В. В. БРУЙ, С. В. КАРЛОВ

LINUX- СЕРВЕР:
ПОШАГОВЫЕ ИНСТРУКЦИИ
ИНСТАЛЛЯЦИИ И НАСТРОЙКИ

Москва
Издательство СИП РИА
2003

УДК 519.248+658.562+681.51
ББК 32.817
Б 67

Бруй В. В. , Карлов С. В.
Б67 LINUX-сервер: пошаговые инструкции инсталляции и настройки. –
М.: Изд-во СИП РИА, 2003. – 572 с.
ISBN 5-89354-153-7

В книге в доступной для неподготовленного читателя форме рассматривается процесс инсталляции и настройки Linux-серверов различного целевого назначения и следующего программного обеспечения:

GnuPG, OpenSSL, OpenSSH – криптографического программного обеспечения, используемого для безопасной передачи данных, проверки подлинности и целостности электронных документов, администрирования удаленных систем;

Sudo, sXid, LogSentry, HostSentry, PortSentry, Snort, ucspi-tcp, xinetd, NTP – программного обеспечения для ограничения доступа к серверу, анализа файлов регистрации и обнаружения попыток деструктивного воздействия;

ISC BIND – программного обеспечения для организации службы DNS;

Squid, SquidGuard, VPN-сервер FreeS/WAN, PPTP-клиент – программного обеспечения, используемого для организации шлюза из локальных сетей в Интернет и объединения локальных сетей с помощью сетей общего пользования;

Exim, Qpopper, SpamAssassin, Doctor Web – программного обеспечения, используемого для организации службы электронной почты с поддержкой фильтрации сообщений, содержащих спам и вирусы;

MySQL – сервера баз данных;

ProFTPD, vsFTPD – программного обеспечения, предназначенного для организации FTP-сервера;

Apache HTTP Server, PHP, mod_perl – программного обеспечения, предназначенного для организации Web-сервера;

Samba – программного обеспечения, используемого для организации совместного доступа к общим сетевым ресурсам (файлам, каталогам и принтерам).

Примеры конфигурационных файлов доступнны на сервере `http://www.bruy.info`.

Книга может оказаться полезной для начинающих системных администраторов и пользователей, желающих более детально ознакомиться с операционной системой Linux.

УДК 519.248+658.562+681.51
ББК 32.817
Б67

ISBN 5-89354-153-7

Оглавление

Введение

Глава 1

Введение или кому и зачем нужна эта книга

В этой главе:

1. Кому нужна эта книга
2. Почему была написана эта книга
3. Пример использования Linux-серверов для организации корпоративной сети
4. Какое программное обеспечение должно быть установлено на сервере
5. Как пользоваться этой книгой
6. Куда обращаться за помощью и технической поддержкой
7. Благодарности

В этой главе содержится важная информация, которая может оказаться незаменимой при принятии решения о необходимости приобретения книги. Кроме того, в первой главе этой книги содержится перечень программного обеспечения необходимого для инсталляции серверов различного назначения и инструкции по использованию этой книги.

Кому и зачем нужна эта книга

Вполне возможно, что эти строки вы читаете по одной из следующих причин:

- в вашем офисе появился канал выделенного доступа в Интернет, и вы не совсем четко представляете, как организовать доступ пользователей локальной сети в Интернет, обеспечив при этом защиту внутренних ресурсов от несанкционированного доступа из вне и установив требуемые ограничения (достаточные для выполнения служебных обязанностей сотрудниками офиса и сводящие к минимуму затраты на оплату услуг доступа в Интернет) на использование внешних ресурсов;
- в вашем офисе необходимо наладить совместное использование сетевых ресурсов (файлов, принтеров) с четким разграничением полномочий различных пользователей и групп пользователей;
- вы, используя имеющийся канал выделенного доступа, хотите организовать представительство вашей компании в Интернет с поддержкой таких служб, как Web-сервер, электронная почта, FTP-сервер и др.;
- вы намерены оградить ваших пользователей от спамерских сообщений, содержащих большое количество никому не нужной информации и отвлекающих их от работы;
- вам необходимо связать в единую сеть локальные сети нескольких офисов, используя сети общего пользования и сохраняя при этом конфиденциальность передаваемой служебной информации;
- имеющиеся в вашем распоряжении сервера не могут обеспечить требуемую производительность при обслуживании клиентских запросов, и вы ищете возможные пути ее повышения при наличии жестких ограничений на объем средств, выделяемых вашей компанией на модернизацию вычислительной техники;
- вы хотите вывести компанию из под удара силовых структур (финансируемых за счет ваших налоговых отчислений в бюджеты различных уровней), руками которых ведущие зарубежные производители программного обеспечения защищают свои права на интеллектуальную собственность, путем замены нелицензионных копий коммерческих программных продуктов на свободно распространяемое программное обеспечение;
- вы просто хотите более детально ознакомиться с операционной системой Linux, оценить её возможности и начать использовать для решения стоящих перед вами задач.

В нашей книге вы найдете ответы на эти и другие вопросы в виде пошаговых инструкций по инсталляции и настройке Linux-сервера. Эти инструкции рассчитаны на то, что в качестве основного варианта инсталляции программного обеспечения используется компиляция из исходных кодов. При таком подходе вы сможете повысить производительность сервера путем:

- уменьшения объема самостоятельно создаваемых исполняемых файлов, программного обеспечения, включая в них только те участки кода, которые действительно необходимы для решения стоящих перед вами задач;
- адаптации исполняемых файлов к архитектуре – типу процессора, дисковой подсистеме – вашего сервера;
- уменьшения шансов злоумышленников на успешную реализацию деструктивного воздействия за счет:
  - а) удаления из исполняемых файлов ненужных для решения ваших задач участков кода, которые могут содержать потенциальные уязвимости;
  - б) оперативного применения патчей, предназначенных для устранения различных уязвимостей, непрерывно выявляемых в программном обеспечении Linux-сообществом.

Все рекомендации по инсталляции и настройке программного обеспечения, приведенные в этой книге, протестированы авторами.

Для проверки воспроизводимости приведенных рекомендаций пользователями, не имеющими достаточной квалификации, ряд рекомендаций, касающихся инсталляции и настройки криптографического программного обеспечения, виртуальных частных сетей, сервера баз данных, FTP-сервера и Web-сервера, тестировался школьниками и студентами младших курсов – пользователями сети ЗАО «Инфолайн» (`http://www.infline.ru`). При этом все участники тестирования достигли желаемых результатов.

В книге подробно рассмотрены общие вопросы инсталляции операционной системы Linux на серверах различного назначения. Особое внимание уделяется повышению производительности и обеспечению безопасности сервера. В книге:

- приведен перечень инструкций по повышению производительности и обеспечению безопасности Linux-сервера;
- приведены инструкции по созданию высокопроизводительного и стойкого к деструктивным воздействиям ядра операционной системы.

В книге рассматривается инсталляция (из rpm-пакетов и исходных кодов), типовые варианты настройки и использования:

GnuPG, OpenSSL, OpenSSH – криптографического программного обеспечения, используемого для безопасной передачи данных, проверки подлинности и целостности электронных документов, администрирования удаленных систем;

Sudo, sXid, LogSentry, HostSentry, PortSentry, Snort, ucspi-tcp, xinetd, NTP – программного обеспечения для ограничения доступа к серверу, анализа файлов регистрации и обнаружения попыток деструктивного воздействия;

ISC BIND – программного обеспечения для организации службы DNS;

Squid, SquidGuard, VPN-сервер, FreeS/WAN, PPTP-клиент – программного обеспечения, используемого для организации шлюза из локальных сетей в Интернет и объединения локальных сетей с помощью сетей общего пользования;

Exim, Qpopper, SpamAssassin, Doctor Web – программного обеспечения, используемого для организации службы электронной почты с поддержкой фильтрации сообщений, содержащих спам и вирусы;

MySQL – сервера баз данных;

ProFTPD, vsFTPD – программного обеспечения, предназначенного для организации FTP-сервера;

Apache HTTP Server, PHP, mod_perl – программного обеспечения, предназначенного для организации Web-сервера;

Samba – программного обеспечения, используемого для организации совместного доступа к общим сетевым ресурсам (файлам, каталогам и принтерам);

tar – утилиты, используемой для резервного копирования критически важной информации.

Почему была написана эта книга

Первым побудительным мотивом послужило массовое подключение к Интернет жителей города Юбилейного, в котором проживают авторы этой книги. Им пришлось отвечать по несколько раз в день на вопросы знакомых, родственников знакомых, знакомых знакомых и даже не очень знакомых людей, связанные с подключением Linux-систем к VPN-серверу провайдера. В результате одним из авторов этой книги было написано соответствующее руководство, которое было опубликовано на сервере, находящемся внутри сети ЗАО «Инфолайн» и в последующем в библиотеке `http://www.linuxportal.ru`. После чего количество задаваемых авторам вопросов пользователями городской сети резко сократилось.

Вторым толчком для написания книги послужила объективная необходимость создания некоего корпоративного стандарта, единого для всех организаций, использующих Linux-сервера, и в различной форме взаимодействующих с авторами этой книги. Такой стандарт был разработан и успешно используется в нескольких организациях. При этом количество вопросов, задаваемых авторам сотрудниками этих организаций, и количество нештатных ситуаций также уменьшилось до вполне приемлемого уровня.

Пример использования Linux-серверов для организации корпоративной сети

У читателя может возникнуть вполне естественный вопрос о том, где конкретно могут использоваться сервера с операционной системой Linux, и как они должны быть интегрированы с локальной сетью предприятия и Интернет. Ответ на этот вопрос мы приводим в виде обобщенной схемы организации корпоративной сети, представленной на рис. 1.1.

В рассматриваемом примере корпоративная сеть содержит:

- шлюз, предназначенный для организации доступа пользователей локальной сети к различным ресурсам в Интернет и защиты локальной сети от несанкционированного доступа из вне;
- первичный и вторичный, имеющий независимое подключение к Интернет, DNS-сервера;
- два VPN-сервера, предназначенные для объединения в единую сеть локальных сетей удаленных офисов с использованием сетей общего пользования (Интернет);
- сервер, предназначенный для организации службы электронной почты;
- сервер баз данных;
- FTP-сервер;
- Web-сервер;
- расположенный внутри локальной сети Samba-сервер, предназначенный для организации доступа к общим сетевым ресурсам файлам и принтерам.

Внутри локальной сети также могут находиться дополнительные сервера, используемые для организации служб, функционирующих в пределах локальной сети.

Рис. 1.1. Обобщенная схема организации корпоративной сети предприятия

Многие могут заметить, что использование десяти серверов для организации корпоративной сети является очень расточительным и практически не реализуемым по экономическим соображениям для большинства организаций. Скорее всего, это действительно так. Для небольшой компании, имеющей всего лишь один офис, отпадает необходимость в использовании двух VPN-серверов, двух DNS-серверов (поддержка DNS может быть предоставлена поставщиком услуги доступа в Интернет), четырех серверов, предназначенных для организации службы электронной почты, сервера баз данных, FTP и Web-сервера. Для организации интернет-представительства компании в этом случае могут использоваться услуги хостинговых компаний. При этом затраты на оплату услуг хостинга, в зависимости от объема и качества предоставляемых услуг, составят от нескольких сотен до нескольких тысяч рублей в месяц, а в корпоративной сети будет только два сервера – шлюз и Samba-сервер. Дальнейшее сокращение числа используемых серверов – за счет установки программного обеспечения для шлюза и Samba на одном сервере – вряд ли целесообразно, т. к., в случае получения злоумышленником доступа к единственному серверу с соответствующими полномочиями, он получит доступ к информации, находящейся в домашних каталогах пользователей локальной сети и обслуживаемых сервером Samba.

Совместная установка других служб на одном сервере также возможна и позволит существенно сократить затраты на организацию корпоративной сети. Решение о совместной установке служб на одном сервере должно приниматься путем установления разумного компромисса между требованиями по обеспечению безопасности и затратами на приобретение и обслуживание оборудования, необходимого для организации корпоративной сети.

Хотелось бы отметить, что рассматриваемый пример носит иллюстративный характер, необходимый для понимания дальнейшего материала. Более подробно с вопросами, касающимися организации корпоративной сети, вы можете ознакомиться на соответствующих Web-ресурсах и в специальной литературе.

Какое программное обеспечение должно быть установлено на сервере

Любой из рассматриваемых в приведенном примере серверов может быть реализован с использованием операционной системы Linux и соответствующего программного обеспечения. Примерный перечень программного обеспечения, для каждого из рассматриваемых типов серверов, представлен в таблице 1.1. В таблице обозначено:

Да – установка программного обеспечения обязательна.

Опц.- установка программного обеспечения возможна для реализации дополнительных возможностей.

Да[1] – на всех серверах, кроме серверов, предназначенных для организации службы DNS и шлюза, рекомендуется установка «облегченного варианта» демона `named–lwresd`, также входящего в комплект поставки ISC BIND.

Да[2] – установка почтового транспортного агента необходима на всех серверах. На серверах, не предназначенных для приема входящих сообщений, возможно использование Sendmail, настроенного только для отправки почтовых сообщений на центральный почтовый концентратор.

