

Fedora Directory Server – сервер каталогов уровня предприятия



Андрей Маркелов

Когда говорят о проекте Fedora, в первую очередь имеют в виду одноименный дистрибутив операционной системы Linux. Однако в рамках Fedora Project идет работа не только над Fedora Linux, но и над рядом смежных проектов. Об одном из них – Fedora Directory Server, очередная версия которого вышла в начале января этого года, – и пойдет речь.

Обзор возможностей FDS и история создания

О серверах каталогов наш журнал уже писал, и не один раз. В обзоре, посвященном конкретному продукту, мы не будем рассматривать основы LDAP или возможные варианты использования каталога, а сразу перейдем к одному из серверов, который до сих пор не попадал в поле зрения «Системного администратора».

Что же такое Fedora Directory Server (FDS)? Это сервер каталогов уровня предприятия с открытым исходным кодом, его особенности см. во врезке «Возможности Fedora Directory Server».

Нужно заметить, что помимо прочего, FDS является основой проекта по созданию централизованного решения для управления информацией о пользователях, политиках и аудита на предприятии – FreeIPA [2].

Как известно, компания Red Hat, спонсирующая проект Fedora, использует наработки этого проекта в своих коммерческих продуктах, предоставляя для них услугу технической поддержки. Такая модель является весьма эффективной, что доказывает тот факт, что вслед за Red Hat подобную схему разработки подобную связку «коммьюнити дистрибутив»-«коммерческий дистрибутив», позаимствовали, например Novell (проект openSUSE) и Sun Microsystems (проект OpenSolaris).

По аналогии с операционной системой компания Red Hat такой подход использует и для своего сервера каталогов. Предыдущей версии FDS 1.0.x соответствовал Red Hat Directory Server (RHDS) версии 7.1. Новая версия RHDS 8.0, которая будет основана на FDS 1.1, скорее всего уже будет доступна к моменту выхода этого номера журнала в свет.

Проект FDS появился не на пустом месте и имеет длинную историю разработки. Она начинается в 1996 году, когда Netscape для работы над своим сервером каталогов нанимает создателей оригинального LDAP-сервера из Университета Мичиган (от которого ведет свою историю OpenLDAP). В 1999 году после покупки Netscape компанией AOL был сформирован альянс iPlanet, в который также входила компания Sun Microsystems. Он просуществовал

до 2001 года, когда Netscape и Sun продолжили разработку каждый своего «форка». В 2004 году компания Red Hat купила Netscape Directory Server, начав процесс открытия исходного кода сервера каталогов. Результатом этого процесса и стал Open Source-сервер каталогов под названием Fedora Directory Server. К настоящему моменту FDS 1.1 (равно как и грядущий RHDS 8.0) собирается исключительно из открытых исходных текстов.

Если говорить о конкретных свободных лицензиях, то нужно учесть, что продукт состоит из нескольких разных компонентов, каждый из которых распространяется под своей лицензией (MPL/LGPL/GPL/X License и другие). Подробности доступны по ссылке [3].

Основные компоненты сервера

Как уже было отмечено ранее, Fedora Directory Server состоит из нескольких основных компонентов. Безусловно, самый главный – это сам сервер каталогов. Архитектурно он содержит:

- «Фронттовую» часть, отвечающую за сетевую коммуникацию.
- Механизм расширений, через который реализуются дополнительные функции, например репликация или контроль доступа.
- Базовое дерево каталога (DIT), содержащее информацию, относящуюся к самому серверу
- «Бэк энд», исполняющий роль «прослойки» между сервером каталогов и БД Berkeley DB. Berkeley DB, как известно, была адаптирована в Sleepycat Software под нужды сервера каталогов, после того как за его разработку взялась Netscape.

Следующий важный компонент – сервер администрирования (Administration Server). Его задачей является управление серверами каталогов как через веб-интерфейс, так и при помощи специальной Java-консоли, которая общается с сервером администрирования по протоколу HTTP или HTTPS. К слову, наиболее заметным

