Начальник сети

Настройка офисного сервера на базе Linux

Инфраструктура малых офисов проста: несколько десятков равнозначных рабочих компьютеров и головной сервер. В целях экономии головной сервер является еще, как правило, маршрутизатором и файловым сервером. Все это объединяется под общим названием SOHO-сервер.

Начинающие системные администраторы обычно устанавливают на такие серверы операционную систему Windows 2000, взгромождая на нее огромное количество серверных и подчас нелицензионных программ, таких как Microsoft Exchange или Wingate. Согласитесь, далеко не каждая фирма в состоянии позволить себе столь недешевое удовольствие. Именно поэтому многие останавливаются на свободно распространяемых операционных системах, таких как Linux или FreeBSD.

Linux — достаточно экономная операционная система. Для создания офисного сервера на ее основе вам понадобится простой IBM-совместимый компьютер с недорогой видеоплатой, жестким диском на 80 Гбайт, 128 Мбайт памяти (желательно больше) и двумя сетевыми платами. Достаточно большой объем жесткого диска объясняется необходимостью хранения огромного количества офисных данных. Две сетевые платы нужны в том случае, если сервер будет являться также и маршрутизатором в Интернет. Помимо этого, нам понадобятся четыре установочных диска операционной системы Fedora Core 2 и немного здравого смысла, чтобы правильно сконфигурировать установленную систему. На все описанные в статье действия уйдет не более четырех часов, так что работу можно начинать сразу после обеда. »

Установка системы

Для начала необходимо установить операционную систему на жесткий диск. В этом процессе есть несколько не совсем очевидных моментов. Рассмотрим их подробнее.

Разбиение диска

Под этим термином понимается, конечно же, не тяжелая работа молотком и напильником, а всего лишь разделение общего объема диска на несколько частей. Необходимо это для того, чтобы в случае «аварии» была возможность спасти хотя бы часть данных. В системах, совместимых с Unix, нет такого разделения на диски, как в Windows. Вы не увидите привычных надписей «Диск C» или «Диск D». Все источники данных собираются (в терминологии Unix — монтируются) в одно большое дерево файловой системы. Как правило, в корневом каталоге файловой системы находятся следующие подкаталоги:

bin — системные исполняемые файлы, например командная оболочка bash;
boot — файлы, необходимые для загрузки системы, а также образ ядра;
dev — в этом каталоге содержатся файлы устройств;
etc — каталог с файлами настроек;
home — каталог, содержащий пользовательскую информацию (раздельно для каждого пользователя);
lib — главные системные библиотеки;
mnt — обычно в этот каталог подключаются файловые системы съемных носителей, таких как дискеты или компакт-диски;
proc — в этом каталоге хранится информация о текущем состоянии системы;
root — домашний каталог администратора системы;
sbin — исполняемые файлы, требующие для запуска прав администратора;
usr — этот каталог содержит практически полную копию корневой структуры, однако большая часть файлов в нем используется не системой, а самими пользователями;
var — каталог для изменяемых данных, таких как информация на HTTP- или FTP-серверах.

Обычно при установке сервера на отдельные файловые системы выделяются каталоги boot, home и var. Отдельный каталог boot позволяет быть уверенным в том, что даже в случае катастрофического нарушения разметки диска удастся хотя бы загрузить систему. Каталог home, содержащий пользовательские данные, тоже стоит выносить в отдельную файловую систему, для того чтобы обеспечить лучший контроль над его содержимым. Папка var — одна из важнейших для сервера, потому что содержит данные, ради которых и работает этот самый сервер. Выделяя ее в отдельную файловую систему, мы не только обеспечиваем большую сохранность данных, но и облегчаем себе задачу по резервному копированию.