Да[3] – необходимо установить только один из рассматриваемых в книге FTP-серверов.

Да[4] – установка FTP-сервера необходима только, если протокол FTP используется при администрировании сервера.

Как пользоваться этой книгой

В название книги содержится фраза «пошаговые инструкции» – это не рекламный слоган, а характеристика способа изложения материала, который един для всей книги, в том числе, и этой главы.

Поэтому нет ничего удивительного в том, что первой пошаговой инструкцией является инструкция по использованию книги при инсталляции Linux-сервера.

Шаг 1

Сформируйте перечень серверов, необходимых для организации вашего варианта корпоративной сети.

Шаг 2

Сформируйте для каждого сервера список программного обеспечения, руководствуясь вашими потребностями и перечнем необходимого для каждого из типов серверов программного обеспечения, представленного в таблице 1.1. В случае установки на сервере программного обеспечения для нескольких служб список необходимого программного обеспечения может быть синтезирован как объединение списков, рекомендованных для каждой из устанавливаемых служб.

Шаг 3

Ознакомьтесь с инструкциями по инсталляции операционной системы Linux.

Шаг 4

Ознакомьтесь с инструкциями по инсталляции и настройке программного обеспечения системы сетевой защиты.

Шаг 5

Ознакомьтесь с инструкциями по инсталляции и настройке криптографического программного обеспечения.

Шаг 6

Ознакомьтесь с инструкциями по инсталляции и настройке программного обеспечения для ограничения доступа к серверу и обнаружения попыток деструктивного воздействия.

Шаг 7

Ознакомьтесь с инструкциями по инсталляции и настройке программного обеспечения, предназначенного для решения целевых задач, перечень которого был сформирован на втором шаге этой инструкции.

Шаг 8

Сформируйте требования, которые должны быть удовлетворены при инсталляции сервера, например, параметры разбиения диска, перечень опций, используемых при конфигурировании ядра, сетевые настройки и т. п.

Шаг 9

Проинсталлируйте, настройте и протестируйте работоспособность операционной системы Linux, руководствуясь вашими потребностями и инструкциями, изложенными в части 1 настоящей книги.

Шаг 10

Проинсталлируйте, настройте и протестируйте работоспособность программного обеспечения системы сетевой защиты, руководствуясь вашими потребностями и инструкциями, изложенными в части 2 настоящей книги.

Шаг 11

Проинсталлируйте, настройте и протестируйте работоспособность криптографического программного обеспечения, руководствуясь вашими потребностями и инструкциями, изложенными в части 3 настоящей книги.

Шаг 12

Проинсталлируйте, настройте и протестируйте работоспособность программного обеспечения для ограничения доступа к серверу и обнаружения попыток деструктивного воздействия, руководствуясь вашими потребностями и инструкциями, изложенными в части 4 настоящей книги.

Шаг 13

Проинсталлируйте, настройте и протестируйте работоспособность программного обеспечения предназначенного для решения целевых задач, руководствуясь вашими потребностями и инструкциями, изложенными в частях 5…12 настоящей книги.

Шаг 14

Удалите ненужное на этапе эксплуатации программное обеспечение, используемое для компиляции исходных кодов, в соответствии с рекомендациями главы 2.

Как уже отмечалось, основным и рекомендуемым способом инсталляции программного обеспечения является компиляция из исходных кодов. Для реализации этого способа необходимо выполнить, как минимум, следующие операции.

Шаг 1

Распакуйте файлы архива `arhiv-version.tar.gz` в некоторый каталог, например, `/var/tmp/`:

```
[root@drwalbr tmp]# tar xzpf arhiv-version.tar.gz
```

В этом примере для распаковки архива используется утилита `tar` с опциями:

`x` – предписывает извлечь файлы из архива;

`z` – указывает на то, что файл архива сжат утилитой `gzip`;

`p` – предписывает сохранить при распаковке архива установленные в нем права доступа к файлам и каталогам;

`f` – указывает на то, что после нее следует только имя распаковываемого архива.

После этого перейдите во вновь созданный каталог `/var/tmp/arhiv-version`:

```
[root@drwalbr tmp]# cd arhiv-version
```

Шаг 2

Сконфигурируйте исходные коды программного обеспечения:

```
[root@drwalbr arhiv-version]# ./configure –-option1 \
–-option2 \
…
--optionN
```

Команда `./configure` конфигурирует исходные коды:

• проверяет наличие на вашей системе библиотек и программ, необходимых для компиляции и нормальной работы устанавливаемого программного обеспечения;

• модифицирует исходные коды программного обеспечения в соответствии со значением параметров `–-option1` … `--optionN`, например, оптимизируя их применительно к архитектуре вашей системы, исключая ненужные вам фрагменты кода, изменяя каталоги, используемые для инсталляции по умолчанию.

В соответствующих разделах этой книги приводится набор опций, необходимый для реализации рассматриваемых вариантов инсталляции программного обеспечения. Вполне возможно, что вам потребуется получить дополнительную информацию об используемых опциях конфигурации исходных кодов. Это можно сделать, воспользовавшись опцией `–-help`:

```
[root@drwalbr arhiv-version]# ./configure --help
```

или просто просмотрев соответствующие фрагменты кода файла `configure`, где содержатся комментарии, описывающие различные опции, используемые при конфигурации исходных кодов. Например, в файле `configure` Squid версии 2.5STABLE1 имеется следующий фрагмент:

```
# Defaults:
ac_help=
ac_default_prefix=/usr/local
# Any additions from configure.in:
ac_help="$ac_help
  --disable-dependency-tracking Speeds up one-time builds
  --enable-dependency-tracking  Do not reject slow dependency extractors"
ac_default_prefix=/usr/local/squid
ac_help="$ac_help
  --enable-maintainer-mode enable make rules and dependencies not useful
                           (and sometimes confusing) to the casual in-
staller"
ac_help="$ac_help
  --enable-dlmalloc[=LIB] Compile & use the malloc package by Doug Lea"
ac_help="$ac_help
  --enable-gnuregex       Compile GNUregex"
ac_help="$ac_help
  --enable-xmalloc-statistics
                          Show malloc statistics in status page"
```

В некоторых вариантах инсталляции программного обеспечения, рассматриваемого в этой книге, используется несколько десятков опций для конфигурирования исходных кодов, поэтому для ускорения инсталляции мы предлагаем файлы с именем `wk-configure`, доступные на сервере `http://www.bruy.info`. Они содержат текст команды `configure` с требуемым набором опций. Вы всегда можете отредактировать этот файл в соответствии с вашими потребностями, скопировать его в командную строку и осуществить конфигурацию исходных кодов одним нажатием клавиши <Enter>.

Шаг 3

Откомпилируйте, проинсталлируйте программное обеспечение, создайте и сохраните в надежном месте список установленных файлов.

Для компиляции исходных кодов используется команда:

```
[root@drwalbr arhiv-version]# make
```

Перед инсталляцией файлов программного обеспечения необходимо создать и сохранить в некотором файле список всех файлов и каталогов, уже имеющихся на вашей системе:

```
[root@drwalbr arhiv-version]# find /* > /root/>arhiv1
```

Инсталляция программного обеспечения может быть осуществлена в автоматическом режиме. Для этого используется команда:

```
[root@drwalbr arhiv-version]# make install
```

и вручную, с одновременной установкой требуемых прав доступа:

```
[root@drwalbr arhiv-version]# install –m 0750 file /path/to/file/new_file
```

После инсталляции из исполняемых файлов можно удалить комментарии и другую отладочную информацию, используя команду `strip`. При компиляции и инсталляции могут использоваться и другие команды. С их назначением вы можете ознакомиться, выполнив команду `man`.

По завершении инсталляции необходимо создать список проинсталлированных файлов. Для этого повторно создайте список файлов и каталогов всех файлов, имеющихся на вашей системе, и сравните его с файлом, созданным до инсталляции. Удалите из полученного списка файлы, имеющие отношение к файловой системе `/proc`, и сохраните его в надежном месте:

```
[root@drwalbr arhiv-version]# find /* > /root/>arhiv2
[root@drwalbr arhiv-version]# diff /root/>arhiv1 /root/>arhiv2 >
/very_reliable_place/arhiv.installed.YYYYMMDD
```

Шаг 4

Удалите более ненужный архив и каталог с исходными кодами:

```
[root@drwalbr arhiv-version]# cd /var/tmp/
[root@drwalbr tmp]# rm -rf arhiv-version/
[root@drwalbr tmp]# rm -f arhiv-version.tar.gz
```

Если вы не очень хорошо знакомы с инсталляцией и настройкой программного обеспечения, операции по удалению архива и каталога с исходными кодами лучше выполнить после проведения удачного тестирования инсталлируемого программного обеспечения. Это обусловлено тем, что в каталоге с исходными кодами часто содержится документация, необходимая при настройке соответствующего программного обеспечения. В любом случае архив с исходными кодами лучше сохранить для того, чтобы использовать его в дальнейшем при повторной инсталляции программного обеспечения.

Шаг 5

Настройте программное обеспечение. Настройка осуществляется путем создания и редактирования соответствующих конфигурационных файлов. Примеры всех конфигурационных файлов, рассматриваемых в этой книге, доступны на сервере `http://www.bruy.info`. Редактирование конфигурационных файлов можно осуществлять с использованием текстового редактора, например vi.

Шаг 6

Протестируйте работоспособность и функциональность инсталлированного программного обеспечения. В случае необходимости повторно выполните операции по его настройке или инсталляции.

Куда обращаться за помощью и технической поддержкой

Вполне возможно, что при установке программного обеспечения вы не сможете в точности реализовать инструкции, описанные в этой книге из-за ошибок, которые могут возникнуть на любой стадии инсталляции и настройки программного обеспечения. Это может быть обусловлено тем, что приведенные инструкции протестированы только для рассматриваемой в книге версии дистрибутива ядра, соответствующего ему патча Grsecurity и программного обеспечения. В случае возникновения подобной ситуации авторы настоятельно рекомендуют изучить документацию на компоненты инсталлируемого программного обеспечения, отличные от рассматриваемых в книге, особенности используемого дистрибутива (версию ядра, компилятора библиотек, структуры каталогов и т. п.) и разработать собственные инструкции по инсталляции, настройке и тестированию программного обеспечения. Большую помощь для не владеющих английским языком читателей в этом случае могут оказать русскоязычные ресурсы, например, `http://www.opennet.ru`, `http://www.linuxdoc.ru`, `http://www.linux.org.ru`, `http://www.linux.ru`, `http://www.linuxportal.ru` и другие ресурсы, которые могут быть найдены с помощью поисковых систем.

В случае неудачного применения на практике самостоятельно разработанной инструкции после подробного изучения документации можно обратиться за получением помощи разработчиков устанавливаемого

программного обеспечения через соответствующие списки рассылки. Обращению к разработчикам должно предшествовать подробное изучение правил, установленных для списков рассылки.

В некоторых случаях очень полезные советы можно получить на различных форумах, посвященных обсуждению Linux и соответствующего программного обеспечения. Перед составлением сообщения нужно ознакомится с правилами, регламентирующими общение пользователей данного форума, и общими рекомендациями по получению консультаций по технической поддержке, содержащихся в документе, разработанном Эриком Раймондом (Eric Raymond) и Риком Мойном (Rick Moen) «Как правильно задавать вопросы» (`http://ln.com.ua/~openxs/articles/smart-questions-ru.html`).

Благодарности

Авторы считают необходимым выразить благодарность за помощь в подготовке, оформлении и издании книги исполнительному директору АНО «Секция инженерные проблемы стабильности и конверсии» Росиийской инженерной академии Прошлякову Дмитрию Константиновичу (СИП РИА `http://www.sipria.ru`), научному консультанту СИП РИА Есину Александру Гавриловичу; заместителю исполнительного директора СИП РИА Пырьеву Владимиру Александровичу, Карловой Марине Васильевне, Усаниной Марине Витальевне.

Часть 1

Инсталляция операционной системы Linux на сервере

Глава 2

Установка ASPLinux

В этой главе:

1. Что нужно знать об аппаратных средствах вашего сервера
2. Взаимодействие с другими операционными системами
3. Первичная установка ASPLinux
4. Как использовать команды rpm
5. Запуск и установка служб
6. Программы, файлы и каталоги, которые должны быть удалены после первичной установки
7. Дополнительно устанавливаемые пакеты

В этой главе рассматривается первоначальная инсталляция операционной системы ASPLinux-7.3 на серверной системе, т. е. создание «сервера-заготовки", который путем установки и настройки соответствующих параметров и служб может быть трансформирован в безопасный и оптимизированный сервер произвольного назначения.

