ALT Linux Master 2.2

Руководство системного администратора

А. Боковой, И. Вергейчик, О. Власенко, М. Забалуев,
Ю. Зотов, С. Иевлев, Д. Левин, И. Муратов,
А. Новодворский, А. Орлов, А. Турбин

ALT Linux Master 2.2: Руководство системного администратора

А. Боковой, И. Вергейчик, О. Власенко, М. Забалуев, Ю. Зотов, С. Иевлев, Д. Левин, И. Муратов, А. Новодворский, А. Орлов, А. Турбин

Большую работу по редактированию книги осуществили: А. Астафьев
А. Добровольский
М. Шигорин

Часть I. Оборудование

Глава 1. Общая информация

Основная информация

`Linux` поддерживает практически все современное оборудование для архитектуры x86, за исключением специально ориентированного на ОС `Windows` (например, так называемые winmodem и winprinter), а также продукцию тех производителей, которые по тем или иным причинам не желают давать спецификации на устройства для написания драйверов.

Информация, предоставленная в этом руководстве, не претендует на полноту описания, поэтому, если вы не найдёте здесь ответа на интересующий вас вопрос, прежде чем писать в список рассылки *ALT Linux*[1], рекомендуется посмотреть следующую документацию:

1. документация к ядру (пакет `kernel-doc`[2]);
2. FAQ и HOWTO по `Linux` можно найти в как в Интернете, так и в дистрибутиве;
3. поиск в Интернете по спискам конференций;
4. исходные коды — это для тех, кто желает в них разобраться.

С точки зрения системного администратора, задачей которого является настройка оборудования и проверка его работоспособности для `Linux`, устройства в первую очередь определяются своим типом, производителем, затем способом подключения.

Для настройки устройств в дистрибутиве *ALT Linux Master 2.2* существуют следующие утилиты для настройки (объединённые в DrakConf):
Утилиты для настройки оборудования

- PCI-, AGP- и USB-устройств — kudzu. При этом рекомендуется, чтобы сервис kudzu загружался автоматически при загрузке системы — в этом случае будут сконфигурированы все устройства, добавленные или удалённые с момента последней перезагрузки системы;
- звуковых карт (преимущественно ISA) — утилита sndconfig;
- графической карты и оболочки XFree86 — XFdrake;

[1] `http://www.altlinux.ru`
[2] Под пакетом `kernel-doc` здесь и далее подразумевается либо `kernel22-doc`, либо `kernel24-doc` в зависимости от того, какое ядро у вас установлено.

- мыши — mousedrake;
- клавиатуры — keyboarddrake;
- принтеров — printerdrake;
- сети — draknet.

На сегодняшний день наиболее распространёнными способами расширения конфигурации компьютера являются *шины* PCI, AGP, ISA[3], а для подключения внешнего оборудования — USB, PCMCIA, SCSI и *порты* COM (последовательные) и LPT (параллельный).

Проще всего под `Linux` проверяется работоспособность оборудования, использующего шину PCI: достаточно набрать команду **/sbin/lspci**, чтобы увидеть информацию обо всех подключённых PCI-устройствах. Команда **lspcidrake** в дополнение к выводу команды **/sbin/lspci** выводит информацию о наличии драйверов (модулей ядра) для них.

Это возможно потому, что каждое PCI- или AGP-устройство содержит пару уникальных *идентификационных номеров* (называемых PCI ID), в которой первым числом определяется производитель устройства, а вторым — само устройство. В дистрибутиве присутствует пакет `ldetect-lst`, который содержит информацию о наличии (или отсутствии) драйверов для каждого известного на момент создания таблицы (`/usr/share/ldetect-lst/pcitable`) PCI-устройства; если обнаружено изменение конфигурации и устройству сопоставлен драйвер, настройка производится автоматически утилитой kudzu (а изначально — программой установки системы).

Основные проблемы возникают в случае, когда для вашего устройства нет драйвера или неизвестны идентификационные номера устройства и его нет в таблице. В этом случае рекомендуется произвести ручную настройку устройства или написать в список рассылки по дистрибутиву. При возникновении проблем с PCI-устройством настоятельно рекомендуется выслать следующую информацию о нем:

1. название, производитель, надписи на самых больших чипах и т.д.;
2. вывод команд **lspcidrake** и **/sbin/spci -vv**;
3. содержимое файла `/proc/bus/pci/devices`;
4. описание проблемы.

[3]Шина ISA, равно как и COM/LPT-порты, ныне относится к разряду «наследственных».

USB- и PCMCIA-шины

Для поддержки «горячего» подключения устройств, разработанных для USB- и PCMCIA-шин, в дистрибутиве *ALT Linux Master 2.2* существует специальная программа hotplug, задача которой заключается в автоматической загрузке драйверов. Эта программа входит в одноимённый пакет, который устанавливается по умолчанию.

При возникновении проблем с USB-устройствами необходимо найти информацию о вашем устройстве в файле `/proc/bus/usb/devices`. Информация в этом файле содержит много технической информации, для её «отсеивания» можно воспользоваться утилитами типа usbview — их вывод будет более понятен начинающему пользователю. Если ни один драйвер не «подхватил» его — скорее всего, это устройство не поддерживается. Для получения помощи можно обратиться в список рассылки *ALT Linux*, при этом настоятельно рекомендуется выслать содержимое файла `/proc/bus/usb/devices`.

Получить информацию о поддержке USB можно на сайте `http://www.linux-usb.org/`.

Шина ISA

Для шины ISA есть следующие варианты: если устройство соответствует стандарту *ISA Plug'n'Play*, настройку аппаратных ресурсов можно проводить через программу isapnp. В ином случае потребуется сконфигурировать плату либо перемычками на ней (например, звуковую), либо утилитой, которую обычно прилагают на дискете с драйверами (большинство сетевых карт). В любом случае все эти параметры придётся указать вручную драйверу устройства для его работы. К счастью, ISA-устройства уже менее распространены.

Устройства, присоединяемые через параллельный, последовательный или игровой порты

Что касается оборудования для последовательных и параллельных портов, а также джойстиков, то практически в каждом случае необходимо вручную настраивать драйвер соответствующего устройства. Исключение здесь составляют только внешние модемы с последовательным интерфейсом, которые не требуют драйверов.

Настройка таких устройств (за исключением принтеров) практически всегда производится вручную — например, для настройки модема необходимо указать COM-порт, к которому он подключён. Для

настройки джойстика необходимо найти драйвер под него и вручную настроить его посредством редактирования конфигурационных файлов.

Рассмотрим теперь варианты настройки различных типов устройств.

Материнские платы и процессоры

ALT Linux[5] *Master 2.2* поддерживает все современные 32-битные процессоры архитектуры *x86*, начиная с Intel Pentium и совместимых; если процессор исправен и хорошо охлаждается — с ним не должно возникнуть никаких проблем. Процессоры, работающие в нештатном режиме, использовать не рекомендуется[6].

Для проверки работоспособности процессора при критических нагрузках рекомендуется запустить в одном сеансе вариант программы burn (из пакета `cpuburn`) — например, burnP6 для Intel Pentium i686 или AMD Athlon, а в другом — компиляцию какого-нибудь большого пакета, гарантированно собирающегося. Обычно при наличии проблем с охлаждением система сразу не зависает, но компиляция останавливается из-за ошибок.

Последние также могут возникать из-за некачественной (или нестабильно работающей) памяти — для её проверки предназначен пакет **memtest86**, который добавляет в меню загрузки системы ещё один вариант.

Специальную настройку материнских плат производить обычно не требуется — за исключением редких случаев, все работает с настройками по умолчанию.

При настройке BIOS стоит обратить внимание на следующие параметры:

1. Параметр Use PNP OS (как вариант — PNP OS installed) — включение этого параметра — ON (или ENABLE) приводит к тому, что BIOS перестаёт настраивать устройства PnP, доверяя это операционной системе. Для `Linux` выключение этого параметра — NO (или DISABLE) может помочь с инициализацией некоторых устройств.
2. На материнских платах с чипсетами семейства VIA (KT133, 133A, 266, 333) рекомендуется выключить параметры Passive Release и Burst Read/Write[7], которые в некоторых случаях также могут служить причиной зависаний и неполадок.

[5] `http://www.altlinux.ru`

[6] Однако при известной аккуратности это возможно.

[7] Или обновить BIOS.

3. Если на материнской плате присутствует AGP-видеокарта, рекомендуется выставить параметр AGP Aperture Size не меньше 64 Мб, в том случае, если объём оперативной памяти компьютера не менее 128 Мб. В том случае, если объём оперативной памяти менее 128 Мб, то не более половины установленной оперативной памяти (т.е. при наличии 64 Мб. установите значение этого параметра равным 32).

Достаточно часто возникают проблемы из-за ошибок в BIOS. Поэтому, если вы столкнулись с какой-либо странной проблемой (например, не работает заведомо поддерживаемая видеоплата) — рекомендуется посмотреть на сайте производителя материнской платы новые версии BIOS и, если в списке изменений присутствует ваша проблема — обновить BIOS. Например, при тестировании материнской платы Asus A7N266-E (на базе чипсета nForce 420D) было обнаружено, что встроенный контроллер USB не работает одновременно с загруженным модулем apm. Проблема решилась обновлением BIOS'а с версии 1001A до 1001D.

Клавиатура

С точки зрения поддержки клавиатур в Linux они отличаются по способу подключения (USB и обычные PS/2 или DIN), а также по количеству клавиш (101, 102, 104 ...).

Обычные клавиатуры настраиваются автоматически, причём дополнительные (т.н. Windows-клавиши) автоматически задействуются как в консоли, так и в X Window. Единственное, что необходимо сделать — указать раскладку клавиатуры при установке системы либо позже при помощи keyboarddrake.

USB-клавиатуры также определяются автоматически; единственное, что требуется для их правильной работы — это настроенный интерфейс USB и установленный пакет hotplug. Настройка раскладки делается точно также, как и для обычных клавиатур.

Важное замечание: USB-клавиатуры не работоспособны при загрузке системы в режимах, в которых не запускается сервис usb (например, при указанию ядру параметра *init=/bin/bash*).

Мышь

Мыши различаются прежде всего по способу подключения: USB, PS/2, COM и BusMouse (сейчас в основном распространены две первые модификации), а также количеством кнопок и наличием колеса прокрутки.

Так как в консоли и в X Window предусмотрена поддержка третьей кнопки (с её помощью реализуется функция вставки), рекомендуется использовать трехкнопочные мыши; при наличии двухкнопочной мыши третья кнопка может эмулироваться одновременным нажатием обеих имеющихся.

Настройка мыши производится в процессе установки, а после неё — при помощи утилиты mousedrake. В настройках этой программы надо выбрать следующее: тип мыши по подключению, протокол её работы (для мышей PS/2 и COM), а также включение эмуляции третьей кнопки.

Рассмотрим поподробнее протоколы мышей:
Протоколы работы мышей

- USB — здесь есть всего два варианта настройки: обычная мышь или мышь с колесом. Соответственно, достаточно взглянуть на свою мышь, чтобы сделать выбор.
- PS/2 — вариантов уже больше:
  - обычная двух- или трехкнопочная мышь — выберите Generic;
  - Logitech MouseMan+ или GlidePoint (встречаются редко) — выберите соответствующую;
  - мышь с колесом — надо выбрать один из следующих вариантов (по производителю):
    - производство Genius — посмотрите на её название (обычно написано на дне мыши) и выберите Genius Netmouse или Genius Netscroll — хотя бывают случаи, когда на мыши написано NetScroll, а работает она по протоколу NetMouse, поэтому в случае неработоспособности мыши стоит попробовать оба протокола. Мышь Netscroll+ также иногда работоспособна при выборе протокола Logitech MouseMan+;
    - Microsoft, Logitech или Mitsumi, а также другая мышь с колесом — стоит попробовать вариант Generic PS/2 Wheel mouse;
    - если мышь все же не заработает — остаётся выбрать вариант Generic (колесо, естественно, при этом работать не будет);

- COM — очень много вариантов, но большинство из них предназначены для специфических и малораспространённых мышей вроде Kensington. Для обычных мышей есть следующие варианты выбора:

  - двухкнопочная — выбирайте 2 button mouse;
  - трехкнопочная — это либо 3 button mouse, либо MouseSystems;
  - мышь с колесом — выбирайте по производителю (как и в варианте PS/2, для безымянных мышей скорее всего подойдёт протокол Microsoft IntelliMouse).

Устройства хранения данных

Жёсткие диски

Современные жёсткие диски производятся со следующими интерфейсами: IDE, SCSI и USB (в основном это Flash-карты, подключённые к системе через Flash-Reader).

Жёсткие диски IDE определяются системой автоматически в процессе загрузки; доступ к ним (и другим устройствам на этой шине) производится посредством специальных *файлов блочных устройств* (`dev/hdXN`[8]).

Имя устройства формируется следующим образом:

- hda — primary master;
- hdb — primary slave;
- hdc — secondary master и т.д.

При этом обращение к файлу устройства подразумевает доступ ко всему диску целиком. Обращение к разделам на диске производится через устройства `/dev/hdXN`, где `/dev/hda1` — первый *основной* раздел (primary partition) на первом диске, `/dev/hda2` — второй основной раздел. Так как основных разделов может быть не более четырёх, то расширенные разделы начинаются с номера 5: `/dev/hda5` — первый *логический раздел* (logical partition) в *расширенном разделе* (extended partition) на первом диске.

Протокол обмена данными с жёсткими дисками IDE для всех современных чипсетов выбирается автоматически при загрузке ядра. Для

[8] В описании файла блочного устройства `X` означает латинскую букву, а `N` — число.

более тонкой ручной настройки IDE-устройств в дистрибутиве присутствует команда hdparm, с помощью которой можно управлять протоколом доступа (т.е. UDMA100, UDMA33, PIO16 и т.д.), а также некоторыми другими параметрами. Подробнее смотрите **man hdparm**.

> **Важно**
>
> Пользоваться программой hdparm рекомендуется исключительно осторожно, т.к. установкой неправильных настроек можно добиться потери информации, а в худшем случае — и неисправности жёсткого диска. Настройки hdparm можно сохранить в файлах конфигурации в каталоге `/etc/sysconfig/harddisk` (в файлах с именами hdX — для каждого устройства, в том числе и CD-ROM/DVD) — тогда они будут применяться автоматически в процессе загрузки системы.

жёсткие диски SCSI также определяются системой автоматически в процессе загрузки ядра. Единственное отличие от IDE для пользователя — то, что устройства называются не `/dev/hdXN`, а `/dev/sdXN`.

Носители данных USB определяются системой автоматически в момент физического их подключения при установленном пакете `hotplug`. Далее всё зависит от наличия/отсутствия поддержки конкретного USB-устройства в системе — если таковая присутствует, доступ к данным можно получить через интерфейс SCSI (например, как `/dev/sda` при условии незанятости этого имени другими SCSI-устройствами, в противном случае выбирается первое свободное имя).

Устройства CD-ROM (CD-RW)

IDE CD-ROM автоматически определяются системой и в процессе установки для них создаются специальные ссылки в каталоге `/dev` — т.е. `/dev/cdrom` для первого привода, `/dev/cdrom2` — для второго и т.д. Также доступ к устройству можно получить через интерфейсы `/dev/hdX` для IDE CD-ROM и `/dev/scdX` — для SCSI. Как и для всех устройств со съёмными носителями, при включении сервиса autofs монтирование и размонтирование их происходит автоматически при попытке прочтения данных из каталога, куда должен быть смонтирован носитель — обычно это `/mnt/cdrom`.

С помощью параметра `-E` команды **hdparm** для некоторых приводов CD-ROM можно регулировать скорость вращения их шпинделя (см. тж. **man hdparm**).

Чуть сложнее обстоит дело с настройкой устройств с функцией записи (перезаписи) дисков (т.е. CD-R/RW). Поскольку эта функциональность реализуется посредством эмуляции SCSI-интерфейса, необходимо включить таковую; это осуществляется автоматически в процессе установки системы при обнаружении такого привода. Для ручного добавления необходимо вставить в файл `/etc/modules` строку `scsi_hostadapter`, а в файл `/etc/modules.conf` — `options ide-scsi units=hdX`, где `hdX` соответствует подключению CD-R/RW (например, `hdc` для «мастера» на втором контроллере). Можно также создать символическую ссылку вида `/dev/cdromN`, указывающую на `/dev/scd0` (если нет других SCSI CD-ROM) для большего удобства. В итоге записывающий привод станет доступен не как устройство `/dev/hdX`, а как устройство `/dev/scdN`. Это относится к любым IDE-устройствам, но необходимо только для CD-R/RW, так как утилита cdrecord может работать только через SCSI-интерфейс.

Сменные устройства типа ZIP

Сменные устройства типа ZIP определяются ядром автоматически в процессе загрузки (если они IDE или SCSI), во время подключения (USB) и вручную при подключении через параллельный порт (для настройки подобный устройств см. `paride.txt` из пакета `kernel-doc`, который находится в каталоге `/usr/share/doc/kernel`).

Единственный нюанс заключается в том, что обычно `FAT` на ZIP-дисках располагается на четвёртом разделе (`/dev/hdX4`).

Флоппи-дисководы

Определяются автоматически в процессе загрузки системы. Для произведения расширенного конфигурирования (например, для форматирования дискет на нестандартную ёмкость) смотрите файл `floppy.txt` из пакета `kernel-doc`, а также документацию из пакета `fdutils`.

Видеокарты

Видеокарты с точки зрения драйверов системы X Window (являющейся в виде XFree86 основой графической подсистемы в большинстве дистрибутивов `Linux`) отличаются в основном типом используемого чипа; если производитель карты не производил «коррекции» его работы, один и тот же драйвер может использоваться с различными продуктами, использующими один и тот же графический процессор.

Настройка производится через утилиту XFdrake, которая автоматически запускается в процессе установки дистрибутива и может быть запущена вручную после установки. Как и большинство утилит настройки, XFdrake имеет эксперт-режим (ключ **--expert**), в котором можно вручную настроить большее количество параметров.

В дистрибутив *ALT Linux Master 2.2* включены две версии XFree86 — 3.3.6 и 4.x.x. Версия 3.3.6 используется для поддержки устаревших видеоплат, драйверы для которых отсутствуют в четвёртой версии. Однако для некоторых видеоплат есть драйвера в обеих версиях XFree86. В этом случае при настройке платы в экспертном режиме появляется возможность выбора версии; в общем случае рекомендуется использовать 4.x.x, однако при наблюдении нестабильной работы можно откатиться на ветку 3.3.6.

Как уже было написано раньше, PCI- и AGP-видеоплаты в большинстве случаев настраиваются автоматически; если этого не произошло, можно попробовать указать тип чипа вручную, выбрав его из списка. Также в подобных случаях рекомендуется прочитать документацию о устройствах PCI в этом же разделе.

Если ваша плата определилась правильно и на экране появилась тестовое изображение — то все нормально и на этом рекомендуется остановиться. Опытные пользователи могут произвести более тонкую настройку видеоплаты — например, для некоторых видеоплат можно вручную выставить параметры в конфигурационном файле XFree86 — обычно это `/etc/X11/XF86Config` (`XF86Config-4` для 4.x.x). Документацию о них можно получить в описаниях из `/usr/X11R6/lib/doc`, а также (значительно более свежую) в дереве исходных текстов проекта XFree86.

Для Matrox существует дополнительный драйвер с закрытым исходным кодом, написанный программистами Matrox, который включает в себя улучшенную поддержку различной функциональности этих плат; для его установки необходимо скачать пакет `XFree86-4.x.x-altx-mga_hal` с нашего FTP-сервера (`ftp://ftp.altlinux.ru`) и установить его. Дополнительно изменять файл конфигурации не требуется.

Аппаратное ускорение 3D-графики в XFree86

В дистрибутиве *ALT Linux Master 2.2* включена поддержка аппаратного 3D-ускорения для некоторых видеоадаптеров. В XFree86 версии 4.x.x входит код из проекта DRI (`http://dri.sourceforge.net`), для XFree86-3.3.6 специально скомпилирован модуль GLX из проекта Utah-GLX.

В любом случае использование аппаратного 3D-ускорения рекомендуется только в XFree86-4.x.x, использование XFree86-3.3.6 с аппаратным 3D-ускорением может привести к нестабильности в работе. Поскольку 3D-ускорение в `Linux` пока ещё находится в состоянии разработки, по умолчанию его включение производится только для наиболее стабильных драйверов.
В версии XFree86-3.3.6 поддерживаются следующие 3D-акселераторы:

- Intel i810/i815 (экспериментальный)
- ATI Mach64
- Matrox G200/G400
- S3 Virge/S3 Savage 3D (экспериментальный)
- nVidia Riva (экспериментальный)
- SiS 6326 (экспериментальный)

Из этого списка достаточной стабильностью и производительностью отличается только драйвер для Matrox. Остальные драйверы являются экспериментальными.
В версии XFree86-4.x.x поддерживаются следующие 3D-акселераторы:

- 3DFX Voodoo (от Banshee до Voodoo 5)
- ATI Rage 128 (как PCI, так и AGP-вариантов)
- ATI Radeon (кроме 8500)
- Matrox (от G200 до G550 и только AGP)
- Intel i810/i815/i830
- 3D Labs Oxygen GMX2000 (экспериментальный)
- SiS 300/630/530 (экспериментальный)

Здесь по умолчанию настраивается 3D-ускорение для всех стабильных драйверов. Экспериментальные драйверы, как и для XFree86-3.3.6, можно настроить, запустив утилиту XFdrake в режиме эксперта. Если проявляются проблемы при использовании 3D, лучше всего либо его отключить (настоятельно рекомендуется, если вам оно не жизненно необходимо), либо обратиться к нам за поддержкой — скорее всего проблема уже будет решена в новой версии XFree86.

Для некоторых других видеокарт (например, на чипе Kyro II) закрытые драйверы выпущены производителями и доступны на соответствующих сайтах.

Видеокарты nVidia

Для видеоплат на чипах nVidia существует два драйвера под `Linux`. Один из них (свободный, входящий в XFree86) достаточно простой и не поддерживает множество функций (например аппаратное 3D, а также несколько других расширений). Другой является закрытым (коммерческий, исходный код недоступен) и написан программистами nVidia. Для его установки в режиме эксперта необходимо запустить XFdrake и выбрать пункт XFree86 4.x.x с аппаратным 3D-ускорением. В других режимах конфигурация будет автоматически настроена с использованием этого драйвера; для возврата к стандартному драйверу XFree86 используйте режим эксперта.

> **Важно**
>
> Не рекомендуется собирать этот драйвер самостоятельно, при выходе его новой версии лучшим решением будет обновление драйвера вместе с ядром дистрибутива из раздела `updates`. Кроме этого, компания *ALT Linux* не несёт ответственности за качество этого драйвера и не осуществляет его поддержку — используйте на свой страх и риск.

Настройка монитора

По умолчанию утилита XFdrake настраивает монитор автоматически, что в большинстве случаев является приемлемым. В то же время опытные пользователи в экспертном режиме могут вручную изменить настройки разрешения и глубины цвета для каждой пары монитор-видеоплата. Помните, что аппаратное ускорение 3D работает только в 16- и 32-х битной глубине цвета. Рекомендуется (если это возможно) устанавливать глубину цвета 16 бит (как это делается в большинстве случаев по умолчанию).

Для получения качественного изображения на экране рекомендуются следующие настройки видеорежимов (помните, что рекомендуется работать при частоте обновления экрана не ниже 85 Гц):

- 14" монитор — 640x480 или 800x600
- 15" монитор — 800x600 или 1024x768
- 17" монитор — 1024x768 или 1152x864
- 19" монитор — 1280x1024 или 1600x1200
- 21" монитор — 1600x1200 или выше.

При прочих равных, лучше выбирать меньшее разрешение, так как в этом случае кадровая частота обновления экрана будет выше; в то же время минимальным практически пригодным для работы является режим `800x600`, а более комфортным — `1024x768` и выше.

Профессионалы также могут вручную настроить специальные параметры видеорежима — например, положение на экране, частоту обновления кадров, нестандартное разрешение (у одного из авторов на 14" мониторе используется разрешение 928x696) и т.д. Это проще всего сделать с помощью утилиты videogen, вручную занеся выданные этой утилиты результаты в файл настроек XFree86. Подробную документацию можно получить из соответствующего пакета (каталог `/usr/share/doc/videogen-*`), а также из xfaq (`http://www.linux.org.ru/books/xfaq.html`).

Звуковые карты

ALT Linux Master 2.2 поддерживает большинство современных звуковых карт. Проще всего настраиваются PCI-карты — это происходит автоматически с помощью программы kudzu.

Звуковые карты с интерфейсом ISA можно настроить с помощью утилиты sndconfig или вручную.

Сейчас существует два различных проекта для поддержки звука в `Linux` — это достаточно старый, но в то же время распространённый стандарт OSS (драйверы для карт в этом стандарте входят в ядро `Linux`), а также новый улучшенный стандарт ALSA (эти драйверы входят в дополнительные пакеты `alsa-*`) для всех ядер, входящих в дистрибутив. По умолчанию в режиме автоматической настройки выбирается наилучший драйвер для каждой карты, но опытные пользователи могут попробовать как OSS, так и ALSA. Единственное, что необходимо помнить — это при использовании драйверов ALSA в файл `/etc/modules.conf` необходимо добавить строку `prereq snd-ваш_драйвер snd-pcm-oss` для включения эмуляции OSS драйверами ALSA.

Кроме того, для плат на основе чипа EMU10K1 (Creative SB Live! и Audigy/Audigy 2) существует пакет `emu10k1-tools` с утилитами, при помощи которых опытные пользователи могут загружать микрокод для поддержки некоторых дополнительных функций.

Сетевые платы

Дистрибутив *ALT Linux*[12] *Master 2.2* поддерживает большинство современных сетевых плат с подключением через ISA, PCI, PCMCIA и

[12] `http://www.altlinux.ru`

USB-интерфейсы. Все адаптеры, за исключением адаптеров для ISA-шины, не требуют специальной настройки и определяются дистрибутивом автоматически.

Исключение составляют адаптеры фирмы Intel (серии EtherExpress100), для которых существует два драйвера — `eepro100` (написанный сообществом `Linux`) и `e100`, написанный фирмой Intel. В случае возникновения проблем рекомендуется попробовать драйвер, отличный от уже настроенного у вас в системе.

Такая же ситуация существует и с драйверами `3c59x` и `3c90x` соответственно для плат 3COM.

Для драйвера `tulip` существует его более старая (и, возможно, более стабильная версия) под названием `tulip_old`. При настройке сетевых плат с интерфейсом ISA, скорее всего, придётся указать параметры для модуля — I/O-порт и IRQ, используемое вашей сетевой платой. При успешной загрузке драйвера в сообщениях ядра (**dmesg**) появится запись об успешной настройке сетевой платы. Если в системе установлены две одинаковые сетевые карты, для их настройки достаточно загрузить один драйвер — он будет обслуживать оба устройства. В случае наличия в системе разных сетевых плат они будут именоваться по порядку загрузки драйверов, т.е. первая — `eth0`, вторая — `eth1` и т.д.

Радио- и видеотюнеры

В *ALT Linux Master 2.2* входят драйвера для различных плат, поддерживающих функции радио- и видеотюнеров. Одними из наиболее популярных на сегодняшний день являются видеотюнеры, основанные на чипах Brooktree (BT848, 878 и т.д.); эти платы определяются и настраиваются автоматически, но в некоторых случаях необходимо произвести ручную более тонкую настройку платы. Как это сделать — описано в документации на драйвер bttv (`/usr/share/kernel*-doc*/video4linux/bttv/*`).

С настройкой радиотюнеров дело обстоит сложнее, т.к. они обычно выполнены для ISA-шины — необходимо вручную определить подходящий драйвер для вашего тюнера (доступные драйвера лежат в каталоге `/lib/modules/kernel-_версия_ядра_/drivers/media/radio/*`) и добавить в файл `/etc/modules.conf` строку вида `alias char-major-81-64 _нужный_драйвер_`). Например, для платы Sound Forge с чипом SF16-FMR2 настройка выглядит так:

```
alias char-major-81-64 radio-sf16fmx2
```

```
options radio-sf16fmx2 io=0x284
```

Управление радиотюнером осуществляется любой программой, соответствующей стандарту *video4linux* (например, qdt или radio из пакета xawtv-radio); управление видеотюнером производится через программы xawtv или kwintv.

Прочее оборудование

Наладонные компьютеры (на основе PalmOS или WinCE)

Для систем на основе WinCE не существует средств для синхронизации их с `Linux`, поэтому для них (как и для Psion) единственным способом обмена данными является перенос данных через Flash-карты или через сеть (или нуль-модемный кабель).Для систем на основе PalmOS существует достаточно много утилит для синхронизации, установки новых программ и т.д. — утилиты нижнего уровня из пакета `pilot-link`, аналог Palm Desktop — программа jpilot и т.д.

Проблемы могут возникнуть, если Palm соединяется с компьютером через USB-интерфейс (Visor или Palm m500) — но обычно всё работает.

Дополнительную информацию можно получить из Palm-HOWTO.

Инфракрасные порты

`Linux` поддерживает множество инфракрасных портов — в том числе высокоскоростные стандартов MIR и HIR; программное обеспечение содержится в пакете `irda-utils`. Информацию по этой теме можно получить в Infrared-HOWTO.

Стриммеры

В дистрибутиве присутствует поддержка различных стриммеров (ленточных накопителей) — в основном это SCSI- и IDE-модели. За дополнительной информацией обращайтесь в список рассылки *ALT Linux* или к содержимому пакета `kernel-doc`.

Сканеры

К сожалению, с поддержкой сканеров в `Linux` дело обстоит не лучшим образом; тем не менее, в состав дистрибутива *ALT Linux Master 2.2* входит система `sane`, поддерживающая устройства, подключаемые

через интерфейс SCSI или параллельный порт. Также поддерживаются некоторые USB-сканеры, для функционирования которых должна быть запущена программа hotplug. Поскольку список поддерживаемых сканеров достаточно мал, перед приобретением сканера настоятельно рекомендуется ознакомиться с документацией из пакета `sane` или на сайте `http://www.mostang.com/sane/`.

Цифровые камеры, mp3-плейеры и прочие дополнительные устройства

В отличие от сканеров, цифровые камеры поддерживаются неплохо; обмен изображениями осуществляется при помощи программ gphoto и gphoto2. В документации к ним находится список поддерживаемых моделей (более 100).

Также поддерживаются некоторые mp3-плейеры на основе Flash-карт и жёстких дисков (с mp3-CD-плейерами, понятное дело, проблем не возникает).

Ссылки

Для получения информации обращайтесь в список рассылки *ALT Linux* или поищите информацию в Интернете:

1. *устройства с USB-интерфейсом*[14];
2. *видеоплаты на чипах nVidia Riva TNT и более поздних*[15];
3. *звуковые платы Aureal*[16];
4. Win-модемы на некоторых чипах (Lucent, 3COM, PCTel) — см. сайты производителей и `http://www.linmodems.org`;

[14] `http://www.linux-usb.org`
[15] `http://www.nvidia.com`
[16] `http://aureal.sourceforge.net`

Часть II. Настройка системы

Глава 2. Файловые системы

Разновидности файловых систем в дистрибутиве *ALT Linux*[18] *Master 2.2*

В дистрибутиве *ALT Linux Master 2.2* поддерживаются следующие файловые системы:

1. `Ext2`;
2. `Ext3` (только для ядра 2.4.x);
3. `ReiserFS` (3.5 – для ядра 2.2.x, 3.5 и 3.6 для ядра 2.4.x);
4. `XFS` (только для ядра 2.4.x);
5. `JFS` (только для ядра 2.4.x);
6. `VFAT`;
7. `NTFS` (только чтение);
8. `ISOFS`;
9. `UDF`;
10. другие (менее распространённые).

Файловые системы 2–5 являются журналируемыми.

Дистрибутив *ALT Linux Master 2.2* может быть установлен на любую из первых трёх систем; при выборе рекомендуется иметь в виду следующие соображения:

`Ext2` является самой «заслуженной» и обкатанной из этих файловых систем; она весьма стабильна, но не является журналируемой;

`Ext3` логическое продолжение `Ext2` в сторону журналируемости; хорошая совместимость с `Ext2` (лёгкое взаимопревращение);

`ReiserFS` журналируемая система, особо оптимизированная под каталоги, содержащие большое количество файлов, а также под небольшие файлы. Для использования в данный момент рекомендуется версия 3.6 для ядер 2.4.x;

Следующие две системы являются экспериментальными. Возможно они будут в списке доступных для установки при условии достаточной стабильности на момент выпуска дистрибутива.

[18] `http://www.altlinux.ru`

`XFS` журналируемая ФС, оптимизированная для хранения больших объёмов информации и хорошей масштабируемости; рекомендуется совместно с samba при необходимости иметь ACL (Access Control Lists);

`JFS` в данный момент для хранения важных данных не рекомендуется вследствие активной доработки.

Файловые системы `ISOFS` и `UDF` используются в носителях CD/DVD-ROM; VFAT и NTFS используются семейством ОС Microsoft.

Работа с файловыми системами

Утилиты для работы с файловыми системами находятся в соответствующих пакетах: для `Ext2` и `Ext3` это e2fsprogs, для `ReiserFS` — reiserfs-utils, `XFS` — xfsprogs, `JFS` — jfsprogs.

Общее назначение утилит

mkfs – создание новой файловой системы (make filesystem);

fsck – проверка файловой системы на ошибки (filesystem check).

Также существуют и другие, специфичные для разных файловых систем утилиты.

Для различения файловых систем используется указание типа файловой системы после параметра -t или в качестве компонента имени утилиты, например:

```
mkfs -t ext2 /dev/hda1
fsck.ext2 /dev/sda2
```

Конвертирование файловых систем

Для преобразования файловой системы из ext2 в ext3 необходимо дать команду

```
tune2fs -j /dev/hdX
```

Замените `hdX` на sdX в случае SCSI-диска. Для обратного преобразования необходимо смонтировать этот раздел как ext2.

Для преобразования файловой системы reiserfs-3.5.x в файловую систему reiserfs-3.6.x необходимо смонтировать эту файловую систему с опцией conv, например:

```
mount -o conv /dev/hdx /mnt/disk
```

После этого файловая система будет преобразована в формат версии 3.6.x. Обратное преобразование невозможно; следовательно, работать со сконвертированным разделом из-под ядер ветки 2.2 тоже не получится[19].

Сохранение копии диска и последующее её использование

Для того, чтобы сохранить копию диска (например, CD-ROM), необходимо сделать следующее:

1. убедиться в наличии в текущем каталоге достаточного свободного места;
2. дать команду

   ```
   dd if=/dev/cdrom of=cdrom.iso bs=1M
   ```

3. после этого можно просмотреть содержимое файла `cdrom.iso`, смонтировав его, например, так:

   ```
   mount -o loop cdrom.iso /mnt/cdrom
   ```

В качестве исходного устройства для копирования также может выступать любое дисковое устройство, например дискета или жёсткий диск. Кроме того, получившийся образ CD-ROM можно записать на матрицу CD-R/RW с использованием программы cdrecord, т.к. файл `cdrom.iso` является полным образом диска.

Для получения дополнительной информации обратитесь к man-страницам на упомянутые команды.

[19] На самом деле использование `ReiserFS` в ядрах 2.2 в любом случае не может быть рекомендовано.

Использование шифрования файловых системам

В *ALT Linux Master 2.2* реализована система шифрования с использованием устройств `/dev/loop*` и поддержкой следующих алгоритмов: `cipher-aes*`, `cipher-blowfish*`, `cipher-des-ede3*`, `cipher-des*`, `cipher-dfc*`, `cipher-rc5*`, `cipher-serpent*`,`cipher-twofish*`.

Процедура создания зашифрованной файловой системы обычно выглядит так:

1. Необходимо создать файл необходимого размера — например, для 8 Мб:

   ```
   dd if=/dev/zero of=test_file count=8 bs=1M
   ```

2. Необходимо настроить алгоритм шифрования:

   ```
   modprobe cryptoloop[20]
   losetup -e blowfish /dev/loop0 test_file
   ```

   Программа спросит размер ключа:
   D1
   ```
   Available keysizes (bits): 128 160 192 256
   Keysize:
   ```

   Далее будет запрошен пароль.После введения пароля алгоритм шифрования blowfish будет подключён к устройству `/dev/loop0`. Данные в зашифрованном виде будут сохраняться в файле `test_file`.