Возможности Fedora Directory Server

- Поддержка LDAPv3.
- Возможность использовать до четырех полностью равноправных мастер-серверов с автоматическим разрешением конфликтов. Каждая из реплик (фактически это копия мастер-сервера, доступная только для чтения) может быть настроена на последовательный опрос всех мастеров, обеспечивая высокую надежность всей системы. Предусмотрены балансировка нагрузки и автоматическое переключение на работу с другим мастером в случае выхода одного из строя.
- Высокая масштабируемость. По заявлениям разработчиков, из расчета на один сервер: тысячи операций в секунду, десятки тысяч пользователей, десятки миллионов записей и сотни гигабайт данных.
- Возможность синхронизации пользователей, групп и паролей с контроллерами домена Active Directory (2000 and 2003) или NT4. Данная возможность осуществляется через специальный компонент Windows Sync, который устанавливается на доменный контроллер. Единицей синхронизации является под-ветвь дерева.
- Утилиты управления с графическим интерфейсом, управления из командной строки и через веб-интерфейс.
- Безопасная аутентификация и транспорт (SSLv3, TLSv1 и SASL).
- Мощный механизм разграничения доступа вплоть до уровня отдельных атрибутов. Правила доступа на основе имени пользователя, групп, IP-адреса, времени суток и других критериев. Стандарт LDAP не описывает, в каком виде сервер каталогов хранит информацию о правах доступа. В FDS используется механизм и синтаксис, аналогичный Sun Java System Directory Server 5.2 – опциональные атрибуты aci (access control instructions).
- Поскольку права доступа могут наследоваться от родительских записей, у администратора имеется возможность воспользоваться функцией определения эффективных прав (GetEffectiveRights).
- Шифрование выбранных атрибутов записей.
- Возможность обновлять схемы, осуществлять импорт, экспорт и работать с резервными копиями в «горячем» режиме без остановки сервера.
- Комплект подробной документации.
- Многое другое. Полный список возможностей можно найти в [1].

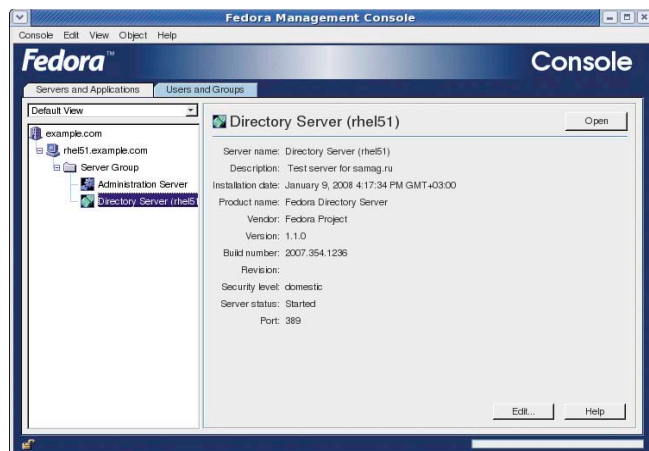


Рисунок 1. Главное окно консоли управления (Linux)

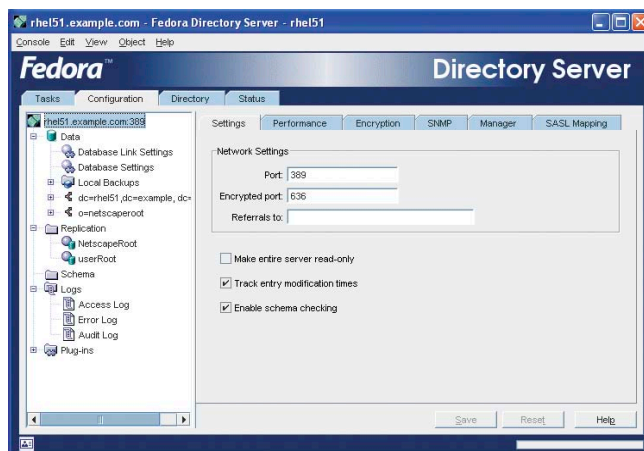


Рисунок 2. Консоль Directory Server (Windows)

отличием FDS от актуальной версии RHDS 7.1 (помимо модели технической поддержки) является использование для сервера администрирования веб-сервера Apache вместо Netscape Enterprise Server 6.2.

Основной графический инструмент управления серверами – консоль Fedora Management Console, написанная на Java. Из главного экрана (см. **рис. 1**) вы можете вызвать консоли для управления самим сервером каталогов (см. **рис. 2**) и сервером администрирования (см. **рис. 3**). Консоль взаимодействует как по протоколу HTTP/HTTPS с сервером администрирования, так и через LDAP с сервером каталогов напрямую.

Fedora Management Console также доступна для управления вашими серверами и с машин, работающих под управлением ОС семейства Windows. Дистрибутив в виде msi-пакета и инструкции по установке расположены на сайте проекта. Обратите внимание на версии Java, с которыми консоль гарантированно работает. На **рис. 2, 3** как раз представлены снимки экрана консоли, запущенной в среде ОС Windows XP.

Также в состав Fedora Directory Server входят ряд CLI-утилит администрирования и скриптов для миграции/импорта/экспорта и др.