Что нужно знать об аппаратных средствах вашего сервера

Залогом успешной установки операционной системы ASPLinux является хорошее знание аппаратных средств компьютера, на котором осуществляется установка. В процессе установки потребуется следующая информация:

- тип процессора;
- количество жестких дисков;
- объем жестких дисков;
- тип жестких дисков (например, IDE ATA/133 или SCSI);
- объем оперативной памяти (например, 256 МБ);
- имеется ли SCSI адаптер? Если да, то - производитель и модель;
- имеется ли RAID массив? Если да, то - производитель и модель;
- тип мыши (например, PS/2 Microsoft, Logitech), количество кнопок;
- параметры настройки сети (IP-адрес, маска сети, IP-адрес шлюза, IP-адреса серверов DNS, имя домена, имя компьютера);
- типы сетевых карт (производитель, модель и название чипсета).

Взаимодействие с другими операционными системами

ASPLinux может мирно сосуществовать на одном компьютере (и даже на одном физическом диске) с другими ОС — Windows 9x/ME, Windows NT/2000/XP, Linux других дистрибутивов, FreeBSD, OpenBSD, QNX - и использоваться совместно с ними. Это достигается с помощью мультисистемных загрузчиков (LILO, GRUB, ASPLoader, Acronis OS Selector), обеспечивающих загрузку требуемой ОС. Подробное описание их можно встретить в документации на эти программные продукты и ASPLinux. Вариант установки нескольких операционных систем на одном компьютере является очень удобным и привлекательным для рабочей станции разработчика-исследователя, но не для серверных систем, к которым предъявляются жесткие требования по уровню безопасности. Если на компьютере совместно с ASPLinux установлена популярная операционная система MS Windows-98/ME, доступ к которой с помощью кнопки <Отмена> на форме ввода логина и пароля может получить кто угодно, общедоступными становятся и критические, с точки зрения обеспечения безопасности системы, файлы ASPLinux, например, с помощью программы `ext2viewer`. Поэтому в дальнейшем будем предполагать, что ОС ASPLinux-7.3 является единственной ОС, установленной на сервере.

Первичная установка ASPLinux

Наиболее простым способом установки ASPLinux является установка с дистрибутивных компакт-дисков. При этом первоначальная загрузка операционной системы осуществляется с первого из них.

Шаг 1

Итак, вставьте первый инсталляционный диск в привод CD-ROM, перегрузите компьютер, установите в BIOS загрузку с CD-ROM и дождитесь появления формы, предлагающей выбрать язык установки. Выберите язык "Russian", форма отобразится на русском языке, после чего нажмите кнопку <Далее>. Если форма не появилась, перегрузите систему и во время запуска программы инсталляции нажмите клавишу <ESC>. На экране появится форма выбора видеорежима установки, с помощью которой выберите видеорежим, поддерживаемый вашей графической подсистемой.

Шаг 2

После нажатия кнопки <Далее>на экране отобразится форма выбора мыши. Выберете тип мыши и нажмите кнопку <Далее>. На экране появится форма выбора типа установки.

Шаг 3

Выберите выборочную установку и нажмите кнопку <Далее>. На экране отобразится форма выбора типа носителя, с которого будет осуществляться установка. Вы можете выбрать установку с "CD-ROM/образ CD-ROM на жестком диске" или "Установку сетевого ресурса (для опытных пользователей)". Проигнорировав устрашающее предупреждение – "только для опытных пользователей" можно выбрать установку с сетевого ресурса. Это имеет смысл при инсталляции ASPLinux на большом числе компьютеров. В этом случае следует разместить rpm-пакеты, входящие в состав дистрибутива, в некотором каталоге на Web-

или FTP-сервере локальной сети и указать его программе инсталляции. Вариант установки с сетевого ресурса может быть использован для установки на компьютерах без привода CD-ROM. В этом случае первоначальная загрузка осуществляется с загрузочной дискеты, процесс создания которой описан в документации по ASPLinux. Выбрав тип носителя, нажмите кнопку <Далее>. На экране отобразится форма выбора метода назначения дискового пространства.

Шаг 4

Выберите "Дополнительно». После этого на экране отобразится форма интерфейса "ASPDiskmanager", с помощью которого можно осуществить разбиение жесткого диска. Данная процедура позволяет создавать на жестком диске изолированные логические разделы, которые ведут себя как отдельные диски. Создание дисковых разделов, пожалуй, наиболее критичный момент инсталляции любой Linux-системы.

Создание нескольких логических разделов дает следующие преимущества:

- защита против атак отказа в обслуживании (DoS);
- защита против программ SUID;
- ускоренная загрузка;
- простота в процессе резервирования и обновлений;
- возможность установки индивидуальных опций монтирования каждой файловой системы;
- возможность избежать неограниченного роста каждой из файловых систем;
- увеличение производительности некоторых программ.

В качестве примера рассмотрим разбиение жесткого диска объемом 20 ГБайт на компьютере с памятью 256 МБайт.

`/boot`	10	МБайт	Здесь хранятся образы ядер и другие файлы, необходимые для загрузки системы.
`<Swap>`	512	МБайт	Раздел виртуальной памяти для увеличения скорости обмена между виртуальной и оперативной памятью. Рекомендуется размещать непосредственно за разделом `/boot` в начальной области диска.
`/`	512	МБайт	Корневой раздел.
`/usr`	1024	МБайт	В этом разделе устанавливаются пользовательские программы.
`/home`	12800	МБайт	В этом разделе находятся пользовательские каталоги.
`/var`	512	МБайт	В этом разделе находятся файлы регистрации (системных журналов).
`/tmp`	329	МБайт	В этом разделе находятся временные файлы.
`/chroot`	512	МБайт	В этом разделе устанавливаются программы, работающие в окружении chroot-jail. (Web-сервер, DNS-сервер и т. п.)
`/var/lib`	2000	МБайт	В этом разделе размещаются базы данных.

Предложенный вариант разбиения жесткого диска не является обязательным и единственно возможным, а служит только примером. Вам самостоятельно следует определить размеры каждого из разделов диска, исходя из прогнозируемого объема соответствующих файлов. При этом следует учесть, что:

- в разделе `/var/lib` находятся файлы баз данных. Если вы предполагаете использовать этот раздел для базы данных прокси-сервера Squid, то предлагаемый размер раздела 2000 Мбайт является достаточным. Если на сервере предполагается установка других баз данных, то размер раздела может быть, соответственно, увеличен или уменьшен;
- раздел /chroot может использоваться для инсталляции DNS-сервера, Web-сервера Apache и других программ, выполнение которых желательно в защищенной среде chroot;
- размещение /tmp и /home на отдельных разделах может быть полезно, если пользователи имеют доступ к командному интерпретатору (защита против программ SUID). Это разбиение также препятствует пользователям переполнять другие файловые системы;
- раздел <Swap> отводится под виртуальную память системы, используемую для размещения команд и данных, если запущенные приложения, например, в период пиковых нагрузок требуют больше оперативной памяти, чем доступно на компьютере. Для несильно загруженных серверов с небольшим объемом оперативной памяти рекомендуется устанавливать размер раздела <Swap> в два раза больше объема оперативной памяти.

Взгляните на пример разбиения диска файл-сервера на «старом добром 486-м компьютере» с диском 640 МБайт и оперативной памятью 32 МБайт:

`/boot` – 10 МБайт
`<Swap>` – 64 МБайт
`/` – 40 МБайт
`/usr` – 200 МБайт
`/home` – 266 МБайт
`/var` – 35 МБайт
`/tmp` – 35 МБайт

Компиляция программ при таком объеме жесткого диска невозможна, поэтому следует устанавливать rpm-пакеты или компилировать программы на другой системе.

RAID-массивы, то есть средства объединения нескольких физических или логических дисков, служат, с одной стороны, для ускорения дисковых операций, с другой – для повышения сохранности данных. В Linux поддерживаются программные RAID-массивы трех уровней:

- 0 – объединение двух (и более) разделов в один, что дает повышение производительности при дисковых операциях за счет распараллеливания чтения/записи;
- 1 – дублирование содержания одного раздела другим (т.н. зеркалирование – mirroring), обеспечивающее повышение надежности хранения данных за счет 100-процентной избыточности;
- 5 – независимое использование нескольких разделов, по которым распределяются данные и их контрольные суммы. При этом в случае отказа какого-либо из разделов его содержание можно восстановить. Одновременно, за счет распараллеливания операций чтения/записи на разные разделы, достигается некоторый выигрыш в производительности.

Обычно это осуществляется с помощью аппаратных RAID-контроллеров. Однако Linux, и ASPLinux-7.3 в частности, поддерживают программные средства создания RAID-массивов, а "ASPDiskmanager" предоставляет простой способ их организации.

Разделы для организации программных RAID-массивов имеют собственный тип файловой системы (autodetect raid). Очевидно, что для массивов уровней 0 и 1 их число должно быть четным (не менее двух), и объем массива в первом случае будет равен их сумме, во втором – объему меньшего из них. Для массива уровня 5 требуется не менее трех разделов, его объем равен произведению минимального раздела на их число минус объем минимального раздела.

Теоретически разделы для RAID-массива могут создаваться как на разных физических дисках, так и на одном. Однако ясно, что в последнем случае надежность хранения резко снижается (по сравнению с первым случаем), а производительность уменьшается, вне зависимости от уровня массива.

Установка на RAID-массив в ASPLinux возможна только при выборочном способе установки и методе назначения дискового пространства "Дополнительно". В этом случае загружается панель ASPDiskManager, имеющая, как уже говорилось, кнопку <RAID>. Кнопка эта не активизирована: Для ее активации следует создать минимум два раздела с файловой системой raid autodetect.

Следует отметить, что понятие файловой системы raid autodetect имеет несколько другой смысл, чем понятие обычных файловых систем. Последние могут быть созданы в дальнейшем внутри нее. Не рекомендуется размещать на RAID-массиве корневую файловую систему и раздел `/boot`. И потому перед созданием разделов для RAID следует предварительно создать минимум два раздела необходимого объема с файловой системой с точкой монтирования `/` и `/boot`.

Конфигурирование RAID-массива осуществляется нажатием кнопки <RAID>, активизируемой после создания второго из RAID-разделов. Нажатие ее приводит к появлению формы "RAID". В верхнем правом ее углу расположены небольшие кнопки для создания RAID-устройства (слева) и его удаления (справа). Нажатие первой позволяет выбрать имя RAID-устройства (имеющего вид md0, md1 и т. д.) из появившегося списка. После создания устройства в списке разделов ниже следует пометить те из них, которые будут включены в его состав (например, hda5 и hda6). Далее в выпадающих списках назначаются:

- уровень RAID (0, 1 или 5);
- тип раздела (Ext2, Reiser или Swap);
- точка его монтирования (/usr, /home и т. д.).

Если в состав устройства включено менее двух разделов (вида `hda#`), попытка продолжения приведет к выдаче сообщения об ошибке и возврату в панель "RAID". То же произойдет и при включении двух разделов, и выборе RAID уровня 5.

Можно создать (при достаточном количестве разделов) несколько устройств RAID разных уровней, с разными файловыми системами и точками монтирования. Например, при наличии двух физических дисков целесообразно создать устройство md0 уровня 0 для подкачки (Swap), что повысит эффективность свопинга, и устройство md1 уровня 1 с файловой системой Ext2fs и точкой монтирования `/home` для повышения сохранности пользовательских данных. Кроме того, можно дополнительно создавать RAID-устройства для отдельных разделов `/usr` или `/usr/local.`

По завершении конфигурирования RAID-массива установка ASPLinux продолжается обычным образом. И после ее окончания пользователь видит единый раздел, соответствующий каждому из созданных RAID-устройств, которые присутствуют в каталоге `/dev` в виде `/dev/md0, /dev/md1` и т. д.

После окончания разбиения диска нажмите кнопку <Далее> на форме ASPDiskManager. На экране отобразится форма для выбора устанавливаемых пакетов.

Шаг 5

Выбору пакетов, то есть базовых компонентов, утилит и приложений, следует уделить особое внимание. Linux – мощная операционная система, которая устанавливает много служб по умолчанию. Многие из них не нужны и содержат потенциальный риск для безопасности. Минимально необходимый набор пакетов авторы предлагают выбрать следующим образом.