3. Необходимо создать файловую систему

   ```
   mke2fs /dev/loop0
   ```

4. Смонтировать зашифрованное устройство

   ```
   mount /dev/loop0 /mnt/disk
   ```

[20] Это необходимо сделать только для ядер 2.4.x.

После этого можно работать с `/mnt/disk` как с обычным устройством, которое по окончании работы необходимо размонтировать. Для последующего использования данных необходимо повторить шаги 2 и 4. Таким образом можно организовать работу с зашифрованными файловыми системами.

Важно

Для обеспечения сохранности ваших данных рекомендуется каждый раз после изменения данных в зашифрованном файле делать его копию. Особенно это важно при обновлении ядра, т.к. файловые системы, зашифрованные на ядрах версии 2.2.x, могут не прочитаться на ядрах версии 2.4.x и наоборот.

Глава 3. Управление пакетами

В нашем дистрибутиве программы (состоящие, как правило, из нескольких файлов) распространяются объединенными в пакеты формата RPM (RedHat Packet Manager).

С помощью программы **rpm** можно легко устанавливать, модифицировать, удалять и создавать пакеты программного обеспечения, а также получать о них разнообразную информацию. Весь дистрибутив ALT Linux Master (кроме программы начальной установки) состоит из таких пакетов.

Каждый пакет определяется именем программы, номером ее версии и номером версии релиза этой программы нашего дистрибутива, а также архитектурой пакета. Например, `bash-2.0.5-alt2.i586.rpm`: в этом пакете имя – `bash`, номер версии – `2.0.5`, номер релиза – `alt2`, архитектура – `i586`. Чем больше номер версии (или при одинаковых номерах версии – чем больше номер релиза), тем, соответственно, новее пакет.

Часто бывает удобнее, однако, применять программу **rpmdrake**, разработанную MandrakeSoft, **kpackage** из KDE, **gnorpm** из GNOME или систему **apt**, подробно описанную на стр. 27.

Проще всего управлять пакетами через графическую оболочку **rpmdrake**, которую можно запустить через панель управления DrakConf (находящуюся на рабочем столе). Можно выбрать два режима работы – установка или удаление – при помощи кнопок в правом верхнем углу. Выделив пакет, можно получить информацию о нем, входящих в его комплект файлах, а также некоторую другую. Нажав кнопку «Удалить выбранное» или «Установить выбранное», можно удалить или установить выбранные пакеты. Часто бывает так, что требуемый пакет для нормального функционирования требует другие; в этом случае программа предложит вам установить или удалить еще несколько пакетов. При удалении пакетов необходимо соблюдать осторожность, чтобы не удалить важные части системы, например пакеты `kernel` или `glibc`. Для использования функции обновления пакетов необходимо указать программе через меню «Файл»→«Настройки» дополнительный источник пакетов, в качестве которого может выступать как ресурс Internet, так и локальный каталог или диск CD-ROM.

Установку пакетов весьма удобно выполнять и через консольную программу **urpmi** – с тем отличием, что все действия будут выполняться менее наглядно. Для установки пакетов, поставляемых ALT

Linux Team, можно даже запускать программу **urpmi** не от имени суперпользователя, а от обычного пользователя; единственное, что необходимо сделать для этого – добавить его в группу **urpmi**.

Управлять пакетами можно из командной строки при помощи программы **rpm**, которая имеет следующий синтаксис:

```
rpm -options rpm_package_name
```

Далее приводятся возможные параметры.

вставить насчет rpm4, db3, ^C, rm -f /var/lib/rpm/__ ---- mike, 02.22.2002, 18:58 ----*

- Установка пакета. Вы можете установить программу, используя опцию **-i** (опции **-v** и **-h** выставлены здесь для того, чтобы включить визуальное отображение процесса установки). Например, для того, чтобы установить klyx, наберите:

  ```
  rpm -ivh klyx-0.10.9-ipl6mdk.i586.rpm
  ```

  (настоящее имя зависит от версии программы на доступном носителе).

  Заметим, что `ipl6mdk` означает, что пакет был модифицирован ALT Linux Team (ранее – IPLabs Linux Team) для русской редакции, это его шестая сборка, он входит в дистрибутив Mandrake. `i586` указывает на то, что он скомпилирован для процессоров не ниже Pentium(tm). Наличие в имени пакета аббревиатуры `alt2` означает, что пакет был собран ALT Linux Team и это его вторая сборка.
- Обновление пакета. Для того чтобы обновить программу (с целью установки более свежей версии), нужно использовать опцию **-U**, вместо **-i**, это позволит сохранить все текущие конфигурационные файлы. Если пакета ранее не было в системе, то он будет установлен.
- Удаление пакета. Если вы желаете удалить пакет из системы, внимательно введите:

  ```
  # rpm -e имя_пакета_без_номера_версии_и_релиза
  ```

  то есть, например, для пакета `klyx`:

  D1`# rpm -e klyx`

  Если в процессе удаления пакета произойдет нарушение зависимостей, программа **rpm** сообщит об этом.

- Информация о пакете. Вы можете запросить у **rpm** ряд полезной информации о пакете, не устанавливая его – например, бывает удобно просмотреть список всех файлов пакета или краткое описание его возможностей. Для этого используйте опцию **-q** (query, запрос).

  - **-qi** используется для получения некоторой информации о ранее установленном пакете;
  - **-qip** используется для еще не установленных пакетов. В этом случае вы должны указать полный путь и имя пакета (например, `/mnt/cdrom/Mandrake/RPMS/klyx-0.10.9-ipl6mdk.i586.rpm`);
  - **-ql** используется для того, чтобы просмотреть список файлов пакета. Добавьте **p**, если пакет еще не был установлен;
  - **-qa** выдает список всех установленных пакетов (не нужно указывать имя пакета).

Будьте осторожны с опцией **--force** – ее можно употреблять только в тех случаях, когда вы хорошо знаете, что делаете. Если надо установить два или более пакетов, зависящих друг от друга, то установите их одновременно:

```
# rpm -ihv foo-1.1-3mdk.rpm libfoo-1.5-2mdk.rpm
```

Для получения дополнительной информации наберите **man rpm**.

Обеспечение и поддержание целостности системы с помощью APT

Введение

Современные системы на базе Linux состоят из огромного числа разделяемых библиотек, исполняемых файлов, скриптов и т.д. Удаление или изменение версии одного из составляющих систему компонентов может повлечь неработоспособность других, связанных с ним компонентов, или даже вывести из строя всю систему. В контексте системного администрирования проблемы такого рода называют нарушением целостности системы, а задачу по обеспечению наличия в системе всех необходимых программных компонент согласованных версий — задачей обеспечения целостности системы.

Для целей поддержания целостности и обеспечения возможности распространения программ в двоичном виде в первую очередь стали использоваться менеджеры пакетов (такие, как RPM в дистрибутивах *RedHat Linux* или `dpkg` в *Debian* GNU/Linux). Менеджеры пакетов давали возможность унифицировать и автоматизировать сборку двоичных пакетов и облегчали их установку, позволяя проверять наличие необходимых для работы устанавливаемой программы компонент подходящей версии непосредственно в момент установки. Однако менеджеры пакетов оказались неспособны предотвратить все возможные коллизии при установке или удалении программ, а тем более эффективно устранить нарушения целостности системы. Особенно сильно этот недостаток сказывается при обновлении систем из централизованного репозитория пакетов, в котором последние могут непрерывно обновляться, дробится на более мелкие и т.д. Этот недостаток и стимулировал создание систем управления программными пакетами и поддержания целостности системы.

Усовершенствованная система управления программными пакетами APT (Advanced Packaging Tool) первоначально была разработана для управления установкой и удалением программ в дистрибутиве *Debian* GNU/Linux. При разработке ставилась задача заменить используемую в *Debian*систему выбора программных пакетов `dselect` на новую, обладающую большими возможностями и простым пользовательским интерфейсом, а также позволяющую производить установку, обновление и повседневные «хозяйственные» работы с установленными на машине программами без необходимости изучения тонкостей используемой в дистрибутиве менеджера программных пакетов.

Эти привлекательные возможности были долгое время доступны только пользователям *Debian* GNU/Linux, поскольку в APT поддерживалась только один менеджер пакетов, а именно применяемый в *Debian* GNU/Linux менеджер пакетов `dpkg`, несовместимый с используемой в *ALTLinux* RPM. Эта несовместимость заключается прежде всего в различии используемых форматов данных (хотя сущесвуют программы-конверторы), хотя имеютсяа и другие различия, обсуждение которых выходит за рамки изложения.

APT, однако, изначально проектировался, как не зависящий от конкретного метода работы с установленными в системе пакетами, и эта особенность позволила разработчикам из бразильской компании *Conectiva*[21] реализовать в нем поддержку менеджера пакетов RPM. Таким образом, пользователи основанных на RPM дистрибутивов

[21] `http://www.conectiva.com.br`

(*ALTLinux* входит в их число) получили возможность использовать этот мощный инструмент.

APT и в настоящее время находится в стадии разработки, а текущая версия с поддержкой RPM классифицируется, как нестабильная. Это, тем не менее, не означает, что операции, выполняемые посредством APT, безусловно приведут к нестабильности системы. Более того, с помощью APT возможен строгий контроль за целостностью системы: проверка нарушенных зависимостей между установленными пакетами и исправление выявленных ошибок.

Системы управления пакетами RPM и `dpkg` используют концепции представления программного обеспечения в виде набора компонент — программных пакетов. Такие компоненты содержат в себе набор исполнимых программ и вспомогательных файлов, необходимых для корректной работы ПО. Часто компоненты, используемые различными программами, выделяют в отдельные пакеты и помечают, что для работы ПО, предоставленного пакетом A, необходимо установить пакет B. В таком случае говорят, что пакет A *зависит* от пакета B или что между пакетами A и B существует *зависимость*.

Отслеживание зависимостей между такими пакетами представляет собой серьезную задачу для любого дистрибутива — некоторые компоненты могут быть взаимозаменяемыми и при удовлетворении тех или иных требований может обнаружиться несколько пакетов, предлагающих затребованный ресурс.

Задача контроля целостности и непротиворечивости установленного в системе ПО еще сложнее. Представим, что некие программы A и B требуют наличия в системе компоненты C версии 1.0. Обновление версии пакета A, требующее обновления компоненты C до новой, использующей новый интерфейс доступа, версии (скажем, до версии 2.0), влечет за собой обязательное обновление и программы B.

Для автоматизации этого процесса и применяется APT. Такая автоматизация достигается созданием одного или нескольких внешних репозиториев, в которых хранятся пакеты программ и относительно которых производится сверка пакетов, установленных в системе. Репозитории могут содержать как официальную версию дистрибутива, обновляемую его разработчиками по мере выхода новых версий программ, так и локальные наработки, например, пакеты, разработанные внутри компании.

Таким образом, в распоряжении APT находятся две базы данных: одна, описывающая установленные в системы пакеты и вторая, с описанием внешнего репозитория. APT отслеживает целостность установленной системы и, в случае обнаружения противоречий в зависи-

мостях пакетов, руководствуется сведениями о внешнем репозитории для разрешения конфликтов и поиска корректного пути их устранения.

Использование APT

Система APT состоит из нескольких утилит. Главной и наиболее часто используемой является утилита управления пакетами **apt-get**: она автоматически определяет зависимости между пакетами и строго следит за их соблюдением при выполнении любой из следующих операций: установка, удаление или обновление пакетов.

apt-get позволяет устанавливать в систему пакеты, требующих для своей работы других, пока еще не установленных. В этом случае он определяет, какие из отсутствующих пакетов необходимо установить, и доустанавливает их, пользуясь всеми доступными репозиториями. Для того, чтобы **apt-get** мог использовать тот или иной репозиторий, информацию о нем необходимо поместить в файл `/etc/apt/sources.list` и выполнить команду

```
# apt-get update
```

Эту команду необходимо также выполнять каждый раз, когда вы собираетесь работать с репозиторием после длительного перерыва, так как при поиске пакетов APT должен руководствоваться базой данных, отражающей актуальное состояние репозитория. Такая база данных создается заново каждый раз, когда в репозитории происходит изменение: добавление, удаление или переименование пакета. Для ускорения работы **apt-get** хранит локальную копию базы данных, которая через некоторое время может уже не соответствовать реальному состоянию репозитория.

В качестве источника пакетов можно использовать и компакт-диски дистрибутива, поскольку на каждом диске присутствует вся необходимая для APT информация о содержащихся на нем пакетах. Для этого необходимо использовать утилиту **apt-cdrom** с единственным параметром `add`:

```
# apt-cdrom add

Используется точка монтирования CD-ROM /mnt/cdrom/
Размонтирование CD-ROM
Пожалуйста, вставьте диск в устройство и нажмите <Enter>
```

```
Монтирование CD-ROM
Используется точка монтирования CD-ROM /mnt/cdrom
Определение... [8d56fef8c93e5255540c843e4b9f49fa-2]
Сканирование диска в поисках индексных файлов...
Найдено 1 бинарных пакетов и 1 исходных пакетов.
Пожалуйста, укажите имя этого диска, например, 'Мой Дистрибутив Диск
1':
Master Disk 1
Этот диск называется
'Master Disk 1'
Reading Indexes... Завершено
Reading Indexes... Завершено
Запись нового списка источников
Список источников для этого диска:
rpm cdrom:[Master Disk 1]/ Mandrake Master
rpm-src cdrom:[Master Disk 1]/ Mandrake Master
```

Повторите этот процесс для всех CD в вашем наборе.

После этого в `/etc/apt/sources.list` появится запись о подключенном диске:

```
rpm cdrom:[Master Disk 1]/ i586/Mandrake Master
rpm-src cdrom:[Master Disk 1]/ Mandrake Master
```

Если подключение к Internet отсутствует, то следует закомментировать те строчки в `/etc/apt/sources.list`, в которых говорится о ресурсах, доступных по Сети. Непосредственно после установки дистрибутива *ALTLinux* в `/etc/apt/sources.list` указаны несколько таких источников:

- репозиторий обновлений в системе безопасности дистрибутива;
- бинарные пакеты из репозитория *Sisyphus*[22] («Сизиф»);
- исходные тексты архивов, использовавшихся для сборки пакетов в репозитории *Sisyphus*.

Проект *Sisyphus* команды *ALT Linux Team* содержит большое количество программ, в том числе и не вошедших в тот или иной дистрибутив. Следует иметь в виду, что он не является самостоятельным дистрибутивом, а отражает текущее состояние разработки и может содержать нестабильные версии пакетов. Периодически на базе этого проекта выпускаются отдельные оттестированные «срезы»-дистрибутивы.

[22] `http://www.altlinux.ru/index.php?module=sisyphus`

Репозиторий ежедневно обновляется разработчиками, поэтому необходимо синхронизировать локальную базу данных с сервером *ALTLinux* (или его зеркалами) перед началом работы с APT. Такую синхронизацию достаточно делать один раз в день командой **apt-get update**. Для репозиториев, подключенных командой **apt-cdrom add**, синхронизацию достаточно сделать один раз в момент подключения.

Установка или обновление пакета

Установка пакета с помощью APT, выполняется командой

```
# apt-get install имя-пакета
```

Иногда, в результате операций с пакетами без использования APT, целостность системы нарушается и **apt-get** отказывается выполнять операции установки, удаления или обновления. В этом случае необходимо повторить операцию, задав опцию `-f`, заставляющую **apt-get** исправить нарушенные зависимости, если это возможно. В этом случае необходимо внимательно следить за сообщениями, выдаваемыми **apt-get**, анализировать их и четко следовать рекомендациям программы.

Команда **apt-get install имя_пакета** используется и для обновления уже установленного пакета или группы пакетов. В этом случае **apt-get** дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе. Если вы не знаете точное название пакета, для его поиска можно воспользоваться утилитой **apt-cache**, описанной ниже.

Пример 3.1. Установка пакета `clanbomber` командой **apt-get install clanbomber** приведет к следующему диалогу с APT:

```
Обработка файловых зависимостей... Завершено
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
clanlib clanlib-mikmod clanlib-sound libmikmod
Следующие НОВЫЕ пакеты будут установлены:
clanbomber clanlib clanlib-mikmod clanlib-sound libmikmod
0 пакетов будет обновлено, 5 будет добавлено новых,
0 будет удалено(заменено) и 0 не будет обновлено.
Необходимо получить 0B/2577kB архивов. После распаковки 3862kБ будет
использовано.
Продолжить? [Y/n] y
Выполняется программа RPM (/bin/rpm -Uv --replacepkgs -h)...
Подготовка... ########################################
libmikmod ############################################
clanlib ##############################################
clanlib-mikmod #######################################
clanlib-sound ########################################
clanbomber ###########################################
```

> **Внимание**
>
> **apt-get** всегда спрашивает подтверждение выполнения операции установки и обновления, за исключением случая, когда реально требуется установить в систему (или обновить) только один пакет. Если вы не уверены в том, что результате выполнения операции система останется работоспособной, запустите **apt-get** с опцией `-S`, которая покажет отчет выполнения операции обновления, но реально обновление произведено не будет.

В случае обнаружения противоречий между установленными в системе пакетами, следует запустить команду **apt-get -f install**, и APT постарается разрешить найденные конфликты, предложив удалить или заменить конфликтующие пакеты. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

Удаление установленного пакета

Для удаления пакета используется команда **apt-get remove имя_пакета**. Для того, чтобы не нарушать целостность системы,

будут удалены и все пакеты, зависящие от удаляемого: если отсутствует необходимая для работы приложения библиотека, то само приложение становится бесполезным). В случае удаления пакета, который относится к базовым компонентам системы, apt-get потребует дополнительного подтверждения производимой операции с целью предотвратить возможную случайную ошибку.

Запрос на подтверждение операции удаления базовой компоненты системы выглядит следующим образом:

```
# apt-get remove filesystem
Обработка файловых зависимостей... Завершено
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
basesystem filesystem ppp sudo
Внимание: следующие базовые пакеты будут удалены:
В обычных условиях этого не должно было произойти, надеемся, Вы точно
представляете, что требуете!
basesystem filesystem (по причине basesystem)
0 пакетов будет обновлено, 0 будет добавлено новых, 4 будет
удалено(заменено) и 0 не будет обновлено.
Необходимо получить 0B архивов. После распаковки 588kБ будет
освобождено.
Вы собираетесь предпринять что-то потенциально вредное
Для продолжения, наберите по-английски 'Yes, I understand this may be
bad'
(Да, я понимаю, что это может быть плохо).
```

Каждую ситуацию, в которой APT генерирует такое сообщение, необходимо рассматривать отдельно. Однако, вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

Обновление всех установленных пакетов

Для обновления всех установленных пакетов используется команда **apt-get upgrade**. Она позволяет обновить те и только те установленные пакеты, для которых в репозиториях, перечисленных в `/etc/apt/sources.list`, имеются новые версии; при этом из системы не будут удалены никакие другие пакеты. Этот способ полезен при работе со стабильными пакетами приложений, относительно которых известно, что они при смене версии изменяются несущественно.

Иногда, однако, происходит изменение в именовании пакетов или изменение их зависимостей. Такие ситуации не обрабатываются командой **apt-get upgrade**, в результате чего происходит нарушение целостности системы: появляются неудовлетворенные зависимости. Например, переименование пакета `MySQL-shared`, содержащего динамически загружаемые библиотеки для работы с СУБД MySQL, в `libMySQL`, отражая общую тенденцию к наименованию библиотек в дистрибутиве, не приводит к тому, что установка обновленной версии `libMySQL` требует удаления старой версии `MySQL-shared`. Для разрешения этой проблемы существует режим обновления в масштабе дистрибутива — **apt-get dist-upgrade**.

В случае обновления всего дистрибутива APT проведет сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, а также отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Все, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчете **apt-get**, которым APT предварит само обновление.

При работе с *Sisyphus* для обновления системы рекомендуется использовать команду**apt-get dist-upgrade**.

Поиск в репозитории

Для поиска нужного пакета можно воспользоваться утилитой **apt-cache**, которая позволяет искать не только по имени пакета, но и по его описанию.

Команда **apt-cache search подстрока** позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Например:

```
$ apt-cache search master

xcdroast - A GUI program for burning Cds
bluefish - A WYSIWYG GPLized HTML editor
xmess - X-Mess Multi Emulator Super System
mkisofs - Creates an image of an ISO9660 filesystem
```

В кратком описании каждого из перечисленных пакетов не присутствует слово «master».

Для того, чтобы подробнее узнать о пакете, можно воспользоваться командой **apt-cache show**, которая покажет информацию о пакете из репозитория и в том числе:

```
Пакет: bluefish
Секция: Networking/WWW
Размер установленных пакетов: 2018
Упаковщик: AEN <aen@logic.ru>
Версия: 1:0.7-alt0.1
..
Предоставляет: bluefish
Архитектура: i586
..
Имя файла: bluefish-0.7-alt0.1.i586.rpm
Описание: A WYSIWYG GPLized HTML editor
Bluefish is a programmer's HTML editor, designed to save the
experienced webmaster some keystrokes.
It features a multiple file editor, multiple toolbars, custom menus,
image and thumbnail dialogs, open from the web, HTML validation and
lots of wizards.
It is in continuous development, but it's already one of the best
WYSIWYG HTML editors.
```

Наличие слова «webmaster» и объясняет наличие этого пакета в результате поиска по слову «master».

Настройка APT

APT позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные — HTTP и FTP, именно они используются для работы с *Sisyphus*[23]. Однако существуют и некоторые дополнительные методы.

Настройка описаний репозиториев задается в файле `/etc/apt/sources.list` в следующем виде:

```
rpm [подпись] метод:путь база название
rpm-src [подпись] метод:путь база название
```

- `rpm` или `rpm-src` — тип репозитория (скомпилированные программы или исходные тексты);
- `подпись` — опциональная строка-указатель на сигнатуру разработчиков. Сигнатуры описываются в файле `/etc/apt/vendor.list`;

[23] `http://www.altlinux.ru/index.php?module=sisyphus`

- `метод` — способ доступа к репозиторию: `ftp`, `http`, `file`, `rsh`, `ssh`, `cdrom`;
- `путь` — путь к репозиторию в терминах выбранного метода;
- `база` — относительный путь к базе данных репозитория;
- `название` — название репозитория;

Например, при установке *ALTLinux* в `/etc/apt/sources.list` записываются следующие настройки:

```
# Sisyphus
rpm [alt]↩
ftp://ftp.altlinux.ru/pub/distributions/ALTLinux/Sisyphus↩
i586/Mandrake sisyphus
rpm-src [alt]↩
ftp://ftp.altlinux.ru/pub/distributions/ALTLinux/Sisyphus↩
i586/Mandrake sisyphus
```

При этом, реальная структура репозитория по адресу `ftp://ftp.altlinux.ru/pub/distributions/ALTLinux/Sisyphus` выглядит следующим образом:

```
ftp://ftp.altlinux.ru/pub/distributions/ALTLinux/Sisyphus
|-- SRPMS
|-- i586
| |-- Mandrake
| | |-- RPMS
| | |-- RPMS.sisyphus -> RPMS
| | |-- SRPMS.sisyphus -> ../../SRPMS
| | |-- base
```

Более подробное описание команд программы **apt-get** можно найти в справочной системе дистрибутива на страницах `apt-get(8)` и `apt.conf(5)`.

Создание собственного репозитория

Вы можете создавать собственные репозитории и использовать их для обновления и/или установки собственных программ. Для этого необходимо создать структуру каталогов, подобную описанной выше. Вы можете выбирать из следующих компонентов (перечисляются по дереву выше):

i586

архитектура, под которую собраны пакет (совпадает с таковой в имени бинарных RPM-пакетов)

Mandrake

название подсистемы. Этот уровень в дереве может отсутствовать (то есть, каталоги `RPMS` и `base` могут идти сразу следом за архитектурой)

RPMS

каталог, в котором размещены бинарные пакеты

SRPMS

каталог, в котором размещены пакеты с исходными текстами программ

RPMS.sisyphus

ссылка на каталог `RPMS`. При этом `sisyphus` заменяется на собственное название репозитория, например, `local`

base

служебный каталог, в котором размещается база данных APT

Следующий шаг в создании своего репозитория заключается в помещении бинарных пакетов в каталог `RPMS`, а пакетов с исходными текстами — в каталог `SRPMS` и в генерации служебной информации для APT при помощи команды **genbasedir**; ее формат:

`genbasedir` [опции] {название подсистемы} {репозиторий 1} [репозиторий 2...]

Из опций, список которых можно увидеть при запуске **genbasedir** без параметров, наиболее важной является опция `--topdir`, позволяющая указать путь к репозиторию. Все остальные параметры задаются относительно этого пути. Выглядит это следующим образом. Допустим, что наше дерево каталогов выглядит так:

```
/opt/repository/
|-- SRPMS
|-- SRPMS.security
|-- i386
| |-- MyDistro
```

```
| | |-- RPMS
| | |-- RPMS.local -> RPMS
| | |-- RPMS.security
| | |-- SRPMS.local -> ../../SRPMS
| | |-- SRPMS.security -> ../../SRPMS.security
| | |-- base
```

Тогда строка запуска **genbasedir** будет выглядеть так:

```
$ genbasedir --topdir=/opt/repository i386/MyDistro local security
```

Этой командой мы создадим информацию для APT в двух репозиториях — `local` и `security`. Для того, чтобы воспользоваться этой информацией, необходимо прописать доступ к репозиториям в `/etc/apt/sources.list`:

```
rpm file:/opt/repository i386/MyDistro local
rpm-src file:/opt/repository i386/MyDistro local
rpm file:/opt/repository i386/MyDistro security
rpm-src file:/opt/repository i386/MyDistro security
```

Репозиторий `MyDistro.security`, хранящий пакеты с исправлениями ошибок в системе безопасности, имеет смысл подписывать PGP-ключом, чтобы при установке пакета можно было проверить аутентичность репозитория и хранящихся в нем пакетов. Для этого необходимо создать соответствующий PGP-ключ, используя программу GnuPG (**gpg**) и запомнить его отпечаток (fingerprint) на клиентских машинах в файле `/etc/apt/vendors.list` в формате:

```
simple-key "краткое название ключа" {
Fingerprint "отпечаток ключа";
Name "Полное название ключа";
}
```

Примером может служить ключ службы безопасности *ALT Linux Team*[24], которым подписаны пакеты репозитория *Sisyphus* и обновления безопасности для различных дистрибутивов *ALTLinux*:

```
simple-key "alt" {
```

[24] `http://www.altlinux.ru`

```
Fingerprint "BB1DD157A9722953847C5DB25B433A0EEAC91CA0";
Name "ALT Security Team <security@altlinux.ru>";
}
```

Для того, чтобы APT проверял аутентичность подписи, необходимо указать, что соответствующий репозиторий подписан PGP-ключом в `/etc/apt/sources.list`:

```
rpm [alt] file:/opt/repository i386/MyDistro security
rpm-src [alt] file:/opt/repository i386/MyDistro security
```

Необходимо также сгенерировать информацию для APT в репозитории с указанием опции `--sign` команды **genbasedir**. Дополнительно, можно указать идентификатор ключа, если он отличается от ключа по умолчанию, используя опцию `--uid=идентификатор`. Значением этой опции является идентификатор ключа в том виде, как он передается программе GnuPG в опции `--default-key`:

```
$ genbasedir --topdir=/opt/repository --sign \
--uid='ALT Security Team' i386/MyDistro security
```

Операцию создания служебной информации для APT необходимо производить каждый раз, когда в репозиторий вносятся изменения.

Часть III. Безопасность

Глава 4. Основы безопасности

Основные правила

Человек устроен таким образом, что задумывается о вопросах безопасности только после того, как почувствовал на себе последствия небрежного отношения к этой проблеме.

Применительно к компьютерной безопасности, зачастую только авария системы либо потеря важных данных заставляют вспомнить о том, что этого можно было легко избежать, следуя несложным правилам:

- Своевременно обновляйте программное обеспечение. Авторы дистрибутива прилагают максимум усилий к выявлению и исправлению ошибок, затрагивающих безопасность системы.
  Подпишитесь на список рассылки `security-announce@altlinux.ru` (это можно сделать по адресу `http://www.altlinux.ru/mailman/listinfo/security-announce`), чтобы быть вовремя проинформированным о новых версиях программ, исправляющих ошибки в сфере безопасности.
- Следуйте разумной политике в использовании паролей для пользователей. Не используйте пароли, попытка установки которых приводит к предостережению от утилиты passwd (см. тж. !!!).
- Не работайте привилегированным пользователем (`root`).
- Не запускайте те сервисы, которыми никто не будет пользоваться и отключайте временно неиспользуемые.
- Следуйте основным правилам сетевой безопасности:

  - Настройте *межсетевой экран* между своим компьютером и остальной сетью, а также между корпоративной сетью и Интернетом.
  - Используйте защищенные протоколы для передачи данных, такие как IPSEC (IP Security) и SSH (Secure Shell).
  - Не используйте электронную почту для передачи конфиденциальной информации; если использование электронной почты для этих целей абсолютно необходимо, например, ввиду отсутствия технической возможности применения защищенных протоколов передачи данных, то воспользуйтесь GnuPG для подписи и шифрования почтовых сообщений.

- Используйте различные пароли к локальным ресурсам и ресурсам, расположенным на удаленных серверах с тем, чтобы пароли к локальным ресурсам не покидали пределов локальной сети.

Помните также, что авторы дистрибутива постарались сделать вашу систему безопасной «из коробки», поэтому не ломайте эту защиту не подумав.

Почему нельзя работать с правами администратора

Ни для кого не секрет, что `Linux` является *многопользовательской* операционной системой — это значит, что она разработана в расчёте на одновременную работу нескольких пользователей. При этом всякая будничная работа под `Linux`, не являющаяся системным администрированием, может и должна выполняться непривилегированными пользователями. Этому правилу необходимо следовать для того, чтобы вероятность приведения системы в нерабочее состояние из-за вашей случайной ошибки или возможных ошибок в используемых вами программах была сведена к минимуму.

К сожалению, немалая часть программного обеспечения написана безграмотно с точки зрения безопасности. Запуская такие программы непривилегированным пользователем, вы тем самым автоматически уменьшаете риск повреждения системы от сбоя и усложняете процедуру вторжения в вашу систему потенциальных взломщиков.

В *Master 2.2* настройки для пользователя `root` определяются спецификой его задач, а потому не приспособлены для повседневной работы и лишь ограниченно локализованы.

Настройка sudo

sudo — это программа, разработанная в помощь системному администратору и позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы. Основная идея — дать пользователям как можно меньше прав, но при этом ровно столько, сколько необходимо для решения поставленных задач.

Команда **sudo** предоставляет возможность пользователям выполнять команды от имени `root` либо других пользователей. Правила, используемые sudo для принятия решения о предоставлении доступа,

находятся в файле `/etc/sudoers`; язык их написания и примеры использования подробно изложены в `sudoers(5)`. Кроме того, пример правил, предоставляющих пользователям, являющимся членами группы `rpm`, возможность устанавливать, обновлять и удалять пакеты в системе, приведен в файле `/usr/share/doc/sudo-<версия>/rpm.sudoers`.

Для редактирования файла `/etc/sudoers` следует использовать программу **visudo**, которая проверяет синтаксис и тем самым позволяет избежать ошибок в правилах.

В большинстве случаев грамотная настройка sudo делает работу от имени суперпользователя ненужной.

Глава 5. Сетевая безопасность

Настройка межсетевого экрана

Межсетевой экран является, пожалуй, наиболее важной компонентой в системе защиты внутренней сети от вторжений извне и регулирования доступа пользователей внутренней сети к внешним ресурсам.

Создание межсетевого экрана начинается с определения политики безопасности в той сети, для которой он разрабатывается. Для этого:

1. определите используемые сервисы;
2. определите группы пользователей;
3. определите, к каким сервисам какие группы должны иметь доступ;
4. объявите все остальные формы доступа запрещенными.

Как только политика безопасности сети определена, можно приступать к созданию правил для конкретного межсетевого экрана. В случае ядра из серии `2.2` синтаксис правил определяется интерфейсной утилитой ipchains, `2.4` — iptables.

Сами правила можно создавать как вручную, так и с помощью вспомогательных утилит конфигурирования — например, gfcc.

Рекомендации по построению политики безопасности сети, а также подробную документацию по ipchains и iptables можно найти ниже в отдельном разделе и в

- `ipchains(8)`, `iptables(8)`
- `/usr/share/doc/ipchains-1.3.10/`
- `/usr/share/doc/HOWTO/HTML/en/Firewall-HOWTO.html`

Secure Shell

Одна из самых распространенных задач, возникающих при работе в сети — удаленный доступ к другим компьютерам и предоставление такого доступа.

Для решения этой задачи используется ставший уже традиционным протокол SSH (Secure Shell). В отличие от устаревших протоколов, таких как telnet и rsh/rlogin/rcp, которые передают данные прямым текстом и подвержены обыкновенному прослушиванию и различным

атакам, SSH реализует соединение с удаленным компьютером, защищающее от:

1. прослушивания данных, передаваемых по этому соединению;
2. манипулирования данными на пути от клиента к серверу;
3. подмены клиента либо сервера путем манипулирования IP-адресами, DNS либо маршрутизацией.

В дополнение к отличным характеристикам в области обеспечения безопасного клиент-серверного соединения, SSH обладает следующими возможностями:

1. сжатие передаваемых данных;
2. туннелирование каналов внутри установленного соединения — в т.ч. соединений с *X-сервером*;
3. широкая распространенность: существуют реализации SSH для самых различных аппаратных платформ и операционных систем.

OpenSSH — это входящая в дистрибутив реализация SSH, поддерживающая версии `1.3`, `1.5` и `2.0` протокола SSH, и распространяемая на условиях лицензии BSD. Эта реализация включает в себя:

1. клиентские программы ssh, scp и sftp (используются для запуска программ на удаленных серверах и копирования файлов по сети);
2. серверные программы sshd, sftp-server (используются для предоставления доступа по протоколу SSH);
3. вспомогательные программы make-ssh-known-hosts, rescp, ssh-keygen, ssh-add, ssh-agent, ssh-copy-id, ssh-keyscan.

Часть IV. Сеть

Глава 6. Общая информация

Сеть – это система, предназначенная для обмена информацией между различными ее узлами, в том числе компьютерами. Рассмотреть все способы работы с сетями, равно как и различные варианты их настройки, в данном руководстве невозможно – поэтому в данном разделе описываются способы работы дистрибутива ALT Linux Master с различными типами сетей.

Приведенная здесь информация является набором общих рекомендаций и советов, применимых к данному дистрибутиву. За более подробной документацией вы можете обратиться как к различной печатной литературе, так и к электронным документам из серии HOWTO, главным из которых является Networking-Overview-HOWTO, который помимо того, что содержит ссылки на другие источники информации, переведен на множество языков (в том числе русский).

Для работы с сетью в дистрибутиве ALT Linux Master можно использовать как общие для всех UNIX-подобных систем команды (например, **ifconfig**, **ping**, **traceroute** и т.д.), так и специальную систему скриптов, написанную специально для облегчения работы с сетью.

Фактически **draknet** всего лишь производит настройки путем изменения некоторых файлов конфигурации из дистрибутива, данные из которых потом используются различными программами. Опытным системным администраторам следует знать месторасположение и назначение этих файлов:

1. `/etc/sysconfig/network` – общие настройки сети;
2. `/etc/sysconfig/network-scripts` – файлы настроек и скрипты для работы с различными типами сетевых устройств и подключений. Например файл `/etc/sysconfig/network-scripts/ifcfg-eth0` содержит информацию о настройке сетевой Ethernet-карты с интерфейсом eth0;
3. `/etc/ppp` – файлы настройки протокола ppp;
4. `/etc/init.d/` – каталог с различными инициализационными скриптами, среди которых скрипты **network**, **firewall** и некоторые другие отвечают за настройку сети в момент загрузки и выключения компьютера.

В общем случае для запуска всех настроенных на данном компьютере соединений (настроенных на автоматический запуск при загрузке) необходимо дать команду **/etc/init.d/network start**, для останова и перезапуска соответственно используются ключи **stop** и **restart**.