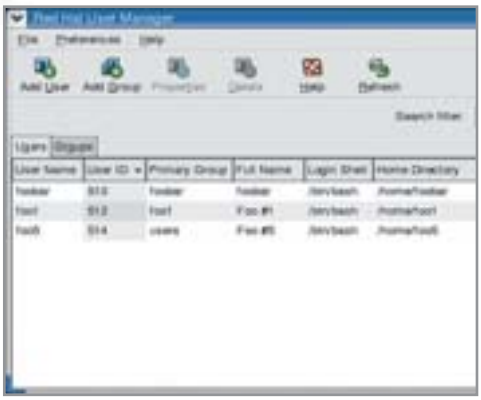
Итак, предположим, что на нашем офисном сервере установлен жесткий диск объемом 80 Гбайт. Тогда отведем под корневую файловую систему (обычно ее обозначают одним символом «/») 4 Гбайт. Этого достаточно даже для полной установки операционной системы Fedora Core 2. Раздел boot не потребует много места, ему достаточно 20 Мбайт. Оставшееся место лучше разделить так: 20 Гбайт под каталог home, а все остальное — для каталога var. С разбиением диска на этом можно закончить.

Выбор набора пакетов

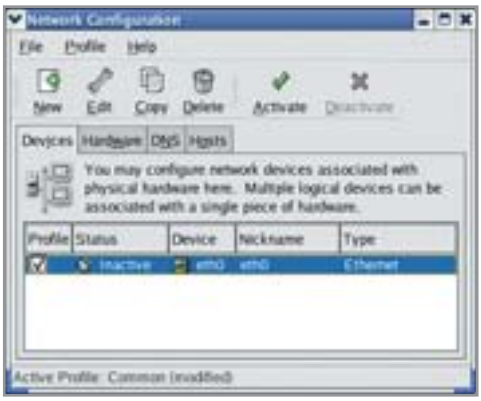
Конечно же, настоящие Linux-гуру выбирают все пакеты из списка самостоятельно. Начинающим же можно порекомендовать остановиться на конфигурации «Сервер». В ней содержатся все необходимые сервисы, использующиеся в типовом сервере. В любом случае, разобраться с составом пакетов, добавить или удалить что-либо можно и после установки. Главные пакеты, которые необходимо установить обязательно, это httpd, vsftp, samba, а также пакеты, необходимые для работы большинства современных веб-программ: язык программирования PHP со всеми расширениями и база данных MySQL. Для максимально удобной работы с сервером почты необходимо установить пакеты sendmail (сервер smtp), dovecot (серверы POP3 и IMAP), а также squirrelmail — для работы с почтой через Веб.

Настройка брандмауэра

В дистрибутивах Fedora Core настройка брандмауэра упрощена до предела. Для начала определимся, какая из сетевых плат будет «смотреть» внутрь, а какая — наружу. В системе Linux сетевые платы обозначаются символьными именами «ethX», где x — порядковый номер, начинающийся с нуля. Давайте условимся, что в нашем случае сетевая плата «eth0» направлена в сторону интернет-провайдера, а «eth1» обслуживает офисную локальную сеть. Чтобы защитить внутреннюю сеть от посягательства злоумышленников, нужно настроить правила доступа к сетевой плате «eth0». А «eth1» можно пометить как доверенный интерфейс. Для интерфейса «eth0» в программе установки нужно разрешить доступ к следующим портам: HTTP, HTTPS, FTP, SMTP и SSH. Доступ ко всем остальным портам по умолчанию закрыт. Заметьте, »



Управление пользователями системы через system-config-users



Создание, удаление и настройка сетевых интерфейсов

» из всех почтовых сервисов из Интернета доступен только SMTP, через который происходит доставка почты на ваш сервер. Из соображений безопасности не стоит разрешать пользователям получать офисную почту из дома или интернет-кафе по протоколу POP3. Для этого существует возможность работы через веб-интерфейс.

Добавление пользователей

В операционной системе Windows большая часть операций по настройке производится от имени пользователя Administrator. В Unix-системах также существует суперпользователь — root. Однако заходить под именем этого пользователя не рекомендуется, так как одной случайной командой можно уничтожить результаты нескольких лет работы. Именно поэтому система установки Fedora Core 2 предлагает добавить в систему новых пользователей. Настоятельно рекомендуем сделать это, внимательно заполняя все поля ввода, в том числе и «Полное имя». Также не надо забывать о возможности разделения всех пользователей операционной системы на группы. Цель этого разделения — обеспечить большее удобство при работе с пользователями, а также организация более гибкой системы контроля доступа к файлам. Написано на эту тему много, поэтому особо останавливаться на ней мы не будем. Важно правильно разбить пользователей на группы, когда в локальной сети необходим файловый сервер.