Выберите установку "Сервер", включите флажок "Выборочно", нажмите кнопку <Далее> и дождитесь появления формы выбора отдельных пакетов. Удалите все наборы пакетов, кроме базового, и нажмите кнопку <Далее>. Альтернативным вариантом выбора пакетов может быть нажатие кнопки <Загрузить список> на форме выбора пакетов для установки, при этом список пакетов должен находиться на дискете, вставленной в дисковод. В результате выполнения этих операций будут выбраны следующие пакеты:

```
anacron-2.3-17                  MAKEDEV-3.3-4.1asp
apmd-3.0.2-10                   man-1.5j-6.asp
aspldr-2.0-4                    man-pages-1.50-1.asp
asplinux-logos-1.1.3-4asp       man-pages-ru-asp-1.2-2asp
asplinux-release-7.3-1.asp      mingetty-1.00-1
at-3.1.8-23                     mkbootdisk-1.4.3-1.asp
authconfig-4.2.8-4.asp          mkinitrd-3.3.10-5.asp
basesystem-7.0-2.asp            mktemp-1.5-14
bash-2.05a-13.asp               modutils-2.4.16-1.asp
bclsecurity-0.4-1.asp           mount-2.11n-12.7.3asp
bdflush-1.5-17                  mouseconfig-4.25-1
bzip2-1.0.2-2                   mt-st-0.7-3
bzip2-libs-1.0.2-2              ncurses-5.2-26
chkconfig-1.3.5-3               netconfig-0.8.11-7.0.asp
console-tools-19990829-40.2asp  net-tools-1.60-4
cpio-2.4.2-26,                  newt-0.50.35-1
cracklib-2.7-15                 ntsysv-1.3.5-3
cracklib-dicts-2.7-15           openldap-2.0.23-4
crontabs-1.10-1                 openssl-0.9.6b-24asp
cyrus-sasl-1.5.24-25            pam_passwdqc-0.5-1.asp
cyrus-sasl-md5-1.5.24-25        pam-0.75-32.2asp
cyrus-sasl-plain-1.5.24-25      passwd-0.67-1
db1-1.85-8                      pchains-1.3.10-13
db2-2.4.14-10                   pciutils-2.1.9-2
db3-3.3.11-6                    pcre-3.9-2
dev-3.3-4.1asp                  popt-1.6.4-7x.18.2asp
dhcpcd-1.3.22pl1-7              procmail-3.22-5
diffutils-2.7.2-5               procps-2.0.7-12
dosfstools-2.8-1                psmisc-20.2-3.73
e2fsprogs-1.27-3                pump-0.8.11-7.0.asp
eject-2.0.12-4                  pwdb-0.61.2-2
ed-0.2-25                       pyiconv-0.1.2-1.asp
file-3.37-5                     python-1.5.2-38.3asp
filesystem-2.1.6-2              quota-3.03-1
fileutils-4.1-10.asp            raidtools-1.00.2-1.3
findutils-4.1.7-4.asp           readline-4.2a-4
gawk-3.1.0-4.1.asp              reiserfs-utils-3.x.0j-3
gdbm-1.8.0-14                   rootfiles-7.2-1
glib-1.2.10-5                   rpm-4.0.4-7x.18.2asp
glib2-2.0.1-2                   rpm-python-4.0.4-7x.18.2asp
glibc-2.2.5-37asp               sed-3.02-11.asp
glibc-common-2.2.5-37asp        sendmail-8.11.6-15.asp
gmp-4.0.1-3                     setserial-2.17-5
gpm-1.19.6-2.asp                setup-2.5.12-1
grep-2.5.1-1                    setuptool-1.8-2
groff-1.17.2-12                 sh-0.3.7-2
grub-0.91-4.1.asp               shadow-utils-20000902-7.asp
gzip-1.3.3-1.asp                sh-utils-2.0.11-14.asp
hdparm-5.1-1.asp                slang-1.4.5-2
hesiod-3.0.2-18                 slocate-2.6-1
hotplug-2002_04_01-3            specspo-7.3-1asp
hwdata-0.14-1.asp               sxid-4.0.1-1.asp
indexhtml-7.2-1.asp             sysklogd-1.4.1-8
info-4.1-1                      syslinux-1.52-2
initscripts-6.67-3asp           SysVinit-2.84-2
iproute-2.4.7-3.asp             tar-1.13.25-4
iptables-1.2.6a-1.asp           tcsh-6.10-6
iputils-20020529-1.asp          termcap-11.0.1-10
kbdconfig-1.9.15-2              textutils-2.0.21-1
```

```
kernel-2.4.18-5asp              time-1.7-16
krb5-libs-1.2.4-1.asp           timeconfig-3.2.7-1.asp
ksymoops-2.4.4-1                tmpwatch-2.8.3-1
kudzu-0.99.52-1.4asp            usbutils-0.9-5
less-358-24                     usermode-1.53-2.asp
libacl-2.0.9-1.asp              utempter-0.5.2-6
libattr-2.0.7-1.asp             util-linux-2.11n-12.7.3asp
libstdc++-2.96-112asp           vconfig-1.5-2.asp
libtermcap-2.0.8-28             vim-common-6.1-2.asp
libuser-0.50.2-1                vim-minimal-6.1-2.asp
lilo-21.7.3-2.asp,              vixie-cron-3.0.1-64
logcheck-1.1.1-7.asp            which-2.13-3
logrotate-3.6.4-1               words-2-18
lokkit-0.50-8                   xfsprogs-2.0.3-1.asp
losetup-2.11n-12.7.3asp         yum-0.9.1a-1.7.3asp
mailcap-2.1.9-2                 yum-headers-7.3-1asp
mailx-8.1.1-22                  zlib-1.1.3-25.7
```

После выбора (тем или иным способом) перечня устанавливаемых пакетов нажмите кнопку <Далее>. Если установка пакетов осуществлялся путем выбора базового набора и удаления всех остальных пакетов – на экране отобразится форма, предлагающая установить ряд пакетов для удовлетворения зависимостей. Разрешите установить все пакеты.

Шаг 6

На экране появится форма, где указаны: количество выбранных для установки пакетов, их суммарный объем, группа приложений, опции разбиения диска, источник установки пакетов, метод установки, тип мыши - то есть все параметры, определенные на предшествующих этапах. Если выбранные параметры соответствуют приведенным выше рекомендациям, нажмите кнопку <Установить>. В противном случае вы можете вернуться назад (кнопка <Назад>) и изменить параметры установки. По окончании установки появится форма с сообщением, что все пакеты нормально установлены. Если появятся сообщения, что некоторые пакеты установлены с ошибками, следует выяснить причину неправильной установки (плохой инсталляционный компакт диск, привод CD-ROM, неразрешенные зависимости и т. п.) и провести установку заново.

ЗАМЕЧАНИЕ В программе установки ASPLinux доступна вторая – текстовая – виртуальная консоль. Переключиться в нее можно нажатием комбинации `Alt+Ctrl+F2`. В ней загружена командная оболочка bash (правда, с несколько ограниченными возможностями). Наличие этой консоли может оказаться полезным при восстановлении системы, когда загрузочная дискета отсутствует, и единственной возможностью загрузить систему является загрузка с первого инсталляционного диска. Можно выполнять разнообразные действия в командной строке (например, для восстановления системы при сбоях). Обратное переключение в графическую консоль программы установки осуществляется комбинацией клавиш `Alt+F7`.

Шаг 7

По завершении копирования пакетов наступает следующий этап - выбор начального загрузчика, то есть программы, управляющей запуском операционных систем. Инсталляционная программа предлагает четыре варианта:

- ASPLoader (по умолчанию);
- LILO;
- GRUB;
- не устанавливать загрузчик.

Вам следует выбрать установку загрузчика GRUB или LILO в MBR (главную загрузочную запись) и нажать кнопку <Далее>.

Шаг 8

Настройка сети осуществляется в два этапа. На первом выбираются сетевые карты. Широко распространенные модели сетевых карт будут, с большой степенью вероятности, определены автоматически. Если имеющиеся у вас карты не определены программой установки, выберите драйвер сетевой карты из раскрывающегося списка, и укажите необходимые параметры (IO порт и IRQ) и нажмите кнопку <Добавить>. Эти операции должны быть выполнены для всех сетевых карт. По окончании выбора сетевых карт нажмите кнопку <Далее>.

На втором этапе осуществляется, собственно, настройка сети. Для каждой из сетевых карт, выбранных на предыдущем этапе, включите опцию «Активизировать при загрузке» и заполните следующие поля: "IP-адрес", "Маска сети", "Адрес подсети", "ШВ адрес", "Имя хоста", "Шлюз", "Первичный DNS", "Вторич-

ный DNS". Эти сведения можно получить у администратора вашей локальной сети (если вы таковым не являетесь). По окончании установки параметров нажмите кнопку <Далее>.

Шаг 9

Локализация системы осуществляется путем:

- выбора модели клавиатуры (например, PC 105-key для стандартных ныне клавиатур с Windows-клавишами);
- определения языка, страны и набора символов (K0I8-R);
- указания необходимых раскладок клавиатуры (English и Russian, например);
- назначения переключателя с латиницы на кириллицу (<Ctrl>+<ShifI>).
- По окончании выбора параметров локализации нажмите кнопку <Далее>.

Шаг 10

Установите (проверьте) дату и время. Эти параметры, как правило, определяются автоматически на основании показаний системных часов. Если последние установлены на время по Гринвичу (GMT), выключите опцию "Часы CMOS установлены в местное время". По окончании установки нажмите кнопку <Далее>.

Шаг 11

Установите пароль суперпользователя `root` и нажмите кнопку <Далее>. После этого должно появиться сообщение об успешном завершении установки системы ASPLinux и предложение перезагрузить компьютер. Если в процессе инсталляции создавалась загрузочная дискета, ее следует удалить из дисковода. Инсталляционный компакт диск извлекается из привода автоматически. На этом первичную установку ASPLinux можно считать законченной.

Как использовать команды rpm

Этот раздел содержит краткий обзор использования команды `rpm` для установки, удаления, обновления и получения информации о rpm-пакетах, установленных в вашей системе. Вы должны ознакомиться с основными приемами использования команды `rpm`, потому что в дальнейшем она будет часто использоваться. Например, в этой главе – при удалении лишних и инсталляции дополнительных пакетов.

ЗАМЕЧАНИЕ Информация об особенностях использования любой команды в Linux может быть получена с помощью соответствующей страницы руководства (man-страницы). Например, для команды `rpm` - `man rpm`. В ASPLinux многие man-страницы переведены на русский язык.

Установка пакета rpm:

Для установки rpm-пакета, используйте команду:

```
[root@drwalbr tmp]# rpm -ihv mc-4.5.55-5.1asp.i386.rpm
Подготовка...                ########################################
[100%]
   1:mc                      ########################################
[100%]
```

Обратите внимание, что в команде используется имя файла, в котором находится пакет с именем `mc-4.5.55-5.1asp.i386.rpm`. Опция `i` предписывает установить пакет, опция `h`- отображать в текстовом режиме с помощью последовательности символов. "#" - степень завершения установки пакета.

Для удаления rpm-пакета, используйте команду:

```
[root@drwalbr tmp]# rpm -e mc
```

Обратите внимание, что в команде используется только название пакета `mc`. Опция `e` предписывает удалить пакет.

Для обновления rpm-пакета (удаления старой версии и установки новой), используйте команду:

```
[root@drwalbr tmp]# rpm -Uhv mc-4.5.55-5.1asp.i386.rpm
Подготовка...                ########################################
[100%]
   1:mc                      ########################################
[100%]
```

При установке rpm-пакета с помощью команды `rpm` пред началом установки проверяется, не будет ли устанавливаемый пакет конфликтовать с другими пакетами и настройками системы. Использование опции `force` позволяет обойти это ограничение.

```
[root@drwalbr tmp]# rpm -Uhv –force mc-4.5.55-5.1asp.i386.rpm
Подготовка...                ########################################
[100%]
   1:mc                      ########################################
[100%]
```

По умолчанию, команда `rpm` проверяет, установлены ли rpm-пакеты, необходимые для установки данного пакета. Если некоторые из них отсутствуют, `rpm` сообщит об этом. Это сделано специально, чтобы избежать проблем и убедиться, что устанавливаемое программное обеспечение будет правильно работать. В некоторых случаях бывает необходимо преодолеть это ограничение, что достигается применением опции `nodeps`. Можно не заботиться о зависимости и использовать опцию для пропуска ее проверки при установке программ:

```
[root@drwalbr tmp]# rpm -Uhv –nodeps mc-4.5.55-5.1asp.i386.rpm
Подготовка...                ########################################
[100%]
   1:mc                      ########################################
[100%]
```

Для определения версии пакета используйте опцию q:

```
[root@drwalbr tmp]# rpm -q mc
mc-4.5.55-5.1asp
```

Для отображения подробной информации об установленном rpm-пакете (названия, версии и краткого описания установленной программы) используйте опции `i` и `q`:

```
[root@drwalbr tmp]# rpm -qi mc
Name        : mc                            Relocations: (not relocate-
able)
Version     : 4.5.55                             Vendor: ASPLinux
Release     : 5.1asp                         Build Date: Срд 17 Июл 2002
19:37:19
Install date: Чтв 26 Дек 2002 16:19:10      Build Host: arena.asplinux.ru
Group       : Системное окружение/Оболочки   Source RPM: mc-4.5.55-
5.1asp.src.rpm
Size        : 3822241                          License: GPL
Packager    : ASPLinux Team <packages@asp-linux.com>
URL         : http://www.gnome.org/mc/
Summary     : Файловый менеджер и визуальная оболочка с дружественным ин-
терфейсом.
Description :
Midnight Commander - это визуальная оболочка и файловый менеджер
со многими дополнительными возможностями. Это приложение
для текстового режима с поддержкой мыши (при запущенном GPM).
Основные возможности Midnight Commander - это поддержка FTP,
просмотр файлов формата TAR, архивов файлов, файлов RPM
```

Для получения списка файлов, входящих в rpm-пакет, наберите:

```
[root@drwalbr tmp]# rpm -ql  mc
/etc/profile.d/mc.csh
/etc/profile.d/mc.sh
/usr/bin/mc
...
/usr/share/man/man1/mc.1.gz
/usr/share/man/man1/mcedit.1.gz
```

Для определения принадлежности некоторого файла к пакету используйте опции `q` и `f`:

```
[root@drwalbr tmp]# rpm -qf /usr/bin/mc
mc-4.5.55-5.1asp
```

Для проверки подлинности и целостности пакета перед его установкой используйте команды:

```
[root@drwalbr tmp]# rpm --checksig mc-4.5.55-5.1asp.i386.rpm
```

и

```
[root@drwalbr /]# rpm --checksig –nogpg mc-4.5.55-5.1asp.i386.rpm
```

Запуск и установка служб

Вам придется неоднократно запускать и останавливать различные службы в процессе настройки и установки сервера. Программа `init` отвечает за запуск служб, которые должны работать после загрузки системы. Каждая из служб имеет собственный файл сценария, находящийся в каталоге `/etc/init.d`, автоматически запускающий, останавливающий, перезапускающий службу при передаче ему таких параметров, как `start, stop` и `restart`. Следующие команды иллюстрируют процесс управления службой на примере Web-сервера.