Для запуска отдельно взятого интерфейса можно дать команду **ifup**интерфейс – например, **ifup ppp0**.

Для выключения интерфейса можно применить команду **ifdown** интерфейс.

Утилита draknet

Наиболее распространенные варианты настройки сети в Master можно произвести с помощью утилиты **draknet** – поэтому рекомендуется сначала попробовать воспользоваться ей, а при недостаточности фукнциональности этой утилиты попробовать произвести требуемые настройки вручную.

Сразу после запуска **draknet** предлагает попробовать определить автоматически сетевые устройства, установленные на вашем компьютере. Обычно стоит выбрать эту опцию за исключением случаев, когда она создает проблемы. После этого вам будет предложено настроить один из сетевых адаптеров, причем устройства, найденные автоматически, будут отмечены особо; далее необходимо ответить на вопросы (указать требуемые параметры), после чего ваша сеть будет настроена.

Глава 7. Подключение к сети

Локальная сеть

Как известно, локальная сеть обычно строится на основе технологии Ethernet; если ваша не является исключением, перед настройкой параметров сети стоит убедиться, что настроена ваша сетевая карта (см. стр.!!!).

Далее для настройки локальной сети можно запустить утилиту **draknet**, с помощью которой можно задать или изменить необходимые параметры.

Из них необходимо знать следующие:

1. IP-адрес данного компьютера;
2. маску подсети;
3. доменное имя данного компьютера;
4. IP-адрес(а) серверов DNS для данной локальной сети;
5. IP-адрес стандартного шлюза для данной сети (обычно это нужно для выхода в Internet).

Параметры, отмеченные звездочкой, являются обязательными.

Если в сети не используются специально выделенные IP-адреса для компьютеров – скорее всего, они раздаются автоматически DHCP-сервером. Для настройки сети с его использованием необходимо выбрать в утилите **draknet** соответствующий пункт.

Настройка локальных сетей, отличных от Ethernet, выходит за рамки этого описания; для получения информации на эту тему можно обратиться к HOWTO.

Для проверки работоспособности сети TCP/IP можно воспользоваться следующей схемой.

Для начала убедитесь в работоспособности только что настроенного вами интерфейса при помощи команды

```
$ ping ip_адрес_интерфейса
```

При получении ответов от него можно проверить командой **ping** доступность любого внешнего интерфейса из той же подсети, что и только что настроенный. После этого необходимо проверить работоспособность серверов DNS с помощью команды

```
$ host имя_хоста имя_сервера_DNS
```

Для проверки возможности доступа к Internet необходимо дать команду **ping** `интернет_сервер`, например, **ping www.altlinux.ru**.

Глава 8. Выход в Internet

Настройка модемного соединения

Таковая осуществляется выбором пункта «Обычное модемное соединение» (Normal modem connection). Если вы не выбрали автоматическое определение устройств – необходимо указать порт, к которому подключен модем. Далее надо ответить на следующие вопросы программы:

1. название соединения;
2. номер телефона провайдера;
3. тип набора номера – импульсный или тоновый. На большинстве АТС в России и СНГ доступен только импульсный тип набора;
4. идентификатор пользователя (Login ID), данный вам провайдером;
5. пароль для входа;
6. тип аутентификации. По умолчанию стоит оставить PAP (так как этот тип наиболее часто используется). Использовать тип CHAP стоит только в случаях, если на удаленном сервере требуется именно этот тип (обычно он используется системами на основе Windows NT). Если же ваш провайдер требует аутентификации вручную (т.е. ввод имени и пароля при доступе к системе), можно сделать этот процесс автоматизированным через скрипт доступа. Для полностью ручного доступа можно выбрать пункт Terminal-Based;
7. имя домена – необходимо заполнять только в том случае, если ваш провайдер требует этого. По умолчанию лучше всего оставить пустым;
8. первичный DNS – если ваш провайдер требует явного указания сервера DNS для выхода в Internet. Обычно сервера DNS назначаются провайдерами автоматически;
9. вторичный DNS – то же самое.

Определитесь, нужно ли, чтобы соединение устанавливалось автоматически при загрузке системы. Для модемного соединения это обычно не нужно.

Затем вы можете проверить новое соединение на работоспособность.

После настройки соединения производить подключение к Internet через модем возможно, например, следющими способами:

1. **/sbin/ifup ppp0** – этот способ работает как из консоли, так и из X-сессии;
2. посредством графической утилиты **kppp**, использующей графический интерфейс KDE.

> **Замечание**
>
> При настройке обратите внимание на то, что при выставленном значении default gateway PPP-соединение не установится; проверить маршрутизацию можно при помощи команды **/sbin/route -n**.

Организация шлюза

Для выхода в Internet должны выполняться следующие условия:

1. присутствие физического канала в Internet (например, модема);
2. функционирование этого канала на одном из компьютеров сети;
3. настроенная соответствующим образом маршрутизация для пересылки пакетов из внутренней локальной сети в Internet;
4. настройка всех компьютеров локальной сети на использование системы, имеющей физическое соединение с Internet, в качестве стандартного шлюза для данной сети; кроме того, должны быть правильно указаны DNS-серверы.

Автоматическую настройку данного варианта соединения можно сделать с помощью утилиты **drakgw**; она производит следующие действия:

1. присваивает интерфейсу `eth0` IP-адрес 192.168.0.1;
2. настраивает сервис DHCP для присвоения клиентам адресов из подсети 192.168.0.x;
3. конфигурирует маршрутизацию таким образом, что все клиентские компьютеры, получившие сетевые настройки через этот DHCP-сервер, будут получать доступ в Internet через указанную систему;
4. создает кэширующий сервер DNS.

В итоге всего этого после завершения работы программы **drakgw** при условии, что ваш компьютер имел настроенный ранее доступ к Internet, все клиентские компьютеры из локальной сети также получают разделяемый доступ к Internet через него.

Для получения более подробной информации по настройке разделяемого доступа к Internet можно прочитать Internet-Sharing-HOWTO.

Маршрутизация

Для настройки обычной маршрутизации в дистрибутиве ALT Linux Master используется стандартная утилита **route**; расширенная конфигурируется при помощи дополнительных утилит (например, **iproute2**).

Базовые сведения по настройке и установке PPTP соединения с провайдером

Введение

Протокол PPTP используется для установления частного соединения с провайдером посредством локальной сети. «Частность» соединения обеспечивается механизмом «имя_пользователя — пароль», т.е. каждый, кто хочет соединиться с провайдером должен иметь «имя_пользователя» и соответствующий ему «пароль». Соединение по этому протоколу часто применяется для предотвращения так называемого *IP-спуфинга*.

Пакет `pptp-client` является реализацией протокола PPTP для Линукс и других UNIX систем. Программы, входящие в него, распространяются на условиях лицензии GPL (см. файл `COPYING`).

Дополнительную более подробную информацию вы можете получить с сайта `http://pptpclient.sourceforge.net`

Руководство по настройке

Для работы PPTP-туннеля необходима поддержка в ядре

- IP: tunneling
- IP: GRE tunnels over IP
- PPP (point-to-point protocol) support

В дистрибутивах *ALT Linux Team* все эти пункты поддерживаются по умолчанию, так что пересборка ядра не требуется.

Настройка pptp с использованием программы pptp-command

Для работы программе pptp необходимо знать IP-адрес сервера для соединения. Этот адрес можно указать как параметр командной строки при вызове программы **pptp**. Второй способ — создать конфигурационный файл с помощью программы **pptp-command**. **pptp-command** — это программа, написанная на перле, она задает вопросы пользователю и в соответствии с ответами создает конфигурационный файл в каталоге `/etc/ppp/peers`.

Запустить программу легко:

```
# pptp-command
```

Вы увидите на экране приглашение для ввода цифры:

```
1.) start
2.) stop
3.) setup
4.) quit
What task would you like to do?:
```

При вводе «1» программа предложит выбрать вам какой туннель вы хотите стартовать и после ввода запустит его.

При вводе «2» прекращают свою работу все работавшие туннели.

При вводе «3» вы попадете в диалог настройки:

```
1.) Manage CHAP secrets
2.) Manage PAP secrets
3.) List PPTP Tunnels
4.) Add a NEW PPTP Tunnel
5.) Delete a PPTP Tunnel
6.) Configure resolv.conf
7.) Select a default tunnel
8.) Quit
?:
```

Для начала нам нужно создать записи с «секретами». Эти записи имеют формат

```
имя_пользователя   имя_сервера   пароль
```

и хранятся в файлах `/etc/ppp/chap-secrets` или `/etc/ppp/pap-secrets` в зависимости от метода авторизации. Вам скорее всего понадобится создать CHAP-секрет (точно может сказать только ваш провайдер). Итак выбираем «1» и видим на экране диалог управления секретами:

```
1.) List CHAP secrets
2.) Add a New CHAP secret
3.) Delete a CHAP secret
4.) Quit
?:
```

При вводе «1» на экран выводится список существующих секретов.

При вводе «3» вам предлагается выбрать из списка секрет для удаления. Секреты создаются и удаляются парами (подробнее ниже), так что нужно выбирать только один.

Для добавления нового секрета вводим «2». На экране видим следующее:

```
Add a NEW CHAP secret.

NOTE: Any backslashes (\) must be doubled (\\).

Local Name:

This is the 'local' identifier for CHAP authentication.

NOTE: If the server is a Windows NT machine, the local name
        should be your Windows NT username including domain.
        For example:

              domain\\username

Local Name:
```

«Local name» — это «имя_пользователя», которое вы должны были придумать сами и сообщить провайдеру или провайдер должен был

придумать сам и сообщить его вам. После ввода имени (я вводил test) на экране появится следующее:

```
Remote Name:

This is the 'remote' identifier for CHAP authentication.
In most cases, this can be left as the default. It must be
set if you have multiple CHAP secrets with the same local name
and different passwords. Just press ENTER to keep the default.

Remote Name [PPTP]:
```

Здесь нужно ввести «имя_сервера», которое будет использоваться при авторизации. Часто серверу не нужно подтверждать свою «персону», так что, если вам провайдер не сообщил имя сервера, то смело жмите ENTER, и имя станет «PPTP». Далее увидим:

```
Password:

This is the password or CHAP secret for the account specified. The
password will not be echoed.

Password:
```

Здесь нужно ввести пароль, соответствующий вашему «имени_пользователя».

После всех этих действий мы снова попадаем в диалог управления секретами. Теперь вы можете выбрать «1» и увидеть ваши секреты. Их два:

```
test    PPTP    *****
PPTP    test    *****
```

Второй нужен для авторизации сервера.

Далее нам нужно создать «туннель». Для этого возвращаемся в главный диалог, введя «4» или «q», и выбираем «4» (Add a NEW PPTP Tunnel). На экране видим следующее:

```
Add a NEW PPTP Tunnel.
```

```
1.) Other
Which configuration would you like to use?:
```

Здесь нам ничего не остается, как ввести «1» для продолжения.

```
Tunnel Name:
```

Имя туннеля, т.е. имя файла в /etc/ppp/peers. Я ввел test.

```
Server IP:
```

IP-адрес сервера, с которым мы будем соединяться (вам его должен был сообщить провайдер). Я ввел 192.168.5.2

```
What route(s) would you like to add when the tunnel comes up?
This is usually a route to your internal network behind the PPTP↩
server.
You can use TUNNEL_DEV and DEF_GW as in /etc/pptp.d/ config file
TUNNEL_DEV is replaced by the device of the tunnel interface.
DEF_GW is replaced by the existing default gateway.
The syntax to use is the same as the route(8) command.
Enter a blank line to stop.
route:
```

Здесь можно создать дополнительные маршруты. В большинстве случаев никаких дополнительных маршрутов создавать не надо. Однако, если вам точно требуется специальный маршрут, то здесь его можно указать, и он будет автоматически создан при старте туннеля. Для создания специального маршрута после приглашения

```
route:
```

нужно ввести команду для работы с таблицей маршрутизации. Вся введенная строка просто передается как параметр команде **route(8)**.

> **Замечание**
>
> Для создания маршрута по умолчанию через туннель используйте параметр `defaultroute` в файле настроек для **pppd**.

После ввода команды появится еще одно приглашение

```
route:
```

Для завершения нажимаем ENTER. Далее видим:

```
Local Name and Remote Name should match a configured CHAP or PAP↩
secret.
Local Name is probably your NT domain\username.
NOTE: Any backslashes (\) must be doubled (\\).

Local Name:
```

Здесь нужно ввести «имя_пользователя» из существующего секрета, которое будет использоваться при соединении.

```
Remote Name [PPTP]:
```

Все вышесказанное относится и к «имени_сервера». После ввода получаем следующее:

```
Adding test - 192.168.5.2 - test - PPTP
Added tunnel test
```

И попадаем в главный диалог. Далее неплохо бы выбрать «туннель по умолчанию» (Select a default tunnel). На экран выводится список туннелей и мы выбираем нужный нам туннель. При этом в каталоге `/etc/ppp/peers` появляется символическая ссылка `__default->файл_туннеля`

Скорее всего нам больше ничего не нужно настраивать и мы выбираем «8». Другие, не описанные здесь пункты диалогов, остаются читателю для самостоятельного изучения.

pptp-command вписывает в файл туннеля такие строки.

```
#
# Include the main PPTP configuration file
#
file /etc/ppp/options.pptp
```

Это означает что дополнительные настройки для **pppd** будут читаться из файла `/etc/ppp/options.pptp`. Поэтому вам необходимо самим создать этот файл. За знаниями обращайтесь к **man pppd**. Параметры, указанные в файлах `/etc/ppp/options.pptp` и `/etc/ppp/peers/имя_туннеля` полностью определяют взаимодействие **pppd** с вашим PPTP-сервером. *НЕПРАВИЛЬНЫЕ ИЛИ НЕДОСТАЮЩИЕ ПАРАМЕТРЫ В ЭТИХ ФАЙЛАХ ЯВЛЯЮТСЯ ПРИЧИНОЙ НЕРАБОТОСПОСОБНОСТИ ТУННЕЛЯ В БОЛЬШИНСТВЕ СЛУЧАЕВ.*

Старт туннеля

Есть два способа старта туннеля.

Первый способ (предпочтительный)

Использовать программу **pptp** как псевдотерминал для **pppd**. Это делается указанием параметра

```
pty "/usr/sbin/pptp 192.168.5.2 --nolaunchpppd"
```

в файле настроек для **pppd** (например в `/etc/ppp/options.pptp`), где 192.168.5.2 IP-адрес PPTP сервера. В этом случае туннель нужно стартовать командой

```
# pppd call имя_туннеля
```

Необходимые действия после старта туннеля можно производить из скрипта `/etc/ppp/ip-up.local` Для дальнейшей информации смотрите файл `options-2Com` в каталоге с документацией к пакету `pptp-client` и **man pppd**.

Второй способ (устаревший)

В пакет `pptp-client` входит стартовый скрипт `/etc/init.d/pptptunnel`, который автоматически стартует туннель, указанный в его файле конфигурации `/ect/sysconfig/pptp`. В этом файле можно указать значения двух параметров:

PPTP_TUNNEL

строка с именем туннеля, который нужно стартовать. Если параметр не указан, используется `/etc/ppp/peers/__default`.

PPTP_SET_HOSTNAME

`yes/no`, если `yes`, скрипт будет автоматически устанавливать доменное имя машины, которое соответствует вашему IP-адресу, полученному от сервера. Для этого скрипт использует команду **nslookup you.new.ip.address**.

Кстати, этот скрипт можно использовать не только для запуска туннеля при старте системы, но и для ручного перезапуска туннеля.

Настройка маршрутизации

Для того, чтобы сетевые соединения пошли через туннель в таблице маршрутизации должен быть указан для них маршрут через туннель. Если туннель используется для соединения с Internet, то через туннель нужно направлять все соединения, кроме локальных. Это делается указанием маршрута по умолчанию в таблице маршрутизации. Демон **pppd** может автоматически добавлять маршрут по умолчанию, если ему указан параметр `defaultroute`. Однако, если уже существует другой маршрут по умолчанию, то **pppd** не добавит маршрут через туннель.

Как правило при настройке соединения с локальной сетью указывается маршрутизатор по умолчанию — GATEWAY. Это означает, что при старте локальных сетевых интерфейсов в таблицу маршрутизации будет добавлен маршрут по умолчанию через указанный маршрутизатор. Так как PPTP-туннель стартует позже локальных сетевых интерфейсов, то даже при указанном параметре `defaultroute` **pppd** не установит маршрут по умолчанию через туннель.

Чтобы выйти из данной ситуации, нужно отключить создание маршрута по умолчанию при старте локальных сетевых интерфейсов. Для этого нужно в файле `/etc/sysconfig/network` удалить две строки

```
GATEWAY=xxx.xxx.xxx.xxx
GATEWAYDEV=ethX
```

`xxx.xxx.xxx.xxx` и `ethX` IP-адрес маршрутизатора и имя сетевого интерфейса, соединённого с маршрутизатором. Эти значения зависят от вашей системы.

После удаления этих двух строк и перезапуска сетевых интерфейсов командой **service network restart** маршрута по умолчанию не будет и вашему компьютеру будет доступна локальная сеть, соответствующая заданной сетевой маске.

Однако, часто бывает так, что у вас есть соединения с локальной сетью, состоящей из нескольких подсетей. В этом случае, после указанной выше операции другие подсети не будут доступны, так как к ним не будет указан маршрут (раньше его роль выполнял маршрут по умолчанию). Чтобы получить доступ к локальным подсетям, необходимо указать статический маршрут в эти сети. Статические маршруты указываются в файле `/etc/sysconfig/static-routes` в формате, близком к синтаксису команды **route(8)**. Например,

```
any net 192.168.0.0/16 gw 192.168.5.2
```

данная строка указывает, что должен быть создан маршрут в сеть `192.168.0.0/16` через маршрутизатор `192.168.5.2`. Слово «`any`» в начале строки — обязательное ключевое слово. В качестве маршрутизатора для этого маршрута как правило следует установить IP-адрес, указанный ранее в параметре `GATEWAY` в файле `/etc/sysconfig/network`.

После перезапуска сетевых интерфейсов и старта туннеля команда **route -n** покажет примерно такую картину:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use↩
Iface
172.30.96.1     0.0.0.0         255.255.255.255 UH    0      0        0↩
ppp0
192.168.5.0     0.0.0.0         255.255.255.0   U     0      0        0↩
eth0
192.168.0.0     192.168.5.2     255.255.0.0     UG    0      0        0↩
eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         172.30.96.1     0.0.0.0         UG    0      0        0↩
ppp0
```

Как видим, маршрут по умолчанию указывает на туннель, также присутствует маршрут в локальную сеть `192.168.0.0`, которые добавляется при старте сетевых интерфейсов и на него не влияет старт туннеля.

Решение проблем

При анализе проблем вам поможет указание параметра `debug` в файле настроек **pppd** и чтение логов. Еще загляните в `howto-diagnosis.html` в каталоге с документацией к пакету `pptp-client`.

Глава 9. Настройка почтового сервера Postfix

Возможно, вас удивит то, что сервер передачи электронной почты Postfix рекомендуется к установке в любой конфигурации *ALT Linux*. Это объясняется тем, что в Unix-подобных системах способность отправлять почту с помощью простого вызова команды из командой оболочки практически обязательна. Некоторые программы (например, сервис cron) пользуются этим для отправки сообщений пользователям. Пересылкой всей электронной почты, проходящей через машину, занимается MTA (Mail Transport Agent), в нашем случае это Postfix. Хотя многие почтовые клиенты способны отправлять сообщения на удалённый SMTP-сервер, имеет смысл поручить и эту задачу системному процессу, чтобы достигнуть эффекта «отправил и забыл». Существуют и другие популярные MTA (например qmail, exim), но они по разным причинам не вошли в данную версию дистрибутива. Sendmail, ветеран Интернета, проигрывает Postfix по ряду параметров, в том числе безопасности, к тому же он неоправданно сложен в настройке. В данном руководстве мы ограничимся рекомендациями по настройке Postfix для нескольких типичных конфигураций. Более полные сведения можно получить из превосходной документации на английском языке, которая входит в состав пакета `postfix`.

Пакеты Postfix

Базовый RPM-пакет для установки сервера Postfix в *ALT Linux* носит, как нетрудно догадаться, имя `postfix`. Есть также несколько дополнительных пакетов, предоставляющих сервисы по приёму и доставке сообщений по сети с различной степенью защищённости. Один из пакетов SMTP-серверов, `postfix-smtpd` либо `postfix-smtpd-sasl`, нужен Postfix для того, чтобы принимать сообщения по протоколу SMTP (или ESMTP) как извне, так и локально. Второй из этих пакетов реализует расширения SASL; подробнее об этом см. далее. Есть также пакет `postfix-sasl`, который расширяет возможности доставки сообщений на случай, если какие-либо принимающие серверы, с которыми взаимодействует данный сервер, пользуются авторизацией по методу SASL.

Конфигурационные файлы

Файлы настройки Postfix располагаются в каталоге `/etc/postfix`. Основные параметры определяются в файле `main.cf`; в частности,

параметры, о которых говорится далее в этой главе, устанавливаются в этом файле, если другой не указан специально.

В изначальном виде этот файл содержит конфигурацию, позволяющую серверу работать в пределах машины, а также развёрнутые комментарии с примерами. После редактирования конфигурации при работающем Postfix её нужно активизировать командой **service postfix reload** или просто **postfix reload**.

Доменная информация

Имя хоста и домена, которые считаются локальными при обработке email-адресов, необходимы для функционирования почтового сервера. Если эти имена для Postfix должны быть отличны от того, что выдаёт команда **hostname**, установите их с помощью параметров *myhostname* и *mydomain*.

Postfix на dialup-машине

Существует несколько проблем, возникающих при попытке отправки исходящей почты с машин, которые не являются полноценными узлами интернет, например, в системах с модемным и другими непостоянными соединениями не всегда возможно немедленно отправить сообщения удалённым адресатам по SMTP и их приходится держать в очереди до тех пор, пока соединение не будет установлено. Для этого используется параметр *defer_transports*, например:

```
defer_transports = smtp
```

Доставка активизируется командой **/usr/sbin/sendmail -q**, которая в *ALT Linux* исполняется автоматически при установке PPP-соединения.

Будучи полноценным MTA, Postfix способен находить серверы, обслуживающие получателей сообщений, при помощи DNS. Тем не менее, для dialup-машин непосредственная доставка сообщений нежелательна, поскольку время соединения ограничено. К тому же это излюбленная тактика распространителей спама, поэтому многие серверы сверяют IP-адрес отправителя с базой известных адресов провайдерских пулов, после чего сообщения с таких адресов отвергаются. Поэтому целесообразно доверить доставку исходящей почты SMTP-серверу провайдера. Этим управляет параметр *relayhost*, например:

```
relayhost = [smtp.provider.net]
```

Postfix на клиентской машине локальной сети

Рабочие станции локальной сети или машины в провайдерской сети, отделённой от Интернета с помощью межсетевого экрана/NAT, должны переправлять исходящую почту на почтовый сервер, обслуживающий данную сеть. Для этого также используется параметр *relayhost*, описанный выше. Если сервер задан IP-адресом, можно отключить использование DNS для ускорения работы:

```
disable_dns_lookups = yes
```

Для того, чтобы в доменной части адреса отправителя фигурировал домен сети, а не имя конкретной машины, установите параметр *myorigin* в имя домена:

```
myorigin = $mydomain
```

Если почтовые ящики пользователей монтируются с сервера по NFS, Postfix на клиентских машинах служит лишь для отправки почты. В такой конфигурации следует отключить агенты `local` и `smtp` в файле `/etc/postfix/master.cf`.

Почтовый сервер для небольших доменов и сетей

Домены, для которых сервер получает почту, отличные от значения *mydomain* и не сконфигурированные как виртуальные домены Postfix (см. ниже), нужно перечислить с помощью параметра *mydestination* либо в дополнительном файле, на который ссылается этот параметр. Аналогичным образом параметр *mynetworks* описывает блоки IP-адресов, которые считаются внутренними и с которых разрешён приём исходящих сообщений. Не следует записывать в *mynetworks* блоки адресов, не принадлежащих сети, которую обслуживает сервер, поскольку этим могут воспользоваться распространители спама.

Для SMTP-аутентификации внешних пользователей, желающих отправлять сообщения через данный сервер, можно использовать поддержку авторизации SASL. Пакет `postfix-smtpd-sasl` предоставляет альтернативу `postfix-smtpd` со включенной поддержкой SASL; возможный недостаток этого расширения — включение кода, в меньшей степени проверенного в плане безопасности. Настройка аутентификации SASL описана в файле `SASL_README` в документации Postfix.

Преобразование глобальных адресов в локальные адреса назначения устанавливается с помощью таблиц типа `virtual` (см. virtual(5)):

```
virtual_maps = hash:/etc/postfix/virtual
```

Пример содержимого `/etc/postfix/virtual`:

```
domain1.ru # Домен в стиле Postfix (текст здесь игнорируется)
name1@domain1.ru user1
name2@domain2.ru user2@otherbox
@domain2.ru user3
```

После редактирования оттранслируйте таблицу в рабочий образ командой **postmap /etc/postfix/virtual**.

Если каким-либо пользователям сети почта должна доставляться по SMTP на их рабочие станции (это предполагает, что на их машинах работают MTA), подставляйте в доменной части их адресов имена машин в таблицах `virtual` либо `aliases` (см. ниже).

Алиасы и преобразования адресов

Имена локальных адресатов либо совпадают с именами пользователей системы, либо подставляются из таблицы `aliases` (см. aliases(5)):

```
alias_maps = hash:/etc/postfix/aliases
alias_database = hash:/etc/postfix/aliases
```

При установке Postfix «с нуля» в этой таблице создаётся алиас на имя `root` для доставки всей корреспонденции, предназначенной администратору и поступающей на другие системные адреса, на имя реального пользователя, который осуществляет функции администратора. Изначально им становится первый зарегистрированный в системе реальный пользователь. Таблица алиасов отличается от остальных таблиц, используемых Postfix; имена слева, которые являются ключами для поиска, отделяются от значений справа двоеточиями. Адресаты справа перечисляются через запятую и могут быть адресами, командами (обозначаются символом | в начале правой части; сообщение подаётся на стандартный поток ввода команды) и именами файлов:

```
John.Smith: john
chief: chief@bosscomputer
trio: stock, hausen, walkman
```

```
robot: | /usr/bin/robot --process-mail
filebox: /dir/file
```

Рабочий образ таблицы строится с помощью команд **postalias /etc/postfix/aliases** или **newaliases**. При отправке сообщения Postfix генерирует адрес отправителя из имени пользователя и собственного домена (или значения *myorigin*). Даже если почтовый клиент выставил заголовок `From:`, этот адрес попадает в служебную информацию сообщения и может быть использован получателем, что не всегда желательно. Преобразование адресов отправителей к глобальным адресам можно задать в таблице типа `canonical` (см. canonical(5)):

```
sender_canonical_maps = hash:/etc/postfix/sender_canonical
```

Аналогичная таблица `recipient_canonical` и соответствующий параметр *recipient_canonical_maps* могут быть использована для преобразования адресов назначения. Для актуализации изменений таблиц используйте команду **postmap** *имя_таблицы*.

Борьба со спамом и почтовыми вредителями

Противодействие спаму (массовым рассылкам непрошенной корреспонденции) — отдельная большая тема, которую невозможно полностью раскрыть в этом руководстве; здесь даны лишь несколько практических советов применительно к конфигурации Postfix. По умолчанию сервер сконфигурирован так, что отвергает попытки переслать сообщения извне на другие удалённые серверы. Со спамом, адресованным локальным получателям, дело обстоит сложнее. Хорошо зарекомендовали себя служба *MAPS RBL* и ей подобные, организованные по принципу «чёрного списка» IP-адресов; чтобы задействовать эти сервисы, предварительно ознакомившись с условиями их использования, занесите имена доменов, работающих по принципу RBL, в конфигурацию:

```
smtpd_client_restrictions = permit_mynetworks, reject_maps_rbl
maps_rbl_domains = relays.ordb.org, blackholes.mail-abuse.org
```

В некоторых случаях требуется адресная работа с отдельными нарушителями почтового этикета. Адресная работа заключается в блокировании SMTP-соединений с их адресов, сетей либо доменов. Для этого предусмотрены таблицы типа `access` (см. access(5)):

```
    smtpd_client_restrictions = permit_mynetworks,↩
hash:/etc/postfix/access
```

Пример таблицы:

```
1.2.3.4 550 No more canned meat, please
1.2.5 REJECT
goodguy.generallybad.com OK
.generallybad.com REJECT
```

Как и с другими таблицами, после редактирования приведите кары в действие командой **postmap /etc/postfix/access**.

Прочие настройки

По умолчанию размер файла почтового ящика при локальной доставке ограничен `51200000` байтами. Это ограничение можно изменить с помощью параметра *`mailbox_size_limit`*. Установка параметра в `0` снимает ограничение.

Использование Postfix

После того, как Postfix настроен и запущен как сервис с предсказуемым именем **postfix**, в настройках почтовых клиентов можно указывать имя или адрес машины (например, `localhost`) как SMTP-сервер. Программа **fetchmail** работает в связке с Postfix, опрашивая внешние почтовые ящики пользователей по протоколам POP3 или IMAP и передавая полученные сообщения системному MTA для локальной доставки. Лог-файлы Postfix находятся в каталоге `/var/log/mail`.

Глава 10. Объединённая служба каталога (LDAP).

Что такое служба каталога и что такое LDAP?

Служба каталога (*Directory Service*) — это программный комплекс для хранения и каталогизации информации. По своей сути это очень похоже на обычную базу данных, но с «уклоном» скорее на чтение данных, нежели на их добавление или модификацию. Обычно служба каталога базируется на клиент-серверной архитектуре. Одна из наиболее известных таких систем — это DNS (*Domain Name Service*): DNS-сервер производит взаимную «трансляцию» имён машин и их IP-адресов. Другие машины в сети могут обращаться к такому серверу за информацией о соответствии имени и адреса. Однако это очень простой пример каталогизации информации. Объекты в такой базе имеют ограниченное количество атрибутов — таких как имя, адрес и ещё несколько дополнительных параметров. Разумеется, служба каталога какого-нибудь предприятия будет содержать более разнообразные данные и иметь гораздо более сложную структуру.

В общем случае, служба каталога должна предоставлять простой, централизованный доступ к данным, которые могут использоваться различными приложениями. Протокол, по которому могла бы работать такая служба, был разработан в ISO (*International Standartization Organization*), получил номер *X.500* и назывался DAP (*Directory Access Protocol*). В соответствии с этим протоколом любое приложение может получить доступ к информации в каталоге. Там же была предложена гибкая и легко расширяемая информационная структура которая позволяла хранить в принципе любой тип данных. К сожалению, X.500 имел и ряд ограничений, таких как зависимость от коммуникационного уровня, который не являлся стандартным протоколом TCP и запутанность требований к правилам именования объектов. В результате решение на базе этого протокола становилось очень дорогим при обслуживании.

Позже появился протокол LDAP (*Lightweight Directory Access Protocol*), который позволил реализовать доступ по TCP/IP и мог легко расширяться. В результате появилось решение, позволяющее организовать службу каталога на предприятии любого масштаба.

Сегодня существует несколько реализаций данного протокола от различных фирм. Наиболее известные из них — это Netscape Directory Service™, Microsoft Active Directory™, Novell Directory Service™. Из некоммерческих реализаций LDAP наибольшее распространение получил проект *OpenLDAP*. Именно его мы и будем рассматривать в данной главе, хотя большинство понятий и определений применимо и к другим реализациям сервера LDAP.

Основные термины

Для понимания работы службы каталога необходимо усвоить несколько ключевых терминов.

- Данные каталога хранятся в виде объектов или сущностей (от англ. *entry*), состоящих из специальных полей называемых *атрибутами* (*attributes*). Набор атрибутов, их синтаксис и правила поиска определяются *схемой каталога* (*scheme*). Все объекты каталога идентифицируются специальным атрибутом — DN (*Distinguished Name*).
- Данные в каталоге можно представить в виде древовидной структуры — DIT (*Directory Information Tree*). Это очень похоже на структуру, используемую многими файловыми системами. Вершиной такого дерева является *корневой объект* (*Root Entry*). DN корневого объекта одновременно является *суффиксом каталога*.
- Каждый последующий объект в структуре каталога идентифицируется уникальным значением DN который описывает путь к объекту в каталоге. Если продолжить аналогию с файловой системой то DN любого объекта так же включает DN всех объектов стоящих выше по иерархии. Отличие в данном случае только в том, что DN формируется не слева направо, как путь к файлу, а наоборот — справа налево.
- *DN администратора каталога* (*Root Distinguished Name*) — это специальный объект, описывающий администратора каталога. Этот объект указывается в конфигурации сервера, но может отсутствовать в самом каталоге. К такому объекту не применяются списки доступа (*ACL*). В некоторых реализациях LDAP такой объект может не иметь суффикса.
- *База поиска* (*Base Distinguished Name*) — объект каталога, начиная с которого производится поиск. Дело в том, что не всегда есть необходимость производить поиск по всему дереву каталога; ограничить область поиска можно указанием в запросе базы поиска. По умолчанию этот параметр соответствует суффиксу.

Объекты и атрибуты

Серверы LDAP могут поставляться с несколькими вариантами *бэкенда* (*backend*). Например, *OpenLDAP* имеет такие варианты, как `LDBM` — собственный формат хранения данных в текстовых файлах; `SHELL` — интерфейс к базе данных, использующий команды `UNIX`; `PASSWD` — простейшая база, использующая стандартные файлы `/etc/passwd` и `/etc/group`; `SQL` — интерфейс к любой базе данных, использующей SQL.

Для процедур импорта и экспорта данных всеми серверами LDAP поддерживается единый формат обмена данными — LDIF. Вот пример такого файла с описанием двух объектов:

```
dn: dc=example,dc=com
objectClass: top
objectClass: organization
o: example.com
o: Example Inc.

dn: ou=People,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People
description: Example Inc. workers
description: Stuff area
```

Описание каждого объекта в таком файле начинается с атрибута DN. Специальный атрибут `objectClass` указывает, к каким классам относится данный объект и, следовательно, какие атрибуты он может иметь. В нашем случае принадлежность к классу top означает, что объект обязательно должен иметь атрибут `objectClass`, а принадлежность к классу `organization` предполагает наличие нескольких атрибутов, из которых атрибут `o` является обязательным.

Второй объект находится на одну ступеньку ниже по иерархии и поэтому в его DN включён DN объекта верхнего уровня. Этот объект относится к классу `organizationalUnit` и поэтому имеет обязательный атрибут `ou`.

Можно заметить что некоторые атрибуты (для которых это применимо) могут иметь несколько значений. В данном примере атрибут `description` имеет два значения. А вот для атрибута `dn` допустимо только одно значение.

Классы, характеризующие объекты, и атрибуты, составляющие классы, описываются схемой базы. Её пример приведён ниже.