Тестовая установка

Рассмотрим типовые шаги по установке сервера каталогов на машину под управлением RHEL/Fedora. В бинарном виде пакеты FDS доступны в репозиториях на сайте проекта для Fedora 6, 7, 8 и 9. У меня также не возникло проблем при установке пакетов Fedora 6

на RHEL 5.1. Что же касается коммерческой версии, то RHDS 8.0 будет доступен в бинарном виде и поддерживается на платформах RHEL 4 и 5 (x86 и x86_64), HP-UX 11i (IA 64) и Sun Solaris 9 (sparc 64-bit).

Следует отметить, что данная статья является всего лишь обзором, поэтому перед практическим знакомством с продуктом следует прочесть руководство по установке и замечания к выпуску на сайте проекта. Весьма полезным источником информации является официальная документация по RHDS на сайте Red Hat [4].

Также нужно обратить внимание читателя, что по сравнению с предыдущей версией FDS 1.0.x в рассматриваемой в обзоре версии 1.1 присутствуют ряд изменений, как раз влияющих на процесс установки сервера:

- Вместо поставки единого пакета компоненты сервера разбиты на отдельные пакеты.
- Более тесная интеграция с Fedora за счет того, что ряд компонентов теперь в самом дистрибутиве операционной системы.
- Размещение файлов согласно FHS [5] вместо привычного расположения в /opt/fedora-ds.
- Изменение названий многих утилит.
- Наконец-то появились Init-скрипты в /etc/rc.d/init.d. Раньше приходилось их скачивать с сайта проекта или писать самому.

Итак, в случае установки на Linux, минимальные требования к серверу – 2 Гб свободного места на жестком диске и 256 Мб оперативной памяти. Согласно [6] настраиваем работу с репо-

зиторию сервера каталогов. Обратите внимание на описанные дополнительные шаги при установке на RHEL 5. Далее при помощи yum скачиваем и устанавливаем пакет fedora-ds:

```
yum install fedora-ds
```

На самом деле, пакет fedora-ds – всего лишь «сборник зависимостей» – мета-пакет, для успешной установки которого требуются другие пакеты, которые как раз и привносят в систему отдельные компоненты сервера каталогов (см. **рис. 4**). В случае использования Fedora 7 или более ранней, вам потребуются проприетарные библиотеки JRE [7].

После окончания установки пакетов запустите скрипт первоначальной настройки сервера администрирования и сервера каталогов – /usr/sbin/setup-ds-admin.pl. Перед запуском создайте пользователя и группу, с правами которого будет работать сервер каталогов.

При настройке тестового сервера можете проигнорировать предупреждения о несоответствии некоторых параметров ядра рекомендуемым. Ознакомьтесь с условиями, относящимися к лицензионному соглашению. Скрипт сообщит, что подробности доступны в файле LICENSE.TXT. Еще раз напомним, что хотя лицензии и свободные, у разных компонентов сервера они отличаются друг от друга. Выбирайте тип установки Express (рекомендуется при первом знакомстве) или Typical. В зависимости от типа установки вам придется ответить на ряд вопросов. Если не уверены с ответами, соглашайтесь с предложенными значениями по умолчанию.

Не забудьте введенные в ходе настройки пароли для администратора конфигурации (по умолчанию имя администратора – admin) и Directory Manager DN (по умолчанию – cn=Directory Manager). По окончании настройки скрипт сообщит вам так называемый «administration URL» вашего сервера, который вы будете использовать в дальнейшем при доступе к серверу администрирования через консоль или напрямую, набрав его в строке адреса вашего браузера.

В версии 1.1 наконец появились стартовые скрипты для самого сервера каталогов и сервера администрирования. Это соответственно `dirsrv` и `dirsrv-admin`. После установки сервер должен быть запущен. Проверить это вам помогут указанные скрипты с параметром `status` или команда `netstat -ltn`. Вы должны увидеть процесс `ns-slapd`, прослушивающий порт, стандартный для LDAP-сервера, порт 389/tcp и `httpd.worker` с портом, указанным вами при установке для сервера администрирования.

Следующий шаг при первоначальном знакомстве – запуск графической утилиты управления сервером Fedora Management Console командой:

```
/usr/bin/fedora-idm-console
```

Если вы скачали и установили консоль для работы под ОС Windows (FedoraConsole.msi), то запустите файл `fedora-idm-console.bat` (ярлык в меню «Start → Programs → Fedora Identity Management Console → Fedora IDM Console»). Возможно, вам придется отредактировать файл bat-файл для того, чтобы указать путь к JRE. В случае возникновения такой необходи-

мости об этом вам сообщит bat-файл при его запуске.

В ответ на приглашение введите Directory Manager DN и пароль, который задали при первоначальной настройке. В качестве administration URL укажите имя сервера и заданный вами порт, на котором ждет подключений сервер администрирования. Надеюсь, в вашей тестовой среде нет проблем с разрешением FQDN имени сервера каталогов? В противном случае отредактируйте `/etc/hosts` и/или `%SystemRoot%\system32\drivers\etc\host`.

