Назад в будущее

вместе с FreeIPA и Samba

В ролях: FreeIPA, SSSD, Samba
Сценарий: Alexander Bokovoy, Stephen Gallagher, Chris Hertel
Иллюстрации Máirín Duffy (CC-BY)

Будущее
(по мнению аналитиков)

- Данные как платформа
- Облачные вычисления
- От серверов к сервисам
- Рост разнообразных рисков
- Социальные сети повсюду
- Простота использования прежде всего

Будущее
(глазами потребителей)

- Где мои данные?
- Всегда онлайн! Ничего не упустить!
- Ты в сети А/Б/В/Г? Подружись со мной!
- Мой браузер тормозит!
- Корпоративные системы такие устаревшие!!!

Настоящее (последние 25 лет)

- “Давай для этого развернем виртуалку!”
  - От мейнфреймов к ПК и мобильнику
- Повсюду LDAP и Kerberos
  - Только за файрволлом
  - А, еще и файрволлы!
- Файлы – не только вложения в почту!
  - Скорость доступа также важна
- Безопасность – просто кошмар
  - Кому доверять?

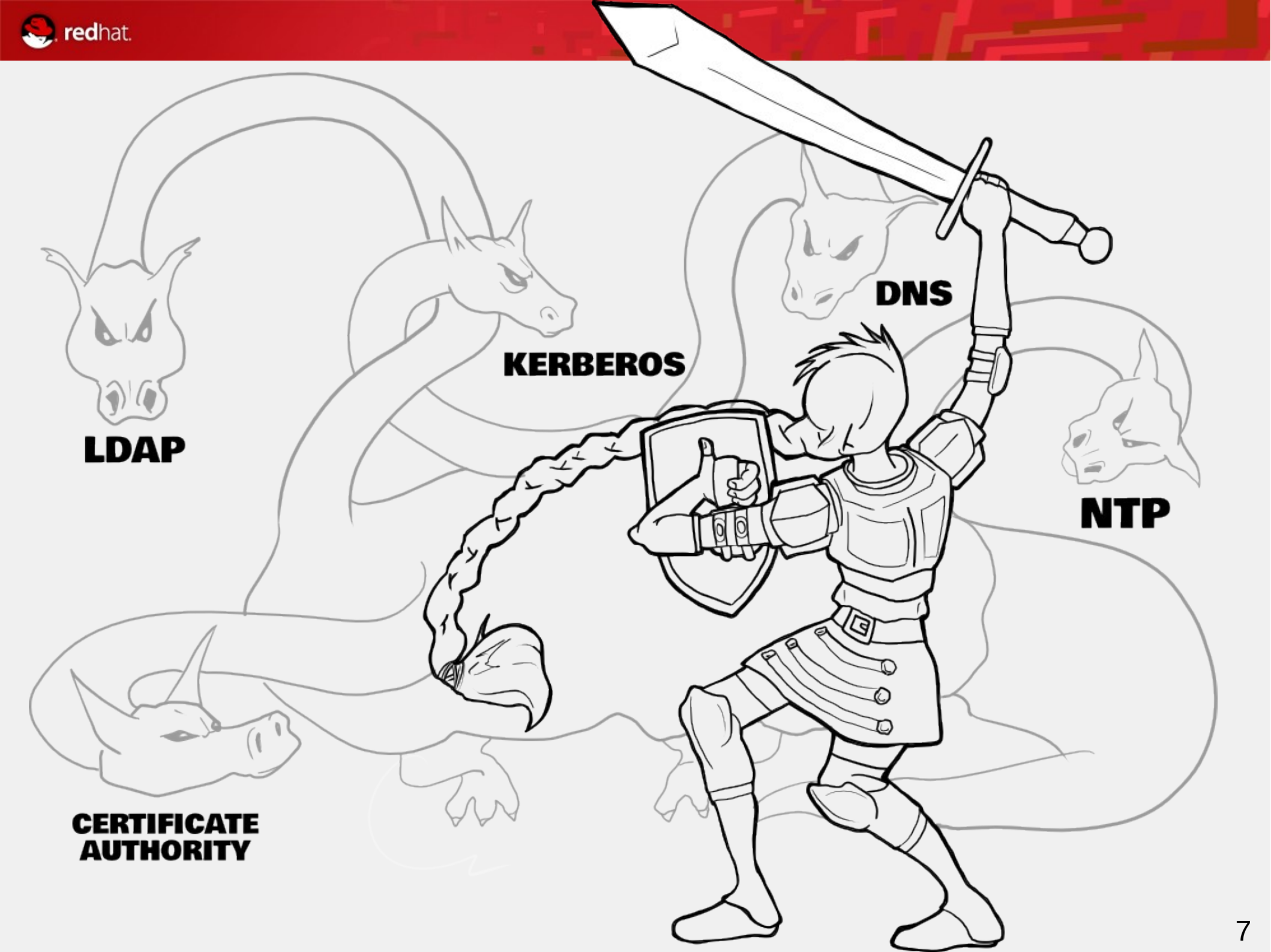
Куски мозаики

(по мнению администраторов)