```
attributetype ( 2.5.4.10 NAME ( 'o' 'organizationName' )
  SUP name
)
attributetype ( 2.5.4.13 NAME 'description'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024}
)
objectclass ( 2.5.6.4 NAME 'organization' SUP top STRUCTURAL
  MUST o
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
    x121Address $ registeredAddress $ destinationIndicator $
    preferredDeliveryMethod $ telexNumber $
teletexTerminalIdentifier $
    telephoneNumber $ internationaliSDNNumber $
    facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
    postalAddress $ physicalDeliveryOfficeName $ st $ l $ description
  )
)
```

В данном фрагменте приводятся описания двух атрибутов и одного класса. Вот что означают эти записи:

- Атрибут `o` (его можно также называть `organizationName`) является расширением атрибута `name`.
- Атрибут `description` — это строка длиной до 1024 байт; при поиске в ней регистр символов не учитывается.
- Класс `organization` является расширением класса `top` и имеет единственный обязательный атрибут `o`. Кроме того имеется большое количество необязательных атрибутов таких как `userPassword`, `businessAddress`, `street`, `postOfficeBox` и т.д.

Много полезной информации о схемах можно найти по ссылкам на *сайте OpenLDAP*[27].

Установка и настройка

Процесс сборки и установки сервера *OpenLDAP* не отличается от сборки и установки другого программного обеспечения, поставляемого

[27] `http://www.openldap.org`

с исходными кодами. Кроме того, практически во всех современных дистрибутивах *Linux* он поставляется в виде готового пакета. Поэтому уделим больше внимания настройке.

Настройка сервера

Сервер LDAP состоит из двух серверных процессов **slapd** и **slurpd**. Процесс **slapd** занимается приёмом и обработкой запросов от клиентов; это основной процесс, который непосредственно работает с базой данных. Сервис **slurpd** используется в тех случаях, когда данные нужно реплицировать на другие сервера — он контролирует изменения в базе и при необходимости пересылает их на подчинённые сервера.

Приведём пример конфигурационного файла:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/nis.schema
```

В первых строках мы подключаем необходимые схемы; в поставке *OpenLDAP* их около полутора десятков. Подключите только те, которые будете использовать. В принципе, схемы являются частью конфигурационного файла, но для наглядности они вынесены в отдельные фрагменты.

```
database ldbm
```

В качестве способа хранения используется собственный формат LDBM. Если предполагается обычная конфигурация сервера, то данный формат предпочтителен.

```
suffix "dc=example,dc=com"
```

Корнем информационной структуры будет являться объект `dc=example,dc=com`. В принципе, суффикс для каталога можно взять любой, например, `o=Example Inc.,c=RU` — это не накладывает абсолютно никаких ограничений на функциональность. Однако последнее время все чаще используется именно первый вид суффикса, который подчёркивает, что информационная структура данного предприятия тесно связана со структурой его домена.

```
rootdn "cn=admin,dc=altlinux,dc=ru"
rootpw secret
```

DN, описывающий администратора и его пароль. В данном случае пароль записан в открытом виде, поэтому файл конфигурации сервера должен иметь соответствующие права доступа, ограничивающие его чтение обычными пользователями. Пароль можно записать и в виде хэша DES или MD5 — тогда строка будет иметь следующий вид:

```
rootpw {MD5}IFJFxyGN3Hap7xsJFBmeTA==
index objectClass eq
```

Формат ldbm поддерживает простейшие индексы с целью ускорения операций поиска. Желательно создать такие индексы по тем атрибутам, по которым предполагается наибольшее количество запросов.

```
access to attr=userPassword
  by self write
  by anonymous auth
  by * none

access to * by * read
```

Не всегда данные каталога находятся в публичном доступе. Для управления доступам могут использоваться *списки доступа* (*access lists*). В данном примере приводятся два списка — в первом из них ограничивается доступ к атрибуту `userPassword` (полный доступ к нему могут иметь только сам объект либо администратор базы; для всех остальных доступ запрещён). Второе правило гласит, что всем даётся доступ на чтение любых данных (кроме ограниченного предыдущим правилом).

```
TLSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCertificateFile /etc/openldap/ssl/slapd.pem
TLSCertificateKeyFile /etc/openldap/ssl/slapd.pem
```

LDAP можно использовать для централизованной авторизации пользователей сети вместо NIS+. В таких случаях из каталога может запрашиваться конфиденциальная информация, например, пароль. Для предотвращения перехвата этих данных желательно использовать протокол LDAPS (LDAP via SSL/TLS).

После настройки можно сразу запустить процесс **slapd** — например, такой командой:

slapd -u ldap -h ldap://127.0.0.1/ ldaps://ldap.altlinux.ru/

или, если вы используете пакет из дистрибутивов *ALT Linux*[28]

service ldap start

Первый объект, которые нужно создать в базе — это *корневой элемент* (*root entry*) который указан в конфигурационном файле как `suffix`.

Настройка репликации

Одной из важных особенностей LDAP являются встроенные средства репликации данных. Этот механизм реализован в виде отдельного серверного процесса, контролирующего изменения в базе данных и пересылающего эти изменения на другие сервера. Прежде чем включать такую репликацию, необходимо убедиться, что соответствующие данные на обоих серверах идентичны. Это связано с тем, что **slurpd** пересылает именно изменения на текущем сервере — он не проверяет и не анализирует состояние данных на удалённом сервере. Настройки **slurpd** находятся в том же файле, что и настройки **slapd** — поэтому перечислим, что нужно добавить к перечисленным выше параметрам:

```
replica /var/log/slapd.replog
```

Прежде всего укажем файл, в который **slapd** будет записывать все свои действия и из которого **slurpd** будет их читать.

```
replica host=ldap2.example.com
  tls=yes
  bindmethod=simple
  binddn="cn=slurpd,ou=lug,dc=example,dc=com"
  credentials=secret
```

[28] `http://www.altlinux.ru`

Для каждого подчинённого сервера описывается такая вот реплика. На подчинённом сервере нужно создать соответствующий объект и указать, что он имеет права на изменение информации. Это делается с помощью соответствующего списка доступа и параметров `updatedn` и `updateref`.

Настройка клиента

Существует огромное количество клиентов, работающих с LDAP. Это могут быть почтовые программы, которые обращаются к каталогу в поисках адреса электронной почты сотрудника или за информацией о маршрутизации почты, FTP-сервер, который берет информацию для авторизации своего клиента и многие другие программы — однако все они имеют схожие настройки. Прежде всего это адрес сервера и порт, на котором работает LDAP (обычно это 389 либо 636, если сервер поддерживает протокол LDAPS). Вторым важным параметром является база поиска (*Base DN*) — в большинстве случаев этот параметр соответствует суффиксу сервера. Третий важный параметр — фильтр поиска. Кроме того, существуют параметры, позволяющие ограничить поиск снизу — например, только самой базой или базой и её под-объектами первого уровня, параметры управляющие поиском в алиасах (*alias*) и т.п.

Трёх этих параметров в большинстве случаев достаточно, чтобы выполнить запрос к любому серверу LDAP. Однако если на сервере существуют ограничения на доступ к данным, то может потребоваться авторизация. Авторизоваться в LDAP можно, указав DN одного из объектов базы данных LDAP; пароль для такого объекта будет искаться в его атрибуте `userPassword`.

Ниже приводится фрагмент настройки почтового сервера Postfix:

```
virtual_maps = ldap:virtual, hash:/etc/postfix/virtual

virtual_server_host = localhost
virtual_search_base = ou=People,dc=example,dc=ru
virtual_query_filter =↩
(&(objectclass=inetLocalMailRecipient)(cn=%s))
virtual_result_attribute = mailLocalAddress,mailRoutingAddress
```

В данном фрагменте описывается, что при определении адреса получателя делается запрос в LDAP с целью найти объект которому это

письмо адресовано. Поиск делается по атрибуту `cn`. Результат берётся из атрибутов `mailLocalAddress` и `mailRoutingAddress`. Эти классы и атрибуты описаны схемой misc.

Использование LDAP

LDAP может использоваться в самых различных ситуациях. Здесь мы рассмотрим несколько наиболее распространённых его применений. Поскольку в LDAP хранится полная информация о сотрудниках предприятия, мы можем брать справочную информацию для почтовых программ прямо оттуда. Для начала настроим сервер:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/misc.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/openldap.schema

pidfile       /var/run/slapd.pid
argsfile      /var/run/slapd.args

directory     /var/lib/ldap/base
database      ldbm
index         objectClass,uid,uidNumber,gidNumber eq
index         cn,name,surName,givenName eq,subinitial
password-hash  {MD5}

suffix        "dc=example,dc=com"
rootdn        "cn=admin,dc=example,dc=com"
rootpw        {md5}$1$ION4SIII$EYyGEeYt4g2hEe9tjICac.

access to attr=userPassword
  by self write
  by dn=".*,ou=Admins,dc=example,dc=com"
  by anonymous auth
  by * none
access to * by * read

loglevel 512

index objectClass,uid,uidNumber,gidNumber    eq
index cn,mail,surname,givenname            eq,subinitial
```

После этого создадим пользователя `ldap`, от имени которого будет работать наш сервер и запустим процесс **slapd** следующей командой:
slapd -u ldap -h 'ldap://127.0.0.1/ ldap//ldap.altlinux.ru/ ldaps://ldap.altlinux.ru'
Теперь можно создать базу данных — например, с помощью утилиты ldapadd:
ldapadd -xWD cn=admin,dc=altlinux,dc=ru -H ldaps://ldap.altlinux.ru -f initial.ldif
Содержимое файла initial.ldif будет такое:

```
dn: dc=example,dc=com
objectClass: top
objectClass: organization
o: Exapmle Inc.
o: exapmle.com

dn: cn=admin,dc=exapmle,dc=com
objectClass: top
objectClass: organizationalRole
cn: admin
description: Example Inc. LDAP manager

dn: ou=People,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People
description: Stuff area

dn: uid=obender,ou=People,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
cn: Ostap Bender
sn: Bender
givenName: Ostap
uid: obender
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/obender
loginShell: /bin/bash
userPassword: {md5}$1$ION4SIII$EYyGEeYt4g2hEe9tjICac.
mail: obender@example.com
```

```
mail: obender@attiresandtoes.com

....

dn: ou=Group,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Group
description: Groups of users

dn: cn=luser,ou=Group,dc=example,dc=com
objectClass: top
objectClass: posixGroup
cn: luser
gidNumber: 1000
description: Default group for users presented by LDAP
```

Проверим, что сервер работает сделав к нему анонимный запрос:

```
$ ldapsearch -xLLL "(uid=obender)"
dn: uid=obender,ou=People,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
cn: Ostap Bender
sn: Bender
givenName: Ostap
uid: migor
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/obender
loginShell: /bin/bash
mail: obender@example.com
mail: obender@attiresandtoes.com
```

Поскольку, согласно нашим настройкам, доступ к атрибуту `userPassword` имеют только сам пользователь и администратор, то этот атрибут мы не получили. Собственно, он нам и не нужен.

Адресная книга

На сегодняшний день почти все популярные почтовые программы поддерживают возможность использовать LDAP как адресную книгу.

В качестве примера возьмём пакет *Mozilla*; установите пакеты `libldap`, `mozilla`, `mozilla-mail` и запустите программу. Далее:

- откройте окно настройки («Edit»→«Preferences...»);
- выберите слева категорию «Mail & Newsgroups», подкатегорию «Addressing»;
- справа в опциях «Address Autocompletion» включите «Directory Server» и нажмите кнопку Edit Directories...;
- в новом окне нажмите кнопку Add и на вкладке «General» заполните поля «Name:» `ExampleLDAP`, «Hostname:»`ldap.example.com` и «BaseDN:»`dc=example,dc=com`;
- при желании на вкладке «Advanced» можно указать ограничение на количество возвращаемых записей (по умолчанию это 100) и фильтр поиска.

После этого сохраните изменения — и теперь при заполнении поля «To:» можно писать не адрес, а имя получателя из атрибута `cn`. Программа произведёт соответствующий поиск и предложит варианты атрибута `mail`, которые найдёт в базе.

Для настройки другого пакета обратитесь к руководству пользователя вашей программы.

Маршрутизация почты в Postfix.

Предположим, что наше предприятие не имеет своего POP3/IMAP-сервера либо для некоторых сотрудников удобнее получать почту через другой сервер. Для этого нам необходимо принять почту пользователя, приходящую в наш домен, и переправить её на тот адрес который для сотрудника удобнее. Решений для этой задачи существует несколько: в простейшем варианте можно создать в домашнем каталоге пользователя файл `.forward`, в котором он сам мог бы указать нужный ему адрес. Однако усложним задание — предположим, что на нашем почтовом сервере нет учётной записи для данного пользователя; тогда получается, что этот файл некуда поместить. Второй вариант — настроить пересылку на самом сервере; для этого создается файл `/etc/postfix/virtual` приблизительного такого вида:

```
obender@example.com obender@attiresandtoes.com
```

а в конфигурационном файле Postfix указывается

```
virtual_maps = hash:/etc/postfix/virtual
```

Теперь остаётся только создать хэш и перезапустить Postfix; однако, если мы имеем много таких пользователей и если почтовых серверов существует несколько, то отслеживать синхронное изменение файлов `/etc/postfix/virtual` становится нелёгкой задачей.

Немного модифицируем наше последнее решение. Перенесём данные из файла `/etc/postfix/virtual` в LDAP; для этого модифицируем приведённую выше базу следующим образом: добавим пользователю класс `inetLocalMailRecipient` и новый атрибут `mailRoutingAddress`.

```
$ ldapmodify -WD cn=admin,dc=example,dc=com
dn: uid=obender,ou=People,dc=example,dc=com
changetype: modify
objectClass: inetLocalMailRecipient
mailRoutingAddress: obender@attiresandtoes.com
```

После этого изменим настройки Postfix:

```
virtual_maps = ldap:virtual
virtual_server_host = ldap.example.com
virtual_search_base = ou=People,dc=example,dc=com
virtual_query_filter =
(&(mail=%s)(objectClass=inetLocalMailRecipient))
virtual_result_attribute = mailRoutingAddress
```

Теперь почта для данного пользователя будет пересылаться на адрес из атрибута `mailRoutingAddress`, тем не менее в адресной книге все останется без изменений и там будет показываться «официальный» адрес пользователя из атрибута `mail`.

Централизованная авторизация.

Разобравшись с почтой, хочется перенести в LDAP и авторизацию. Обычно для этих целей используют NIS+, однако хочется использовать для этого более совершенную технологию — в конце концов, у нас уже есть сервер LDAP, содержащий все необходимые данные по нашим пользователям. Для того, чтобы система искала своих пользователей не только в файле `/etc/passwd`, необходимо установить пакеты `nss_ldap` и `pam_ldap`. Оба пакета имеют общий конфигурационный

файл `/etc/ldap.conf` (в других дистрибутивах это могут быть другие файлы, но синтаксис у них одинаковый).

```
uri ldaps://ldap.example.com
ldap_version 3
base dc=example,dc=com
timelimit 15
ssl on
```

Подправим файл `/etc/nsswitch.conf`:

```
passwd: files ldap
shadow: tcb ldap
group: files ldap
```

Теперь проверяем, подключены ли пользователи из базы:

```
$ id obender
uid=1000(obender) gid=1000 groups=1000
```

Обратите внимание на то, что сейчас мы обращаемся к серверу по защищённому протоколу LDAPS. Поскольку теперь мы берём из базы крайне важную информацию — пароль пользователя, дополнительная степень защиты будет весьма кстати.

Приложения

Ссылки

Список ссылок на информационные ресурсы Internet, посвящённых LDAP:

- *University of Michigan LDAP Page*[29]
- *University of Michigan LDAP Documentation Page*[30]
- *OpenLDAP Administrator's Guide*[31]
- *Manually Implementing Roaming Access*[32]
- *Customizing LDAP Settings for Communicator 4.5*[33]

29
30
31
32
33

- *Introducing to Directory Service (X.500)*[34]
- *Linux Directory Service*[35]

RFC

Список RFC, поддерживающих LDAP:

- RFC 1558: A String Representation of LDAP Search Filters
- RFC 1777: Lightweight Directory Access Protocol
- RFC 1778: The String Representation of Standard Attribute Syntaxes
- RFC 1779: A String Representation of Distinguished Names
- RFC 1781: Using the OSI Directory to Achieve User Friendly Naming
- RFC 1798: Connectionless LDAP
- RFC 1823: The LDAP Application Programming Interface
- RFC 1959: An LDAP URL Format
- RFC 1960: A String Representation of LDAP Search Filters
- RFC 2251: Lightweight Directory Access Protocol (v3)
- RFC 2307: LDAP as a Network Information Service

[34]
[35]

Глава 11. Служба FTP

Протокол FTP (file transfer protocol, протокол передачи файлов) широко используется для обмена файлами в Интернете и локальных сетях. Это — специализированный протокол, который предназначен только для передачи файлов и хорошо приспособлен для выполнения этой задачи. К сожалению, изначально протокол спроектирован таким образом, что пароли, данные и управляющие команды передаются открытым текстом, и их можно легко перехватить. Однако это не является проблемой при работе с многочисленными серверами, которые предоставляют только анонимный доступ.

В этом документе изложены рекомендации, которые помогут вам правильно настроить FTP-сервер и свести к минимуму риски атак на вашу систему через этот вид сервиса.

FTP-сервер vsftpd

В состав дистрибутива *ALT Linux Master 2.2* входит `vsftpd` (Very Secure FTP Daemon) — полнофункциональный FTP-сервер, позволяющий обслуживать как анонимные запросы, так и запросы от пользователей, зарегистрированных на сервере и имеющих полноценный доступ к его ресурсам. Именно `vsftpd` рекомендован разработчиками дистрибутива для использования в качестве FTP-сервера.

Разумеется, слова «very secure» (очень защищённый) в названии сервера не являются гарантией полной безопасности, однако указывают на приоритеты его разработчиков. Они стремились создать как можно более надёжную, аккуратно спроектированную и написанную программу, максимально устойчивую к разного рода атакам. Каждая строка кода неоднократно подвергалась тщательным проверкам со стороны специалистов по безопасности информационных систем.

Однако преимущества `vsftpd`, которым он обязан своей популярностью, не ограничиваются его надёжностью и защищённостью. Это производительный, хорошо масштабируемый FTP-сервер. Демонстрацией его возможностей может служить серверный пул *ftp.redhat.com*[36], обрабатывающий до `15000` соединений одновременно.

Наконец, важным достоинством сервера являются простота и гибкость настройки. Все необходимые настройки осуществляются посредством редактирования единственного конфигурационного файла `/etc/vsftpd.conf`, который фактически является символической ссылкой на файл `/etc/vsftpd/conf`.

[36] `ftp://ftp.redhat.com`

Организация анонимного доступа на основе vsftpd

Если вам необходимо создать анонимный FTP-сервер, вы можете использовать `vsftpd` в сочетании с пакетом `anonftp`. Установки этих двух пакетов достаточно для того, чтобы получить работоспособный сервер. В целях безопасности сервер по умолчанию сконфигурирован именно для предоставления анонимного доступа. Запрещены любые команды записи, а также доступ локально зарегистрированных пользователей.

Для обеспечения надёжности системы архитектура сервера `vsftpd` позволяет устанавливать соединения от имени специально указанного непривилегированного пользователя, который определяется директивой `nopriv_user` в конфигурационном файле. Для того, чтобы риск был минимальным, этот пользователь должен обладать как можно меньшими привилегиями. С этой целью при установке `vsftpd` в системе автоматически создается учётная запись псевдопользователя `novsftpd`. Это регистрационное имя не должно использоваться кемлибо для входа в систему, поэтому реальный пароль для него не задаётся. Вместо командного интерпретатора указывается `/dev/null`.

При установке пакета `anonftp` автоматически создается каталог, который будет корневым при анонимном подключении, — `/var/ftp` с необходимыми правами доступа. Владельцем этого каталога является пользователь `root`, а не псевдопользователь, от имени которого работает `vsftpd`. Это сделано для обеспечения безопасности FTP-сервера и системы в целом. Группой-владельцем каталога является специальная группа `ftpadmin`, предназначенная для администраторов FTP-сервера.

Если вы хотите создать в области для анонимного доступа дерево каталогов, начните с каталога `/var/ftp/pub`. Этот каталог традиционно используется для размещения общедоступных файлов. Для него следует установить права доступа `2775`. При этом анонимным пользователям FTP-сервера будет предоставлен доступ на чтение к файлам, находящимся в каталоге. Владельцем каталога сделайте `root`. В качестве группы, которой принадлежит `/var/ftp/pub`, целесообразно назначить `ftpadmin`, включив в неё пользователей, которым необходимо изменять содержимое каталогов FTP-сервера (не стоит работать с содержимым от имени `root`).

Чтобы разрешить анонимным пользователям вашего сервера доступ на запись, создайте каталог `/var/ftp/incoming` с правами доступа `3773` (владелец — `ftpadmin`, группа-владелец — `ftpadmin`), тем самым предоставив анонимным пользователям право записи в этот каталог, но лишив их возможности просмотра его содержимого. О том, какие изме-

нения в конфигурации сервера должны быть сделаны для того, чтобы разрешить запись, рассказано ниже в этой главе.

> **Замечание**
>
> Наличие каталога, открытого для анонимной записи по протоколу FTP, делает возможным злонамеренное или случайное переполнение диска данными, что может привести к нарушению работы системы в целом. Для предотвращения подобных атак и недоразумений старайтесь размещать каталог, открытый для записи, на отдельном разделе файловой системы.

Доступ к серверу зарегистрированных пользователей

Чтобы предоставить доступ к FTP-серверу для локально зарегистрированных пользователей, необходимо внести изменения в конфигурационный файл `/etc/vsftpd.conf`. Для этого достаточно удалить знак комментария перед директивой `local_enable=YES`. В такой конфигурации клиенты FTP-сервера получат доступ к любым каталогам файловой системы, для которых такой доступ разрешён исходя из прав соответствующих локальных пользователей. Это могут быть как домашние каталоги пользователей, так и системные каталоги. Если в настройках `vsftpd` разрешена запись (см. ниже), клиенты получат и все права на запись, которыми располагают эти пользователи.

Сервер `vsftpd` позволяет ограничить возможность пользователей, зарегистрированных локально, перемещаться по дереву каталогов. При этом процесс, работающий с клиентом, будет выполняться в изолированной среде (chrooted environment), и пользователь будет иметь доступ лишь к своему домашнему каталогу и его подкаталогам. Чтобы ограничить таким образом доступ к каталогам для отдельных пользователей, удалите знаки комментариев у следующих строк в конфигурационном файле:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

В файле `/etc/vsftpd/chroot_list` перечислите регистрационные имена пользователей, для которых должна использоваться изолированная среда выполнения. Вы можете использовать для этого и другой файл, указав его имя в строке `chroot_list_file` конфигурационного файла.

Чтобы ограничить доступ к дереву каталогов для всех пользователей, зарегистрированных локально, добавьте в конфигурационный файл директиву `chroot_local_user=YES`.

В этом случае имена пользователей, перечисленные в файле `/etc/vsftpd/chroot_list` (при условии, что у строк, указанных выше, удалены знаки комментария), имеют противоположное действие. Для них не используется изолированная среда выполнения, и перемещение по файловой иерархии не ограничивается домашним каталогом.

Чтобы запретить анонимный доступ к FTP-серверу, поставьте знак комментария в начале строки `anonymous_enable=YES` в конфигурационном файле.

Дополнительные сведения о настройке сервера

Сервер `vsftpd` способен осуществлять всю передачу данных в пассивном режиме, что сопряжено со значительно меньшим риском, однако не всегда удобно. Чтобы разрешить использование только пассивного режима, достаточно удалить символ комментария у директивы `port_enable=NO` в конфигурационном файле.

Чтобы разрешить запись файлов на сервер, удалите знак комментария у директивы `write_enable=YES`. Этого достаточно для того, чтобы пользователи, зарегистрированные локально, получили возможность загружать файлы в те каталоги, для которых они располагают правами на запись. Чтобы разрешить запись файлов анонимным пользователям, необходимо, кроме этого, удалить знак комментария у строки `anon_upload_enable=YES`. Кроме того, специальный непривилегированный пользователь, используемый для работы с анонимными клиентами, должен иметь права на запись в один или несколько каталогов, доступных таким клиентам.

Для получения дополнительной информации о настройке FTP-сервера `vsftpd` и параметрах конфигурационного файла обратитесь к странице руководства

vsftpd.conf

.

Многие параметры использования `vsftpd`, в том числе относящиеся к безопасности, могут быть заданы при помощи `xinetd` (демона Интернет-служб). В частности, этот сервер позволяет ограничить количество одновременно выполняемых процессов как по системе в целом, так и для каждого отдельного пользователя, указать пользователя, от имени которого будет выполняться служба, задать приоритет

процесса (nice), указать адреса, с которых разрешено подключение к данной службе, а также время доступа и множество других параметров. Вот пример файла конфигурации `xinetd` для `vsftpd`:

```
# default: off
    # description: The vsftpd FTP server.
    service ftp
    {
        disable = no # включает службу
        socket_type = stream
        protocol = tcp
        wait = no
        user = root
        nice = 10
        rlimit_as = 16M # устанавливает лимит адресного ↩
пространства
        server = /usr/sbin/vsftpd # путь к исполняемому ↩
файлу
        only_from = 192.168.0.0 # предоставляем доступ из ↩
всей подсети 192.168.0
        only_from = 207.46.197.100, 207.46.197.101 # ↩
доступ с указанных адресов
    #     only_from = 0.0.0.0 # неограниченный по адресам ↩
доступ
        access_times = 2:00-9:00 12:00-24:00 # время, ↩
когда возможен доступ
    }
```

Для получения дополнительной информации по использованию `xinetd` обратитесь к страницам руководства `xinetd` и `xinetd.conf`.

Глава 12. Samba

Аннотация

Данный раздел документации предназначен прежде всего для тех, кто только начинает знакомиться с Samba, но между тем уже имеет достаточные знания в области TCP/IP и сетей Microsoft™.

Все, что сказано ниже, относится непосредственно к пакету `samba-2.2.5`, входящему в состав ALTLinux Master; тем не менее, многое будет справедливо как для предыдущих, так и для последующих версий.

Общие сведения о Samba

Данный продукт представляет собой комплект серверного и клиентского программного обеспечения для осуществления связи UNIX-машин с сетями Microsoft™ и LanManager, которые сами по себе представляют собой подклассы[37] сетей SMB.

Исходно сети SMB были разработаны фирмой IBM™, базировались на протоколе NetBIOS, предназначались прежде всего для сетей Token Ring и были в полной мере реализованы в OS/2 Warp LanServer. Позднее в Windows 95 этот протокол был заменён на NetBEUI (несколько упрощённая версия NetBIOS).

Чуть ранее в OS/2 Warp и NT 3.5 была реализована более удобная для сложных гетерогенных сетей реализация, работающая поверх TCP/IP — «NetBIOS over TCP/IP». Ввиду явных преимуществ данного подхода он используется и поныне. Когда где-либо в Windows вы организовываете работу с сетевыми разделяемыми ресурсами по TCP/IP, то на самом деле используется «NetBIOS over TCP/IP» (о чем, например, в Win95 в свойствах TCP/IP в закладке NetBIOS есть соответствующая отметка).

Samba также использует протокол «NetBIOS over TCP/IP», что позволяет ей успешно взаимодействовать с такими реализациями SMB, как входящие в OS/2 3-4, Windows 9X-ME, NT3.5-4/2000/XP, UNIX-системами с Samba и, возможно, другими подобными. Менее очевидно то, что Samba не может работать без использования TCP/IP (на NetBIOS и NetBEUI). Об этом не стоит забывать при проектировании сетей.

Итак, для работы в сетях SMB необходимы:

- клиент;

[37] На самом деле Microsoft™ существенно расширила исходную спецификацию SMB.

- сервер;
- средства администрирования.

Все это есть в пакетах `samba-client`, `samba-client-cups`, `samba-common`, `samba`, `samba-swat`, входящих в состав дистрибутива.

При использовании SMB доступны следующие ресурсы:

- сетевые диски;
- прямые пути к дискам;
- принтеры;
- доменная авторизация и управление.

Первые три пункта поддерживаются Samba в полном объёме, последний — частично, но это направление стремительно развивается и весьма полно реализовано в Samba 3.0, описанной ниже.

Также доступен весьма объёмный комплект документации в пакете `samba-doc`; большинство ссылок данного раздела будут указывать именно на содержимое этого пакета.

Краткий обзор каталогов и файлов

Все файлы конфигурации и авторизации Samba расположены в каталоге `/etc/samba` и его под-каталогах. Рассмотрим их несколько подробнее.

`MACHINE.SID`

системный идентификатор машины, формируется автоматически при старте сервера и предназначен для идентификации компьютера в домене сети Microsoft™;

`codepages/`

каталог, содержащий файлы с таблицами перекодировки;

`lmhosts`

то же, что и `/etc/hosts`, но предназначен для преобразования IP<=>NetBIOS. Как правило содержит только одну запись:

```
127.0.0.1 localhost
```

но можно считать удачной идеей[38] заносить туда хосты из других подсетей (когда по ряду причин невозможно надёжно провести преобразование IP<=>NetBIOS ни широковещательными запросами, ни с использованием WINS) или наоборот — ключевые сервера собственного домена;

`secrets.tdb`

ключевой файл для идентификации машины в домене сети Microsoft™. С точки зрения безопасности имеет ту же ценность, что и файлы `/etc/tcb/*/shadow` — а потому права доступа должны быть `root.root 0600`;

`smb.conf`

основной конфигурационный файл Samba. Он нужен не только серверной части, но и всем остальным компонентам этой системы;

`smbpasswd`

аналог `/etc/passwd` и `/etc/tcb/*/shadow` — файл пользователей сервера Samba с паролями. С точки зрения безопасности имеет ту же ценность, что и `/etc/tcb/*/shadow` — а потому права доступа должны быть `root.root 0600`. Соответствие пользователей Samba и системных производится на основе общего UID; данный файл используется Samba при отсутствии данных о пользователе на PDC или при отсутствии самого PDC;

`smbusers`

файл соответствий имён сетевых и локальных пользователей SMB; это удобный метод для организации административных и гостевых входов на сервер. Соответствие пользователей Samba и системных производится на основе символьных имён;

`/var/log/samba/*`

лог-файлы серверной части Samba. Из них `log.smbd`, `log.nmbd`, `log.winbind` — журналы соответствующих процессов, а все прочие — логи взаимодействия сервера с отдельными клиентскими хостами в формате именования по умолчанию `log.<Client_NetBIOS_NAME>`. При превышении заданного в `smb.conf` предела производится ротация логов и формируются файлы `*.old`;

[38] Как и с `/etc/hosts`, увлекаться содержанием распределённых данных в локальных файлах не стоит.

`/var/spool/samba`

каталог динамического спулинга печати сервера Samba. На не сильно загруженных серверах печати он обычно пуст; наличие там множества файлов в то время, когда ни один из клиентов не печатает — явный признак сбоев сервера печати;

`/var/cache/samba/*`

файлы (как правило, двоичные базы данных), формируемые в процессе работы различных компонентов Samba. Наиболее примечательны:

`browse.dat` **и** `wins.dat`

текстовые файлы, их названия говорят сами за себя;

`winbindd*.tdb`

базы данных доменных пользователей, формируемых winbind (см. “Использование winbind”). Время от времени их необходимо архивировать: если при апгрейде, «переезде» или переустановке сервера winbind сгенерирует эти файлы с нуля, то соответствия системных и доменных символьных и числовых имён изменятся и права доступа на восстановленные из архива файлы окажутся заведомо перепутанными. Поэтому настоятельно рекомендуется архивировать файлы `/var/cache/samba/winbindd*.tdb`;

`/var/lib/samba/*`

служебные каталоги для администратора сервера.

Список выполняемых файлов Samba можно получить командой:

```
$ rpm -ql ‘rpm -qa | grep samba‘ | grep bin/
```

и подробно ознакомиться с каждым, прочитав соответствующие разделы документации.

Здесь же мы остановимся лишь на самых важных и наиболее часто используемых компонентах.

1. серверные компоненты:

   `/usr/sbin/nmbd`
   сервер преобразования имён и адресов;

`/usr/sbin/smbd`
файловый сервер;

`/usr/sbin/winbindd`
сервер импорта пользователей и групп с PDC;

`/usr/sbin/swat`
средство конфигурирования Samba с web-интерфейсом;

`/etc/init.d/smb` **и** `/etc/init.d/winbind`
управляющие скрипты инициализации сервисов.
Следует отметить, что у скрипта `/etc/init.d/smb` есть два режима рестарта — `restart` и `reload`, которые радикально отличаются следующими особенностями:

a. `restart` производит полный рестарт процессов **smbd** и **nmbd** со сбросом текущих соединений. Как правило, клиенты сами производят автоматическое переподключение к ресурсам, однако если в момент рестарта были открыты файлы, то возможны проблемы с клиентскими приложениями (например, MS Office и 1C);
b. `reload` заставляет **smbd** и **nmbd** только лишь перечитывать файлы конфигурации без рестарта и сброса соединений. При этом старые соединения продолжают существовать по старым правилам, а ко всем новым соединениям будут применены уже новые правила на основании файлов конфигурации.

2. клиентские компоненты:

`/usr/bin/smbclient`
интерактивное приложение для просмотра сетевых ресурсов;

`/sbin/mount.smb`, `/sbin/mount.smbfs`, `/usr/bin/smbumount`, `/usr/sbin/smbmnt`, `/usr/bin/smbmount`
средства монтирования/размонтирования сетевых файловых систем.

3. утилиты:

`/usr/bin/smbpasswd`
управление пользователями и подключением к домену;

`/usr/bin/wbinfo`
отображение списка пользователей, импортированных **winbindd**;

`/usr/bin/testparm`
проверка синтаксиса конфигурационных файлов;

`/usr/bin/smbstatus`
отображение статуса процессов **smbd** и **nmbd**;

`/usr/bin/nmblookup`
программа разрешения имён WINS (аналог **nslookup** для DNS).

Настройка сервера

В большинстве случаев настройка Samba заключается в редактировании основного конфигурационного файла `/etc/samba/smb.conf` и управлении пользователями с помощью **smbpasswd**. Если это непривычно — попробуйте использовать web-интерфейс SWAT (Samba Web Administration Tool); для этого установите пакет `samba-swat` и откройте URL `http://localhost:901/` в браузере.

Обычный сервер

Под таковым мы понимаем компьютер, предоставляющий в сеть файловые ресурсы. Фактически это простейший независимый файловый сервер, имеющий собственную базу авторизации пользователей.

Для того, что бы создать такой сервер, необходимо лишь немного подправить стандартный конфигурационный файл `smb.conf` (подставить требуемые имя рабочей группы и имена ресурсов) и создать учётные записи пользователей, как описано ниже, а также учесть рекомендации по безопасности, изложенные в конце параграфа.

Вот основные записи в smb.conf, которые создадут нам «обычный сервер».

```
[global]

# Секция [global] определяет общие настройки серверной части Samba в
# целом для всех ресурсов.
# Имя рабочей группы OFFICE
workgroup = OFFICE

# Уровень определения прав доступа на уровне пользователей
security = user

# Приоритет данного сервера среди других компьютеров рабочей группы:
# определяет, кто именно будет главной машиной, отвечающей за
# отображение ресурсов сети. Для сравнения, у Win9X os level = 34, а
# у NT4 os level = 64.
os level = 65
```

```
# Очевидно, что раз нет домена - нет и мастера.
domain master = no

# Не стоит становиться сервером паролей для окрестных машин. Так что
# если к Вам прибежал разъярённый администратор соседнего↩
NT-сервера с
# жалобами что его не пускают на его собственный сервер - поставьте
# domain logons = no ;-)
domain logons = no

# Обычно в простейшей сети WINS не нужен, мы его отключаем и у себя то
# же.
wins support = no
```

Ну а теперь надо определить, какие именно каталоги мы предоставим в сеть. Для каждого ресурса существует отдельная секция.

Самый простейший вариант для обычных ресурсов - обычный каталог с именем `public`[39] :

```
# имя ресурса, видимое в сети

[public]

# комментарий, видимый в сети как комментарий к ресурсу
comment = Public Stuff

# путь к каталогу ресурса
path = /home/samba/public

# отметка о доступе на чтение всем авторизованным пользователям (в↩
том
# числе и гостевым, если они определены)
public = yes

# запрещение работы на запись всем пользователям
writable = no

# разрешение работы на запись всем пользователям, входящим в↩
системную
# группу staff
write list = @staff
```

[39] Так называемая «файлопомойка» :-).

Подобным образом можно создать различные сетевые ресурсы сервера с различными правами доступа; за более подробной справкой по директивам и их синтаксису обратитесь к справочному руководству.

Поскольку Samba исполняется не в `chroot`, внутри ресурсов можно использовать любые символические ссылки на расположенные локально и в сети (NFS, SMB, Coda и т.д.) файловые объекты, что очень удобно в плане администрирования системы.

Особые ресурсы — например, домашние каталоги пользователей:

```
# имя ресурса, которое автоматически будет заменено именем
# домашнего каталога пользователя, под которым подключился клиент
# и именно название его домашнего каталога будет отображено в сети
# как имя ресурса.

# Для получения доступа к этому ресурсу клиент должен предоставить
# серверу соответствующие имя и пароль, все прочие пользователи к
# этому ресурсу доступа не имеют вовсе.