На этом этап установки системы завершен. Можно переходить непосредственно к настройке. Перед этим надо лишь определиться с задачами, которые будет выполнять ваш сервер. Обычно на него возлагается ответственность за следующие аспекты жизни офиса:

- Выполнение функций файл-сервера.
- Предоставление доступа в Интернет.
- Обеспечение доступа к e-mail.
- Выполнение функций FTP- и HTTP-сервера.

Начальная настройка офисного сервера

В состав Fedora Core 2 входит специальный набор программ — System Configurators. Это выдержанные в едином стиле программы, обеспечивающие доступ почти ко всем настройкам операционной системы. Как известно, имя всеобщего любимца, живущего на крыше, точно не знал никто. Ясно было только то, что начиналось оно на «Карл» и заканчивалось на «сон». Так и здесь, благодаря общей системе наименований имя исполняемого файла каждой программы начинается с «system-config-», а заканчивается английским названием того, что необходимо настроить. Например, для того чтобы настроить время и дату на сервере, необходимо запустить программу system-config-date.

Samba

В Linux-системах для предоставления доступа к сети Microsoft используется файловый сервер Samba. До последнего времени настройка этого сервиса, как правило, производилась вручную прямо в конфигурационном файле. Однако благодаря разработчикам Fedora Core 2 это перестало быть явной проблемой. По уже упоминавшейся выше схеме наименования программ система настройки файлового сервера называется system-config-samba.

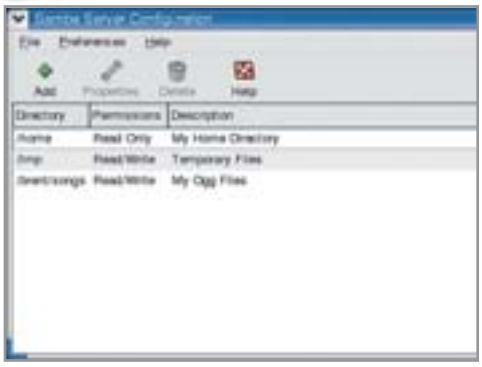
Теперь создадим в каталоге var, выделенном нами для хранения серверной информации, подкаталог samba. В большинстве организаций файловый сервер находится во всеобщем пользовании, поэтому установим права доступа на каталог var/samba в режим 777, то есть разрешим всем пользователям любые операции с этим каталогом. Однако довольно часто на файловом сервере требуется хранить и более конфиденциальную информацию. Поэтому в папке var/samba создадим еще один каталог под названием topsecret, установив права доступа так, чтобы читать и писать в нем могли лишь определенные пользователи. Теперь остается только запустить system-config-samba и добавить оба каталога в доступ к Microsoft Network. Проверять работоспособность уже настроенного сервиса лучше всего из операционной системы Windows. Подключившись из нее к сети, проверьте, есть ли доступ к настроенному вами серверу. Для этого найдите ваш сервер в «Сетевом окружении» и создайте на нем еще одну папку. Если вам это удалось, файловый сервер работает нормально.

Настройка маршрутизации

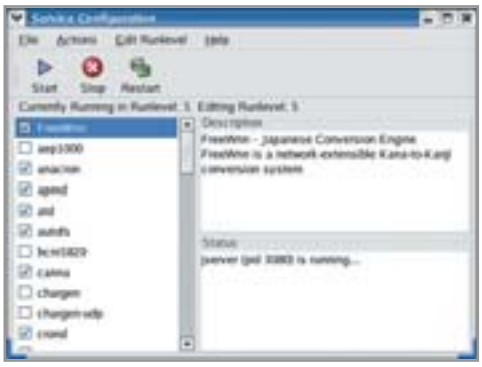
Настройка доступа в Интернет — это единственный момент, который требует обязательного редактирования конфигурационного файла. Бояться здесь нечего, вся задача сводится к правке единственной строки. Перейдите в директорию etc, откройте файл sysctl.conf и в строке

```
net.ipv4.ip_forward = 0
```

»