- LDAP
  - 1993, на основе X.500 из 1984-1986
- Kerberos
  - проект Athena, 1983
- NTP
  - ранее 1985
- DNS
  - 1982
- Сертификаты
  - с 1969 (стандарт X.509 принят в 1988)
- Файловые системы
  - NFS – 1984, SMB – 1983

1982 – 1986... что-то это все напоминает?

Photo: Adam Lautenbach, CC-BY-2.0


DNS
KERBEROS
LDAP
NTP
CERTIFICATE
AUTHORITY

LDAP

- Механизм для хранения структурированных пользовательских данных
- Индустриальный стандарт
- Расширяемый до невозможности

Классический LDAP

- Сложное структурирование данных
- Каждое внедрение использует свое распределение данных
- Отсутствуют гарантии целостности отношений между данными
- Постоянно заново изобретаются одни и те же схемы данных
- Сложные средства управления

LDAP во FreeIPA

- Сервер 389-ds и около десятка плагинов к нему обеспечивают:
  - Предопределенную схему
  - Принудительное сохранение целостности отношений между данными и группами данных
  - Централизованное выделение ID
  - Гибкую систему контроля доступа к данным
- Совместимость со стандартными клиентами LDAP

LDAP во FreeIPA

- Интерфейс XML-RPC для настройки
- Утилиты командной строки для предметно-ориентированной настройки объектов LDAP
- Веб-интерфейс для графической настройки
- Глобальные описания правил доступа к ресурсам на клиентских машинах

System Security Services Daemon

- На клиентской стороне: реализация служб NSS и PAM
- Оффлайновая поддержка пользователей, групп и сетевых групп
- Аутентификация LDAP с поддержкой Kerberos GSSAPI
- Подробнее о SSSD: статья Marko Myllynen в Linux Weekly News (lwn.net): https://lwn.net/Articles/457415/

LDAP

Kerberos

- Надежная аутентификация
- Поддержка единой точки входа (SSO) для приложений
- Совместимость с GSSAPI для зашифрованного обмена данными

Классический Kerberos

- Легко ошибиться в настройке
- Используется отдельная база данных для хранения аутентификационных материалов
- Постоянные проблемы с синхронизацией времени между клиентами и серверами