Для остановки службы `httpd` наберите:

```
[root@drwalbr /]# /etc/init.d/httpd stop
Останавливается  httpd:                [OK]
```

Для запуска службы `httpd`:

```
[root@drwalbr /]# /etc/init.d/httpd start
Запускается  httpd:                    [OK]
```

Для перезапуска службы `httpd`:

```
[root@drwalbr /]# /etc/init.d/httpd restart
Останавливается  httpd:                [OK]
Запускается  httpd:                    [OK]
```

Программы, файлы и каталоги, которые должны быть удалены после первичной установки

Некоторые программы после окончания первичной установки, в целях улучшения безопасности, должны быть удалены вручную. Ниже описан процесс удаления и приведены краткие пояснения необходимости выполнения этих шагов.

Пакет `anacron`

Пакет `anacron` является аналогом планировщика команд `cron`, который адаптирован для работы на непрерывно функционирующих системах. В серверной системе, которая должна работать 24 часа в сутки, нет необходимости в его присутствии. Для удаления пакета выполните:

```
[root@drwalbr /]# /etc/init.d/anacron stop
[root@drwalbr /]# rpm -e anacron
[root@drwalbr /]# rm -rf /var/spool/anacron/
```

Пакет `apmd`

Пакет `apmd`, содержащий утилиты Advanced Power Management Daemon, используется на портативных компьютерах для отслеживания состояния батарей. Для удаления пакета выполните:

```
[root@drwalbr /]# /etc/init.d/apmd stop
[root@drwalbr /]# rpm -e apmd
```

Пакет `at`

Пакет `at` содержит утилиты, позволяющие исключать службы из автозапуска. Работает не очень надежно. Для удаления пакета выполните:

```
[root@drwalbr /]# /etc/init.d/atd stop
[root@drwalbr /]# rpm -e at
```

Пакет `dhcpcd`

Пакет `dhcpcd` содержит протокол, который позволяет системе получать информацию о собственной сетевой конфигурации от DHCP-сервера. Если вы собираетесь использовать DHCP в вашей сети, рекомендуем установить DHCP-клиента, включенного в пакет `pump`. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e dhcpcd
```

Пакет `eject`

Пакет `eject` содержит программу, которая позволяет пользователю извлекать сменные носители (такие, как CD-ROM, гибкие диски, lomega Jaz или Zip-диски). Как правило, эта программа нужна только при осуществлении копирования файлов на ленту. Для удаления пакета наберите:

```
[root@drwalbr /]# rpm -e eject
```

Пакет `hotplug`

Пакет `hotplug` содержит приложение для загрузки модулей USB-устройств. Такие устройства на сервере не используются. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e hotplug
```

Пакет `lokkit`

Пакет `lokkit` содержит приложение для конфигурации системы сетевой защиты, ориентированной на рабочую станцию для среднего пользователя (удаленный доступа к сети и модемное соединение), и не предназначен для конфигурирования системы сетевой защиты сервера. Для настройки сетевой защиты авторы рекомендуют использовать `GIPTables`. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e lokkit
```

Пакет `ipchains`

Пакет `ipchains` содержит утилиту, используемую с ядром Linux версии 2.2 для управления возможностями фильтрации пакетов. Существует новый и более мощный инструмент, известный как `IP-Tables`. Именно его мы будем использовать позже для установки системы сетевой защиты на сервере. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e ipchains
```

Пакет `ksymoops`

Пакет `ksymoops` содержит приложения, сообщающие об ошибках ядра. Этот пакет полезен для разработчиков, которые занимаются отладкой ядра, или для пользователей, которые хотят использовать сообщения об ошибках ядра. Тот же самый результат может быть достигнут с помощью команды `dmesg`. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e ksymoops
```

Пакет `kudzu`

Пакет `kudzu` содержит средства автоматической диагностики и конфигурирования устройств при загрузке системы. На сервере, где конфигурация устройств практически постоянна, в наличии данного пакета нет никакой необходимости. Удалите его:

```
[root@drwalbr /]# rpm -e kudzu
```

Пакет `mailcap`

Пакет `mailcap` используется программой `Metamail` для определения того, как должны быть воспроизведены мультимедийные файлы. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e mailcap
```

Пакет `pciutils`

Пакет `pciutils` содержит различные утилиты для того, чтобы сканировать и устанавливать PCI-устройства. Удалите пакет:

```
[root@drwalbr /]# rpm -e pciutils
```

Пакет `raidtools`

Пакет `raidtools` включает средства, которые необходимы для установки и поддержки программного обеспечения RAID-устройств. Этот пакет следует оставить только в случае, если предполагается использовать RAID. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e raidtools
```

Пакет `asplinux-logos`

Пакет `asplinux-logos` содержит графические файлы (иконки, рисунки, эмблемы) ASPLinux. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e asplinux-logos
```

Пакет `asplinux-release`

Пакет `asplinux-release` содержит файлы с версией дистрибутива ASPLinux. При удалении пакета необходимо создать файлы `/etc/asplinux-release` и `/etc/redhat-release`, куда следует записать произвольную строку, которая будет впоследствии отображаться при загрузке системы:

```
[root@drwalbr /]# rpm -e --nodeps asplinux-release
[root@drwalbr /]# echo You string > /etc/asplinux-release
```

```
[root@drwalbr /]# cp  /etc/asplinux-release /etc/redhat-release
```

Пакет `setserial`

Пакет `setserial` содержит системные утилиты для отображения и управления последовательным портом. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e setserial
```

Пакет `hdparm`

Пакет `hdparm` содержит утилиту для оптимизации настроек жестких дисков с IDE-контроллерами. Если у вас SCSI жесткие диски, этот пакет следует удалить. Выполните:

```
[root@drwalbr /]# rpm -e hdparm
```

Пакет `mkinitrd`

Пакет `mkinitrd` необходим на системах с жесткими дисками SCSI или RAID. Если у вас установлены жесткие диски с IDE-контроллером, этот пакет следует удалить. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e --nodeps mkinitrd
```

Пакеты `kbdconfig, mouseconfig, timeconfig, netconfig, authconfig, ntsysv` и `setuptool`

Данные пакеты предназначены для установки языка и типа клавиатуры, типа мыши, заданного по умолчанию часового пояса, устройств Ethernet, NIS и паролей, многочисленные символьные ссылки в каталоге `/etc/rc.d` и утилиту, которая позволяет в режиме текстового меню изменять эти настройки. Если когда-нибудь потребуется изменить данные настройки, достаточно будет просто установить эти пакеты. Для удаления пакетов выполните:

```
[root@drwalbr /]# rpm -e kbdconfig mouseconfig timeconfig netconfig auth-
config ntsysv setuptool
```

Пакет `newt`

Пакет `newt` содержит библиотеку для текстовых интерфейсов, в том числе и для только что удаленных конфигурационных утилит. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e newt
```

Пакет `lilo`

Пакет `lilo` содержит загрузчик системы – LILO. Если вы собираетесь его использовать, то не нужно удалять этот пакет. Авторы рекомендуют использовать GRUB. В этом случае можно удалить данный пакет:

```
[root@drwalbr /]# rpm -e lilo
```

Пакет `asplrd`

Пакет `asplrd` содержит загрузчик системы ASPLoader. Если вы собираетесь использовать именно его, то не удаляйте этот пакет. В противном случае удалите данный пакет:

```
[root@drwalbr /]# rpm -e aspldr
[root@drwalbr /]# rm -f /etc/aspldr.conf
```

Пакет `reiserfs-utils`

Пакет `reiserfs-utils` содержит множество утилит для администрирования (создания, проверки, изменения и восстановления) файловой системы Reiserfs. В нашем варианте установки используются файловые системы Ext2 или Ext3, поэтому можно удалить пакет:

```
[root@drwalbr /]# rpm -e reiserfs-utils
```

Пакет `quota`

Пакет `quota` содержит средства для контроля и ограничения использования файловой системы диска различными пользователями и группами. Эта программа должна быть установлена только на серверах, где в этом есть необходимость. В остальных случаях можно удалить пакет:

```
[root@drwalbr /]# rpm -e quota
```

Пакет `indexhtml`

Пакет `indexhtml` содержит HTML-код и графику для начальной страницы, показываемую браузером при использовании графического интерфейса инсталляции. Эти HTML-страницы содержат информацию о программном обеспечении ASPLinux. На самом деле, нет никакой надобности в этом пакете при инсталляции сервера и особенно в случае, когда графический интерфейс пользователя не доступен. Поэтому можно спокойно удалить этот пакет из системы. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e indexhtml
```

Пакет `usbutils`

Пакет `usbutils` содержит средства взаимодействия ОС с USB-устройствами, которые на сервере не используются. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e usbutils
```

Пакет `hwdata`

Пакет `hwdata` содержит данные о конфигурации USB-устройств, используемые, в основном, XFree86. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e hwdata
```

Пакет `hesiod`

Пакет `hesiod` – еще один пакет, который можно удалить после завершения конфигурации сервера. Программа использует существующие функциональные возможности DNS для обеспечения доступа к базам данных с редко изменяемой информацией. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e hesiod
```

Пакет `mt-st`

Пакет `mt-st` содержит средства управления накопителями на магнитной ленте. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e mt-st
```

Пакеты `man-pages` и `man-pages-ru-asp`

Данные пакеты содержат страницы руководства (man-страницы). Их место – на рабочей станции администратора сервера. Для удаления пакетов выполните:

```
[root@drwalbr /]# rpm -e man-pages
[root@drwalbr /]# rpm -e man-pages-ru-asp
```

Пакет `sendmail`

Даже если вы не хотите использовать вашу систему в качестве почтового сервера, почтовый транспортный агент (Mail Transport Agent) необходим для доставки сообщений, посылаемых пользователю `root` различными службами. Авторы не рекомендуют использовать `sendmail` из соображений безопасности. Вы должны удалить данный пакет и обратиться к той части книги, где описана установка и конфигурация альтернативного программного обеспечения – `Exim` или `Qmail`. Для удаления пакета выполните:

```
[root@drwalbr /]# /etc/init.d/sendmail stop
[root@drwalbr /]# rpm -e sendmail
```

Пакет `procmail`

Пакет `procmail` содержит программу обработки почты, используемую `sendmail`. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e procmail
```

Пакет `openldap`

Пакет `openldap` предназначен для обращения к базам данных, содержащих информацию об адресах, телефонах для пользователей сети и сервисов. Эта полезная программа устраивает не всех пользователей. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e --nodeps openldap
```

Пакеты `cyrus-sasl`, `cyrus-sasl-md5`, `cyrus-sasl-plain`

Данные пакеты содержат дополнительные средства идентификации для программы Cyrus, которая является электронной программой передачи сообщений, подобно Sendmail. Cyrus SASL в данном дистрибутиве используется совместно с Sendmail. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e --nodeps cyrus-sasl
```

Пакет `openssl`

Пакет `openssl` содержит средства шифрования, которые, как предполагают его разработчики, гарантируют и обеспечивают сохранность и конфиденциальность информации, передаваемой по сетям общего пользования. Эта часть программного обеспечения - одна из самых важных, с точки зрения обеспечения безопасности системы, и обязательно должна быть установлена. К сожалению, тот пакет, который идет в дистрибутиве ASPLinux – устаревшей версии. Поэтому сейчас его следует удалить. К нему мы обратимся в главах, связанных с установкой программ безопасности. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e --nodeps openssl
[root@drwalbr /]# rm -rf /usr/share/ssl/
```

Пакеты `ash`, `tcsh`

Пакеты `ash`, `tcsh` содержат командные интерпретаторы, не используемые нами. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e ash
[root@drwalbr /]# rpm -e tcsh
```

Пакет `specspo`

Пакет `specspo` содержит объектные каталоги для интернационализации ASPLinux. Не думаем, что этот пакет действительно необходим. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e specspo
```

Пакет `krb5-lib`

Пакет `krb5-lib` содержит динамические библиотеки, необходимые программе Kerberos 5. Поскольку данная программа у нас не используется, можно удалить этот пакет. Для удаления пакета выполните:

```
[root@drwalbr /]# rpm -e krb5-libs
[root@drwalbr /]# rm -rf /usr/kerberos/
```

Удаление ненужных файлов документации.