[homes]

# комментарий, видимый в сети как комментарий к ресурсу
comment = Home Directories

# признак невидимости - данный ресурс виден в сети только тому
# пользователю,который является его владельцем. К этому
# ресурсу можно обратиться непосредственно задав его имя, но в
# браузинге сети он будет виден только владельцу.
browseable = no

# Разрешение на запись.
writable = yes
```

Принтеры:

```
# имя ресурса, которое будет видно в сети. Кроме него, в сети будут
# также видны и локальные принтеры под теми же именами, что и в
# системе по команде lpq.

[printers]

# комментарий, который игнорируется.
comment = All Printers
```

```
# Путь к каталогу, в котором располагается спул принтеров,
# предоставляемых в сеть через Samba
path = /var/spool/samba

# невидимость ресурса в браузинге, он подменяется системным
# ресурсом.
browseable = no

# разрешение на печать для гостевого захода.
guest ok = yes

# запрещение на запись, поскольку в спул пишет сама Samba, а не
# пользователь.
writable = no

# признак того, что это именно принтер, а не файловый ресурс
printable = yes

# маска для создания файлов заданий на печать
create mode = 0700

# Команды, выполняемые Samba для того, что бы напечатать документ.
# использование драйвера клиента, применяется для не-UNIX
# клиентов.
print command = lpr-cups -P %p -o raw %s -r

# Использование драйвера CUPS на стороне сервера (на стороне
# клиентов используется generic PostScript драйвер).
; print command = lpr-cups -P %p %s

# Следующие команды являются стандартными при установке printing=cups,
# их можно изменить в случае необходимости.
lpq command = lpq -P %p
lprm command = cancel %p-%j
```

Сервер в составе существующего домена NT

Подключим вновь созданную машину Samba с именем `COMP` к существующему домену `DOM`, администратором которого является пользователь `Administrator` и PDC этого домена реализован на другом компьютере.

Первым делом необходимо убедиться, что машины с таким же именем, как и та, которую мы собираемся подключить, в домене ещё нет. В противном случае эту машину необходимо удалить из состава домена средствами самого PDC или выбрать другое имя.

На машине `COMP` в `/etc/samba/smb.conf` необходимо внести следующие изменения:

```
[global]

workgroup = DOM
netbios name = COMP
security = domain
password server = *
allow trusted domains = yes
nt acl support = yes
```

После чего необходимо остановить Samba-сервер, если он работает, командой **service smb stop**.

Теперь необходимо послать запрос на PDC с целью авторизации нового члена домена с помощью следующей команды:

```
$ smbpasswd -j DOM -r DOMPDC -U Administrator
```

и в ответ на запрос ввести пароль пользователя `Administrator` — тот самый, с которым этот пользователь зарегистрирован в домене.

Если получено сообщение:

```
Joined domain DOM.
```

все работает; иначе в `smb.conf` надо написать:

```
[global]

log level = 4
```

повторить последнюю команду и по подробным логам разбираться, что не так. При таком уровне `log level` в `log.smbd` содержится подробный отчёт об обмене с PDC. Вполне возможно, что были допущены ошибки в написании имён или ошибочно введён пароль; также возможны какие-либо неполадки на стороне PDC.

С этого момента, когда к Samba обратился пользователь «user123» с паролем «passw», она:

- сначала ищет его в /etc/samba/smbpasswd, если пароль и имя совпадают — пускает, иначе отказывает в авторизации или считает гостем (в зависимости от настройки);
- если такого имени в упомянутом файле нет — смотрит в /etc/passwd (проверив соответствия через файл /etc/samba/smbusers) и
- если такой пользователь есть — спрашивает PDC, числится ли за пользователем «user123» полученный пароль «passw»;
- если это так — пускает, иначе отказывает в авторизации либо переключает на гостевой заход, в соответствии с настройкой.

Обычно при работе в домене на рядовых рабочих станциях /etc/samba/smbpasswd должен быть абсолютно пустым либо содержать только административные учётные записи, с доменом никак не связанные.

Данная логика работы применима только в том случае, если не используется winbind. Для того, чтобы доменные пользователи автоматически оказывались в /etc/passwd при первом же удачном обращении (правильность паролей была подтверждена PDC), в /etc/samba/smb.conf необходимо написать одну строку

```
[global]

add user script = /usr/sbin/useradd -d /home/domain/%u -g 600 -m\
-k /etc/skel_domain -s /bin/false %u
```

соответственно каталоги /home/domain и /etc/skel_domain, а также группа 600 должны уже существовать. Все конкретные имена и параметры **useradd** можно менять в зависимости от конкретных применений.

По директиве add user script, которая активизируется в тех случаях, когда пользователь ещё не зарегистрирован на данной машине, можно вызывать не только /usr/sbin/useradd с ключами, но и любые другие программы; если подойти с фантазией, то с помощью данной директивы можно делать очень интересные вещи.

Не стоит забывать и о безопасности — программы, запущенные при помощи add user script, будут выполняться от всемогущего в

пределах системы пользователя `root`, а параметры их вызова частично определяются пользователем, что потенциально опасно!

Теперь можно включить сервер Samba командой: **service smb start** и работать в домене сети Windows на правах рядового члена домена.

Сервер как PDC домена

Для создания Primary Domain Controller (PDC) необходимо в `smb.conf` внести/изменить следующие записи

```
[global]

# Имя сервера; если данный параметр не определён,
# то он примет значение, соответствующее имени хоста.
netbios name = COOLSERVER

# Имя домена
workgroup = COOLDOMAIN

# Режим работы системы авторизации сервера.
security = user

# Разрешение на использование шифрованных паролей
encrypt passwords = yes

# Путь к локальному файлу паролей
smb passwd file = /etc/samba/smbpasswd

# Стать мастер-браузером для домена
local master = yes

# Быть PDC
domain master = yes

# Сразу при старте постараться стать мастер-браузером домена
preferred master = yes

# Быть сервером паролей домена
domain logons = yes

# Расположение профайла пользователей домена
logon path = \\%L\Profiles\%U

# Административная группа домена, присутствие в списке
```

```
# пользователя "administrator" весьма желательно, без
# этого данный пользователь не получит административных
# прав на клиентских машинах Windows.
domain admin group = root @wheel administrator

# Быть WINS-сервером. WINS-сервер имеет смысл когда в сети более 10
# машин, работающих по протоколу SMB. Наличие такого сервера в⏎
сложных
# сетях существенно снижает широковещательный трафик.
wins support = yes

# Порядок разрешения имён NetBIOS, по аналогии с записью в
# /etc/host.conf для разрешения имён DNS. Значение wins
# имеет смысл только при наличии в сети wins-сервера,
# в противном случае оно замедлит работу.
name resolve order = wins lmhosts bcast
```

Также необходимо создать ресурсы для работы домена.

Ресурс `netlogon` необходим для работы PDC и домена в целом. Он просто должен существовать.

```
[netlogon]

comment = Network Logon Service
path = /var/lib/samba/netlogon
guest ok = yes
writable = no
write list = admin, administrator
```

Данный ресурс необходим для создания и хранения профайлов пользователей домена:

```
[Profiles]

path = /var/lib/samba/profiles
browseable = no
read only = no
create mask = 0600
directory mask = 0700
```

При создании пользователя домена в `/var/lib/samba/profiles` автоматически создаётся каталог с именем, идентичным имени создаваемого пользователя и принадлежащий ему (с правами `0700`). В этом каталоге будут храниться личные настройки пользователя.

Для того, чтобы включить клиентскую машину в домен, необходимо произвести следующие действия.

Первый метод — вручную:

Прежде всего необходимо создать локального пользователя системы с именем, соответствующим `NetBIOS-name` подключаемой к домену машины. К имени на конце добавляется символ «$». Для добавления машины с именем `machine_name` необходимо от имени пользователя `root` выполнить следующие команды:

```
# /usr/sbin/useradd -g machines -d /dev/null -c "machine nickname" -s
/bin/false machine_name$

# passwd -l machine_name$
```

Теперь, когда создан пользователь (символ «$» в конце имени означает что это NetBIOS-имя компьютера, а не имя пользователя), можно добавить его в домен, выполнив от имени `root` команду: **smbpasswd -a -m machine_name**.

Теперь компьютер подключён к домену.

Второй метод — автоматический:

Работу со созданию машинного аккаунта можно переложить на Samba, включив в `smb.conf` следующую запись:

```
[global]

add user script = /usr/sbin/useradd -d /dev/null -g machines -s
/bin/false -M %u
```

Теперь Samba будет принимать от клиентских машин запросы на включение в домен и автоматически регистрировать их аналогично NT Server.

С этого момента начинает существовать домен и PDC на базе Samba-сервера. Пользователи могут входить под своими именами и паролями

с любой машины домена с сохранением настроек, а также самостоятельно менять свои пользовательские пароли без помощи администратора сети.

Учётные записи пользователей

Все учётные записи хранятся в файле `/etc/samba/smbpasswd`.

Учётные записи пользователей, используемые Samba делятся на две категории:

- записи о компьютерах, входящих в домен;
- записи о пользователях, зарегистрированных на данном сервере.

Следует учитывать, что для того, что бы создать и использовать любую учётную запись в `/etc/samba/smbpasswd`, предварительно необходимо создать соответствующую запись в `/etc/passwd`. Общее правило — для каждого пользователя в `/etc/samba/smbpasswd` обязательно должен существовать пользователь в `/etc/passwd`. Обратное утверждение неверно.

Для управления учётными записями предназначена утилита **smbpasswd**; полный список её возможностей можно узнать из соответствующей man-страницы, здесь же рассмотрим наиболее частые методы использования.

Создание нового пользователя:

```
# smbpasswd -a <User_name>
```

Смена пароля у существующего пользователя:

```
# smbpasswd <User_name>
```

Удаление существующего пользователя:

```
# smbpasswd -x <User_name>
```

Приостановление учётной записи без удаления:

```
# smbpasswd -d <User_name>
```

Подключение данного компьютера к существующему домену:

```
# smbpasswd -j <Domain_name> -U <Administrator_name>
```

Использование winbind

Сервис winbind является новым средством, предназначенным для более полной интеграции Samba в домены Windows; он появился, начиная с Samba 2.2.0. Данный сервис считывает свою конфигурацию из `/etc/samba/smb.conf` и динамически взаимодействует с PDC домена, автоматически синхронизируя списки пользователей и групп домена и машины Samba. Таким образом, winbind является весьма удобным средством для автоматического поддержания актуальности базы пользователей домена на рабочих станциях Samba.

Работа данного сервиса происходит без изменения содержимого каких либо авторизационных файлов в `/etc` и при перезагрузке машины доменные пользователи появляются в системе только после запуска **winbindd**. Если во время работы остановить **winbindd**, то доменные пользователи и группы не исчезнут из системы до перезагрузки, однако динамического обновления списков имён и паролей происходить не будет.

Для того, что бы при рестарте компьютера (или только сервиса **winbindd**) не нарушались соответствия внутренних UID и доменных SID, он сохраняет текущее состояние списков в файлах `/var/cache/samba/winbindd*.tdb`.

Для нормального функционирования **winbindd** в файле `/etc/samba/smb.conf` обязательно должны быть объявлены следующие директивы:

```
[global]

# Диапазон номеров локальных пользователей, который будет
# использован для динамического создания пользователей домена.
winbind uid = 10000-20000

# Диапазон номеров локальных групп пользователей, который будет
# использован для динамического создания групп пользователей
# домена.
winbind gid = 10000-20000

# Символ-разделитель, используемый для составления доменных имён
# пользователей и располагающийся между именем домена и именем
```

```
# пользователя.
winbind separator = +

# Интервал времени (в секундах) между запросами winbind к PDC
# в целях синхронизации списков пользователей и групп.
winbind cache time = 10

# Шаблон имени домашних каталогов доменных пользователей,
# автоматически присваиваемых каждому пользователю. Сами каталоги,
# однако, динамически не создаются. Вместо переменой %D подставляется
# имя домена, а вместо %U подставляется имя пользователя.
template homedir = /home/%D/%U

# Командный интерпретатор, назначаемый по умолчанию для
# пользователей, авторизованных через winbindd.
template shell = /bin/bash
```

Также необходимо внести изменения в файле `/etc/nsswich.conf` в разделы `passwd` и `group`, вписав директиву `winbind` — например, таким образом:

```
passwd: files winbind
group: files winbind
```

С этого момента можно использовать имена доменных пользователей в `/etc/samba/smb.conf` с целью разграничения доступа, в правах на файлы и каталоги, для подключения к сетевым ресурсам данного хоста со стороны других хостов.

Принт-сервер на CUPS

По умолчанию Samba сконфигурирована на использование CUPS в качестве спулера печати. Подразумевается, что CUPS уже настроен и запущен. В `/etc/samba/smb.conf` присутствуют следующие директивы:

```
[global]

printcap name = lpstat
load printers = yes
printing = cups
```

Также необходимо создать ресурс `[printers]`; его создание и назначение директив подробно описано в разделе “Обычный сервер” в части Особые ресурсы.

Настройка клиента

Для подключения компьютера Linux к сетям SMB существуют клиентские функции Samba.

Обычный клиент

Клиентские функции Samba представлены средствами просмотра сетевого окружения и монтирования файловых систем **/usr/bin/smbclient** и **/usr/bin/smbmount** соответственно. Также доступны **mount.smb** и **mount.smbfs**, являющиеся символическими ссылками на `/usr/bin/smbount`.

При запуске эти программы считывают текущую конфигурацию из файла `/etc/samba/smb.conf` и используют доменные функции в случае, если машина подключена к домену Windows.

Также файловые системы возможно монтировать системной командой mount, указав в качестве типа файловой системы smbfs, и использовать эти записи в `/etc/fstab` для автоматического монтирования при загрузке системы.

Например, для того что бы смонтировать в каталог `/mnt/disk` ресурс `public` с машины `SMALLSERVER` под именем `cooluser`, нужно выполнить команду: **smbmount //smallserver/public /mnt/disk -o username=cooluser**

Регистр написания имён компьютеров, ресурсов и пользователей роли не играет. Для того, что бы получить список Samba-ресурсов данной машины и список машин рабочей группы или домена достаточно выполнить команду: **smbclient -L localhost -N**

Более подробные сведения можно прочесть в man-страницах по **smbclient** и **smbmount**.

В составе дистрибутива поставляются два графических клиентских приложения — LinNeighborhood и gnomba [40], которые работают поверх утилит **smbclient** и **smbmount**.

По адресу `http://www.public.iastate.edu/~chadspen/homepage.html` можно получить весьма качественное графическое клиентское приложение xSMBrowser.

[40] Предпочтительнее использовать первый из них.

Клиент в составе существующего домена NT

Подключение происходит аналогично рассмотренному в п. “ Сервер в составе существующего домена NT ”. Далее вся работа происходит точно так же, как описано в предыдущем пункте.

Особенности локализации клиента и сервера

Для того, чтобы все компоненты Samba правильно работали с русскими именами файловых объектов и ресурсов, в /etc/samba/smb.conf необходимо добавить следующие директивы:

```
[global]

client code page =
character set =
```

Далее приводятся наборы значений этих директив и системных кодировок, наиболее часто используемых в России, Белоруссии и на Украине:

```
$LANG = ru_RU.KOI8-R
client code page = 866
characte set = koi8-r

$LANG = ru_RU.CP1251
client code page = 866
characte set = 1251

$LANG = be_BY.CP1251
client code page = 866
character set = 1251

$LANG = uk_UA.KOI8-U
client code page = 1125
character set = koi8-u

$LANG = uk_UA.CP1251
client code page = 1125
character set = 1251U
```

```
$LANG = ru_UA.CP1251
client code page = 1125
character set = 1251U
```

В двух последних случаях `1251U` — специальное обозначение внутри Samba для комбинации локально «`1251` — удалённо `1125`». В Samba определение удалённой кодировки делается по имени локальной [42].

Также необходимо проследить, чтобы на тех компьютерах Windows, с которыми предполагается взаимодействие через Samba, были установлены соответствующие системные настройки локализации. В противном случае велика вероятность, что вместо кириллических символов будут отображены знаки «?» либо другие непрошеные символы.

Указанные директивы `/etc/samba/smb.conf` воздействуют на работу всех компонентов Samba — и серверных, и клиентских. На данный момент поддерживаются кириллические написания имён — файлов, каталогов и ресурсов.

Некоторые вопросы безопасности

Данный раздел относится в основном к серверной части Samba.

Прежде всего необходимо определить, какие интерфейсы должны прослушиваться Samba в ожидании запроса на соединение (по умолчанию прослушиваются все имеющиеся в системе).

Например, для того, чтобы ограничить прослушивание локальным хостом и первой сетевой картой, необходимо написать в `/etc/samba/smb.conf`:

```
[global]

interfaces = 127.0.0.1 eth0
bind interfaces only = Yes
```

Далее можно ограничить диапазоны адресов, с которых позволительно обращаться к данному серверу. Действие данных директив аналогично воздействию `/etc/hosts.allow` и `/etc/hosts.deny` на `xinetd` и `ssh`: если IP-адрес хоста не подпадает под разрешающее правило,

[42] Например, кодовая страница `1251` в качестве локальной однозначно задаёт удалённую `866`.

то соединение не будет установлено вовсе. Для того, что бы ограничить доступ двумя подсетями и локальной системой, дополнительно исключив при этом один хост, можно написать:

```
[global]

hosts allow = 192.168.1. 192.168.2. 127.
hosts deny = 192.168.1.12
```

Все вышеперечисленные директивы ограничивают соединения на уровне интерфейсов и IP-адресов до какой либо авторизации. Следующие директивы управляют режимом авторизации пользователей.

Во избежание перехвата чувствительных данных при передаче их по сети открытым текстом принято шифровать пароли. Samba и все версии Windows, начиная с версии Win98, по умолчанию используют шифрование паролей. Данная директива включает его в Samba:

```
[global]

encrypt passwords = yes
```

Файл переопределений имён пользователей является весьма мощным средством управления пользовательскими аккаунтами, однако при неразумном использовании это средство опасно и поэтому по умолчанию отключено. Внимательно ознакомьтесь с содержимым файла `/etc/samba/smbusers`, прежде чем использовать его.

```
[global]

; username map = /etc/samba/smbusers
```

Особенности использования Samba 3.0

Samba 3.0 имеет заметные отличия от более ранних версий; наиболее выдающимися из них являются улучшенная по сравнению с версией 2.2 поддержка Unicode, поддержка гораздо большего количества кодовых страниц, новая утилита администрирования **net**, призванная заменить **smbpasswd**.

В поставку входят пакеты `samba3-client`, `samba3-client-cups`, `samba3-common`, `samba3`, `samba3-swat`.

Задание кодовых страниц

Для задания кодировок используются следующие новые параметры `smb.conf`:

```
unix charset = <charset>
dos charset = <charset>
display charset = <charset>
```

где `<charset>` — любая кодировка, поддерживаемая `iconv`. Список возможных кодировок можно узнать, выполнив команду **iconv -list**.

Параметры `client code page` и `character set` больше не поддерживаются. Параметр `unix charset` указывает кодировку, в которой будут храниться файлы на диске, в которой заданы параметры в `smb.conf`. Наконец-то появилась возможность хранить имена файлов в UTF-8!

Параметр `dos charset` указывает кодировку, в которой Samba будет общаться с клиентами, не поддерживающими Unicode. Все версии Windows, начиная с 95, понимают Unicode — но все же стоит установить `dos charset = cp866`, что соответствует `client code page = 866` в более старых версиях.

Параметр `display charset` указывает в какой кодировке должны выводить информацию программы, непосредственно обменивающиеся информацией с пользователем, например **smbclient**, **net**, **wbinfo** и другие.

Утилита net

Утилита **net** призвана заменить **smbpasswd** и обеспечивает гораздо большие возможности по получению информации о сети и управлению сетью. Формат команд утилиты очень похож на формат одноимённой команды Windows NT/2000.

Основные применения команды **net**:

- создание и удаление пользователей: **net user**
- включение машины в домен: **net ads join** — Active Directory; **net rpc join** — NT Domain;
- получение информации о домене, машине, открытых файлах, сессиях: **net info**, **net ads status**, **net rpc status**;

- создание и удаление разделяемых ресурсов на удалённых машинах: **net share**;
- синхронизация времени с windows-сервером: **net time**

Управление машиной с Samba из Microsoft Management Console

Начиная с версии 2.2, Samba имеет возможность удалённого администрирования из MMC (Microsoft Management Console). Эта возможность полезна, когда Samba является членом NT-домена или AD. Администратор домена может создавать, удалять и изменять сетевые ресурсы на UNIX-машине с запущенной Samba.

Как сконфигурировать Samba для удалённого администрирования? Для управления ресурсами служат параметры `/etc/samba/smb.conf`:

```
[global]

add share command = <add script>
```

Параметр указывает скрипт, который будет вызван при попытке создания нового ресурса в MMC. Скрипту передаётся четыре параметра:

- имя конфигурационного файла (например, `/etc/samba/smb.conf`);
- имя создаваемого ресурса;
- путь к существующей директории на диске;
- комментарий.

Скрипт должен завершаться с кодом `0` в случае успешного создания и ненулевым в случае ошибки.

```
change share command = <change script>
```

Параметр указывает скрипт, который будет вызван при попытке изменения существующего ресурса в MMC. Скрипту передаётся четыре параметра:

- имя конфигурационного файла (например, `/etc/samba/smb.conf`);
- имя создаваемого ресурса;
- путь к существующей директории на диске;
- комментарий.

Скрипт должен завершаться с кодом 0 в случае успешного создания и ненулевым в случае ошибки.

```
delete share command = <delete script>
```

Параметр указывает скрипт, который будет вызван при попытке удаления существующего ресурса в MMC (Stop sharing). Скрипту передаётся два параметра:

- имя конфигурационного файла (например, /etc/samba/smb.conf);
- имя создаваемого ресурса;

Скрипт должен завершаться с кодом 0 в случае успешного создания и ненулевым в случае ошибки.

Чтобы скрипты могли изменять конфигурационные файлы Samba, они должны выполняться с правами root. Для этого нужно установить отображение пользователей домена, имеющих право изменять ресурсы, в root. Это можно сделать либо с помощью файла /etc/samba/smbusers, прописав там строку вида

```
root = administrator <user 1> ... <user n>
```

либо с помощью параметра admin users в /etc/samba/smb.conf:

```
admin users = administrator
```

При создании нового ресурса Windows позволяет просматривать дерево директорий. Для этого в /etc/samba/smb.conf нужно задать служебные ресурсы, заканчивающиеся символом «$», например:

```
[C$]

path = /drives/c
```

После этого при создании нового ресурса можно будет просматривать и выбирать все директории ниже /drives/c.

Работа в среде Active Directory

Для объединения компьютеров в домены Widows 2000 Server использует схему, отличную от NT-доменов, которая называется Active

Directory; эта схема обладает гораздо большей масштабируемостью и позволяет централизованно администрировать машины, входящие в домен. Active Directory базируется на протоколе авторизации Kerberos, при котором имя пользователя и пароль не передаются по сети, а используется механизм так называемых билетов, выдаваемых сервером на определённое время. Получив билет, машина, входящая в домен, может авторизоваться на других машинах домена без участия сервера.

Установка Samba

Samba 3.0, в отличие от более ранних версий Samba, имеет возможность работать в сетях Wndows, работающих в режиме Active Directory (или Windows 2000 native mode). Если требуется эта функциональность, следует установить пакет `samba3-3.0` вместо `samba-2.2`.

Active Directory имеет другую схему именования доменов, компьютеров и пользователей, основанную на DNS. Допустим, существует сеть с именем `my.firm.com` и компьютерами `host1.my.firm.com`, `host2.my.firm.com`, `host3.my.firm.com`; тогда домен Active Directory будет называться `my.firm.com`, а пользователи Active Directory будут иметь имена вида `user@my.firm.com`.

Настройка

`/etc/krb5.conf` должен содержать по крайней мере следующие строки:

```
[realms]

MY.FIRM.COM = {
kdc = your.kerberos.server
}
```

где `MY.FIRM.COM` - имя домена (или «царства», в терминологии Kerberos; задаётся обязательно в верхнем регистре), а `your.kerberos.server` — имя или IP-адрес KDC (Kerberos Domain Controller), аналог PDC (Primary Domain Controller) в доменах Windows NT — например, `server.my.firm.com` или `192.168.117.11`.

Правильность указания параметров можно проверить, выполнив команду (замените имя пользователя на актуальное — например, `administrator@MY.FIRM.COM`):

```
# kinit username@REALM
```

и убедившись, что пароль был принят сервером. `REALM` всегда задаётся в верхнем регистре.

Вы также должны убедиться, что возможно получить имя KDC по его IP адресу (так называемый Reverse DNS lookup). Имя KDC должно либо совпадать с NetBIOS-именем компьютера (имя машины в сети Windows без указания домена) либо состоять из NetBIOS-имени и имени домена. Если получить имя KDC по адресу невозможно, вы получите ошибку «local error» при попытке войти в домен.

Если ваш DNS не поддерживает Reverse lookup либо KDC не зарегистрирован в DNS, вы можете указать соответствие IP-адреса и имени в `/etc/hosts`.

Редактирование `/etc/samba/smb.conf`

Для работы в Active Directory `smb.conf` должен содержать следующие параметры:

```
[global]

# Задаёт Kerberos realm, обычно совпадает с именем домена в
# верхнем регистре, например realm = MY.FIRM.COM
realm = <REALM>

# Это обычно часть реалма до первой точки, например
# workgroup = MY
workgroup = <WORKGROUP>

# Тип домена - Active Directory.
security = ADS

# В случае Active Directory пароли всегда шифруются.
encrypt passwords = true

# Обычно этот параметр указывать не обязательно, т.к. Samba сама
# определяет адрес KDC, если в сети есть WINS-сервер и он указан
# в smb.conf
ads server = <your.kerberos.server>
```

Регистрация компьютера в Active Directory домене

Убедитесь что Samba не запущена. Если запущена, её нужно остановить:

```
# service smb stop; service winbind stop
```

Чтобы включить компьютер в домен, выполните команду:

```
# net ads join -U administrator
```

где `administrator` — имя пользователя домена, имеющего право создавать новые учётные записи.

Если не было выдано сообщение об ошибке, то машина успешно зарегистрирована в домене — иначе проверьте правильность задания параметров в `/etc/samba/smb.conf` и `/etc/krb5.conf`. Убедитесь, что пользователь, указанный после `-U` в **net ads join**, имеет необходимые права на создание новых учётных записей.

Теперь можно запустить необходимые службы:

```
# service smb start; service winbind start
```

Проверка правильной работы в Active Directory

Для работы с компьютерами, зарегистрированными в Active Directory, не требуется указывать имя пользователя и пароль. Попробуйте выполнить команду:

```
$ smbclient -k -L <имя компьютера в домене>
```

Вы должны получить список доступных ресурсов, при этом **smbclient** не должен запрашивать имя пользователя и пароль.

Чтобы проверить, что доступ к ресурсам вашей машины возможен с других машин домена, вы можете попробовать выполнить все ту же команду:

```
$ smbclient -k -L <имя вашего компьютера в домене>
```

и получить список доступных ресурсов. Можно также попробовать открыть какой-нибудь ресурс на вышей машине с Windows-машины, входящей в домен. В любом случае имя пользователя и пароль запрашиваться не должны.

Некоторые особенности работы в Active Directory

В отличие от доменов Windows NT, авторизация в Active Directory производится не по имени и паролю, а с помощью билетов протокола Kerberos. Из-за этого работа с **smbclient** может поначалу показаться необычной.

Во-первых, при вызове **smbclient** нужно указывать параметр `-k`. Во-вторых, билеты Kerberos даются на определённое время (обычно на сутки, но это зависит от настроек сервера). Поэтому их нужно периодически обновлять с помощью команды **kinit**:

```
# kinit username@REALM
```

где `username` — ваше имя в Actiev Directory домене `REALM`.

Так что если **smbclient** вдруг перестаёт подключаться к доменным ресурсам, попробуйте обновить билет — скорее всего, дело именно в этом.

Литература

[inet] *Официальный сайт проекта http://www.samba.org*[43] .

[local] `/usr/share/doc/samba-*/docs/*` — комплект документации .

[man] man-страницы `samba(7)`, `smb.conf(5)`, `smbmount(8)`, `smbclient(1)`, `smbpasswd(8)`, `winbindd(8)` .

[43] `http://www.samba.org`

Глава 13. Zope

Краткое руководство пользователя пакета

Основная идея

Основная идея нашего варианта пакета - дать возможность эксплуатации нескольких независимых друг от друга экземпляров Zope (в пакете, полученном в рамках проекта Zope rpm такой возможности нет). Для каждого такого экземпляра создается домашний каталог, содержащий специфические для него файлы: прикладные пакеты, внешние процедуры и собственно базу данных - ZODB3.

Пакет содержит скрипты и файлы настройки, обеспечивающие интеграцию Zope с остальными компонентами операционной среды. Обеспечиваются следующие возможности:

- рестарт сервера при перезагрузке системы,
- переупаковка базы данных,
- создание нового экземпляра сервера.

Формат и расположение файлов настройки

Привязка пакета к операционной среде определяется следующими конфигурационными файлами:

/etc/sysconfig/zope_default — Конфигурация экземпляров сервера по умолчанию, параметры из этого файла загружаются до файла конфигурации экземпляра;

/etc/sysconfig/zope/* — Каждый файл в этом каталоге является конфигурационным файлом экземпляра сервера;

/etc/sysconfig/zope_hosts.cfg — Список виртуальных хостов Zope, доступных через модуль proxy веб-сервера Apache, если он используется (см. также /etc/httpd/conf/zope_proxy.conf). Формат файла - две колонки, первая колонка содержит имя виртуального хоста, вторая - url соответствующего объекта в Zope.

/etc/httpd/conf/zope_proxy.conf Дополнительный конфигурационный файл к веб-серверу Apache, его использование должно быть явно разрешено в конфиге Apacha. Конфигурационный файл описывает использование модулей proxy и rewrite для доступа к виртуальным серверам, хранимых в Zope. Список виртуальных серверов вносится в /etc/sysconfig/zope_hosts.cfg.

Переменные конфигурационных файлов экземпляров сервера

Каждый из конфигурационных файлов zope_default и /etc/sysconfig/zope/* содержит строки вида :

```
<СТРОКА> :== <ПЕРЕМЕННАЯ> '=' <ЗНАЧЕНИЯ>
```

Предполагается наличие следующих переменных:

INSTANCE_HOME=/var/lib/zope/<ИДЕНТИФИКАТОР> Рабочая зона экземпляра Zope. Содержит все данные, расширения и продукты уникальные для этого экземпляра;

ZOPE_HOME=/usr/share/zope Каталог в котором расположен шаблон домашнего каталога. Из этого каталога утилита addzopesite.py копирует файлы при создании нового домашнего каталога;

ZOPE_INSTANCE_HOME=/var/lib/zope Каталог, в котором расположены рабочие зоны экземпляров серверов. Если при создании экземпляра не указывать полный путь, а указать только идентификатор, то рабочая зона для этого экземпляра будет создана в этом каталоге и ее имя будет совпадать с идентификатором;

user=zope Пользователь, под которым запускается Zope;

port=8000 Базовый порт относительно которого захватываются порты Zope :

port + 80	http сервер;
port + 21	ftp сервер;

threads=8 Количество тредов в стартующем севере;

days=7 Количество дней между переупаковками сервера;

ignore=0 Игнорировать наличие данного экземпляра сервера при старте, если данный сервер не был указан явно (0 - запускать, 1 - игнорировать);

name="Основной Z-сервер" Имя сервера, отображаемое в сообщениях скриптов и др.;

LC_ALL=ru_RU.KOI8-R Локаль сервера по умолчанию. Если не указана - сервер стартует без ключа -L и игнорирует какие-либо установки локали. Для не-англоязычных серверов это может оказаться фатальным : не будет работать поиск посредством ZCatalog и форматирование с использованием StructuredText.

ZOPE_PROFILE_PUBLISHER=0 Если установлена и не равна 0, то Zope будет работать в режиме профилирования. Посмотреть текущий профиль Zope можно на вкладке ControlPanel/DebugInfo/manage_profile. Для профилирования используется файл

```
/var/tmp/zope.<ИДЕНТИФИКАТОР>.profile;
```

. Убедитесь что в этом каталоге достаточно места.

ZOPE_TRACE=0 Включить трассировку запросов : будет создан специальный лог

```
/var/log/zope/<ИДЕНТИФИКАТОР>.trace.log
```

. , в котором будет сохранятся подробная трассировка запросов к серверу с указанием отметок времени;

ZOPE_STUPID_LOG=0 Включить логинг отладочной информации :

```
/var/log/zope/<ИДЕНТИФИКАТОР>.stupid.log
```

, в котором будет сохранятся вывод отладочной информации о работе сервера. Содержимое лога является подмножеством того, что выводится на консоль при старте в отладочном режиме;

ZOPE_READONLY=0 Если установлена и не равно 0, то при старте в отладочном режиме Zope будет монтировать хранилище в режиме READONLY : все завершенные транзакции будут сохранятся во временной памяти и при рестарте ZOPE произойдет автоматический откат изменений.

ZOPE_STORAGE=ZODB Тип хранилища;

Поддерживаемые типы хранилищ

Существует несколько типов хранилищ для Zope, практически все из них находятся в состоянии вечных бета-версий, тем не менее при некоторых обстоятельствах оказывается интересным использовать хранилище, отличное от стандартного ZODB или же ZODB, смонтированное в нестандартном режиме (например "Только для чтения")

Обычный способом нестандартного монтирования хранилищ - размещение в каталоге /usr/lib/zope/lib/python модуля custom_zodb.py, который и выполняет собственно монтирование. Мы включили в ниш дистрибутив готовый модуль custom_zodb.py, управлять которым можно посредством переменных ZOPE_STORAGE и ZOPE_READONLY конфигурационных файлов экземпляра сервера.

Переменная ZOPE_STORAGE может принимать одно из следующих значений:

ZODB Обычное хранилище ZODB;

BSDPackless Хранилище BerceleyDB в режиме Packless;
BSDMinimal Хранилище BerceleyDB в режиме Minimal;
BSD или BSDFull Хранилище BerceleyDB в стандартном режиме;
ZODB Обычное хранилище ZODB;

Для любого их этих хранилищ может быть установлена переменная ZOPE_READONY, после чего все закрываемые транзакции будут записываться во временное хранилище и исчезнут при перезапуске сервера (таким образом работает сервер demo.neural.ru).

Серьезному тестированию работоспособности подвергалось только хранилище ZODB - как в нормальном режиме так и в READONLY, остальные типы хранилищ добавлены исключительно для тех, кто знает что делает. Мы не поддерживаем хранилище ZEO (хотя частично протестировали возможность такой поддержки), так как считаем что большая часть пользователей не заинтересована в нем, а те кто заинтересован - все равно будут собирать пакет сами.

Состав и назначение утилит

Создание экземпляра Zope

С помощью этой утилиты вы можете создать новую рабочую зону для сервера Zope, установить права доступа к файлам и зарегистрировали ее в конфигурационных файлах. При создании экземпляра Zope в него копируется файл inituser, что вызывает при старте сервера установку суперпользователя admin с паролем 12345678 - помните, сразу после старта сервера вы должны создать другого пользователя, дать ему роль Manager и стереть пользователя admin

Вызов

```
addzopesite.py [-sl] <КАТАЛОГ_ДЛЯ_УСТАНОВКИ> <ПОРТ>
```

Параметры

КАТАЛОГ_ДЛЯ_УСТАНОВКИ Каталог, в котором будет установлена рабочая зона экземпляра сервера, в простейшем случае указывается идентификатор экземпляра, при этом установка производится в каталог

	/var/lib/zope/<КАТАЛОГ_ДЛЯ_УСТАНОВКИ если параметр начинается с символа "/" - то он рассматривается как путь к каталогу для установки от корня сервера;
ПОРТ	Базовый порт, от которого будет отсчитывать рабочие порты Zope;

Ключи

-u <UID>	Пользователь;
-g <GID>	Группа;
--zope_home=<path>	Путь к прототипам;
--cfg_default=<path>	Конфигурация по умолчанию;
--cfg_dir=<path>	Каталог с конфигурациями серверов;
--instance_name=<str>	Название сервера;
--instance_id=<str>	Идентификатор сервера;
--threads=<int>	Количество тредов;
--force	Вносить в новую конфигурацию все переменные иначе вносятся только необходимые);
--locale=<locale>	Локаль, которая будет установлена для сервера;
--storage="ZODB"|"BSDFull"|"BSDPackless"|"BSDMinimal"	тип используемого хранилища;
--[no]readonly	Хранилище должно монтироваться в режиме readonly;
--[no]profile[=<path>]	Включить профилирование;
--[no]log[=<path>]	Включить отладочный логинг;
--[no]trace[=<path>]	Включить трассировку запросов; Включить трассировку запросов;

Переупаковка ZODB

Этот скрипт должен вызываться на регулярной основе, что бы выполнять переупаковку ZODB

Вызов