Kerberos во FreeIPA

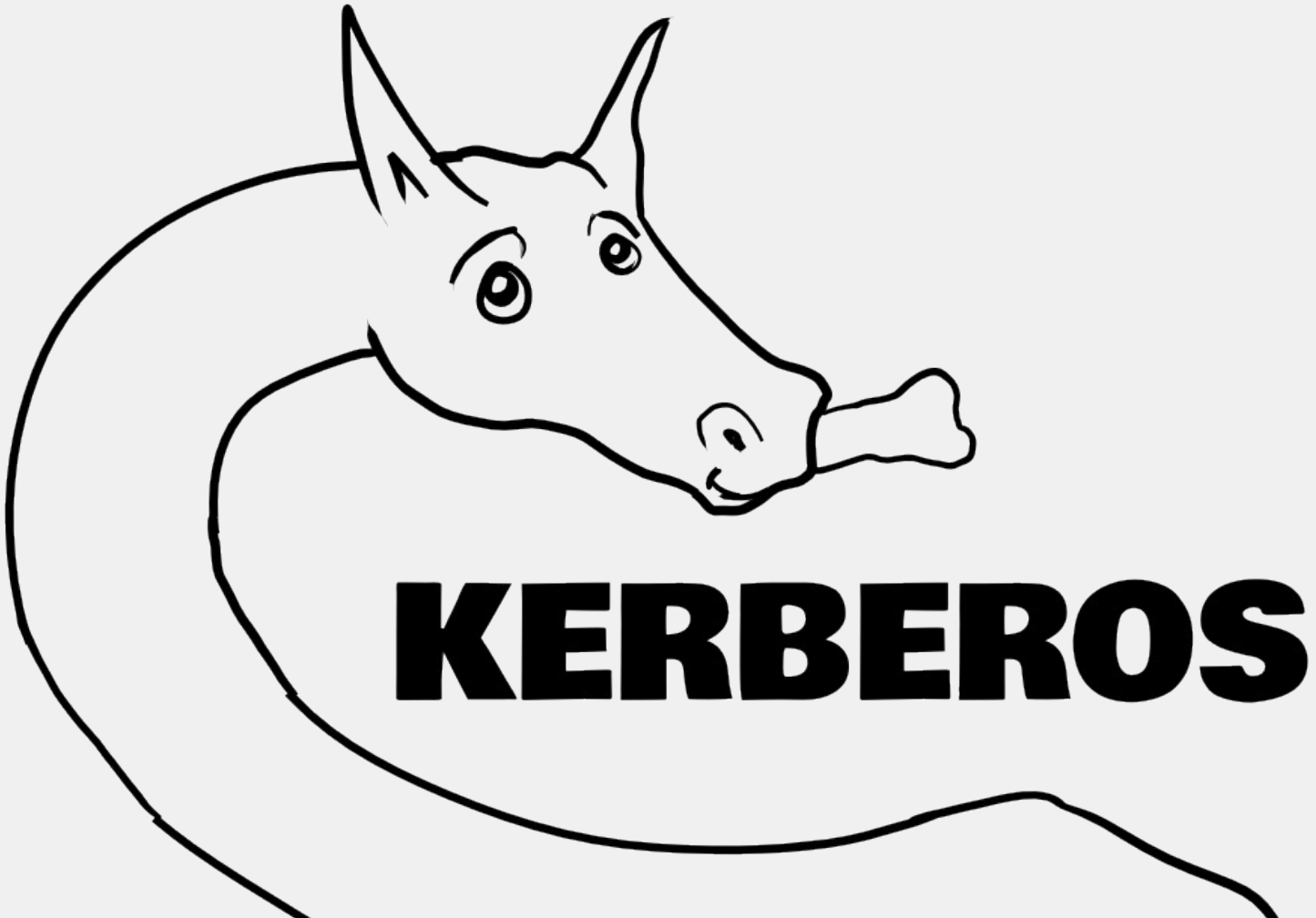
- Данные Kerberos хранятся в LDAP
- Простая настройка и управление средствами FreeIPA
- Клиенты FreeIPA автоматически синхронизируются по времени
- Методика автоматической миграции паролей пользователей

System Security Services Daemon

- Офлайновое кеширование паролей Kerberos
- Можно настроить для автоматического получения TGT (ticket granting ticket) при подключении к сети (например, вход в VPN)
- Может автоматически обновлять имеющиеся билеты Kerberos

System Security Services Daemon

- Поддерживает защищенную миграцию паролей пользователей LDAP в Kerberos при использовании вместе с FreeIPA
- Поддерживает правила FreeIPA для контроля доступа к ресурсам (host-based access-control, HBAC)


KERBEROS

NTP

- Синхронизация времени между различными системами
- Высокая точность, отличная коррекция расхождений часов

NTP во FreeIPA

- Клиент FreeIPA автоматически настраивается на сервер FreeIPA как достоверный источник времени
- Не требуется вмешательство пользователей или администраторов

NTP

DNS

- Обеспечивает преобразование между адресами IPv4 или IPv6 и доменными именами, понятными большинству пользователей
- Позволяет автоматически обнаруживать сетевые службы
- Предоставляет средства балансировки нагрузки для разных сетевых служб

Классический DNS

- Настройка вручную путем редактирования файлов описаний зон
- Сложность для настройки динамических обновлений соответствий адресов и имен машин

DNS во FreeIPA

- Настройка средствами FreeIPA поверх интерфейса XML-RPC
- Графический интерфейс для настройки доменных зон
- Утилита командной строки для скриптования
- Автоматическая настройка LDAP и Kerberos для обнаружения служб через DNS

System Security Services Daemon

- Автоматическое обновление имен машин в DNS при изменении IP-адреса клиента
- Выполняется по защищенному каналу на основании выданного и подписанного билета Kerberos


DNS

Сертификаты

- Используются для гарантий доверенности сетевых служб
- Сертификаты сетевых служб должны быть подписаны доверяемым источником сертификатов

Классические сертификаты

- Сертификаты выпускаются доверяемым агентством
  - Дорого
  - Внешнее доверие не всегда надежно (случай DigiNotar)
- Самоподписанные сертификаты
  - Плохо устанавливаемое доверие
- Настройка своего агентства сертификатов
  - Довольно сложно