По умолчанию большинство пакетов rpm, устанавливаемых под Linux, идет с документацией по соответствующим программам. Эта документация содержит первоначальные файлы из архива программ tar, подобно `readme`, `faq`, `bug`, `install`, `news`, `projects` и другим. Многие из них могут быть легко найдены на том Web-узле, откуда программа была загружена. Нет особого смысла сохранять их на системе. Конечно, емкости жестких дисков значительно возросли, но зачем оставлять документацию на сервере с высоким уровнем безопасности, к которой почти не будут обращаться? Тем не менее, взгляните на эти файлы еще раз и решите, оставить их или удалить. Для удаления файлов документации выполните:

```
[root@drwalbr /]# cd /usr/share/doc/
[root@drwalbr doc]# rm -rf *
```

Удаление ненужных (пустых) файлов и каталогов.

Существуют некоторые файлы и каталоги, которые можно безболезненно удалить. Некоторые их них – ошибки сценария инсталляции ASPLinux, другие созданы по умолчанию. Для их удаления выполните:

```
[root@drwalbr /]# rm -f /etc/exports
[root@drwalbr /]# rm -f /etc/printcap
[root@drwalbr /]# rm -f /etc/hosts.allow
[root@drwalbr /]# rm -f /etc/hosts.deny
[root@drwalbr /]# rm -f /etc/csh.login
[root@drwalbr /]# rm -f /etc/csh.cshrc
[root@drwalbr /]# rm -f /etc/fstab.REVOKE
[root@drwalbr /]# rm -f /etc/pam_smbd.conf
[root@drwalbr /]# rm -rf /etc/xinetd.d/
[root@drwalbr /]# rm -rf /etc/opt/
[root@drwalbr /]# rm -rf /var/nis/
[root@drwalbr /]# rm -rf /var/yp/
[root@drwalbr /]# rm -rf /var/lib/games/
[root@drwalbr /]# rm -rf /var/spool/lpd/
[root@drwalbr /]# rm -rf /usr/lib/games/
[root@drwalbr /]# rm -rf /usr/local/
[root@drwalbr /]# rm -rf /usr/dict/
[root@drwalbr /]# rm -rf /usr/X11R6/
[root@drwalbr /]# rm -f /usr/lib/X11
```

ЗАМЕЧАНИЕ Если в будущем возникнет необходимость в установке программы, которой потребуются некоторые из удаленных файлов или каталогов, то программа сама их создаст в процессе инсталляции.

Указанные выше операции могут быть легко осуществлены с помощью скрипта `deinstall`, приведенного ниже:

```
#!/bin/sh
##########################################################
#######Скрипт для деинсталляции ненужных пакетов и######
#######   и удаления файлов и каталогов           ######
##########################################################
#Удаляем anacron
#/etc/init.d/anacron stop
#rpm -e anacron
#rm -rf /var/spool/anacron/
#Удаляем apmd
#/etc/init.d/apmd stop
#rpm -e apmd
#Удаляем at
#/etc/init.d/atd stop
#rpm -e at
#Удаляем gpm
#/etc/init.d/gpm stop
#rpm -e gpm
#Удаляем другие пакеты
#rpm -e dhcpcd eject hotplug lokkit ipchains ksymoops kudzu mailcap \
#pciutils raidtools asplinux-logos
#rpm -e –-nodeps asplinux-release
#echo You string /etc/asplinux-release
#cp /etc/asplinux-release /etc/redhat-release
#Удаление hdparm только для SCSI систем
#rpm -e hdparm
#Удаление
#rpm -e mkinitrd
#Удаляем пакеты конфигурирования X-сервера
#rpm -e kbdconfig mouseconfig timeconfig netconfig \
#authconfig ntsysv setuptool
#Удаляем newt
#rpm -e newt
#Удаляем LILO если используем GRUB
#rpm -e lilo
#Удаляем asplrd
#rpm -e aspldr
#rm –f /etc/asplrd.conf
#Удаляем reiserfs-utils
#rpm -e reiserfs-utils
#Удаляем quota#
#rpm -e quota
#Удаляем
#rpm -e indexhtml usbutils hwdata hesiod
#Удаляем man-страницы
#rpm -e man-pages
#rpm -e man-pages-ru-asp
#Удаляем sendmail
#/etc/init.d/sendmail stop
#rpm -e sendmail
#Удаляем procmail
#rpm -e procmail
#Удаляем openldap
#rpm -e --nodeps openldap
#Удаляем cyrus-sasl
#rpm -e --nodeps cyrus-sasl cyrus-sasl-md5 cyrus-sasl-plain
#Удаляем openssl
#rpm -e --nodeps openssl
#rm -rf /usr/share/ssl/
#Удаляем ash и tcsh
#rpm -e ash tcsh
#Удаляем specspo
#rpm -e specspo
#Удаляем krb5-libs
```

```
#rpm -e krb5-libs
#rm -rf /usr/kerberos/
#Удаляем yum
#rpm -e yum
#Удаляем ненужные файлы и каталоги
#rm -f /etc/exports
#rm -f /etc/printcap
#rm -f /etc/hosts.allow
#rm -f /etc/hosts.deny
#rm -f /etc/csh.login
#rm -f /etc/csh.cshrc
#rm -f /etc/fstab.REVOKE
#rm -f /etc/pam_smbd.conf
#rm -rf /etc/xinetd.d/
#rm -rf /etc/opt/
#rm -rf /var/nis/
#rm -rf /var/yp/
#rm -rf /var/lib/games/
#rm -rf /var/spool/lpd/
#rm -rf /usr/lib/games/
#rm -rf /usr/local/
#rm -rf /usr/dict/
#rm -rf /usr/X11R6/
#rm -f /usr/lib/X11
```

Удалите комментарии из строк, ответственных за удаление пакетов, каталогов, файлов, ненужных в требуемой конфигурации, и запустите скрипт.

Дополнительно устанавливаемые пакеты

Если планируется компилировать программное обеспечение на сервере, необходимо установить ряд дополнительных пакетов – пакеты, содержащие языки программирования, используемые ими библиотеки, пакеты, разрешающие зависимости, и файловый менеджер `mc` (аналог популярного файлового менеджера для DOS Norton Commander). В противном случае – т. е. если вы не собираетесь заниматься компиляцией программ на сервере, устанавливаете и обновляете программное обеспечение, используя только rpm-пакеты, например, используя рабочую станцию для разработки, компиляции и создания собственных rpm-пакетов с последующей их установкой на сервере – не следует выполнять приведенные ниже рекомендации по установке дополнительных пакетов.

Установка дополнительных пакетов осуществляется следующим образом.

Шаг 1

Скопируйте первый, второй и третий диски в некоторый каталог, например, `/home/distrib`/. Для этого сначала создайте его:

```
[root@drwalbr /]# mkdir /home/distrib
```

Вставьте первый инсталляционный диск в привод CD-ROM. Выполните команды:

```
[root@drwalbr /]# mount /mnt/cdrom
[root@drwalbr /]# cp /mnt/cdrom/ASPLinux/RPMS/* /home/distrib
[root@drwalbr /]# umount /mnt/cdrom
```

Вставьте второй инсталляционный диск в привод CD-ROM. Выполните команды:

```
[root@drwalbr /]# mount /mnt/cdrom
[root@drwalbr /]# cp /mnt/cdrom/ASPLinux/RPMS/* /home/distrib
[root@drwalbr /]# umount /mnt/cdrom
```

Вставьте третий инсталляционный диск в привод CD-ROM. Выполните команды:

```
[root@drwalbr /]# mount /mnt/cdrom
[root@drwalbr /]# cp /mnt/cdrom/ASPLinux/RPMS/* /home/distrib
[root@drwalbr /]# umount /mnt/cdrom
```

Шаг 2

Установите необходимые пакеты:

```
[root@drwalbr /]# cd /home/distrib
```

```
[root@drwalbr distrib]# rpm -ihv binutils-2.11.93.0.2-11.i386.rpm
[root@drwalbr distrib]# rpm -ihv cpp-2.96-112asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv freetype-2.0.9-2.i386.rpm
[root@drwalbr distrib]# rpm -ihv m4-1.4.1-7.i386.rpm
[root@drwalbr distrib]# rpm -ihv make-3.79.1-8.i386.rpm
[root@drwalbr distrib]# rpm -ihv patch-2.5.4-12.i386.rpm
[root@drwalbr distrib]# rpm -ihv perl-5.6.1-34.99.6.i386.rpm
[root@drwalbr distrib]# rpm -ihv libjpeg-6b-19.i386.rpm
[root@drwalbr distrib]# rpm -ihv libpng-1.0.12-2.i386.rpm
[root@drwalbr distrib]# rpm -ihv gd-1.8.4-4.asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv libtool-libs-1.4.2-7.i386.rpm
[root@drwalbr distrib]# rpm -ihv pspell-0.12.2-8asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv mc-4.5.55-5.1asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv bison-1.35-1.i386.rpm
[root@drwalbr distrib]# rpm -ihv byacc-1.9-19.i386.rpm
[root@drwalbr distrib]# rpm -ihv cproto-4.6-9.i386.rpm
[root@drwalbr distrib]# rpm -ihv cdecl-2.5-22.i386.rpm
[root@drwalbr distrib]# rpm -ihv ctags-5.2.2-2.i386.rpm
[root@drwalbr distrib]# rpm -ihv flex-2.5.4a-23.i386.rpm
[root@drwalbr distrib]# rpm -ihv glibc-kernheaders-2.4-7.14.asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv glibc-devel-2.2.5-37asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv gcc-2.96-112asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv libstdc++-devel-2.96-112asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv gcc-c++-2.96-112asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv db3-devel-3.3.11-6.i386.rpm
[root@drwalbr distrib]# rpm -ihv freetype-devel-2.0.9-2.i386.rpm
[root@drwalbr distrib]# rpm -ihv gdbm-devel-1.8.0-14.i386.rpm
[root@drwalbr distrib]# rpm -ihv gd-devel-1.8.4-4.asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv libjpeg-devel-6b-19.i386.rpm
[root@drwalbr distrib]# rpm -ihv zlib-devel-1.1.3-25.7.i386.rpm
[root@drwalbr distrib]# rpm -ihv libpng-devel-1.0.12-2.i386.rpm
[root@drwalbr distrib]# rpm -ihv ncurses-devel-5.2-26.i386.rpm
[root@drwalbr distrib]# rpm -ihv pam-devel-0.75-32.2asp.i386.rpm
[root@drwalbr distrib]# rpm -ihv pspell-devel-0.12.2-8asp.i386.rpm
```

Указанные выше операции могут быть легко осуществлены с помощью сценария:

```
#!/bin/sh
############################################################
#######Скрипт для установки дополнительных пакетов ######
############################################################
rpm -ihv binutils-2.11.93.0.2-11.i386.rpm\
cpp-2.96-112asp.i386.rpm \
freetype-2.0.9-2.i386.rpm \
m4-1.4.1-7.i386.rpm \
make-3.79.1-8.i386.rpm \
patch-2.5.4-12.i386.rpm \
perl-5.6.1-34.99.6.i386.rpm \
libjpeg-6b-19.i386.rpm \
libpng-1.0.12-2.i386.rpm \
gd-1.8.4-4.asp.i386.rpm \
libtool-libs-1.4.2-7.i386.rpm \
pspell-0.12.2-8asp.i386.rpm \
mc-4.5.55-5.1asp.i386.rpm \
bison-1.35-1.i386.rpm \
byacc-1.9-19.i386.rpm \
cproto-4.6-9.i386.rpm \
cdecl-2.5-22.i386.rpm \
ctags-5.2.2-2.i386.rpm \
flex-2.5.4a-23.i386.rpm \
glibc-kernheaders-2.4-7.14.asp.i386.rpm \
glibc-devel-2.2.5-37asp.i386.rpm \
gcc-2.96-112asp.i386.rpm \
libstdc++-devel-2.96-112asp.i386.rpm \
gcc-c++-2.96-112asp.i386.rpm \
```

```
db3-devel-3.3.11-6.i386.rpm \
freetype-devel-2.0.9-2.i386.rpm \
gdbm-devel-1.8.0-14.i386.rpm \
gd-devel-1.8.4-4.asp.i386.rpm \
libjpeg-devel-6b-19.i386.rpm \
zlib-devel-1.1.3-25.7.i386.rpm \
libpng-devel-1.0.12-2.i386.rpm \
ncurses-devel-5.2-26.i386.rpm \
pam-devel-0.75-32.2asp.i386.rpm \
pspell-devel-0.12.2-8asp.i386.rpm \
```

Если размеры жесткого диска не позволяют скопировать три первых диска дистрибутива, можно ограничиться только копированием требуемых пакетов.