```
zope_pack.py [ключи] [<zope1> [<zope2> ... ]]
```

Параметры

zope1, zope2 конфигурационные файлы Z-сервера;

Ключи

-v Трассировка выполнения;

-h Помощь;

-i Игнорировать все операции;

-d <days> Количество дней при упаковке данных;

--max_ratio=<float> Доля свободного пространства по отношению к размеру базы, при котором запускается переупаковка;

--min_ratio=<float> Доля свободного пространства по отношению к размеру базы, при котором переупаковка считается невозможной;

--force = (1|2|3) Принудительная упаковка, модификаторы: 1 - игнорировать игнор, 2 - игнорировать max_ratio, 3 - игнорировать min_ratio;

--cfg_default=<path> Конфигурация по умолчанию;

--cfg_dir=<path> Каталог с конфигурациями серверов.

Рестарт сервера

Скрипт для System V init scripts, выполняющий запуск сервера Zope в различных режимах и его останов.

Вызов

```
zope <КОМАНДА> [<zope1> [<zope2> ... ]]
```

Параметры

zope1, zope2 экземпляры Zope, которые будут затронуты командой, если пусто - то команда последовательно выполняется для всех экземпляров;

Команды

-u <UID>	Пользователь;
start	старт сервера;
stop	останов сервера;
reload,restart	остановка и повторный старт сервера;
status	статус Zope;
debug	рестарт сервера в отладочном режиме, нажатие CTRL/C вызывает повторный рестарт сервера;
help	помощь по командам и переменным Z;

Генерация новой базы

Скрипт используется для создания хранилища для последующего использования в Zope в качестве основного или монтируемого хранилища.

Вызов

```
./zope_storage.py [-sl] <zope> [<path>]
```

Параметры

zope	экземпляр Zope в котором будет создана база;
path	путь к базе;

Ключи

-u <UID>	Пользователь;
-u <UID>	Пользователь;
-g <GID>	Группа;
--cfg_default=<path>	Конфигурация по умолчанию;
--cfg_dir=<path>	Каталог с конфигурациями серверов;
--external	Создать точку монтирования;
--external_name=<id>	Идентификатор точки монтирования;
--storage="ZODB"|"BSDFull"|"BSDPackless"|"BSDMinimal"	Тип создаваемого хранилища;

Быстрый старт

Установка и первоначальная настройка Zope включает в себя следующие шаги :

Установка пакетов

Для установки пакетов необходимо отдать команду вида :

```
rpm -ivh Zope-2.5.*rpm \
   Zope-Module-2.5.*.i586.rpm \
   Zope-core-2.5.*.i586.rpm \
   Zope-DateTime-2.5.*.i586.rpm \
   Zope-DocumentTemplate-2.5.*.i586.rpm \
   Zope-RestrictedPython-2.5.*.i586.rpm \
   Zope-StructuredText-2.5.*.i586.rpm \ Zope-TAL-2.5.*.i586.rpm \
   Zope-Testing-2.5.*.i586.rpm \ Zope-ZHome-2.5.*.i586.rpm \
   Zope-ZODB-2.5.*.i586.rpm \
   Zope-ZPublisher-2.5.*.i586.rpm \ Zope-ZServer-2.5.*.i586.rpm \
   Zope-ZUtils-2.5.*.i586.rpm
```

Если вы используете apt, то более простой и правильный способ установки:

```
apt-get install Zope
```

В процессе установки этих пакетов проводится ряд настроек :

- Создается пользователь и группа Zope, под которыми по умолчанию будет работать сервер;
- Создается рабочая зона Zope : /var/lib/zope;
- Устанавливаются вспомогательные пакеты Zope, эти пакеты могут использоваться без использования Zope;
- Устанавливается сам Zope;

Добавление рабочей зоны сайта

После установки пакетов одна рабочая зона создана - var/lib/zope/basic - вы можете добавить дополнительные рабочие зоны вызовом скрипта addzopesite.py, например, сама зона basic была создана командой :

```
addzopesite.py basic 8000
```

здесь 8000 - номер базового порта, от которого отсчитываются порты веб-сервера (базовый порт + 80) и ftp (базовый порт + 21)

Настройка рабочей зоны сайта

По умолчанию, вновь созданная рабочая зона не является автоматически запускаемой, т.е. при перезагрузке системы сервер для этой рабочей зоны не будет запущен. Изменить ситуацию можно установив в значение 0 параметр ignore в файле /etc/sysconfig/zope/<ИМЯ РАБОЧЕЙ ЗОНЫ> (/etc/sysconfig/zope/basic для основной зоны).

Старт сервера

Первый раз стартовать сервер лучше в отладочном режиме, командой

```
/etc/rc.d/init.d/zope debug &lt;ИМЯ РАБОЧЕЙ ЗОНЫ&gt;
```

например :

```
/etc/rc.d/init.d/zope debug test
```

При работе в отладочном режиме, сервер будет выводить отладочную информацию на терминал, с которого он стартован : это удобно при диагностировании ужасных проблем, вызываемых установкой особенно кривых продуктов;

Создание пользователей

Любая вновь созданная рабочая зона имеет пользователя admin с паролем 12345678. Единственная операция, которая может быть выполнена от имени этого пользователя - редактирование других пользователей. Поэтому, рекомендуется создать пользователя с ролью "Manager" и удалить пользователя admin, в дальнейшем, все работы проводить от имени пользователя с ролью Manager. Что бы сделать это, стартуйте сервер и проделайте следующие шаги:

1. Запустите ваш любимый браузер
2. Введите url http://127.0.0.1:8080/manage

3. В появившемся запросе на ввод логина и пароля введите логин "admin" пароль "12345678".
4. Перейдите в папку acl_users (http://127.0.0.1:8080/acl_users/manage)
5. Нажатием кнопки "добавить" добавьте пользователей, хотя бы один из которых должен иметь роль "Manager" и "Owner".
6. Удалите пользователя admin. При возникновении аварийных ситуаций вы сможете создать его заново утилитой /usr/sbin/zpasswd, так что его удаление вполне безопасно, что нельзя сказать о противоположенном случае: дело в том, что из-под этого пользователя нельзя создавать какие-либо объекты, т.к. работать они нормально все равно не смогут. Обычно, Zope блокирует такие попытки, но, есть способы это обойти - во всяком случае, даже такая умница как я, однажды импортировала реплику от имени этого пользователя и потом четыре часа тихо отъезжала -x---X;-), так глючило все.
7. Введите url http://127.0.0.1:8080/manage
8. В появившемся запросе на ввод логина и пароля введите логин и пароль пользователя с ролью "Manager".

В дальнейшем, пользователь с ролью Manager всегда может изменить логины и пароли других пользователей. Если будут утеряны все логины и пароли пользователей с ролью Manager, то можно создать пользователя admin используя утилиту zpasswd.py, и затем повторить все шаги данного раздела.

Интеграция с веб-сервером Apache

Все сайты, создаваемые с использованием сервера приложений Zope, рекомендуется запускать за proxy-сервером, в качестве которого может использоваться web-сервер apache с активированным модулем mod_proxy. Такое решение позволяет обеспечить более высокую производительность, создавать сайты дя виртуальных доменов и защитить Zope от некоторых направленных против него атак.

В пакет Zope-ZUtils-2.5.*.i586.rpm входит добавление к конфигурационному файлу Apache, /etc/httpd/conf/zope_proxy.conf, содержащее пример настройки web-сервера. С этими настройками веб-сервер будет читать содержимое файла /etc/sysconfig/zope_hosts.cfg и для перечисленных в нем виртуальных серверов запросы будут отображаться на папки Zope, при этом среда означивания запроса будет настраиваться для работы с виртуальным хостом посредством экземпляра класса VirtualHostMonster, предварительно созданного в корне сайта: иначе базовые URL'ы будут строится неверно.

Активация модулей mod_proxy и mod_rewrite

Что бы активировать mod_proxy необходимо:

1. В конфигурационном файле /etc/httpd/conf/httpd.conf нужно раскомментировать следующие строки :

```
LoadModule rewrite_module    modules/mod_rewrite.so LoadModule
proxy_module modules/libproxy.so
AddModule mod_rewrite.c AddModule mod_proxy.c
```

   Желательно убрать из файла существующее определение прокси, хотя будет работать и с ним. Какие проблемы при этом возникнут - потом расскажите.
2. В конец файла добавить вызов конфига прокси директивой :

```
Include conf/zope_proxy.conf
```

   Обратите внимание на то, что данный файл должен существовать. Он входит в пакет ZUtils).
3. Рестартовать web-сервер командой /etc/rc.d/init.d/httpd restart

Добавление виртуального сервера в конфигурацию

Список виртуальных серверов хранится в файле /etc/httpd/zope.cfg, каждая строка которого соответствует одному виртуальному серверу и содержит два параметра: URL, видимый при обращении к прокси, и URL, на который такие обращения будут отображаться. Например, для сервера zope.localdomain:

```
 zope.localdomain ↩
http://localhost:8080/VirtualHostBase/http/zope.localdomain:80/Zope/Main/V
```

Каталоги VirtualHostBase и VirtualHostRoot не должны специально создаваться : это псевдоимена, активирующие объект класса VirtualHostMonster, расположенный в корневом объекте Zope, и вызывающие переопределение среды таким образом, что в качестве базового URL при обработке запроса будет использоваться http://zope.localdmain:80/, а пути будут отсчитываться от папки

/Zope/Main - это совсем не тоже самое, что chroot на файловой системе, но приводит к сходным последствиям при программировании.

Создание контейнера под виртуальный сервер в Zope

После того, как отображение виртуального сервера добавлено в Конфигурацию прокси, можно создать контейнер под этот сервер в Zope. Мы рекомендуем для любого виртуального сервера создавать в иерархии Zope два уровня контейнеров:

- Контейнер служебного уровня ("подвал"), имя которого совпадает с именем виртуального сайта;
- Вложенную в него папку Main, содержащую корень сайта.

При таком планировании сервера, в контейнере служебного уровня будут размещаться файлы, необходимые для дизайна, коннекторы к базам данных и почтовым серверам, контейнеры авторизации пользователей (acl_users) и хранимые процедуры, а в папке Main - собственно контент-наполнение сайта.

Настройка VirtualHostMonster

Вы должны создать объект класса VirtualHostMonster в корне сайта, для этого нужно набрать в браузере url http://localhost:8080/manage и добавить объект (п. меню Add VirtualHostMonster) с именем VirtualHostMonster. Без добавления этого объекта при обращении к серверу через proxy не произойдет смещение корня виртуального сайта и вы получите ошибку 404 (not found);

Проверка

После выполнения предыдущих шагов, при вводе URL http://zope.localhost вы должны видеть страницу index_html означенную в контексте папки Zope/Main. Обратите внимание, все вычисляемые ссылки (конструкцией вида <dtml-var absolute_url>) должны указывать на URL'а сайта http://zope.localhost.

Настройка сервера для работы через https-соединение

Говорят, для этого есть специальный продукт под Zope - я даже не смотрел его, так как в любом случае использование таких специфических сервисов непосредственно в Zope выглядит не самой лучшей идеей. Более привлекательной кажется идея использования для закрытия канала между сервером и пользователем модуля mod_ssl

веб-сервера apache. Входящий в наш пакет конфигурационный файл apache zope_proxy.conf предусматривает такой механизм. Для его активации вы должны проделать следующее (предполагается, что вы уже настроили сервер для обычной работы):

1. Установить модуль mod_ssl для веб-сервера apache;
2. При установке модуля будет создан каталог /etc/httpd/conf/ssl, содержащий конфиги mod_ssl;
3. После установки модуля вы должны сгенерировать ключи к серверу обычным способом - т.е. так, как это описано в руководстве к apache, mod_ssl и openssl;
4. Файл /etc/httpd/conf/ssl/ssl.default-vhost.conf содержит конфигурацию доступа к сайту по умолчанию. Вы должны добавить в эту конфигурацию, непосредственно перед закрывающей скобкой вызов того же конфигурационного файла что и для обычного сайта, что бы в защищенном режиме также происходила обработка виртуального хостинга, конец файла после добавления должен выглядеть так :

   ```
   Include conf/zope_proxy.conf
   </VirtualHost>
   ```

   Такая конфигурация, возможно, не совсем идеальна, но достаточна для демонстрации принципа решения;
5. Рестартуйте apache;

Для проверки попробуйте ввести в браузере url'ы вида :

```
http://zope.localdomain/
```

м

```
https://zope.localdomain/
```

В обоих случаях вы должны увидеть ваш сайт, в последнем случае может (а может и дОлжно) появится предупреждение об установлении защищенного канала.

Как должна была показать проверка, проведенных настроек вполне достаточно для того, что бы пользователи могли работать с сайтом как через http, так и через https. Но желательно, что бы через https

работали только зарегистрированные пользователи, тогда как обычным лучше работать через http (кэширование, нагрузка на железо при выполнении процедуры зашифрования и т.п.). Кроме того, желательно гарантировать что бы никто из авторизованных пользователей в следствии ошибок или же злого умысла не начал работать через http.

Простейший способ добиться этого - выполнить редирект на https-канал при попытке авторизации. Если на вашем сайте используется http-авторизация, то раскомментируйте в файле zope_proxy.cfg следующие строки:

```
RewriteCond   %{SERVER_PORT} !^443$
RewriteCond   %{HTTP:Authorization} ^Basic.*
RewriteRule   ^(.*) https://%{HTTP_HOST}$1 [R,L]
```

Теперь, увидев в запросе заголовок авторизации, apache инициирует редирект на защищенный канал.

Для проверки такого редиректа, попробуйте ввести в браузере URL вида :

```
http://zope.localdomain/manage
```

Обычно, этот url используется для входа в менеджерский интерфейс Zope. Если сайт использует http-авторизацию, то вы увидите запрос для ввода логина и пароля, а после удачного ввода обнаружите что уже работаете в с url'ом вида :

```
https://zope.localdomain/manage
```

Обратите внимание, что уведомление о входе в https режим появилось уже после ввода пароля : это означает, к сожалению, что вы передали-таки пароль по открытому каналу. Такой автоматический редирект не гарантирует сокрытия вашего пароля но гарантирует, что авторизованные пользователи после ввода пароля будут работать только по https.

Для гарантированного сокрытия пароля вы должны либо явно вызывать https сразу при попытке обращения к закрытой части ресурса (попробуйте настроить соответствующим образом ссылке на вашем сайте), либо вызывать редирект на https до выполнения авторизации, по факту обращения к защищаемой странице.

Это было бы легко сделать, если бы не гибкая система настройки прав в Zope : любая страница может быть защищена. Таким образом, мы не можем предложить универсального решения, но можем предложить решение частного случая : редирект при попытке доступа к ZMI.

Что бы включить такой редирект, раскомментируйте в zope_proxy.cfg следующие строки:

```
RewriteCond    %{SERVER_PORT} !^443$
RewriteCond $1 .*/manage_.*
RewriteRule   ^(.*) https://%{HTTP_HOST}$1 [R,L]
```

Этот код будет инициировать редирект при обращении к странице вида ".*manage.*", т.е. странице интерфейса ZMI.

Хотя работа через https возможна и для других способов авторизации, автоматического редирект в момент авторизации будет организовать несколько труднее. Для частного случая использования mysqlUserFolder можно попробовать раскомментировать следующие строки в zope_proxy.conf:

```
RewriteCond    %{SERVER_PORT} !^443$
RewriteCond    %{HTTP_COOKIE} .*__ac_user.*
RewriteRule   ^(.*) https://%{HTTP_HOST}$1 [R,L]
```

Эксплуатация сервера

Дальнейшая эксплуатация сайта требует регулярного выполнения таких операций, как переупаковка базы данных и репликация каталогов сайта. Объектная база ZODB3, поверх которой построен сервер приложений, предоставляет возможность отменяемых транзакции: любая последовательность операций, изменяющих содержимое базы данных, может быть отменена без потери целостности сайта. Это полезное свойство имеет сторонний эффект: при любых изменениях размер базы данных увеличивается. Именно поэтому, на регулярной основе должна инициироваться процедура переупаковки базы, стирающая старые версии объектов. Эта процедура может быть инициирована со страницы http://zope.localhost/Control_Panel/Database/manage_pack, где можно указать параметры упаковки, но, т.к. процедура должна проводится на регулярной основе, в состав нашего пакета `Zope-ZUtils` входит

скрипт инициирующий процедуру переупаковки по crontab посредством утилиты zope_pack.py.

Скрипт запускается ежедневно, но переупаковка базы инициируется при соблюдении двух условий:

1. База занимает объем не меньше указанного в процентах от свободного пространства на диске;
2. Свободное пространство на диске не меньше указанного в процентах от размера базы.

Эти параметры хранятся в конфигурационном файле etc/sysconfig/zope_default.cfg. Старт скрипта проверяет все экземпляры сервера, конфиги которых размещены в /etc/sysconfig/zope.

Бакап сайтов, размещенных в Zope, может осуществляться сохранением базы ZODB3 :

```
/var/lib/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>/var/Data.fs
```

или репликацией отдельных папок сервера приложений. В первом случае ряд источников рекомендует пользоваться утилитой rsync (см. www.zope.org), но второй подход существенно более удобен и может выполнятся, например, регулярным запуском команды wget со строкой вида :

```
wget -sS -O <ID> $(date +%Y%m%d).zexp \
↩
"http://<LOGIN>:<PASSWD>@localhost:8080/manage_exportObject?download:int=1&id=<ID>"
```

ID идентификатор сохраняемой папки в корне Zope;
LOGIN логин пользователя в Zope;
PASSWD пароль пользователя в Zope;

При этом сервер отдает файл реплики в формате zexp. Вы можете получать реплику в формате *.xml, но: это будет работать более медленно, процесс репликации при ряде условий может сбоить и полученная реплика может занимать существенно больший объем - иными словами, это не выгодно (как впрочем и многие другие "модные" технологии).

Реплика может быть восстановлена импортом в Zope - в тот же самый экземпляр сервера или в любой другой. Для этого реплика должна быть размещена в каталоге :

```
/var/lib/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>/import,
```

после чего импорт может быть инициирован нажатием на кнопку "import/export" в любом контейнере менеджерского интерфейса. Подробно, импорт реплик описан в ImportSite.txt.

Эксплуатация сайта также включает в себя решение ряда административных проблем связанных с устранением ошибок и противостоянием вторжению. Существует ряд пакетов, помогающих справится с этими проблемами, часть которых подробно описана в InstallExtensionPackages.txt, кроме того, Digital Creations регулярно выпускает т.н. Hotfixes к текущим версиям Zope: Hotfix не изменяет сервер и не требует выполнения сложных процедур миграции сервера, он лишь в момент старта сервера переопределяет часть методов, исправляя таким образом ошибки, связанные, как правило, с дырами в защите. Hotfixes должны размещаться в каталоге /usr/lib/zope/lib/python/Products, более подробно процедура их установки описана в InstallExtensionPackages.txt и на сайте www.zope.org. Русскоязычным пользователям мы рекомендуем обязательно устанавливать продукт CrayFIX - это исправление ошибок не вошедшее в основной релиз и выполненное нами специально для русскоязычной аудитории: это не только правка языковых проблем, но и противодействие ошибкам в браузерах, распространенных на территории России.

Заключение

В заключении просто дадим ряд ссылок:

http://www.zope.org	Сайт Zope, содержит продукты расширения и много подробной документации на Zope;
http://www.python.org	Zope реализован на языке Python, этот сайт содержит всю необходимую документацию;
http://www.neural.ru	Мой сайт, я на нем вывешиваю некоторую информацию по поддерживаемым пакетам;

Установка ранее разработанного сайта

Сервер приложений Zope позволяет делать реплики базы данных и сохранять содержимое сайта в переносимом формате. При соблюдении ряда условий, такая реплика может быть в последствии импортирована в новый сервер. Благодаря этому возможна разработка сайтов "под заказ" на сервере исполнителя и передача готового сайта заказчику в виде реплик базы данных, внешних процедур и определений объектов. Данный документ описывает обычную процедуру восстановления реплик такого сайта и проблемы, которые могут при этом возникнуть.

Виды передаваемых файлов

Как правило, результаты работ передаваемые заказчику включают в себя следующие группы файлов, точные названия вы должны уточнить у поставщика:

1. Реплики базы ZODB3 содержащие сам сайт - обычно файлы с расширением *.zexp импортируемые в корень Zope;
2. Реплики базы ZODB3 содержащие определения Z-объектов - обычно файлы с расширением *.zexp импортируемые в папку /Control_Panel/Products;
3. Внешние процедуры - обычно файлы с расширением *.py размещаемые вы каталог Extensions экземпляра Zope;
4. Специализированные модули расширения Zope - архивы модулей расширения, идентичные описанным в InstallExtensionPackages.txt;
5. Реплики внешних баз данных - обычно используются реплики базы mysql;
6. Вспомогательные скрипты и утилиты серверной части - состав, формат и правила установки определяются производителем;
7. В последующих разделах будут подробно описаны процедуры установки этих файлов, рекомендуется выполнять их именно в этом порядке;

Установка реплик внешних баз данных

Поставщик должен предупредить вас, какие именно значения параметров подключения (хост, порт, логин, пароль и т.п.) используются vo стороны Zope, в противном случае, установка реплик, содержащих некоторые продукты (например, mysqlUserFolder) может оказаться невозможной. Подавляющее большинство баз данных не поддерживаются стандартной поставкой Zope (единственное исключение - ZGadFly, демонстрационная SQL-база). Поэтому, вы должны установить коннекторы к используемой вами базе данных. Для Zope 2.5.1 рекомендуемые коннекторы:

MySQL Пакеты ZMySQLDA-2.0.8, MySQL-python-0.9.2 : в варианте, поддерживаемом нами, отключено порождение исключений по невозможности отката транзакций, кроме того, пакет ZMySQLDA-2.0.8 был доработан для совместимости с MySQL-python-0.9.2 : обычный пакет работать правильно не будет;

PostgreSQL Пакеты psycopg-1.0.12, psycopg-ZPsycopgDA-1.0.12 : пожалуйста, не используйте другие коннекторы, или по крайней мере не пишите нам о том, что они не работают : наш выбор - коннектор psycopg

Установка специализированных модулей расширения Zope

Как правило, процесс установки таких модулей идентичен описанному в InstallExtensionPackages.txt и не вызывает проблем какого-либо рода, за исключением необходимости установить другие пакеты, на которые ссылаются данные.

Установка внешних процедур

Если не указано обратное, просто разместите внешние процедуры в каталоге

```
/var/lib/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>/Extensions
```

Установка реплик ZODB3

В первую очередь должны импортироваться реплики с определениями Z-объектов, следом за ними - реплики, содержащие сам сайт. Для выполнение импорта, все реплики нужно положить в каталог

```
/var/lib/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>/import
```

Определения Z-объектов импортируются в папку /Control_Panel/Products, для этого:

1. Введите url /Control_Panel/Products/manage;
2. Нажмите на кнопку import/export;
3. Внизу страницы найдите форму импорта;
4. В поле import file name введите имя файла реплики;
5. Выберите Take Owner Ship of imported objects;
6. Нажмите кнопку OK;
7. Если продукт импортирован удачно, папка продукта должна появиться на вкладке /Control_Panel/Products/manage_main;

Сами сайты, как правило, импортируются в корневую папку, для этого:

1. Введите url /manage;
2. Нажмите на кнопку import/export;
3. Внизу страницы найдите форму импорта;
4. В поле import file name введите имя файла реплики;
5. Нажмите кнопку OK;
6. Если сайт импортирован удачно, папка с ним должна появиться на вкладке /manage_main;

Если импортируемый сайт содержит SiteRoot, то, скорее всего вы должны изменить настройки прокси, чбы переадресовывать обращения к этому сайту. Если вы используете apache mod_proxy и наш конфигурационный файл apache, то конфигурационный файл должен быть включен в /etc/httpd/conf/httpd.conf директивой Include conf/zope_proxy.conf, а доступ к новому сайту прописывается в файле /etc/sysconfig/zope_hosts.cfg в следующем формате:

```
<ИМЯ ВИРТУАЛЬНОГО ХОСТА> <URL реального хоста>
```

, например:

```
zope.localdomain       http://10.0.0.9:8080/Zope/Main
```

. Помните, единственный способ отредактировать SiteRoor - это стереть его, ухищрения типа SUPPRESS_SITEROOT=1 - лишь способ, облегчающий его стирание.

Если для доступа к импортируемому сайту использовался VirtualHostMonster, то строчки в файле /etc/sysconfig/zope_hosts.cfg будут немножко длиннее:

```
zope.localdomain
↩
http://localhost:8080/VirtualHostBase/http/zope.localdomain:80/Zope/Main/V
```

.

Как либо редактировать или стирать VirtualHostMonster не надо, просто убедитесь что в корневой папке Zope есть объект этого типа;

Типичные проблемы при импорте сайтов

Права пользователей и Proxy роли

Если каким-либо методам назначены Proxy роли (т.е. проверка допусков при их обработке осуществляется так, как будто вызывавший их пользователь обладает такой ролью), то при выдаче прав будет выполняться проверка того, обладает ли этой ролью владелец этого метода. Если при импорте была изменена информация о владельцах таких методов, то обязательно проверьте, что бы новый владелец существовал и обладал требуемыми ролями.

Связанные с эти проблемы чаще всего проявляются в запрете выполнения на сайте анонимным пользователем таких операций как регистрация, отправка сообщений в форум, использования почтовых и других форм. Если проблем возникла - попробуйте исправить поля Proxy Roles и Ownership для метода, выполняющего запрещенную операцию.

Особый случай - mysqlUserFolder. Без подробных комментариев: выбирайте п. retain existing ownership information и создавайте учетную запись администратора, логин которой совпадает с логином разработчика создавшего объект mysqlUserFolder. Иначе это может не работать.

Изменение SiteRoot

Сайт имеет SiteRoot и вписанное в него доменное имя нужно изменить. Рекомендуемые действия :

1. Перезапустите сервер с установленной переменной SUPPRESS_SITEROOT, например командой

```
SUPPRESS_SITEROOT=1 /etc/rc.d/init.d/zope restart <ИМЯ СЕРВЕРА>;
```

2. Сотрите существующий объект SITE_ROOT (не тратте время на его редактирование, не выйдет);
3. Создайте новый объект SITE_ROOT и при создании введите правильные данные;
4. Перезапустите сервер без переменной SUPPRESS_SITEROOT, например командой

```
/etc/rc.d/init.d/zope restart <ИМЯ СЕРВЕРА>;
```

Без подробных комментариев: редактирование объекта SITE_ROOT не работает. Всегда стирайте и создавайте заново;

Отсутствующий продукт

Какой-либо используемый продукт не существует. Тогда при попытке входа на страницу управления экземпляром класса этого продукта вы увидите надпись "This object is broken, because ...", исправить можно только одним способом - установить недостающий продукт;

Не настроена внешняя система авторизации

Логичный выход - настроить ее. К сожалению, это не всегда возможно : система авторизации может не поддерживаться в вашей среде, вам могут быть неизвестны пароли и тому подобные вещи. В тех случаях, когда есть или может быть получена XML-реплика, смелые парни, вроде меня, открывают ее VI и вычеркивают из ObjectManager ссылку на идентификатор acl_users. Те, для кого это пустой звук, могут попробовать сделать так :

```
sed -s "s/acl_users/acl_sonofbitch/g" <входная_реплика.xml↩
>выходная_реплика.xml
```

После этого объекты acl_users перестанут быть таковыми, вы можете попробовать импортировать реплику обратно и стереть объекты acl_sonofbitch.

Еще раз - этот способ для смелых парней, которым нечего терять. Остальным лучше так не делать.

Установка и использование дополнительных пакетов

Сервер приложений Zope позволяет устанавливать расширения, дающие пользователям дополнительные возможности, такие как использование внешних баз данных, фильтрация и преобразование запросов, вспомогательные объектные модели для создания сайтов. Ниже описана процедура установки таких расширений и перечислен список расширений, рекомендуемых нами. Все эти расширения проверяются на совместную работу и тестируются на совместимость с текущей версией сервера. Если вы хотите расширить список поддерживаемых нами расширений, то свяжитесь с нами - cray@neural.ru.

Общее описание установки пакета расширения

Любой пакет расширения может быть установлен либо использование всем сервером, либо для использования одним из серверов. В первом случае, корневой каталог пакета (т.е. каталог содержащий файл __init__.py) должен быть скопирован в каталог :

```
/usr/lib/zope/lib/python/Products,
```

во втором - в каталог :

```
/var/lib/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>/Products.
```

В любом случае, сервер должен быть перезапущен.

Пакет расширения может быть получен в виде архива tar (в частности, в таком виде пакеты распространяет www.zope.org) или в виде rpm (в таком виде, пакеты лежат в нашем дистрибутиве). Если вы имеете дело с пакетом tar, его установка проводится следующим образом:

1. Читаем доку на пакет, не сказано ли там что-либо иное, если не сказано, выполняем остальные пункты;
2. cd /usr/lib/zope
3. tar xvzf <ИМЯ ПАКЕТА>.
4. Все ;)

Архив пакетов формируется так, что бы распаковываться от корня сервера приложений. Если вы хотите установить пакет только для экземпляра сервера, вы должны проделать иную операцию:

1. cd /var/lib/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>
2. tar xvzf <ИМЯ ФАЙЛА ПАКЕТА>

Пакеты RPM - из-за ряда ограничений, присущих как RPM так и Python, пакеты RPM устанавливаются только для всего сервера, для чего нужно отдать команду rpm -ivh <ИМЯ ПАКЕТА>. Разумеется, никто не мешает вам скопировать файлы продукта из каталога :

```
/usr/lib/zope/lib/python/Products
```

в каталог :

```
/var/lib/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>/Products,
```

только обязательно сотрите после этого файлы с расширением рус :

```
rm -i *.pyc
```

по данным ряда источников, использование файлов рус построенных в другом каталоге может приводить к сбоем в работе Python.

Есть еще один вариант пакета расширения - пакеты в форматах zexp (xml), их установка подробно описана в ImportSite.txt.

Каким бы путем вы не устанавливали пакет, как правило, в результате его установки должен появится продукт в списке продуктов стартованного сервера, получить доступ к этому списку можно введя URL :

```
http://zope.localdomain:8080/Control_Panel/Products/manage_main
```

и логин и пароль пользователя, имеющего роль "manager".

CrayFIX : Фиксация ошибок интерфейса

Россия - страна, которая отличается от других, поэтому проблемы, возникающие перед Российскими пользователями мало интересны другим. Именно поэтому мы поставляем этот пакет. Итак, этот пакет рекомендуется к установке в одном из следующих случаев:

1. Вы говорите и пишите по русски;
2. Вы используете продукт IIGFS;
3. Вы являетесь счастливым обладателем MSIE for Linux, ну или хотя бы for Windows;

На первом случае остановимся подробно : пакет изменяет часть файлов DTML менеджерского интерфейса таким образом, что бы для них устанавливалась кодировка, выбранная администратором сервера. Если этого не сделать, то ряд версий MS Internet Explorer не сможет сохранять результаты редактирования материалов сайта в менеджерском интерфейсе Zope в правильной кодировке.

Кроме того, пакет добавляет удобную возможность горячего отключения или включения объекта RequestDecoder, а при установленном пакете IIGFS - доступ к "закладкам".

После установки пакета вы должны задать кодировку, которая будет установлена на менеджерских страницах, для этого нужно выполнить следующее действие:

1. Войти в папку, в которой вы хотите использовать данную кодировку, рекомендуется - в корневую папку сервера, для чего нужно ввести URL http://zope.localdomain:8080/manage_main
2. Войти в свойства папки (вкладка Properties) http://zope.localdomain:8080/manage_propertiesForm

3. Добавить новое свойство default_charset типа string и значением желаемой кодировки, например - koi8-r.
4. Помните, под действием заимствования данная настройка распространяется на все вложенные папки и для ее отключения вы должны задать этот атрибут в той папке, где хотите отключить (или изменить) настройку еще раз.

Еще раз повторю - без этого пакета вы не сможете работать с сайтом на русском языке из ряда версий ряда продуктов ряда компаний, в основном - MSIE 5.0 - 5.5.

AqGuard : Защита от неограниченного заимствования

Особенностью, порождаемой концепцией заимствования в сервере приложений Zope является то, что любой сайт имеет в принципе неограниченное множество допустимых url'ов. Такие URL могут строится, например, повторением элемента пути любое количество раз. Например, для url'а :

```
"http://zope.locadomain/Search/Forum"
```

существует бесконечное множество допустимых URL'ов вида :

```
"http://zope.locadomain/Search/" + "Search/" * n + "Forum",
```

где n = [0:+inf]. Это не представляло бы проблемы, если бы не упорство роботов, выполняющих зеркалирование и индексирование сайтов и не ошибки в HTML и самих поисковых роботах: на сайте может появится ссылка на "неподвижную точку", т.е. ссылка вида

```
"http://zope.locadomain/Search/" + "Search/" * n + "Forum",
```

вызывающая получение той же самой страницы, но содержащей ссылку вида:

```
"http://zope.locadomain/Search/" + "Search/" * (n + 1) + "Forum",
```

Очевидно, робот, перешедший по такой ссылке, попадает в бесконечный цикл, что вызывает проблемы не только у самого робота, но и у сайта: при достижении n величин порядка десятков и сотен такая

деятельность робота больше напоминает DoS - атаку. Характерные примеры неподвижных точек - конструкции вида:

```
<a href="<dtml-var URLPATH0>/<dtml-var "getId()">"> _. </a>;
```

```
<a href="<dtml-var "getId()">"> _. </a>
```

Или более сложные конструкции, использующие теги base и подобные возможности. Ситуацию осложняет то, что не все парсеры html обрабатывают относительные ссылки одинаково - причем, именно дешевые парсеры используемые в роботах страдают ошибками в этой области. Из-за этого проблема не может быть решена устранением ошибки в HTML, да и поиск неподвижной точки представляет достаточно сложную задачу.

Продукт AqGuard позволяет решить проблему иначе: запретить использование url-ов в которых идентификатор одного и того же объекта повторяется больше некоторого порогового значения. Если такая ситуация обнаруживается, то AqGuard генерирует исключение AqGuardBlocked или вызывает специальный метод.

Установка и настройка AqGuard включает следующие шаги:

1. Установить пакет как описано в начале документа;
2. Перезапустить защищаемый экземпляр Zope командой :

   ```
   service zope restart <ИМЯ_ЭКЗЕМПЛЯРА>
   ```

3. Войти в менеджерский интерфейс Zope введя URL вида http://zope.localdomain/manage;
4. Войти в контейнер, в который вложены объекты, при отображении которых наблюдается это неприятное явление;
5. Создать в этом контейнере объект типа AqGuard (желательно назвать его AqGuard - иначе возможны проблемы в старых версиях Zope)
6. Войти в объект AqGuard и выбрать вкладку "Настройка";

7. Подробно, настройка AqGuard описана в файле помощи, здесь заметим только возможность указать пороговое количество повторений объектов установкой атрибута max_repeats : с атрибутами по умолчанию AqGuard будет блокировать появление любых имен в пути при обращении к объектам ниже содержащего его контейнера более 4рех раз;
8. Включить AqGuard установкой флага use_aqguard;
9. Ввести запрещенный (теперь) Url что бы проверить работоспособность - вы должны увидеть страницу с ошибкой: текст ошибки может быть изменен редактированием или перекрытием DTML-метода :