Сертификаты во FreeIPA

- Интеграция с системой сертификатов Dogtag
- Частное агентство сертификации с простым способом настройки
- XML-RPC, Web-интерфейс и средства командной строки для управления сертификатами
- Упрощенный способ настройки клиентов для доверения частному агентству сертификации

Certmonger

- Автоматически ведет учет сертификатов на клиентской машине
- Отправляет запросы на перевыпуск сертификатов служб до того, как они прекратят действовать
- Автоматически настраивается на каждом клиенте FreeIPA


CERTIFICATE
AUTHORITY

FreeIPA v2.1

- Версия FreeIPA 2.1.4 вышла 6 декабря 2011 года
- Полностью поддерживаемая “фича” основной системы RHEL 6.2
- Доступна всем заказчикам RHEL в рамках базовой лицензии, включая полную поддержку репликации
- Доступна всем пользователям Fedora 16

Назад в будущее
FreeIPA v3

- Поддержка доверительных отношений между доменами Kerberos
- Улучшенная интеграция с существующими доменами Active Directory
- Поддержка многофакторной аутентификации
- Поддержка множества клиентских платформ
- Подробнее будет на Fedora DevConf 2012
- https://fedoraproject.org/wiki/DeveloperConference2012

Upstream и Downstream

- Поддержка множества клиентских платформ во FreeIPA
- FreeIPA 2.1.1 включает “платформизацию”
  - Абстракция деталей реализации системных служб
  - Изначально планировалась для поддержки systemd в Fedora 16
- Предварительная поддержка Ubuntu Oneiric
  - 20 шагов настройки вручную в сентябре 2011, сокращены до ~5 к декабрю
  - Canonical уже добавила необходимые пакеты в базу Precise Pangolin

Samba

- Samba 3.6.0 выпущена 9 августа 2011
- Реализация протокола SMB 2
  - Первый выпуск с SMB 2, по умолчанию отключен
- Переписан механизм настройки ID
  - Упрощена настройка
  - Отличается от 3.0
- Интегрирован SMB Traffic Analyzer
  - Больше методов тюнинга высокопроизводительных систем

Samba

- Поддержка печати
  - Подсистема spoolss переписана
  - Лучше совместима с клиентами печати Windows
- End-point mapper
  - Позволяет отделить обработчиков протоколов и основной процесс Samba
  - Ключ к сосуществованию Samba и других служб CIFS на том же сервере (OpenChange, FreeIPA v3)

Samba Team и Microsoft

- Storage Developers Conference 2011
  - Microsoft представила протокол SMB 2.22 and альфа версию своих утилит
  - SMB 2.22 спецификация
  - Начата работа по реализации SMB 2.22 в свободном ПО
    - Патчи для Wireshark были опубликованы через неделю после конференции!
    - Экспериментальная поддержка SMB 2.22 в git master Samba уже в декабре 2011
  - Сервер Samba 4 AD server протестирован на совместимость с реализациями других вендоров
- Подробнее

http://www.samba.org/samba/news/developers/2011-snia-sdc-report.html

Samba Team и Microsoft

- IOLab на территории Microsoft
  - Ежегодная недельная встреча с инженерами Microsoft для “сверки часов”: что работает и что не работает по обе стороны
- Protocol Freedom Information Foundation
  - Создан в декабре 2007 для соответствия решению Еврокомиссии от 25 марта 2004 в деле об антимонопольном поведении Microsoft.
  - Дает лицензионное соглашение "Microsoft Work Group Server Protocol Program License Agreement (No Patents) for Development and Product Distribution" на условиях, совместимых с GNU GPLv3
  - Дает субконтракторам PFIF приоритетную поддержку со стороны команд разработки и документирования Microsoft

Samba 4

- Полная замена Active Directory
  - Протоколы Active Directory Windows 2000 и старше
- Статус: альфа, Samba 4.0 alpha 17
  - Будет выпущена, когда будет готова!
  - Объединит функционал Samba 3.6 и предыдущих альф Samba 4
  - Постепенное “слияние”, см. git master и s3fs-wip у tridge
  - Включает собственные сервера Kerberos и LDAP
  - Начальная стадия поддержки репликации DRS
  - Поддержка Samba4 как внешний источник аутентификации пакетов MS-SNTP уже интегрирована в NTP

Ресурсы

- FreeIPA:
  - http://www.freeipa.org
- SSSD:
  - http://fedorahosted.org/sssd

Вопросы?

42