«Пройдитесь» по интерфейсу, посмотрите доступные функции и настройки. Руководство «Managing Servers with Red Hat Console» (читайте Fedora Management Console) доступно на сайте Red Hat [4].

Теперь для экспериментов можно импортировать в наш каталог тестовый `ldif`-файл, представляющий данные о полутора сотнях сотрудников виртуальной компании `example.com`. Если вы во время установки выбрали суффикс для вашего дерева каталога отличный от `dc=example,dc=com`, то исправьте все вхождения этого суффикса в `ldif`-файле. Вероятно, наиболее просто это сделать при помощи `sed`. Файл `Example.ldif` с примерами расположен в `/usr/share/dirsrv/data/`. Импортировать можно через Fedora Management Console (консоль «Directory Server → вкладка Tasks → иконка Import Databases») или при помощи привычных утилит OpenLDAP (пакет `openldap-clients`).

Попробуйте при помощи графической консоли исследовать импортированные данные, а также добавлять, удалять изменять данные о сотрудниках.

Обратите внимание, что версия 1.1 не включает в себя веб-приложения `phonebook`, `gateway` и `org chart`. Их планируют включить в состав сервера каталогов в будущих релизах. Тем не менее вы можете при помощи браузера зайти на ваш сервер администрирования, указав в качестве порта, тот, который был задан при выполнении скрипта `/usr/sbin/setup-ds-admin.pl`, и познакомиться с веб-интерфейсом Fedora Administration Express.

Что дальше?

Вы задумываетесь о внедрении сервера каталогов? У вас в руках мощный и бесплатный продукт с открытым кодом. Изучите документацию. Подпишитесь на список рассылки [8] – читайте и задавайте вопросы. Экспериментируйте. Если же необходимо использовать сервер каталогов в производственной среде, где имеется необходимость в технической поддержке с гарантированным временем отклика, обратитесь к Red Hat Directory Server.

Удачи! 🍀

1. <http://directory.fedoraproject.org/wiki/Features>.
2. <http://www.freeipa.org>.
3. <http://directory.fedoraproject.org/wiki/Licensing>.
4. <http://www.redhat.com/docs/manuals/dir-server>.
5. <http://www.pathname.com/fhs>.
6. <http://directory.fedoraproject.org/wiki/Download>.
7. http://directory.fedoraproject.org/wiki/Release_Notes.
8. http://directory.fedoraproject.org/wiki/Mailing_Lists.

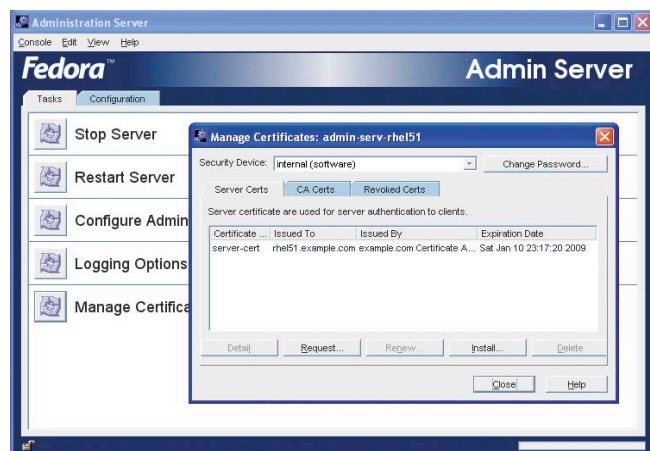


Рисунок 3. Консоль Administration Server (Windows)

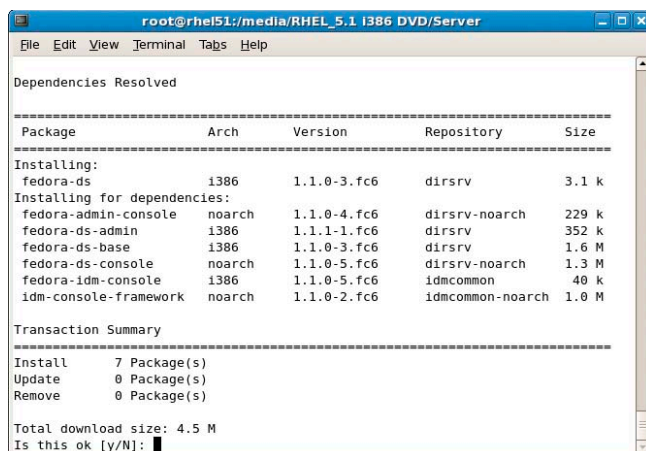


Рисунок 4. Устанавливаем мета-пакет `fedora-ds`