```
standard_error_message
```

   или явным указанием обработчика ошибок;

Не рекомендуется оставлять в AqGuard настройки по умолчанию - это всегда работает, но далеко от оптимального;

FloodGuard : Защита от флуда

Флуд - малоприятное явление, состоящее в том, что какой-то типчик заходит к вам на сайт, пишет двадцать сообщений в гостевой книге, начинает писать сам себе сообщения в форуме или даже пытается подобрать пароль к чьей-то учетной записи. По нашему опыту, такой типчик скорее всего на ваш сайт не зайдет, но уж если зайдет, то вам придется пережить не мало неприятных минут объясняя высшему руководству вашей компании особенности протокола http, html, tcp/ip и выслушивая основные положения КЗОТ.

Продукт FloodGuard дает, возможно, не лучшее, но обобщенное решение проблемы: предоставляется возможность задать маску повторяющегося события и разрешенную частоту его повторений за указанный период времени с данного IP-адреса. Маска события включает в себя путь к объекту, возможно заданный как регулярное выражение и ноль или более имен переменных.

Последовательностью событий считается появление совпадающих путей, снабженных совпадающими значениями этих переменных. При превышении порогового значения генерируется исключение FloodGuardBlocked;

Установка и настройка

После установки пакета так, как описано в начале документа, вы должны его настроить и активировать, предприняв следующие шаги:

1. Войти в менеджерский интерфейс Zope введя URL вида http://zope.localdomain/manage;
2. Войти в контейнер, содержащий объекты, в отношении отображений которых может быть предпринят флуд;
3. Создать объект типа FloodGuard (желательно с именем FloodGuard, иначе в ряде версий Zope возможны ошибки);
4. Войти в объект FloodGuard и выбрать вкладку "Настройка";
5. Подробно настройка описана в файле помощи, здесь отметим лишь возможность указать флаг use_referer - если он установлен, то при обращении с опознанной сигнатурой проверяется атрибут HTTP_REFERER запроса, и если он не указывает на тот же самый сайт, что и текущий, то запрос отбрасывается (это останавливает только особенно тупых злонамеренных флудеров, но их доля в общей массе может достигать заметных величин по оценке ряда экспертов (см. публикации студии Артемия Лебедева);
6. Вы должны указать сигнатуру запроса : по умолчанию, указана сигнатура запрещающая интенсивную работу с интерфейсом менеджера;
7. Установить флаг use_floodguard;
8. Отдать несколько раз запрос, удовлетворяющий сигнатуре атаки;
9. После перехода порогового значения должна отобразится страница с ошибкой, текст ошибки может быть изменен редактированием или перекрытием DTML-метода :

```
standard_error_message
```

или явными указанием обработчика ошибок;

Продукт FloodGuard позволяет посмотреть лог обращений с IP-адресами. Если Zope закрыт Proxy-сервером, то прокси должен передавать IP-адрес в переменной ip, как это сделано, например, в нашем конфигурационном файле /etc/httpd/conf/zope_proxy.conf : прокси устанавливает переменную ip, если путь в URL заканчивается строчкой :ipset. Для нормальной работы FloodGuard все опознаваемые маски событий должны запрашиваться с такой строчкой и переменная ip

должна быть указана в маске события : будьте внимательны в своих настройках!

Другой вариант передачи IP-адреса возможен при использовании HTTP/1.1 proxy (например apache > 1.3.27). Если такой прокси имеет место вы должны установить флаг use_http11. Подразумевается, что прокси-сервер будет передавать IP-адрес в специальном заголовке.

Какой бы способ передачи IP вы не использовали, продукт будет устанавливать в запросе переменную REMOTE_ADDR в значение равное этому адресу.

RequestDecoder : Перекодирование запросов и защита от мата ;)

Особенностью пользователей Российского интернет является не только использование шести кодировок, но и то, что из всех доступных браузеров всегда выбирается тот, который обрабатывает их наиболее кривым образом. При отсутствии ошибок, проблема кодировок полностью решается установкой заголовка charset, к сожалению, жизнь оказывается более суровой и ошибки имеют место. Устав объяснять счастливым обладателям решения от микрософт причины непристойного поведения их браузера мы написали этот продукт.

Цель продукта	Не обращая внимания на то, под видом какой кодировки пытается браузер отдать запрос, определить реальную кодировку запроса по его содержанию и перекодировать в кодировку сервера.
Метод	Частотный анализ признаков.
Достижения	Работает на сайте www.f-abrika.ru, 2000 хостов в день, с тех пор как метод был применен там, я стал спать дольше на полтора часа в сутки, повысился вес, улучшилось настроение и т.п. - мне больше не нужно объяснять счастливым пользователем известной компании где и кого ошибка. Последняя версия RequestDecoder легко интегрируется в сайт и обладает некоторыми дополнительными возможностями, скрашивающими жизнь редакторов сайта.

Установка и настройка

После обычной процедуры установки выполните следующие шаги:

1. Войти в менеджерский интерфейс Zope введя URL вида http://zope.localdomain/manage;
2. Войти в контейнер, содержащий объекты, при обработке запросов к которым запрос должен перекодироваться (например, корневой контейнер);
3. Создать объект типа RequestDecoder (желательно с именем RequestDecoder, иначе в ряде версий Zope возможны ошибки);
4. Войти в объект RequestDecoder и выбрать вкладку "Настройка";
5. Подробно настройка описана в файлах помощи, здесь отметим лишь возможность указать флаг use_censor - если он установлен, то запрос будет проверяться на наличие матерных выражений, рекомендуем вам сбросить этот флаг, если вы хотите использовать продукт на реальном сайте : флаг введен как опция, включающая прототип продукта SemanticGuard - любые предложения по ней приветствуются;
6. Вы должны перечислить регулярные выражения, описывающие пути к объектам, запросы к которым перекодируются. Настройки по умолчанию перекодируют запросы к менеджерскому интерфейсу;
7. Если вы хотите что бы RequestDecoder был по умолчанию активен, вы должны установить флаг "use_decoder";
8. Если установлен продукт CrayFIX, то в левом фрейме появится кнопка, позволяющая включить или выключить RequestDecoder для текущей сессии;
9. Вы можете перейти на вкладку "тест" и ввести текст в неверной кодировке, протестировав таким образом перекодировщик. В текущей версии, RequestDecoder обслуживает только кодировки koi8-r и windows1251.

SemanticGuard : Семантический фильтр

RequestDecoder содержит модельный прототип продукта SemanticGuard - продукта, проверяющего текст запроса в поиске запрещенных выражений и при их появлении генерирующий прерывание Uncensored. Разработчики обладают необходимыми знаниями в области лингвистических технологий что бы довести этот функционал до промышленного уровня, если пользователи найдут его полезным.

В текущей версии, это просто игрушка, позволяющая запретить ввод матерных выражений на сайте - эксперименты в ее использовании крайне приветствуются, если будут отзывы предложения и пожелания, то, возможно, работы над продуктом будут продолжены.

psycopg

API для работы с базами PostgreSQL из утилит на языке Python. Должен быть установлен для использования любых продуктов Z, ориентированных на использование postgresql. Устанавливается установкой пакета rpm ;)

psycopg-ZPsycopgDA : Коннектор к базе данных postgresql

Коннектор используется для описания подключения экземпляра сервера приложений Zope к серверу баз данных postgresql. Установка требует выполнения пунктов, перечисленных в начале документа.

Несмотря на все достоинства этого продукта, он не содержит явного способа установить кодировку клиента при работе с базой данных postgresql с кодировкой, отличной от кодировки сервера. Лучший способ решения данной проблемы - добавление строчки вида :

```
export PGCLIENTENCODING=<КОДИРОВКА КЛИЕНТА>
```

в файл :

```
/etc/sysconfig/zope/<ИМЯ ЭКЗЕМПЛЯРА СЕРВЕРА>
```

подробности такого решения можно узнать в документации на postgresql.

Пожалуйста, не пытайтесь добавлять команду set clientencoding при отдаче каждого запроса : мало того что это методологически неверно, так это еще приведет к нерациональному расходу сил и трудно диагностируемым ошибкам.

MySQL-python

API для работы с базами MySQL из утилит на языке Python. Должен быть установлен для использования любых продуктов Z, ориентированных на использование mysql. Устанавливается установкой пакета rpm ;)

ZMySQLDA : Коннектор к базе данных mysql

Коннектор используется для описания подключения экземпляра сервера приложений Zope к серверу баз данных MySQL. Установка требует выполнения пунктов, перечисленных в начале документа. Предупреждение : в нашей версии отключена генерация исключения по невозможности откатки транзакции. Дело в том, что это исключение генерируется всегда при ошибочном завершении любой транзакции, заканчивающейся ошибочно по каким-либо причинам, что и не дает возможности ни отдиагностировать, ни обработать корректно исходную ошибку.

Если вы считаете такой патч пакета неверным - свяжитесь с нами.

mysqlUserFolder : "Папка пользователей", хранимая в mysql

В сервере приложений Zope существует единое API для хранения учетных записей пользователей. Один из вариантов использование этого API - mysqlUserFolder, позволяющий хранить учетные записи в базе данных MySQL. Предлагаемый пакет mysqlUserFolder полностью совместим с оригинальным пакетом, но существенно доработан нами для работы в России. Подробности доработок пакета см. в документации на пакет.

Установка и настройка

После установки пакета, необходимо выполнить следующие шаги по его настройке:

1. Создать базу MySQL под список учетных записей пользователей;
2. Залить начальную версию базы из файла /usr/lib/zope/lib/python/Products/mysqlUserFolder/sql/create_tables.sql
3. Войти в менеджерский интерфейс Zope введя URL вида http://zope.localdomain/manage;
4. Войти в контейнер, в котором будут действовать учетные записи, хранимые в этой базе;
5. Создать в этом контейнере объект типа mysqlUserFolder, объекту будет присвоен идентификатор acl_users. При создании объекта нужно указать параметры подключения к базе mysqlUserFolder;
6. Войти в acl_users и перейти на вкладку "Manage Users";
7. Нажать кнопку "Create User" и заполнить поля формы, в поле Role укажите Manager;

8. Перезапустите браузер и обратившись к контейнеру, содержащей этот объект, попробуйте войти в менеджерский интерфейс, введя логин и пароль только что созданного пользователя.
9. По умолчанию, в базу пользователей добавляются две роли - Manager и Anonymous. Для более тонкой настройки прав вы должны либо добавить дополнительные роли в таблицу Roles через интерфейс командной строки MySQL, либо использовать локальные роли Zope;

Заключение

Мы рекомендуем поставить все перечисленные здесь продукты и использовать их. Мы, как водится, не гарантируем какой-либо пригодности для частных целей и не отвечаем за, ну, ни за что. Но, в процессе написания данной методички мы поставили все перечисленные продукты в перечисленном порядке - вроде работает. Успехов!

Глава 14. WWWOFFLE

Вступление

WWWOFFLE (World Wide Web Offline Explorer) — это прокси-сервер, предназначенный для использования на компьютерах с ограниченным доступом к Интернету (dial-up).

Сервер работает в двух режимах: `online` (при установленном соединении с Интернетом) и `offline` (при отсутствии соединения). В режиме `offline` доступны для просмотра страницы, закэшированные ранее в режиме `online`. Кроме того, в режиме `offline` можно «заказать» для просмотра страницы, которые будут загружены (**fetch**) при следующем подключении к сети. Поддерживается регулярный мониторинг страниц, а также рекурсивная загрузка. Сервер имеет много возможностей и настроек.

Установка и настройка

Установку проще всего произвести стандартными средствами (**apt-get install wwwoffle**). Сразу после установки нужно проверить, включена ли загрузка сервера по умолчанию (с помощью утилиты chkconfig), и запустить сервер (**service wwwoffle start**).

В настройках браузера необходимо указать адрес сервера:

```
localhost:8080 (HTTP, FTP)
```

Сервер также поддерживает протокол *finger* и *HTTPS*-туннелирование).

Для того, чтобы при подключении к Интернету (а также при установленном соединении) сервер автоматически менял режим работы, небходимо отредактировать конфигурационные скрипты `/etc/ppp/ip-up.local` и `/etc/ppp/ip-down.local` (если они не существуют, их нужно создать с правами доступа `0755 root:root`). В первый из них нужно поместить команды:

```
#!/bin/sh
wwwoffle -online
wwwoffle -fetch
```

Во второй файл следует поместить команды:

```
#!/bin/sh
wwwoffle -offline
```

Еженедельно на компьютере будет запускается процесс удаления (**purge**) устаревших документов в кэше.

Настройку сервера можно осуществлять двумя способам: с помощью редактирования конфигурационного файла (`/etc/wwwoffle.conf`) и с помощью web-интерфейса (`http://localhost:8080`). После редактирования конфигурационного файла нужно перезагрузить конфигурацию сервера (**service wwwoffle reload**).

Далее перечислены некоторые конфигурационные директивы сервера:

- `request-changed` — время, по истечении которого сервер будет считать документы считать устаревшими, то есть не будет загружать одну и ту же страницу слишком часто; для этой и других директив можно задавать разные значения по шаблону адреса документа: например, рисунки можно кэшировать «сильнее», чем html-страницы;
- `request-expired`, `request-no-cache` — должен ли сервер строго придерживаться правил обновления страниц при повторной загрузке;
- `FetchOptions` — позволяет настроить автоматическую загрузку рисунков, стилей и скриптов вместе со страницами;
- `add-cache-info` — добавляет к страницам информацию о кэшировании;
- `DontGet` — список шаблонов для игнорирования файлов (позволяет отключать баннерную рекламу);
- `disable-webbug-images`, `disable-dontget-iframes` — позволяет отключить загрузку рисунков и фрэймов размером 1x1;
- `LocalNet`, `AllowedConnectHosts`, `AllowedConnectUsers` — опции управления доступом к серверу.
- `Purge` — управление очисткой кэша; есть возможность хранить на диске закэшировнные страницы в сжатом виде.

Предостережение

В настоящее время WWWOFFLE не рекомендуется использовать на серверах с повышенными требованиями к безопасности.

Часть V. Шрифты

Глава 15. Протокол X11 и шрифты.

Протокол X11, разработанный в середине 80-х годов, определяет взаимодействие между приложением и системой отображения графики. Приложения называется *клиентом* X11, а система отображения — *сервером* X11. Таким образом, вопреки сложившимся житейским представлениям, *сервер* X11 работает на компьютере или X-терминале пользователя, а приложение (*клиент* X11) может быть запущено как локально, так и удалённо.

Протокол X11 представляет шрифт как набор матриц из нулей и единиц (растров). Каждый шрифт имеет ряд характеристик (имя, размер, кодировка и т.д.). Сервер ищет требуемый приложением растр шрифта с запрошенными свойствами сам, при помощи своего шрифтового модуля, или обращается за ним к специальному серверу шрифтов, запущенному локально или удалённо. Таким образом, протокол X11 был изначально ориентиован на работу с растровыми (bitmap) шрифтами (PCF, BDF), при этом приложение (*клиент*) может лишь запрашивать шрифт, но само с его растрами не работает.

С ростом возможностей печатающих устройств, они стали использовать т.н. скалируемые шрифты, задаваемые векторно, что позволило легко масштабировать их, а также осуществлять другие преобразования. Более того, при выводе на качественные устройства печати символы шрифтов отображаются не одним цветом, а оттенками цвета, что позволяет создать эффект сглаживания (антиалиасинга). `UNIX`™ прекрасно справлялся и справляется с красивой печатью скалируемыми шрифтами при помощи знаменитых программ nroff (groff в варианте GNU), *TeX*, ghostscript, но программы просмотра выходных форматов этих программ не пользуются шрифтовыми возможностями протокола *X*, ограниченного растром, а посылают серверу *X* уже сформированную картинку, что сильно замедляет работу и делает практически невозможным днамическое отображение текста в процессе набора или использование его в элементах интерфейса.

Для использования в оконной системе *X* скалируемых шрифтов (*Type1*, *TTF*, *Speedo*), необходимо преобразовывать их символы (глифы) в растры. В свободной реализации *X*, *XFree86*, это делает либо сам *сервер* X11, собранный с библиотекой растеризации `freetype1` (сейчас это более распространенный способ), либо сервер шрифтов. При этом существенно увеличивается количество доступных шрифтов, появляется возможность использовать для отображения и печати одни

и те же шрифты, но вот качество отображения оставляет желать лучшего, так как на экране символ по-прежнему остается одноцветным, без полутонов, т.е. сглаживания.

Глава 16. Сглаживание шрифтов.

Сглаживание шрифтов в XFree86, не модифицирующее протокол X11, было реализовано около двух лет назад. Для создания картинки из глифа использовалась библиотека `freetype2`[45], для отрисовки её на экране с использованием, при возможности, аппаратной акслерации — расширение `Render` сервера X, а для управления шрифтами и взаимодействия с расширением `Render` — библиотека `Xft1`.

Важно, что картинка сглаженного глифа создается клиентом из шрифтов на стороне клиента, а расширение `Render` на стороное сервера X11 отрисовывает её, согласуя с фоном. При этом расширение `Render` аппаратно-зависимо и, к сожалению, существует не для всех видеочипов. Тем более его нет на стандартных X-терминалах. Вот почему сглаживание шрифтов, использующее библиотеку `Xft1`, работает не на всех системах.

Летом 2002 года Кейт Паккард (Keith Packard), автор новой концепции рендеринга для X и библиотеки `Xft1`, выпустил её новую, переработанную редакцию — `Xft2`. Кейт выделил библиотеку управления шрифтами клиента, назвав её fontconfig, а в `Xft2` добавил возможность отрисовки на сервере X11 картинок сглаженных глифов даже в том случае, если расширения `Render` на нем нет. При этом, конечно, трафик между клиентом и сервером заметно возрастает.

[45] http://www.freetype.org

Глава 17. Управление шрифтами

Сервер X

Каталоги со шрифтами, управляемыми самим сервером X11, описываются в секции «Files» файла конфигурации `/etc/X11/XF86Config-4` (здесь и далее приводится расположение файлов, принятое в *ALT Linux*). В каждом таком каталоге должен быть файл `fonts.dir` (созданный, например, при помощи утилиты mkfontdir для каталогов с растровыми шрифтами и утилитой ttmkfdir — для каталогов с TTF) с описанием шрифтов и, возможно, файл `fonts.alias` с альтернативными описаниями шрифтов каталога. Для того чтобы изменения в секции «Files» (равно как и в других секциях `XF86Config`) вступили в силу, требуется перезапуск сервера X11. В то же время, добавить или удалить шрифты в процессе работы можно при помощи утилиты xset [+|-]fp. В умалчиваемой конфигурации XFree86 в *ALT Linux* непосредственное управление шрифтами сервером X не используется.

Сервер шрифтов xfs

В большинстве современных дистрибутивов `Linux` для управления шрифтами X11 используется сервер шрифтов xfs. Для того, чтобы указать серверу X11 на необходимость обращения к серверу шрифтов, достаточно указать в `XF86Config-4` его сетевой адрес и протокол доступа. В случае, если xfs запущен локально, в `XF86Config-4` есть строчка

```
FontPath "unix/:-1"
```

в секции «Files». Каталоги со шрифтами перечисляются в `/etc/X11/fs/config/`. Самый удобный способ добавления/удаления каталогов шрифтов — утилита chkfontpath, которая изменяет файл настроек xfs и перезапускает сервер шрифтов.

Просмотреть шрифты, доступные системе, можно при помощи программы xfontsel.

Управление шрифтами клиента средствами fontconfig

Файл системных настроек шрифтов клиента, управлемых при помощи библиотеки fontconfig, `./etc/fonts/fonts.conf`, предсталяет из себя файл в разметке XML. Его формат описан в man-странице fontconfig. Утилита fc-list позволяет увидеть список доступных шрифтов, а утилита fc-cache — пересоздать файлы описания `fonts.cache-NN` для каталогов со шрифтами. Утилита fontconfig позволяет управлять не только скалируемыми, но и растровыми шрифтами в кодировке `iso10646-1` (Unicode).

Система управления шрифтами на основе fontconfig позволяет пользователю легко добавлять новые шрифты без перезапуска серверов. Для этого достаточно разместить их в каталоге `~/.fonts` и выполнить команду

fc-cache ~/.fonts

Шрифты станут доступны всем вновь запущенным приложениям, использующим fontconfig.

Утилита fontconfig используется не только приложениями, работающими с сервером X, но и, например, библиотекой печати `gnome-print2`. Унификация управления шрифтами, которую предлагает fontconfig, — одна из задач, которую предстоит решить в ближайшем будущем.

Другие средства управления шрифтами

Свои средства подключения и настройки шрифтов имеют интерпретатор языка *PostScript* — GNU *GhostScript*, издательская система *TeX*, программы форматирования текстов groff и GNU enscript.

Расположение файла описания шрифтов *GhostScript* — `Fontmap`, а также каталогов со шрфитами, определяется системной переменной `GS_LIB`. В *ALT Linux* файл `Fontmap` находится в каталоге `/etc/gs`. Значение переменной `GS_LIB` удобно наблюдать в выводе команды **gs -help**.

В пакете `teTeX-2.0`, входящем в *ALT Linux*[46] *Master*, значительно улучшена и упрощена работа со шрифтами *Type1*. Именно они, а не шрифты *Metafont*, как ранее, являются основными в нашем пакете.

[46] `http://www.altlinux.ru`

Глава 18. Шрифты в ALT Linux Master 2.2.

Растровые шрифты

Основными растровыми шрифтами в *ALT Linux* являются шрифты `misc` из поставки `XFree86`, а также шрифты Дмитрия Болховитянова `XFree86-cyr_rfx-75dpi` в различных кириллических кодировках и шрифты `XFree86-75dpi-unicode`, созданные *ASP Linux* путем объединения шрифтов `XFree86` и шрифтов Дмитрия Болховитянова.

Для правильной работы некоторых приложений с кириллицей важно, чтобы шрифты в требемой кириллической кодировке стояли первыми в списке шрифтов xfs. При установке системы это требование соблюдается, но если вы изменили основную кодировку системы, то может понадобиться доустановить пакет шрфитов в новой кодировке и поменять порядок путей в `/etc/X11/fs/config`.

Скалируемые шрифты.

Type1

Свободные шрифты `Type1` в *ALT Linux Master 2.2* стали основными шрифтами для приложений, использущих сглаживание (антиалиасинг). Современные версии библиотеки `freetype2` позволяют обеспечить их качественный рендеринг.

Большинство приложений *Qt*/KDE и *Gtk*+2/GNOME 2 используют по умолчанию шрифты пакета `urw-fonts` с кириллическими глифами Валентина Филиппова. Эти же шрифты используются при печати из большинства приложений.

Мы рекомендуем также установить пакеты свободных шрифтов `sharatype-fonts` и `dmtr40in-fonts`, созданных Сергеем Шарашкиным (на основе шрифтов `bitstream`) и Дмитрием Сорокиным (оригинальный шрифт `XlinSans`).

Пакет шрифтов `cm-super`, созданный Владимиром Воловичем на основе шрифтов Ольги Лапко, является основным для нашего пакета `teTeX`, но, отчасти, может быть использован для отображения и печати. Система наименования шрифтов в *TeX* и библиотеках, работающих со шрифтами `Type1`, отличается, потому большинство этих прекрасных шрифтов пока недоступны вне *TeX*.

Наконец, в *ALT Linux Master 2.2* включены декоративные шрифты проекта *Vedi*[47]. Они не свободные, но бесплатные для многих применений, не забудьте ознакомиться с их лицензией.

True Type

Если вы используете сглаживание, то в установке шрифтов `True Type` нет большой необходимости. В противном случае, можно установить пакет `val-ttf`, созданный Валентином Филипповым на основе `urw-fonts`.

Шрифты фирмы *Monotype*, знакомые пользователям операционных систем `Windows`, мы не можем включать в коробочную версию дистрибутива из-за лицензионных ограничений, однако, пакет с ними доступен на нашем FTP в каталоге `updates`.

Для его установки достаточно с правами `root` дать команду

apt-get install ms-ttf

или воспользоваться программой synaptic. Внимательно ознакомьтесь с лицензией, поставляемой в этом пакете.

Сглаживание шрифтов.

По умолчанию сглаживание шрифтов включено в приложениях *Qt*/KDE, *Gtk+2*/GNOME и Mozilla. В WindowMaker, fvwm2, waimea, xjed оно также доступно, но по умолчанию выключено. В документации к соответсвующим пакетам (`/usr/share/doc/<имя пакета>-<версия>` вы можете прочитать о способах настройки шрифтов в этих приложениях.

Выключить сглаживание шрифтов в KDE и GNOME 2 можно через меню настроек этих систем, а также установив в «0» системные переменные `QT_XFT` и `GDK_USE_XFT` соответственно.

Установка шрифтов

Мы настоятельно рекомендуем всем пользователям тщательно проверять любые шрифты, не входящие в комплект *Master 2.2*, перед их установкой в системные каталоги, используя пользовательскую установку при помощи **xset [+|-]fp или fc-cache**, как это было описано выше в этой главе.

Если шрифты уже проверены, то лучший способ их установки — сборка шрифтового пакета на примере пакетов, входящих в Master

[47] http://vedi.d-s.ru

2.2. Если со сборкой таких пакетов возникают проблемы, то можно обратиться за консультацией в наши списки рассылки.

Часть VI. Печать

Глава 19. Введение

Электронный документооборот на протяжении нескольких последних лет все больше и больше набирает силу. Однако не менее актуальным остаётся и бумажная, «твёрдая» копия. Настроив компьютер, человек как правило первым же делом начинает устанавливать принтер. В этой главе вы узнаете, как настроить печать в дистрибутиве *Master*, какие препятствия вас ждут на пути и как их можно преодолеть. Сначала обсудим несколько общих вопросов, которые прольют свет на проблемы печати в `Linux`.

Какие виды принтеров бывают?

Инженерная мысль не останавливалась ни на секунду; с момента появления первого печатающего устройства опробована и введена в эксплуатацию масса новых технологий. На данный момент наиболее распространены следующие технологии печати:

матричные принтеры

Матричные принтеры постепенно доживают свой век, но, обладая удивительной простотой и надёжностью, продолжают ещё использоваться. С настройкой этого типа принтеров, за редкими исключениями, проблем не должно возникать.

лазерные принтеры

Лазерные принтеры обладают высокой скоростью печати, незаменимы в офисах организаций всех типов. Моделей существует множество, но, к счастью, для большинства можно найти «родной» драйвер или подобрать совместимый.

струйные принтеры

Главный лозунг струйных принтеров «дёшево и в цвете». Так как в этой индустрии не появилось явного лидера, то процветает множество стандартов и существует вероятность иметь очень экзотический с точки зрения `Linux` принтер.

GDI- или Windows-принтеры

«Дёшево любой ценой». Используют компьютер вместо того, чтобы все делать самим. Проблемы очень вероятны, так как протокол работы зачастую закрыт. К счастью, существуют несколько моделей имеющих интерфейс, напоминающий интерфейс полноценных принтеров, позволяющий все-таки производить печать с низким разрешением.

Где находится драйвер принтера?

Если вам доводилось работать в `Windows`™, то вы прекрасно знаете, что в комплекте с каждым принтером поставляется дискета или компакт-диск с драйвером для настройки печати. К великому сожалению, в мире UN*X пока так и не договорились о едином стандарте драйверов . В настоящее время стандартом де-факто является пакет GhostScript фирмы *Aladdin Software*.

Что такое GhostScript?

GhostScript (далее GS) — это программа перевода из векторного формата в растровый (RIP). На вход программы подаётся документ в формате *PostScript* или PDF, а на выходе получается документ на языке, понятном конкретной модели принтера или графическое изображение страницы. Большинство программ `Linux` формируют документ в формате *PostScript*, поэтому оказывается, что применения GS вполне достаточно для выполнения задач.

Что такое *PostScript*?

PostScript — это самый настоящий язык программирования, который используется для того, чтобы описать содержимое страницы. Например, пишутся такие серии команд: переместиться туда-то, напечатать слово такое-то, сменить шрифт на такой-то. Существуют модели принтеров, непосредственно понимающие *PostScript* для всех остальных требуется посредник, и GS успешно с этим справляется. Вы спросите, как он поддерживает столько принтеров? Дело в том, что количество языков принтеров намного меньше возможных моделей. Например, известные всем HP LaserJet `4`, `4L`, `5`, `5L`, `6`, `6L`, `1100`, `2100` «понимают» один и тот же язык PCL5. Если вы не страшитесь этих слов и вам любопытно посмотреть, какие драйвера языков поддерживает ваш GS — дайте команду **gs** `--help`. Так, например, ljet4 как раз и обслуживает вышеупомянутую линейку моделей принтеров.

Итак, теперь вам стало понятно, как устроена печать в любом дистрибутиве `Linux`: программа формирует документ, GS переводит его на язык принтера, установленного в вашей системе и передаёт эстафету принтеру.

Но это ещё далеко не всё. А что если вам надо послать документ на принтер, установленный на другой машине, или напечатать сразу несколько документов и нет времени ждать, пока каждый из них будет обслужен GhostScript и уступит место следующему? Для этого

существует так называемый сервер печати или спулер (*spooler*), обслуживающий очереди печати. Последний термин более точно отражает суть, поэтому им мы и будет пользоваться и писать дальше просто «спулер».

Глава 20. Спулер lpd

В UN*X стандартным спулером является lpd (Line Printer Daemon). Он состоит из сервера lpd и набора клиентских программ для работы с ним. Нас в первую очередь будут интересовать lpr, lpq и lprm.

lpr

lpr используется для отправки документа на печать. Если в вашей системе печать уже настроена, то можете дать команду **lpr мой_файл** для вывода на печать документа `мой_файл`. Если настроено несколько принтеров (например, printer1 и printer2), то для посылки документа на конкретный принтер следует добавить параметр `-P имя_принтера`, например для печати на принтере printer1 используйте команду **lpr -P printer1 мой_файл**.

lpq

lpq используется для просмотра очереди из всех посланных на печать заданий. Для этого дайте команду **lpq**. Если вас интересует состояние очереди конкретного принтера, то следует добавить ключ `-P имя_принтера`.

lprm

lprm удаляет из очереди последнее (или имеющее заданный идентификатор) задание.

Как видите, все гениально и просто. Все программы посылают документ на печать, запуская команду **lpr**, так что если у вас не работает печать из какого-нибудь офисного приложения, попробуйте вручную дать команду **lpr мой_файл**. Если печать прошла успешно, значит виновато само приложение — например, оно формирует неправильный файл в *PostScript*. Большие графические среды, такие как *GNOME* и *KDE* имеют свои общие интерфейсы печати. Поэтому если не печатают все приложения такой среды, значит что-то не так в ней. Кроме того если не получается распечатать из одной (например *GNOME*, из Gedit) попробуйте напечатать из другой (*KDE*, например Kedit).

Как всякий сервер, lpd имеет свой файл конфигурации. Выглядит он несколько жутковато (сказывается возраст программы), но его вполне можно понять. Находится он по адресу `/etc/printcap`. Описание каждого принтера пишется в одну строчку или несколько строк, разделённых символом \ непосредственно перед символом конца строки. Формат записи следующий:

```
<имя принтера> | <альтернативное имя> | <ещё одно имя> :
: <параметр> = <значение>::<параметр>:\
:<параметр>#<значение>
```

Все параметры двухбуквенные, чаще всего используются следующие:

`lp` (line printer)	устройство, к которому подсоединён принтер. Пример: lp=/dev/lp0
`sd` (spool directory)	каталог, где будут накапливаться задания, поставленные в очередь. Пример: sd=/var/spool/lpd
lf (log file)	файл журнала, в который будут записываться сообщения об ошибках. Пример: lf=/var/log/lpd/messages
if (input filter) фильтр	программа, через которую будет пропущен документ, прежде чем будет отправлен на принтер. Здесь и появляется GhostScript, который переводит на язык принтера. Устройство фильтра зависит от того, какая система настройки печати используется в системе, но общий принцип действия неизменный — на стандартный вход подаётся документ, а со стандартного вывода забирается результат.
sh (supress headers)	поскольку сервер используется для печати с нескольких машин, то перед и после документа, как правило, идут страницы с указанием, кому принадлежит это задание. Данная опция отключает эту возможность, так как на домашних машинах такое не требуется.
mx (maximum)	ограничение максимального размера файла. Если параметр установлен в ноль, то ограничений нет. Пример: mx#0
rp (remote printer)	имя удалённого принтера, на который будут уходить документы.
rm (remote machine)	имя машины на которой установлен этот принтер.

Вот пример файла `/etc/printcap`, настроенного на принтер HP LaserJet, подключённого к первому параллельному порту машины:

```
printer||HP LaserJet 6L||lp:\
:sd=/var/spool/lpd/printer:\
:lf=/var/log/lp-errs:\
:if=/usr/sbin/lpdomatic:\
:af=/etc/foomatic/lpd/printer.lom:\
:lp=/dev/lp0:\
:sh:\
:mx#0:
```

Если вы печатаете на удалённом принтере, то файл может выглядеть примерно следующим образом:

```
lp|dj|deskjet:\
:sd=/var/spool/lpd/dj:\
:rm=machine.out.there.com:\
:if=/usr/bin/filter:\
:rp=printername:\
:sh:
```

Более подробную информацию о значении параметров вы можете почерпнуть из страниц руководств *man*.

Глава 21. Спулер CUPS

Со времён первых версий lpd было предпринято несколько попыток сделать что-нибудь более гибкое и удобное в настройке. В *ALT Linux Master* помимо классического (и соответственно простого и лёгкого) lpd включена также могучая ультрасовременная система печати CUPS (Common Unix Printing System). Эта система печати постепенно завоёвывает все больше поклонников и практически уже стала новым стандартом среди спулеров.

Особенности CUPS

CUPS предоставляет достаточно много новых возможностей. Среди них:

Уникальная система настройки Вы просто запускаете свой любимый web-браузер, направляете его по адресу `http://localhost:631` — и перед вами красивый интерфейс, где вы можете удалить из системы или добавить в неё принтер, посмотреть очереди каждого из них, перезапустить уже выполненные задания и т.д.

Лёгкость настройки удалённой печати Если у вас в офисе уже есть настроенный CUPS-сервер, то вам ничего не надо больше настраивать. Все CUPS общаются между собой; ваш сервер узнает, что уже есть сосед с настроенным принтером и посылает сразу задание на него.

Поддержка самых современных и защищённых протоколов Основной протокол обмена данными между клиентом и сервером IPP, допустима печать через защищённое SSL-соединение.

Поддержка многих языков Старенький lpd мог печатать только в одном системном языке. CUPS может обслуживать пользователей с самыми различными кодировками.

Единая система хранения описаний принтеров, так называемые `PPD-файлы` Благодаря этому производитель может поставить это описание вместе с принтером (это, правда, не избавляет от необходимости иметь нужный драйвер в GhostScript).

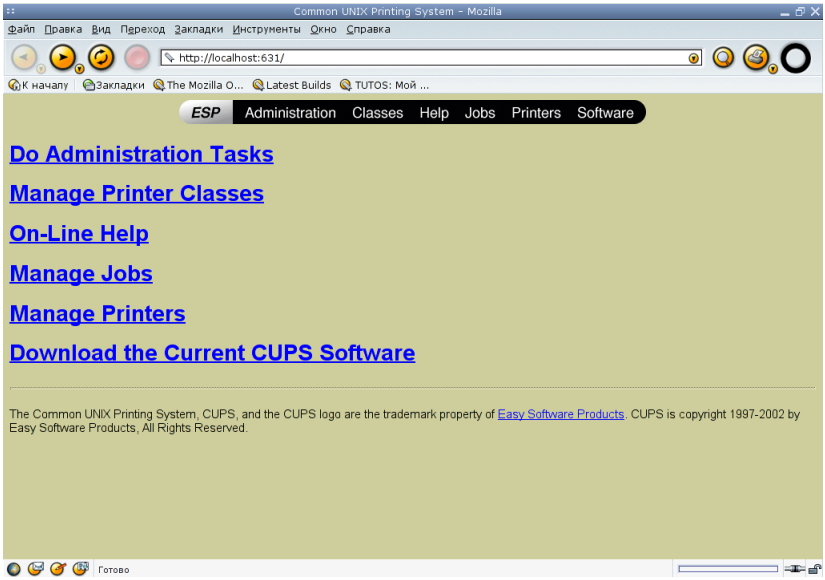

Рисунок 21.1. Настройка CUPS через web-интерфейс

Конфигурационные файлы CUPS

Конфигурационные файлы CUPS находятся в каталоге `/etc/cups` и формат их более понятен для пользователей. Файл `/etc/cups/cupsd.conf` содержит описание главных параметров сервера, каждый из которых сопровождается подробным описанием. Приведём некоторые, наиболее часто используемые из них:

- `LogLevel` — уровень подробности протоколирования. По умолчанию значение равно *info*. Если у вас какие-то проблемы с CUPS, а в протоколе нет ничего информативного, можете поднять уровень до максимального — *debug2*. Пример:

  ```
  LogLevel info
  ```

  .

- `Port` — TCP-порт, который будут использовать клиенты для соединения с сервером. По умолчанию это значение `631` (зарезервированное для протокола IPP). Пример:

  ```
  Port 631
  ```

  .

- `Location`, `Order`, `Allow`, `Deny` — серия директив, аналогичных имеющимся в web-сервере Apache. `Order` — порядок просмотра значений `Allow` и `Deny`, `Allow` — адреса, с которых разрешён доступ, `Deny` — адреса, с которых доступ запрещён. Пример:

```
<Location />
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
</Location>
```

  Это означает, что сначала сервер будет смотреть, запрещён ли доступ с машины (здесь запрещено для всех), а потом разрешён ли (здесь разрешён доступ только с самого сервера). Последний параметр понадобится вам для организации одного CUPS-сервера на всю организацию. Организация доступа может быть устроена сколь угодно сложно благодаря поддержке концепции классов.

Это означает, что сначала сервер будет смотреть, запрещён ли доступ с машины (здесь запрещено для всех), а потом разрешён ли (здесь разрешён доступ только с самого сервера). Последний параметр понадобится вам для организации одного CUPS-сервера на всю организацию. Организация доступа может быть устроена сколь угодно сложно благодаря поддержке концепции классов.

Файл `/etc/cups/client.conf` содержит настройки для клиентской части. В нём указываются всего два параметра — местоположение сервера и защищённость соединения. Скорее всего, вам не придётся там что-либо менять. менять.

Файл `/etc/cups/printers.conf` содержит описание принтеров. Формат записи интуитивно понятен и похож на XML. Ниже приведён пример настройки на локальный принтер.