На первом диске находятся:

```
cpp-2.96-112asp.i386.rpm
freetype-2.0.9-2.i386.rpm
gd-1.8.4-4.asp.i386.rpm
libjpeg-6b-19.i386.rpm
libpng-1.0.12-2.i386.rpm
libtool-libs-1.4.2-7.i386.rpm
m4-1.4.1-7.i386.rpm
make-3.79.1-8.i386.rpm
mc-4.5.55-5.1asp.i386.rpm
patch-2.5.4-12.i386.rpm
perl-5.6.1-34.99.6.i386.rpm
pspell-0.12.2-8asp.i386.rpm
```

На втором диске находятся:

```
bison-1.35-1.i386.rpm
byacc-1.9-19.i386.rpm
cproto-4.6-9.i386.rpm
cdecl-2.5-22.i386.rpm
ctags-5.2.2-2.i386.rpm
flex-2.5.4a-23.i386.rpm
gcc-2.96-112asp.i386.rpm
gcc-c++-2.96-112asp.i386.rpm
glibc-devel-2.2.5-37asp.i386.rpm
glibc-kernheaders-2.4-7.14.asp.i386.rpm
```

На третьем диске находятся:

```
db3-devel-3.3.11-6.i386.rpm
freetype-devel-2.0.9-2.i386.rpm
gdbm-devel-1.8.0-14.i386.rpm
gd-devel-1.8.4-4.asp.i386.rpm
gd-devel-1.8.4-4.asp.i386.rpm
libjpeg-devel-6b-19.i386.rpm
libpng-devel-1.0.12-2.i386.rpm
libstdc++-devel-2.96-112asp.i386.rpm
ncurses-devel-5.2-26.i386.rpm
pam-devel-0.75-32.2asp.i386.rpm
pspell-devel-0.12.2-8asp.i386.rpm
zlib-devel-1.1.3-25.7.i386.rpm
```

Для копирования дополнительных пакетов в раздел `/home/distrib/` вставьте первый инсталляционный диск в привод CD-ROM. Выполните команды:

```
[root@drwalbr /]# mount /mnt/cdrom
[root@drwalbr /]# cd /mnt/cdrom/ASPLinux/RPMS
[root@drwalbr RPMS]# cp cpp-2.96-112asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp freetype-2.0.9-2.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp m4-1.4.1-7.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp make-3.79.1-8.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp patch-2.5.4-12.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp perl-5.6.1-34.99.6.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp gd-1.8.4-4.asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp libjpeg-6b-19.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp libpng-1.0.12-2.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp libtool-libs-1.4.2-7.i386.rpm /home/distrib/
```

```
[root@drwalbr RPMS]# cp pspell-0.12.2-8asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp mc-4.5.55-5.1asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cd /
[root@drwalbr /]# umount /mnt/cdrom/
```

Вставьте второй инсталляционный диск в привод CD-ROM. Выполните команды:

```
[root@drwalbr /]# mount /mnt/cdrom/
[root@drwalbr /]# cd /mnt/cdrom/ASPLinux/RPMS
[root@drwalbr RPMS]# cp bison-1.35-1.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp byacc-1.9-19.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp cproto-4.6-9.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp cdecl-2.5-22.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp ctags-5.2.2-2.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp flex-2.5.4a-23.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp gcc-2.96-112asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp gcc-c++-2.96-112asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp glibc-kernheaders-2.4-7.14.asp.i386.rpm
/home/distrib/
[root@drwalbr RPMS]# cp glibc-devel-2.2.5-37asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cd /
[root@drwalbr /]# umount /mnt/cdrom
```

Вставьте третий инсталляционный диск в привод CD-ROM. Выполните команды:

```
[root@drwalbr /]# mount /mnt/cdrom
[root@drwalbr /]# cd /mnt/cdrom/ASPLinux/RPMS
[root@drwalbr RPMS]# cp db3-devel-3.3.11-6.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp freetype-devel-2.0.9-2.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp gdbm-devel-1.8.0-14.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp gd-devel-1.8.4-4.asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp libjpeg-devel-6b-19.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp libpng-devel-1.0.12-2.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp libstdc++-devel-2.96-112asp.i386.rpm
/home/distrib/
[root@drwalbr RPMS]# cp ncurses-devel-5.2-26.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp pam-devel-0.75-32.2asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp pspell-devel-0.12.2-8asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp zlib-devel-1.1.3-25.7.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cp gd-devel-1.8.4-4.asp.i386.rpm /home/distrib/
[root@drwalbr RPMS]# cd /
[root@drwalbr /]# umount /mnt/cdrom
```

Для установки пакетов выполните команды:

```
[root@drwalbr /]# cd /home/distrib/
[root@drwalbr distrib]# rpm –ihv *.rpm
```

ЗАМЕЧАНИЕ Выше описан процесс установки только самых необходимых пакетов для компиляции программ. Некоторое программное обеспечение может потребовать установить дополнительные пакеты как для компиляции, так и для своей работы. Обычно это отражено в документации.

Шаг 3

После окончания инсталляции, компиляции и настройки всех программ на сервере необходимо удалить все дополнительно установленные пакеты, т. к. они занимают место на диске и негативно влияют на безопасность системы. Например, если взломщик программной защиты получит доступ к вашему серверу, он не сможет компилировать, не установив соответствующие пакеты, и, следовательно, установить свои варианты исполняемых файлов.

Глава 3

Общие мероприятия по обеспечению безопасности сервера

В этой главе:

1. Настройки BIOS
2. Отключение сервера от сети
3. Концепция безопасности
4. Выбор правильного пароля
5. Учетная запись суперпользователя root
6. История оболочки командного интерпретатора
7. Однопользовательский режим входа в систему
8. Отключение возможности выключения системы с помощью комбинации клавиш <Ctrl>+<Alt>+<Delete>
9. Ограничение заданного по умолчанию числа запущенных виртуальных консолей ttys
10. LILO и файл /etc/lilo.conf
11. GRUB и файл /boot/grub/grub.conf
12. Файл /etc/services
13. Файл /etc/security
14. Специальные учетные записи
15. Управление монтированием файловых систем
16. Права доступа к файлам сценариев запуска и остановки процессов
17. Специальные символы у программ, владельцем которых является root
18. Запрещение внутренним компьютерам сообщать серверу свой MAC-адрес
19. Необычные или скрытые файлы
20. Обнаружение файлов и каталогов, изменяемых любым пользователем
21. Файлы без владельцев
22. Поиск файлов .rhosts
23. Копии файлов регистрации на жестких носителях и удаленных системах
24. Удаление страниц руководства

Безопасность сервера определяется не только типом и версией установленной операционной системы, но в основном, грамотной его настройкой. В этой главе рассматриваются некоторые из основных методов, обеспечивающих безопасность вашей системы, которые можно использовать для предотвращения атак из внешней или локальной сети.

Настройки BIOS

Отключите в настройках BIOS возможность загрузки системы с дискеты и/или загрузочного компакт-диска и установите пароль на вход в BIOS. Это предотвратит попытки сторонних лиц загрузить систему, используя специальный загрузочный диск или изменить настройки BIOS (например, разрешить начальную загрузку диска или загрузку сервера без ввода пароля). Обратите внимание, что существует принципиальная возможность обойти эту меру защиты, получив физический доступ к серверу. Поэтому авторы настоятельно рекомендуют ограничить доступ как в помещение, где расположен сервер, так и внутрь его корпуса.

Отключение сервера от сети

Изменение настроек безопасности сервера не рекомендуется проводить на работающей в сети системе. Для остановки всех сетевых интерфейсов системы (программного отключения) выполните:

```
[root@drwalbr /]# /etc/init.d/network stop
Деактивируется интерфейс eth0:              [OK]
Деактивируется интерфейс eth1:              [OK]
```

Для запуска всех сетевых интерфейсов системы выполните:

```
[root@drwalbr /]# /etc/init.d/network start
Устанавливаются параметры сети:      [OK]
Активизируется интерфейс lo:                [OK]
Активизируется интерфейс eth0:              [OK]
Активизируется интерфейс eth1:              [OK]
```

Для остановки и запуска только одного сетевого интерфейса, выполните, соответственно:

```
[root@drwalbr /]# ifdown eth0
[root@drwalbr /]# ifup eth0
```

Концепция безопасности

Важно подчеркнуть, что нельзя успешно осуществлять действия, направленные на повышение безопасности, без четкого представления, чего вы хотите добиться и от чего должны быть защищены. Необходимо выработать концепцию безопасности, т. е. перечень организационно-технических мероприятий, которые обеспечат разумный компромисс между функциональностью системы и уровнем ее безопасности. Любая концепция безопасности должна основываться на некоторой степени недоверия к людям, как внутри, так и за пределами вашей организации.

Выбор правильного пароля

Отправная точка возведения здания безопасности сервера – пароль. Много людей сохраняют свою ценную информацию и файлы на компьютере. Единственной вещью, защищающей ее от постороннего внимания, является строка из нескольких символов, называемая паролем. В отличие от общераспространенного мнения, не существует паролей, которые нельзя было бы расшифровать. В действительности все пароли могут быть получены методами «социальной инженерии» или простым последовательным перебором.

Социальная разработка паролей сервера – самый простой и самый популярный способ получения доступа к учетным записям и серверам. Человеческий фактор еще никто не отменял. Часто знание таких простых вещей, как названия компаний, действующих или временных должностей пользователей, даты известных событий и др. приводят к потрясающим результатам.

Было бы неплохо запускать взломщика пароля на вашей системе каждую неделю. Он поможет в поиске и замене паролей, которые легко могут быть раскрыты. Также необходим механизм, проверяющий пароли с целью недопущения ненадежных паролей при выборе пользователями начальных паролей или изменении старых. Символьные строки, которые являются обычными словами или набранные в одном регистре, не содержащие чисел или специальных символов, не должны приниматься в качестве нового пароля.

Авторы рекомендуют следующие правила выбора паролей:

- пароль должен состоять, по крайней мере, из восьми символов, включая, одну цифру или специальный символ;

• пароль не должен быть тривиальным, т. е. чтобы его нельзя было предсказать, используя общедоступную информацию о пользователях (фамилии, адреса, памятные даты, телефоны и др. информация личного характера);

• пароль должен иметь ограниченный срок действия, по истечении которого должен быть выбран новый;

• пароль должен блокироваться после нескольких (двух…трех попыток) его неправильного ввода.

Учетная запись суперпользователя root

Учетная запись `root` – самая привилегированная учетная запись на Unix-системе. Она не имеет никаких ограничений по безопасности. Поэтому очень просто, допустив ошибку в наборе команды, удалить критически важные системные файлы. При использовании этой учетной записи важно быть очень осторожным и внимательным.

Часто администраторы, зарегистрировавшись в качестве суперпользователя `root`, забывают выйти из системы после окончания работы. Поэтому желательно использовать автоматическое завершение сеанса оболочки `bash` после бездействия консоли в течение определенного периода времени.

Шаг 1

Установите специальную переменную, названную TMOUT, равную интервалу времени в секундах, по истечении которого при отсутствии ввода с клавиатуры произойдет выход из системы. Для этого в файле `/etc/profile` добавьте следующую строку где-нибудь после строки, начинающейся с `HISTSIZE =:`

```
HOSTNAME= ' /bin/hostname '
HISTSIZE=1000
TMOUT=3600
```

Значение, присвоенное переменной TMOUT = , выражено в секундах и составляет 1 час ((60*60)*1=3600*1=3600 с).

ЗАМЕЧАНИЕ Если вышеупомянутая строка вставлена в файл `/etc/profile`, то через 1 час произойдет автоматическое завершение сеансов всех пользователей системы. Если вы желаете установить для разных пользователей различные значения `TMOUT` то строка `TMOUT=…` должна быть добавлена в файл `.bashrc` , находящийся в домашнем каталоге пользователя.

Шаг 2

В файле `/etc/profile` в строке:

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE INPUTRC
```

добавьте параметр `TMOUT`:

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE TMOUT INPUTRC
```

Для вступления изменений в силу завершите сеанс и зарегистрируйтесь в системе как суперпользователь `root`.

История оболочки командного интерпретатора

Для облегчения ввода повторяющихся команд, командный интерпретатор сохраняет до 1000 команд в файле `~/.bash_history` (где " `~/` " является вашим домашним каталогом). Пользователь может вместо повторного набора команды с помощью клавиш <Стрелка вверх> и <Стрелка вниз> вывести ранее набранную команду в командную строку и исполнить ее нажатием клавиши <Enter>. Некоторые команды могут запрашивать пароль. В результате ошибочных действий пользователя этот пароль может быть введен в командную строку и, следовательно, сохраниться в файле `.bash_history`. Сокращение числа запоминаемых команд уменьшает вероятность сохранения в этом файле паролей, ошибочно введенных открытым текстом в командную строку. Для этого выполните некоторые действия.

Шаг 1

Значение параметра `HISTSIZE` в файле `/etc/profile` определяет число сохраняемых старых команд в файле `.bash_history` для всех пользователей системы. Для всех учетных записей мы рекомендовали бы устанавливать значение параметра `HISTSIZE` в файле `/etc/profile` не более 10.

