учетной записи, которая существует для него в доверяющем домене.

Для преобразования можно использовать службу Global Catalog в корневом домене леса Active Directory. Она содержит информацию об учетных записях во всем лесу.

FreeIPA

FreeIPA как Active Directory

На самом деле, FreeIPA не является Active Directory

Пользователи из доверяемого леса Active Directory могут использовать ресурсы на машинах в домене FreeIPA

FreeIPA реализует двухстороннее (начиная с версии 3.0) и односторонее (начиная с версии 4.2) доверие лесу Active Directory.

Однако пользователи FreeIPA не могут использовать интерактивные службы Windows, даже если между лесами Active Directory и FreeIPA установлено двухстороннее доверие.

Поддержка Global Catalog

Global Catalog — это специальный LDAP сервер в Active Directory, хранящий ограниченный набор атрибутов всех учетных записей в лесу Active Directory.

FreeIPA пока не представляет Global Catalog и поэтому службы на стороне Active Directory не могут использовать FreeIPA для преобразования имен пользователей FreeIPA в SID-ы при входе в систему или назначении прав доступа.

FreeIPA Global Catalog

Работа над поддержкой Global Catalog в FreeIPA запланирована на версию 4.4

Сложности:

- [x] Схема LDAP для Global Catalog несовместима с FreeIPA (или любой другой схемой в мире не-Windows) на уровне базовых атрибутов. Это означает использование отдельного сервера LDAP.

FreeIPA Global Catalog

Работа над поддержкой Global Catalog в FreeIPA запланирована на версию 4.4

Сложности:

- Схема LDAP для Global Catalog несовместима с FreeIPA (или любой другой схемой в мире не-Windows) на уровне базовых атрибутов. Это означает использование отдельного сервера LDAP.
- Требуется реализовать синхронизацию и пополнение по запросу этого отдельного сервера данными из основного сервера LDAP для FreeIPA.

Samba AD

Samba AD

В Active Directory состояние информации о пользователях и доменах синхронизировано между разными протоколами. Можно добавить учетную запись средствами запросов SMB и далее авторизоваться силами Kerberos и получить доступ к LDAP. Установление доверительных отношений между лесами Active Directory требует ”скачков” между LDAP и SMB на отдельных этапах процесса.

Когда Andrew Tridgell работал в IBM Research в 2003 году, он “форкнул” собственный код Samba для эксперимента над единой базой данных для многопротокольного доступа. Эта работа переросла в Samba Active Directory как часть Samba 4.0 в 2012. Первая тестовая версия была выпущена в 2006.

Потребовалось порядка 10 лет для того, чтобы добраться до релиза.

Samba AD: служебный роман

Samba AD была построена так, чтобы LDAP, Kerberos, SMB, и DNS сервера работали в рамках одного процесса.

В 2003-2006 годах считалось, что невозможно быстро и итеративно вести анализ недокументированных расширений протоколов LDAP, Kerberos и SMB в Active Directory с эффективным взаимодействием между многими свободными проектами.

Samba Team реализовала собственные версии серверов SMB, LDAP и DNS, а также интегрировала реализацию Heimdal Kerberos. Схема LDAP следует за Active Directory и несовместима со стандартными схемами в UNIX.

Samba AD: служебный роман

* В декабре 2007, благодаря решению суда по делу European Commission vs Microsoft, Microsoft начала публикацию документации на серверный стек протоколов Windows под лицензией, позволявшей реализацию, совместимую с GNU GPL v3. Samba Team была ключевым свидетелем в судебном процессе и для лицензирования протоколов была создана Protocol Freedom Foundation, членом которой может стать любой разработчик, планирующий использовать документацию Microsoft для работы над Samba.

Samba AD: встроенный сервер Kerberos

Использование встроенного сервера Heimdal Kerberos в Samba AD делает невозможным внедрение Samba AD в большинстве дистрибутивов Linux.

Fedora и OpenSuSE используют MIT Kerberos. Сервер MIT Kerberos (KDC) нельзя встраивать в другие приложения как библиотеку. Он не поддерживает и некоторые из интерфейсов, которые Samba использует в Heimdal. Совместимость на уровне протокола не означает совместимость ABI или API — как со стороны сервера, так и со стороны клиента.

Samba AD: встроенный сервер Kerberos

Andreas Scheinder и Guenther Deschner три года работали над переходом Samba AD с Heimdal на MIT. Проблему встраивания Kerberos сервера решили с помощью `socket_wrapper` — MIT KDC теперь можно запускать в отдельном процессе.

Samba 4.3 включается частичную поддержку сборки Samba AD с MIT Kerberos. Примерно 50-70 патчей еще надо интегрировать и дописать до Samba 4.4.

Samba AD: cross-forest trust

Samba 4.3 также включает и базовую инфраструктуру для доверия между лесами Active Directory.

Samba AD может доверять и быть доверяемой FreeIPA: пользователи из Samba AD могут использовать службы на машинах из FreeIPA.

Это выглядит простым достижением, но оно потребовало около года разработки и все еще не завершено.

Fedora 24?

Мы планируем интегрировать Samba AD в Fedora 24.

Для промышленной эксплуатации Samba AD нужно еще сделать довольно много:

- Скрипты развертывания необходимо активно тестировать
- Интеграция с FreeIPA и SSSD требует доработку Samba AD для использования совместимых методов idmap и автоматическую настройку GPO
- Необходимо провести анализ безопасности кода Samba AD и реализовать недостающие правила разделения доступа между группами безопасности.
- Необходимо доработать репликацию в Samba AD (DRS, FRS/DFSR, read-only DC)
- Необходимо дописать недостающие функции NetLogon и LSA
- … и многое другое: активные проекты Samba Team

Файловый сервер: поддержка SMB3

Samba AD — только часть Samba. Файловый сервер живет свой жизнью и требует своего внимания.

С выходом протокола SMB3, потребовалось начать работу над целым рядом новинок:

- ☒ новая инфраструктура шифрования [4.0]
- ☒ защищенное установление соединения [4.0]
- ☒ долгоживующие контексты v2 [4.0]
- ☒ постоянные файловые контексты [WIP/glusterfs]
- ☒ многоканальные соединения [WIP]
- ☒ SMB direct (RDMA) [designing/starting]
- ☒ Witness protocol [WIP+]

Infrastructure или просто пакеты?

Наша задача в Fedora — обеспечить больше, чем просто доступность собранных пакетов.

У Samba более 500 конфигурационных настроек только для файловой части. Samba has more than 500 configuration options for file server alone.

Samba AD добавляет LDAP схему AD и отдельные настройки для внешних служб.

FreeIPA содержит собственную схему LDAP и собственные расширения. Мы хотим унифицировать POSIX часть схемы так, чтобы оба сервера могли бы использоваться одновременно и прозрачно, а поддержка дистрибутивов не погибла бы под комбинаторным ростом возможных сценариев.

Infrastructure или просто пакеты?

С интеграцией Samba AD мы хотим добиться использования FreeIPA для управления машинами под Linux и Samba AD для управления машинами Windows для организаций малого и среднего бизнеса.

Вопросы?