```
<DefaultPrinter printer>
DeviceURI parallel:/dev/lp0
State Idle
Accepting Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
</Printer>
```

Существенными параметрами являются `Accepting` (принимает ли принтер задания) и `DeviceURI` (специальное описание местоположения принтера). О том как правильно составлять URI, будет рассказано ниже, когда речь пойдёт о foomatic.

Описание каждого установленного принтера (соответствующий PPD-файл) находится в `/etc/cups/ppd/<имя_принтера>.ppd`. При каждом старте сервер сканирует каталог `/usr/share/cups/model` на предмет появления новых описаний принтеров (PPD-файлов) и проверяет последовательные и параллельные порты компьютера. В связи с этим запуск занимает некоторое время.

Для посылки заданий на печать можно использовать ту же команду **lpr**, для просмотра очереди заданий — **lpq**. Для отмены задания используйте команду **cancel номер_задания**.

Глава 22. Настройка систем CUPS и lpd

Имеющихся знаний уже вполне хватит для того, чтобы попытаться настроить принтер вручную. Но это делать незачем, так как есть более удобные и наглядные способы.

Настройка CUPS через web-браузер

Запустите свой любимый браузер и зайдите по адресу http://localhost:631 (например, **lynx localhost:631**) — вы увидите интерфейс настройки CUPS. Выберите раздел «Manage Printers», далее раздел «Add Printer». Затем у вас спросят имя и пароль администратора CUPS; по умолчанию это администратор системы (`root`).

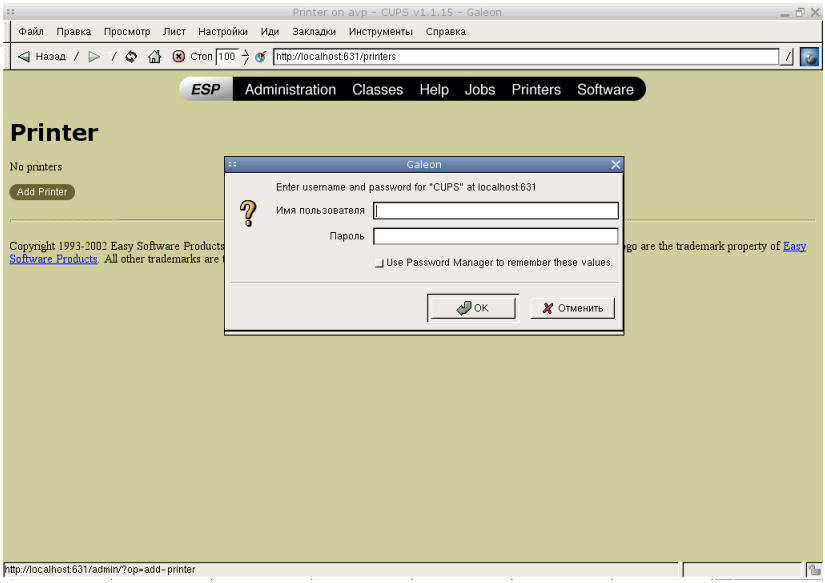

Рисунок 22.1. Вход на web-CUPS для администратора

Появится первый диалог — достаточно указать имя (Name) принтера, описание (Description) носит вспомогательный характер, а местоположение (Location) нужно только, если у вас настроена сложная система разграничения доступа в CUPS.

В следующем диалоге производится выбор устройства, к которому подключен принтер.

Два последующих — выбор модели и производителя принтера. Описания моделей (PPD) находятся в каталоге `/usr/share/cups/model`. Если вы видите подозрительно мало моделей, доустановите пакет cups-drivers. Обратите внимание на то, что этот пакет конфликтует с пакетом foomatic — другой системой настройки, поэтому определитесь, какой метод будете использовать.

Напоследок вы можете заказать печать пробной страницы.

Настройка CUPS и lpd через foomatic

Сложно дать краткое описание того, что же такое foomatic. Это и база описаний моделей принтеров, и интерфейс настройки одновременно. Более того, foomatic умеет настраивать практически все известные на сегодняшний день спулеры, в частности CUPS и lpr.

Процедуру настройки лучше всего рассмотреть на конкретном примере. Пусть мы хотим настроить printer HP LaserJet 1100, расположенный на `Windows`™-машине `SOMEHOST` в рабочей группе `SOMEGROUP` под именем `SOMEPRINTER`.

1. Шаг1. Сформируем URI, описывающее расположение принтера. Общий формат <протокол>://<местоположение>. Местоположение зависит от протокола:
   Если удаленный сервер совместим с lpd, то URI имеет вид : `lpd://имя_машины/имя_принтера`
   Если принтер подключен локально, то URI — `file://путь_к_файлу`, в частности может быть указан файл-устройство (например, `/dev/lp0`.
   D1 Если удаленный сервер работает под управлением `Windows`™ (наш случай), то URI — `smb://user:password@SOMEGROUP/SOMEHOST/SOMEPRINTER`. Некоторые поля в описании могут отсутствовать.
   Наконец, в случае Netware-сервера URI — `ncp://user:password@SERVER/PRINTER`
2. Шаг2. Посмотрим доступные описания моделей принтеров. Для этого запустим команду **foomatic-configure -O | less**. Описание будет выведено на экран в формате XML. Выделим подходящее описание:

```
<printer>
<id>62816</id>
<make>HP</make>
<model>LaserJet 1100</model>
<functionality>A</functionality>
<autodetect>
<parallel>
<commandset>MLC,PCL,PJL</commandset>
<description>HP LaserJet 1100
Printer</description>
<manufacturer>Hewlett-Packard</manufacturer>
<model>HP LaserJet 1100</model>
</parallel>
</autodetect>
<drivers>
<driver>ljet4</driver>
<driver>stp</driver>
</drivers>
</printer>
```

Нас прежде всего интересует идентификатор-описание, заключенный в теги <id> — в нашем случае это 62816. Выберем также драйвер GhostScript™ — выбор того или иного драйвера дело опыта и вкуса. Мы остановимся на ljet4 — основной рабочей лошадке всего этого семейства принтеров.

3. Шаг3. Мы собрали теперь достаточно информации для того чтобы произвести конфигурацию принтера. Это делается одной командой foomatic-configure. Мы укажем желаемый спулер (параметр `-s`), имя принтера (параметр `-n`) идентификатор описания, драйвер и URI.
   **foomatic-configure -s cups -n Laser_Jet -p 62816 -d ljet4 -c **
   smb://user:password@SOMEGROUP/SOMEHOST/SOMEPRINTER

Вот и все готово. Настройки можете посмотреть непосредственно в конфигурационных файлах спулера или при помощи команды **foomatic-configure -Q**. Данная программа на моей машине сообщила следующее:

```
<defaultqueue>printer</defaultqueue>
<queue foomatic="1" spooler="cups">
<name>Laser_Jet</name>
<printer>62816</printer>
```

```
    <driver>ljet4</driver>
   ↩
<connect>smb://user:password@SOMEGROUP/SOMEHOST/SOMEPRINTER</connect>
    <description>HP LaserJet 1100</description>
    </queue>
    <queue foomatic="0" spooler="cups">
    <name>lexmark</name>
    <connect>file:/dev/lp0</connect>
    </queue>
    <queue foomatic="1" spooler="cups">
    <name>printer</name>
    <printer>62368</printer>
    <driver>ljet4</driver>
    <connect>file:/dev/lp0</connect>
    </queue>
    </queues>
```

Все понятно без лишних комментариев.

Настройка CUPS и lpd с помощью printerdrake

В составе пакета drakxtools имеется утилита настройки принтера printerdrake; фактически это интерфейс над описанным выше foomatic. Полезно помнить следующие дополнительные аргументы printerdrake:

- `--expert` — конфигуратор запускается в режиме «Эксперт» — . Вам будут задавать больше вопросов, но зато вы сможете произвести более тонкие настройки;
- `--lpd` — в качестве спулера будет использоваться lpd;
- `--cups` — в качестве спулера будет использоваться CUPS.

При задании принтера вы пройдете через несколько диалогов: выбор действия, выбор местоположения принтера, уточнение местоположения (например, пароля и имени для доступа к удаленному серверу), задание имени принтера, выбор модели принтера и драйвера, печать тестовых страниц.

Все диалоговые окна интуитивно понятны, приведем лишь несколько примеров. Итак, диалог выбора действия:

Диалог выбора типа подключения принтера, вам скорее всего подойдет локальное подключение:

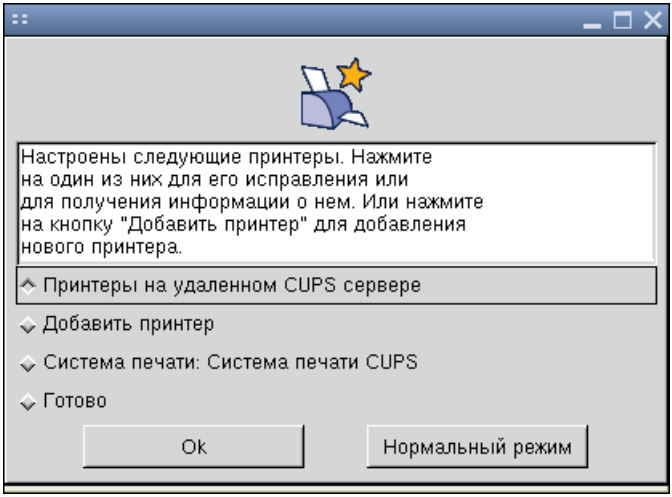

Рисунок 22.2. Диалог выбора действия

Диалог, предлагающий распечатать тестовую страницу. Если вы загрузили printerdrake в режиме «Эксперт», то вам будет предложено два варианта страниц, иначе один. На самом деле одной страницы вполне достаточно.

Еще один момент. Перед запуском printerdrake проверяет установленное программное обеспечение и доустанавливает, если это необходимо, необходимые пакеты. В частности, если вы установили GIMP, то printerdrake дополнительно поставит дополнительные драйверы gimp-print.

Как удалить лишние принтеры?

Если вы слишком увлеклись настройками и теперь путаетесь между десятком заведенных принтеров, то самое время удалить лишние.

Удаление можно производить вручную удалением описания из конфигурационых файлов спулера (для lpd это `/etc/printcap`, для CUPS — `/etc/cups/printers.conf`). Для CUPS можно вновь воспользоваться Web-интерфейсом. Если вы использовали foomatic (или printerdrake), то полезно знать команду

foomatic-configure -s тип_спулера -n имя_принтера -R

где тип_спулера — CUPS или lpd.

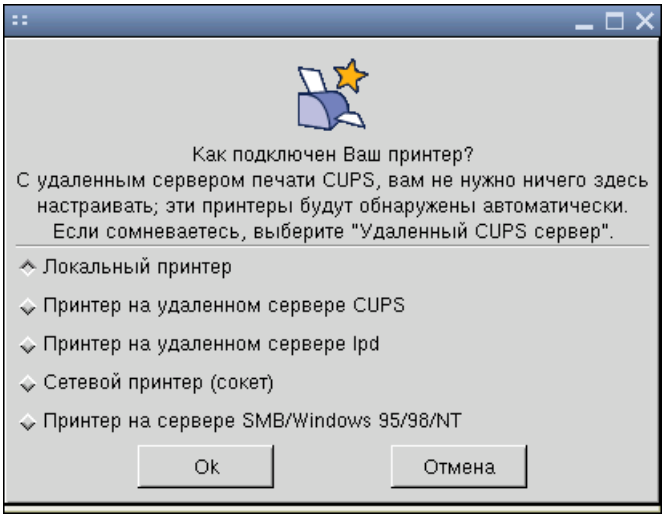

Рисунок 22.3. Выбор локального типа подключения принтера

Глава 23. Резюме

Подведём итоги. Система печати в `Linux` состоит из трёх составных частей:

1. Интерфейс настройки printerdrake, foomatic)
2. Спулер (CUPS, lpd)
3. Фильтр (GhostScript)

Для качественной печати из графического редактора GIMP да и вообще для печати на струйных принтерах полезно воспользоваться пакетом gimp-print; он делится на три составных части: плагин для GIMP, описания принтеров в формате PPD, описания принтеров в формате foomatic. После установки пакета у вас появится пункт «Print» в меню GIMP, а также возможность выбрать новый драйвер gimp-print при настройке печати. Обязательно попробуйте этот драйвер, в большинстве случаев качество печати будет выше.

Рисунок 23.1. Настройка gimp-print

Если вы используете CUPS и не желаете печатать через lpr, то к вашим услугам его графические аналоги qtcups и xpp. Последний, помимо всего прочего, позволяет задать большое количество дополнительных настроек для сервера CUPS.

Что выбрать — CUPS или lpd? Сложный вопрос. Если вы настраиваете систему через foomatic, то последний сглаживает различия между различными системами печати и тут лучше выбрать то, что лучше подходит к вашим задачам. Если вы великолепно настраиваете вручную один спулер, а другой не умеете — выбирайте то, что знаете. CUPS имеет много полезных функций и незаменим в сетях с большим количеством пользователей. lpd, в свою очередь, более лёгок на подъём, проще устроен и, возможно, лучше подходит для рабочей станции с локально подключённым принтером.

Перевод на русский язык лицензии GNU на свободную документацию

История переиздания
Издание 0.1 9 Aug 2001

Текст GFDL на английском языке вы можете прочитать здесь: `http://www.gnu.org/copyleft/fdl.html`

GNU Free Documentation License

История переиздания
Издание 1.1 март 2001 г.

Каждый вправе копировать и распространять экземпляры настоящей Лицензии без внесения изменений в ее текст.

0. Преамбула

Цель настоящей Лицензии — сделать свободными справочник, руководство пользователя или иные документы в письменной форме, т.е. обеспечить каждому право свободно копировать и распространять как с изменениями, так и без изменений, за вознаграждение или бесплатно указанные документы. Настоящая Лицензия также позволяет авторам или издателям документа сохранить свою репутацию, не принимая на себя ответственность за изменения, сделанные третьими лицами.

Настоящая Лицензия относится к категории «copyleft» [54]. Это означает, что все произведения, производные от документа, должны быть свободными в соответствии с концепцией «copyleft». Настоящая Лицензия дополняет General Public License GNU, которая является лицензией «copyleft», разработанной для свободного программного обеспечения.

Настоящая Лицензия разработана для применения ее к документации на свободное программное обеспечение, поскольку свободное программное обеспечение должно сопровождаться свободной документацией. Пользователь должен обладать теми же правами в отношении руководства пользователя, какими он обладает в отношении свободного программного обеспечения. При этом действие настоящей Лицензии не распространяется только на руководство пользователя. Настоящая Лицензия может применяться к любому текстовому произведению независимо от его темы или от того, издано ли данное произведение в виде печатной книги или нет. Настоящую Лицензию рекомендуется применять для произведений справочного или обучающего характера.

1. Сфера действия, термины и их определения

Условия настоящей Лицензии применяются к любому руководству пользователя или иному произведению, которое в соответствии с уведомлением, помещенным правообладателем, может распространяться на условиях настоящей Лицензии. Далее под термином «Документ» понимается любое подобное руководство пользователя или произведение. Лицо, которому передаются права по настоящей Лицензии, в дальнейшем именуется «Лицензиат».

«Модифицированная версия Документа» — любое произведение, содержащее Документ или его часть, скопированные как с изменениями, так и без них и/или переведенные на другой язык.

[54] Термин «copyleft» используется авторами проекта GNU Free Software Foundation в качестве одного из основных понятий в концепции свободного программного обеспечения (free software). Данный термин образуется за счет замены в английском языке термина «copyright» (авторское право) на «copyleft». Как указывают авторы проекта, «copyleft» — это наиболее общий способ сделать программное обеспечение свободным и обеспечить соблюдение условий, в соответствии с которыми все измененные и распространяемые версии программного обеспечение также сохраняли бы статус свободного программного обеспечения. Более подробно о концепции «copyleft» вы можете прочитать здесь: `http://www.gnu.org/copyleft/copyleft.html`. *(прим. перев.)*

«Второстепенный раздел» — имеющее название приложение или предисловие к Документу, в котором отражено исключительно отношение издателей или авторов Документа к его содержанию в целом, либо к вопросам, связанным с содержанием Документа. Второстепенный раздел не может включать в себя то, что относится непосредственно к содержанию Документа. (Например, если часть Документа является учебником по математике, во Второстепенном разделе не может содержаться что-либо имеющее отношение непосредственно к математике). Во Второстепенных разделах могут быть затронуты вопросы истории того, что составляет содержание или что связано с содержанием Документа, а также правовые, коммерческие, философские, этические или политические взгляды относительно содержания Документа.

«Неизменяемые разделы» — определенные Второстепенные разделы, названия которых перечислены как Неизменяемые разделы в уведомлении Документа, определяющем лицензионные условия.

«Текст, помещаемый на обложке» — определенные краткие строки текста, которые перечислены в уведомлении Документа, определяющем лицензионные условия, как текст, помещаемый на первой и последней страницах обложки.

«Прозрачный» экземпляр Документа — экземпляр Документа в машиночитаемой форме, представленный в формате с общедоступной спецификацией при условии, что документ может просматриваться и редактироваться непосредственно с помощью общедоступных текстовых редакторов или общедоступных программ для векторной или растровой графики (в случае, если в документе содержатся изображения векторной или растровой графики). Указанный формат должен обеспечить ввод текста Документа в программы форматирования текста или автоматический перевод Документа в различные форматы, подходящие для ввода текста Документа в программы форматирования текста. Экземпляр Документа, представленный в ином формате, разметка которого затрудняет или препятствует внесению в Документ последующих изменений пользователями, не является Прозрачным. Такой экземпляр документа называется *«Непрозрачным»*.

Форматы, в которых может быть представлен Прозрачный экземпляр Документа, включают простой формат ASCII без разметки, формат ввода Texinfo, формат ввода LaTeX, SGML или XML с использованием общедоступного DTD, а также соответствующий стандартам простой формат HTML, предназначений для внесения модификаций человеком. «Непрозрачные» форматы включают в себя PostScript, PDF, форматы, которые можно прочитать и редактировать только с

помощью текстовых редакторов, права на использование которых свободно не передаются, форматы SGML или XML, для которых DTD или инструменты для обработки не являются общедоступными, а также генерируемый машиной HTML, который вырабатывается некоторыми текстовыми редакторами исключительно в целях вывода.

«Титульный лист» — для печатной книги собственно титульный лист, а также следующие за ним страницы, которые должны содержать сведения, помещаемые на титульном листе в соответствии с условиями настоящей Лицензии. Для произведений, формат которых не предполагает наличие титульного листа, под Титульным листом понимается текст, который помещен перед началом основного текста произведения, после его названия, напечатанного наиболее заметным шрифтом.

2. Копирование без внесения изменений

Лицензиат вправе воспроизводить и распространять экземпляры Документа на любом носителе за вознаграждение или безвозмездно при условии, что каждый экземпляр содержит текст настоящей Лицензии, знаки охраны авторских прав, а также уведомление, что экземпляр распространяется в соответствии с настоящей Лицензией, при этом Лицензиат не вправе предусматривать иные лицензионные условия дополнительно к тем, которые закреплены в настоящей Лицензии. Лицензиат не вправе использовать технические средства для воспрепятствования или контроля за чтением или последующим изготовлением копий с экземпляров, распространяемых Лицензиатом. Лицензиат вправе получать вознаграждение за изготовление и распространение экземпляров Документа. При распространении большого количества экземпляров Документа Лицензиат обязан соблюдать условия пункта 3 настоящей Лицензии.

Лицензиат вправе сдавать экземпляры Документа в прокат на условиях, определенных в предыдущем абзаце, или осуществлять публичный показ экземпляров Документа.

3. Тиражирование

Если Лицензиат издает печатные экземпляры Документа в количестве свыше 100, и в соответствии с уведомлением Документа, определяющем лицензионные условия, Документ должен содержать Текст,

помещаемый на обложке, Лицензиат обязан издавать экземпляры Документа в обложке с напечатанными на ней ясно и разборчиво соответствующими Текстами, помещаемыми на обложке: Тексты, помещаемые на первой странице обложки — на первой странице, Тексты, помещаемые на последней странице — соответственно на последней. Также на первой и последней странице обложки экземпляра Документа должно быть ясно и разборчиво указано, что Лицензиат является издателем данных экземпляров. На первой странице обложки должно быть указано полное название Документа без пропусков и сокращений, все слова в названии должны быть набраны шрифтом одинакового размера. Лицензиат вправе поместить прочие сведения на обложке экземпляра. Если при издании экземпляров Документа изменяются только сведения, помещенные на обложке экземпляра, за исключением названия Документа, и при этом соблюдаются требования настоящего пункта, такие действия приравниваются к копированию без внесения изменений.

Если объем текста, который должен быть помещен на обложке экземпляра, не позволяет напечатать его разборчиво, Лицензиат обязан поместить разумную часть текста непосредственно на обложке, а остальной текст на страницах Документа, следующих сразу за обложкой.

Если Лицензиат издает или распространяет Непрозрачные экземпляры Документа в количестве свыше 100, Лицензиат обязан к каждому такому экземпляру приложить Прозрачный экземпляр этого Документа в машиночитаемой форме или указать на каждом Непрозрачном экземпляре Документа адрес в компьютерной сети общего пользования, где содержится Прозрачный экземпляр без каких-либо добавленных материалов, полный текст которого каждый пользователь компьютерной сети общего пользования вправе бесплатно, не называя своего имени и не регистрируясь, записать в память компьютера с использованием общедоступных сетевых протоколов. Во втором случае Лицензиат обязан предпринять разумные шаги с тем, чтобы доступ к Прозрачному экземпляру Документа по указанному адресу сохранялся по крайней мере в течение одного года после последнего распространения Непрозрачного экземпляра Документа данного тиража, независимо от того, было ли распространение осуществлено Лицензиатом непосредственно или через агентов или розничных продавцов.

Прежде чем начать распространение большого количества экземпляров Документа Лицензиату заблаговременно следует связаться с авторами Документа, чтобы они имели возможность предоставить Лицен-

зиату обновленную версию Документа. Лицензиат не обязан выполнять данное условие.

4. Внесение изменений

Лицензиат вправе воспроизводить и распространять Модифицированные версии Документа в соответствии с условиями пунктов 2 и 3 настоящей Лицензии, при условии что Модифицированная версия Документа публикуется в соответствии с настоящей Лицензией. В частности, Лицензиат обязан передать каждому обладателю экземпляра Модифицированной версии Документа права на распространение и внесение изменений в данную Модифицированную версию Документа, аналогично правам на распространение и внесение изменений, которые передаются обладателю экземпляра Документа. При распространении Модифицированных версий Документа Лицензиат обязан:

A. поместить на Титульном листе и на обложке при ее наличии название Модифицированной версии, отличающееся от названия Документа и названий предыдущих версий. Названия предыдущих версий при их наличии должны быть указаны в Документе в разделе «История». Лицензиат вправе использовать название предыдущей версии Документа с согласия издателя предыдущей версии;
B. указать на Титульном листе в качестве авторов тех лиц, которые являются авторами изменений в Модифицированной версии, а также не менее пяти основных авторов Документа либо всех авторов, если их не более пяти;
C. указать на Титульном листе наименование издателя Модифицированной версии, с указанием, что он является издателем данной Версии;
D. сохранить все знаки охраны авторского права Документа;
E. поместить соответствующий знак охраны авторского права на внесенные Лицензиатом изменения рядом с прочими знаками охраны авторского права;
F. поместить непосредственно после знаков охраны авторского права уведомление, в соответствии с которым каждому предоставляется право использовать Модифицированную Версию в соответствии с условиями настоящей Лицензии. Текст уведомления приводится в Приложении к настоящей Лицензии;
G. сохранить в уведомлении, указанном в подпункте F, полный список Неизменяемых разделов и Текста, помещаемого на обложке, перечисленных в уведомлении Документа;

H. включить в Модифицированную версию текст настоящий Лицензии без каких-либо изменений;

I. сохранить в Модифицированной версии раздел «История», включая его название, и дополнить его пунктом, в котором указать так же, как данные сведения указаны на Титульном листе, название, год публикации, наименования новых авторов и издателя Модифицированной версии. Если в Документе отсутствует раздел «История», Лицензиат обязан создать в Модифицированной версии такой раздел, указать в нем название, год публикации, авторов и издателя Документа так же, как данные сведения указаны на Титульном листе Документа и дополнить этот раздел пунктом, содержание которого описано в предыдущем предложении;

J. сохранить в Модифицированной версии адрес в компьютерной сети, указанный в Документе, по которому каждый вправе осуществить доступ к Прозрачному экземпляру Документа, а также адрес в компьютерной сети, указанный в Документе, по которому можно получить доступ к предыдущим версиям Документа. Адреса, по которым находятся предыдущие версии Документа, можно поместить в раздел «История». Лицензиат вправе не указывать адрес произведения в компьютерной сети, которое было опубликовано не менее чем за четыре года до публикации самого Документа. Лицензиат вправе не указывать адрес определенной версии в компьютерной сети с разрешения первоначального издателя данной версии;

K. сохранить без изменений названия разделов «Благодарности» или «Посвящения», а также содержание и стиль каждой благодарности и/или посвящения;

L. сохранить без изменений названия и содержание всех Неизменяемых разделов Документа. Нумерация данных разделов или иной способ их перечисления не включается в состав названий разделов;

M. удалить существующий раздел Документа под названием «Одобрения». Такой раздел не может быть включен в Модифицированную версию;

N. не присваивать существующим разделам Модифицированной версии название «Одобрения» или такие названия, которые повторяют название любого из Неизменяемых разделов.

Если в Модифицированную версию включены новые предисловия или приложения, которые могут быть определены как Второстепенные разделы и которые не содержат текст, скопированный из Документа,

Лицензиат вправе по своему выбору определить все или некоторые из этих разделов как Неизменяемые. Для этого следует добавить их названия в список Неизменяемых разделов в уведомлении в Модифицированной версии, определяющем лицензионные условия. Названия данных разделов должны отличаться от названий всех остальных разделов.

Лицензиат вправе дополнить Модифицированную версию новым разделом «Одобрения» при условии, что в него включены исключительно одобрения Модифицированной версии Документа третьими сторонами, например оценки экспертов или указания, что текст Модифицированной версии был одобрен организацией в качестве официального определения стандарта.

Лицензиат вправе дополнительно поместить на обложке Модифицированной версии Текст, помещаемый на обложке, не превышающий пяти слов для первой страницы обложке и 25 слов для последней страницы обложки. К Тексту, помещаемому на обложке, каждым лицом непосредственно или от имени этого лица на основании соглашения с ним может быть добавлено только по одной строке на первой и на последней страницах обложки. Если на обложке Документа Лицензиатом от своего имени или от имени лица, в интересах которого действует Лицензиат, уже был помещен Текст, помещаемый на обложке, Лицензиат не вправе добавить другой Текст. В этом случае Лицензиат вправе заменить старый текст на новый с разрешения предыдущего издателя, который включил старый текст в издание.

По настоящей Лицензии автор(ы) и издатель(и) Документа не передают право использовать их имена и/или наименования в целях рекламы или заявления или предположения, что любая из Модифицированных Версий получила их одобрение.

5. Объединение документов

Лицензиат с соблюдением условий п. 4 настоящей Лицензии вправе объединить Документ с другими документами, которые опубликованы на условиях настоящей Лицензии, при этом Лицензиат должен включить в произведение, возникшее в результате объединения, все Неизменяемые разделы из всех первоначальных документов без внесения в них изменений, а также указать их в качестве Неизменяемых разделов данного произведения в списке Неизменяемых разделов, который содержится в уведомлении, определяющем лицензионные условия для произведения.

Произведение, возникшее в результате объединения, должно содержать только один экземпляр настоящей Лицензии. Повторяющиеся в

произведении одинаковые Неизменяемые разделы могут быть заменены единственной копией таких разделов. Если произведение содержит несколько Неизменяемых Разделов с одним и тем же названием, но с разным содержанием, Лицензиат обязан сделать название каждого такого раздела уникальным путем добавления после названия в скобках уникального номера данного раздела или имени первоначального автора или издателя данного раздела, если автор или издатель известны Лицензиату. Лицензиат обязан соответственно изменить названия Неизменяемых разделов в списке Неизменяемых разделов в уведомлении, определяющем лицензионные условия для произведения, возникшего в результате объединения.

В произведении, возникшем в результате объединения, Лицензиат обязан объединить все разделы «История» из различных первоначальных Документов в один общий раздел «История». Подобным образом Лицензиат обязан объединить все разделы с названием «Благодарности» и «Посвящения». Лицензиат обязан исключить из произведения все разделы под названием «Одобрения».

6. Сборники документов

Лицензиат вправе издать сборник, состоящий из Документа и других документов, публикуемых в соответствии с условиями настоящей Лицензии. В этом случае Лицензиат вправе заменить все экземпляры настоящей Лицензии в документах одним экземпляром, включенным в сборник, при условии, что остальной текст каждого документа включен в сборник с соблюдением условий по осуществлению копирования без внесения изменений.

Лицензиат вправе выделить какой-либо документ из сборника и издать его отдельно в соответствии с настоящей Лицензией, при условии, что Лицензиатом в данный документ включен текст настоящей Лицензии и им соблюдены условия Лицензии по осуществлению копирования без внесения изменений в отношении данного документа.

7. Подборка документа и самостоятельных произведений

Размещение Документа или произведений, производных от Документа, с другими самостоятельными документами или произведениями на одном устройстве для хранения информации или носителе не

влечет за собой возникновения Модифицированной версии Документа, при условии, что Лицензиат не заявляет авторских прав на осуществленный им подбор или расположение документов при их размещении. Такое размещение называется *«Подборкой»*, при этом условия настоящей Лицензии не применяются к самостоятельным произведениям, размещенным вышеуказанным способом вместе с Документом, при условии, что они не являются произведениями, производными от Документа.

Если условия пункта 3 настоящей Лицензии относительно Текста, помещаемого на обложке, могут быть применены к экземплярам Документа в Подборке, то в этом случае Текст с обложки Документа может быть помещен на обложке только собственно Документа внутри подборки при условии, что Документ занимает менее четвертой части объема всей Подборки. Если Документ занимает более четвертой части объема Подборки, в этом случае Текст с обложки Документа должен быть помещен на обложке всей Подборки.

8. Перевод

Перевод является одним из способов модификации Документа, в силу чего Лицензиат вправе распространять экземпляры перевода Документа в соответствии с пунктом 4 настоящей Лицензии. Замена Неизменяемых разделов их переводами может быть осуществлена только с разрешения соответствующих правообладателей, однако Лицензиат вправе в дополнение к оригинальным версиям таких Неизменяемых разделов включить в текст экземпляра перевод всех или части таких Разделов. Лицензиат вправе включить в текст экземпляра перевод настоящей Лицензии при условии, что в него включен также и оригинальный текст настоящей Лицензии на английском языке. В случае разногласий в толковании текста перевода и текста на английском языке предпочтение отдается тексту Лицензии на английском языке.

9. Расторжение лицензии

Лицензиат вправе воспроизводить, модифицировать, распространять или передавать права на использование Документа только на условиях настоящей Лицензии. Любое воспроизведение, модификация, распространение или передача прав на иных условиях являются недействительными и автоматически ведут к расторжению настоящей Лицензии и прекращению всех прав Лицензиата, предоставленных ему

настоящей Лицензией. При этом права третьих лиц, которым Лицензиат в соответствии с настоящей Лицензией передал экземпляры Документа или права на него, сохраняются в силе при условии полного соблюдения ими настоящей Лицензии.

10. Пересмотр условий лицензии

Free Software Foundation может публиковать новые исправленные версии GFDL. Такие версии могут быть дополнены различными нормами, регулирующими правоотношения, которые возникли после опубликования предыдущих версий, однако в них будут сохранены основные принципы, закрепленные в настоящей версии (смотри `http://www/gnu.org/copyleft/`).

Каждой версии присваивается свой собственный номер. Если указано, что Документ распространяется в соответствии с определенной версией, т.е. указан ее номер, или любой более поздней версией настоящей Лицензии, Лицензиат вправе присоединиться к любой из этих версий Лицензии, опубликованных Free Software Foundation (при условии, что ни одна из версий не является проектом Лицензии). Если Документ не содержит такого указания на номер версии Лицензии Лицензиат вправе присоединиться к любой из версий Лицензии, опубликованных когда-либо Free Software Foundation (при условии, что ни одна из версий не является Проектом Лицензии).

Порядок применения условий настоящей Лицензии к вашей документации

Чтобы применить условия настоящей Лицензии к созданному вами документу, вам следует включить в документ текст настоящей Лицензии, а также знак охраны авторского права и уведомление, определяющее лицензионные условия, сразу после титульного листа документа в соответствии с нижеприведенным образцом:

© имя (наименование) автора или иного правообладателя, год первого опубликования документа
Каждый имеет право воспроизводить, распространять и/или вносить
изменения в настоящий Документ в соответствии с условиями GNU Free
Documentation License, Версией 1.1 или любой более поздней версией,

опубликованной Free Software Foundation;
Данный Документ содержит следующие Неизменяемые разделы, (указать
названия Неизменяемых разделов); данный документ содержит следующий
Текст, помещаемый на первой странице обложки (перечислить),
данный документ содержит следующий Текст, помещаемый на последней
странице обложки (перечислить).
Копия настоящей Лицензии включена в раздел под названием "GNU Free
Documentation License".

Если документ не содержит Неизменяемых разделов, укажите «Данный документ не содержит Неизменяемых разделов». Если документ не содержит Текста, помещаемого на первой или последней страницах обложки, укажите «Данный документ не содержит Текста, помещаемого на первой странице обложки», соответственно укажите для последней страницы обложки.

Если ваш документ содержит имеющие существенное значение примеры программного кода, мы рекомендуем вам выпустить их отдельно в соответствии с условиями одной из лицензий на свободное программное обеспечение, например GNU General Public License, чтобы их можно было использовать как свободное программное обеспечение.

Содержание

Список иллюстраций

Список примеров