Конфигурация файлового сервера Samba



Здесь можно выбрать, какие сервисы запускать при старте системы

» вместо значения «0» укажите «1». Объясняется это действие очень просто. В нашей системе есть две сетевые платы, одна из которых направлена внутрь, то есть в локальную сеть, а другая — наружу. По умолчанию с одной сетевой платы на другую пакеты передаваться не могут. Заменяя 0 на 1, мы открываем доступ из локальной сети в Интернет, то есть пакеты с «внутренней» сетевой платы могут передаваться на «внешнюю». После редактирования указанного файла необходимо выполнить команду

```
sysctl -p
```

или просто перезагрузить компьютер. Теперь доступ в Интернет для пользователя локальной сети открыт. При необходимости вы также можете настроить максимальную пропускную способность канала, однако описание этого процесса выходит за рамки нашей статьи.

Squid

Большинство пользователей локальной сети посещают один и тот же довольно небольшой набор сайтов. Таких, например, как Yandex.ru или Lenta.ru .Чтобы не загружать одни и те же страницы несколько раз, необходимо настроить прокси-сервер. В Fedora Core 2 роль прокси-сервера выполняет программа Squid. Никакой особенной дополнительной настройки он не требует. На всякий случай отметим, что вся конфигурация этого сервера хранится в файле etc/squid/squid.conf. Важным моментом, который нужно запомнить, является только то, что по умолчанию прокси-сервер Squid настроен на работу по порту 3128. Учтите этот факт при настройке клиентских машин.

Mail

Для того чтобы реализовать функциональность почтового сервера, никаких дополнительных настроек тоже не требуется. Единственное, что может быть важно, — это настройка доступа к серверу SMTP, так называемый «Relaying». Для этого в каталоге etc/mail/access необходимо перечислить доменные имена компьютеров, с которых разрешена отправка почты. После этого надо перезапустить сервис sendmail. Подсистемы POP3 и IMAP работают сразу по умолчанию, так что все, что остается делать для организации корректной работы почты, это добавлять, а иногда и удалять пользователей. Для выполнения последней операции будет удобно пользоваться системной программой system-config-users.

В связи с многократно увеличившимся потоком рекламных писем пользоваться электронной почтой становится все сложнее и сложнее. Поэтому в дистрибутив Fedora Core 2 входит одна из самых качественных систем фильтрации корреспонденции с нежелательным содержанием — Spam Assassin. После установки этого пакета спам-фильтр начнет работать, помечая письма, содержащие, по его мнению, нежелательную информацию, специальной маркой «x-spam».

HTTP

В начале статьи, на этапе установки, мы выбрали пакеты httpd и vsftp. Первое, что вам необходимо запомнить, — это то, как они используют файловую систему. Под скромным названием httpd скрывается самый широко известный в Интернете веб-сервер Apache. Все файлы, раздающиеся им по протоколу HTTP, расположены в каталоге var/www. Если разработкой и публикацией сайта занимается не системный администратор, хорошо было бы дать доступ к этому каталогу через подсистему Samba так же, как это было сделано ранее с другими каталогами. Обратите внимание на то, что в этом каталоге уже расположены файлы веб-почты squirrelmail. Для проверки работоспособности веб-сервера Apache в любом из браузеров попробуйте обратиться к странице «http://ваш_домен/mail». Если все настройки в порядке, появится приглашение ко входу во внутреннюю службу веб-почты.

FTP

По умолчанию все файлы FTP-сервера находятся в каталоге var/ftp. Структура подкаталогов совершенно идентична большинству остальных FTP-серверов: каталог pub открыт для чтения всем желающим, запись же разрешена только в каталог incoming. В последнее время участились случаи, когда анонимные FTP-серверы использовались злоумышленниками для хранения своих файлов нелегального содержания. Чаще всего это нелицензионные программы. Обычный образ действий злоумышленников — найти FTP-сервер с открытым каталогом incoming, поместить в него необходимые файлы и раздавать ссылки на этот FTP всем желающим. Для того чтобы максимально усложнить жизнь преступникам, настройте доступ к каталогу таким образом, чтобы в него можно было только положить файлы. Перемещением необходимых файлов из директории incoming в pub должен заниматься системный администратор. ■ ■ ■ **Григорий Бакунов**