Для этого в файле `/etc/profile` измените:

```
HISTSIZE=1000
```

на:

```
HISTSIZE=10
```

Шаг 2

Для того, чтобы файл `.bash_history` уничтожался при каждом выходе пользователя из системы, в файл `/etc/profile` после строки, в которой устанавливается значение параметра `HISTSIZE`, добавьте строку:

```
HISTSIZE=10
HISTFILESIZE=0
```

Шаг 3

В файле `/etc/profile` в строке:

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE TMOUT INPUTRC
```

добавьте параметр `HISTFILESIZE`:

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTFILESIZB TMOUT
INPUTRC
```

Для вступления изменений в силу завершите сеанс и зарегистрируйтесь в системе как суперпользователь `root`.

Однопользовательский режим входа в систему

При использовании загрузчика LILO имеется возможность входа в однопользовательский режим. Это достигается путем ввода при загрузке LILO команды:

```
LILO: linux single
```

При этом вы регистрируетесь в системе как суперпользователь `root` без ввода пароля. Для того, чтобы система запрашивала пароль при входе в однопользовательский режим необходимо выполнить некоторые действия.

Шаг 1

В файле `/etc/inittab` измените строку:

```
id:3:initdefault:
```

на:

```
id:3:initdefault:
~~:S:wait:/sbin/sulogin
```

Добавление этой строки потребует ввода пароля `root` перед продолжением загрузки в однопользовательском режиме (программа `init` инициализирует выполнение программы `sulogin` перед входом в оболочку).

Шаг 2

Для того, чтобы сделанные изменения вступили в силу, выполните:

```
[root@drwalbr /]# /sbin/init q
```

Отключение возможности выключения системы с помощью комбинации клавиш <Ctrl>+<Alt>+<Delete>

Для отключения возможности выключения (перезагрузки) системы с помощью комбинации клавиш `<Ctrl>+<Alt>+<Delete>` в файле `/etc/inittab` удалите (закомментируйте) строку:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

т. е.:

```
#ca::ctrlaltdel:/shin/shutdown-t3-r now
```

Шаг 2

Для того, чтобы сделанные изменения вступили в силу, выполните:

```
[root@drwalbr /]# /sbin/init q
```

Ограничение заданного по умолчанию числа запущенных виртуальных консолей ttys

По умолчанию в ASPLinux допускается одновременный запуск шести виртуальных консолей в стандартных выполняемых уровнях. На сервере с высоким уровнем безопасности следует ограничиться двумя виртуальными консолями и заодно сэкономить некоторые ресурсы, которые могут быть задействованы для выполнения других процессов.

Шаг 1

В файле `/etc/inittab` удалите (закомментируйте) следующие строки:

```
1:2345: respawn: /sbin/mingetty ttyl
```

```
2:2345: respawn: /sbin/mingetty tty2
3:2345: respawn: /sbin/mingetty tty3
4:2345: respawn: /sbin/mingetty tty4
5:2345: respawn: /sbin/mingetty tty5
6:2345: respawn: /sbin/mingetty tty6
```

т. е.:

```
1:2345: respawn: /sbin/mingetty ttyl
2:2345: respawn: /sbin/mingetty tty2
#3:2345: respawn: /sbin/mingetty tty3
#4:2345: respawn: /sbin/mingetty tty4
#5:2345: respawn: /sbin/mingetty tty5
#6:2345: respawn: /sbin/mingetty tty6
```

Шаг 2

Для того, чтобы сделанные изменения вступили в силу, выполните:

```
[root@drwalbr /]# /sbin/init q
```

LILO и файл /etc/lilo.conf

Если вы используетесь LILO в качестве загрузчика операционной системы, то для обеспечения безопасности системы необходимо установить ряд параметров загрузчика в файле `/etc/lilo.conf`. К числу таких параметров относятся:

- параметр `timeout=00` – определяет длительность интервала времени в десятых долях секунды в течение которого LILO ожидает пользовательского ввода (например, команды на переход в однопользовательский режим, выбор загружаемого образа ядра и т. п.);
- опция `restricted` – указывает на необходимость запроса пароля только, если параметры определены в командной строке (например, `linux single`). Эту опцию следует использовать только совместно с параметром `password`;
- опция `password=Secretnoe$l0vo` – указывает на необходимость запроса пароля при загрузке образа ядра (при использовании опции `restricted` пароль будет запрашиваться только при введении параметров загрузки в командной строке, обычная загрузка будет осуществляться без ввода пароля).

Для установки опций безопасности выполните следующий алгоритм.

Шаг 1

Отредактируйте файл `/etc/lilo.conf`, добавив или изменив строки, в соответствии с рекомендациями:

```
boot=/dev/hda
prompt
timeout=00
lba32
default=linux-2.4.18

# ASPLinux
image=/boot/vmlinuz-2.4.18-5asp
initrd=/boot/initrd.2.4.18-5asp.img
restricted
password= Secretnoe$l0vo
label=ASPLinux-2.4.18
root=/dev/hda8
read-only
```

Шаг 2

Поскольку конфигурационный файл `/etc/lilo.conf` теперь содержит незашифрованный пароль, доступ к нему следует разрешить только пользователю `root`:

```
[root@drwalbr /]# chmod 600 /etc/lilo.conf
```

Для того, чтобы сделать файл неизменяемым, наберите:

```
[root@drwalbr /]# chattr +i /etc/lilo.conf
```

ЗАМЕЧАНИЕ В случае необходимости переконфигурирования LILO не забудьте снять атрибут запрета изменений с файла `/etc/lilo.conf` с помощью команды:

```
[root@drwalbr /]# chattr -i /etc/lilo.conf .
```

Шаг 3

Для того, чтобы изменения вступили в силу, выполните:

```
[root@drwalbr /]# /sbin/lilo –v
LILO version 21.7-3, Copyright (C) 1992-1998 Werner Almesberger
Linux Real Mode Interface library Copyright (C) 1998 Josh Vanderhoof
Development beyond version 21 Copyright (C) 1999-2001 John Coffman
Released 29-Mar-2001 and compiled at 06:06:43 on Jun  4 2002.

Reading boot sector from /dev/hda
Merging with /boot/boot.b
Boot image: /boot/vmlinuz-2.4.18-5asp
Mapping RAM disk /boot/initrd.2.4.18-5asp.img
Added ASPLinux-2.4.18 *
/boot/boot.0300 exists - no backup copy made.
Writing boot sector.
```

GRUB и файл /boot/grub/grub.conf

GRUB очень важна, так как это первая выполняемая программа при запуске компьютера, и мы должны обеспечить безукоризненную ее работу во избежание всевозможных сбоев. В заданной по умолчанию инсталляции она уже достаточно хорошо защищена. Мы постараемся объяснить, как сделан ее конфигурационный файл. На наш взгляд, по сравнению с LILO, GRUB более удобен при конфигурации. Далее приводятся значения заданного по умолчанию конфигурационного файла GRUB и рекомендуемые методы защиты. Полужирный текст – части конфигурационного файла `/boot/grub/grub.conf`, которые должны быть откорректированы в соответствии с вашими потребностями:

```
default 0
splashimage=/boot/grub/splash.xpm.gz
timeout 0
password --md5 $1$RFEae/$MxXN6ck3laZMTy8ajwINk0
title ASPLinux-2.4.18
root (hd0,0)
kernel /boot/vmlinuz-2.4.18-5asp ro root=/dev/sda5
initrd /boot/initrd.2.4.18-5asp.img
boot
```

Опция `default`

используется в конфигурационном файле для определения заданной по умолчанию загрузки. Значение "`0`" обозначает заданный по умолчанию вариант. Для сервера, где Linux – единственная операционная система, заданная по умолчанию загрузка будет и единственной. Другие варианты не задаем.

Опция `timeout`

используется для определения времени ожидания в секундах перед тем, как автоматически загрузить заданный по умолчанию вариант загрузки.

Опция `splashimage`

определяет графическое изображение, отображаемое при загрузке GRUB. Решайте сами – сохранять этот параметр или удалять. Если вы хотите удалить его, то удалите и вышеупомянутую строку со сжатым изображением.

Опция `password`

используется для сообщения GRUB о необходимости ввода пароля и отвергает любое интерактивное управление, пока вы не нажимаете клавишу <p> и не введете правильный пароль. Параметр `-md5` сообщает GRUB, что в качестве пароля требуется значение в формате MD5. Если он пропущен, GRUB предполагает, что указанный пароль – обычный текст. При установке ASPLinux загрузчик GRUB устанавливается без опции `password` и, следовательно, строки, содержащей пароль в зашифрованном виде, в вашем конфигурационном файле не будет. Для установки пароля выполните:

```
[root@drwalbr /]# grub-md5-crypt
Password:SecretnoeSlovo
$1$RFEae/$MxXN6ck3laZMTy8ajwINk0
```

В результате выполнения команды пароль автоматически будет занесен в конфигурационный файл. После использования команды новый пароль уже записан в конфигурационном файле.

Опция `title`

используется для определения имени варианта загружаемой системы. Она очень полезна при использовании нескольких операционных систем. В данном случае введите любую строку.

Опция `root`

один из самых важных параметров GRUB. Используется для определения текущего корневого устройства при загрузке операционной системы. Как видите, определение параметра несколько необычно. Приведем объяснение его значений:

- параметр `hd0` означает использование всего диска;
- параметр `hd0, 0` обозначает использование раздела диска (или загрузочного сектора раздела при инсталляции GRUB).

Обозначение `hd` здесь не обозначает диски SCSI и IDE, хотя для них используется аналогичная символика.

Опция `kernel`
используется для загрузки начального изображения (т. е. ядра). Параметр для этой опции – просто путь, где GRUB должен найти нужное изображение ядра для загрузки. Дополнительные строки – для сообщения того, что изображение ядра расположено в разделе `sda5`, и что необходимо загружать его в режиме доступа только для чтения, из соображений безопасности.

Опция `initrd`
является дополнительной и появляется в конфигурационном файле GRUB, если есть SCSI-устройства. Для компьютера с IDE жестким диском эта опция не нужна. Параметр просто сообщает программе GRUB, где находится начальный образ виртуального диска.

Файл /etc/services

Номера портов, которые используются службами, определены в RFC 1700. Файл `/etc/services` дает возможность серверу и клиентским программам устанавливать соответствие между названиями служб и номерами (портов). Только суперпользователю `root` должно быть разрешено вносить изменения в этот файл. Для этого установите запрет на внесение изменений в файл `/etc/services`:

```
[root@drwalbr /]# chattr +i /etc/services
```

Файл /etc/security

Этот файл позволяет определить, на каких консолях (`tty` и `vc` устройствах) разрешена регистрация суперпользователя `root`. Файл `/etc/security` читается программой, отвечающей за регистрацию в системе (`/bin/login`). Формат файла – список разрешенных `tty` и `vc`.

Отключите все ненужные `tty` и `vc` устройства. Настоятельно рекомендуется разрешить регистрацию суперпользователя `root` только с двух консолей, для этого в файле `/etc/security` закомментируйте или удалите лишние строки:

```
vc/1
#vc/2
#vc/3
#vc/4
#vc/5
#vc/6
#vc/7
#vc/8
#vc/9
#vc/10
#vc/11
tty1
#tty2
#tty3
#tty4
#tty5
#tty6
#tty7
#tty8
#tty9
#tty10
#tty10
```

Специальные учетные записи

Удалите все создаваемые при установке и неиспользуемые при работе сервера учетные записи. Эту операцию следует выполнять после каждого обновления или инсталляции программного обеспечения. Про-

грамма установки ASPLinux устанавливает дополнительные учетные записи операционной системы, даже если соответствующие им службы не установлены на сервере. Наличие неиспользуемых учетных записей упрощает несанкционированный доступ к системе.

Шаг 1
Удаление учетной записи пользователя из системы осуществляется с помощью команды вида:
```
[root@drwalbr /]# userdel username
```

Сведения о пользователях, имеющих учетные записи на системе, содержатся в файле `/etc/passwd`:
```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/bin/bash
mailnull:x:47:47::/var/spool/mqueue:/dev/null
```

Необходимо удалить пользователей, учетные записи которых выделены жирным шрифтом.

Шаг 2
Удаление группы пользователей осуществляется с помощью команды:
```
[root@drwalbr /]# groupdel groupname
```

Сведения о группах пользователей содержатся в файле `/etc/group`:
```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:
gopher:x:30:
dip:x:40:
ftp:x:50:
lock:x:54:
nobody:x:99:
users:x:100:
floppy:x:19:
vcsa:x:69:
utmp:x:22:
rpm:x:37:
mailnull:x:47:
```

```
slocate:x:21:
```

Необходимо удалить группы пользователей, выделенные жирным шрифтом.

Шаг 4

Установка атрибута `immutable` (т. е. запрет любых изменений) может использоваться для предотвращения случайного удаления или перезаписи защищенного файла. Он также препятствует созданию символьной ссылки к файлу, которая может использоваться для атаки, основанной на удалении файлов `/etc/passwd`, `/etc/shadow`, `/etc/group` или `/etc/gshadow`.

Для установки атрибута `immutable` для файлов паролей и групп выполните:

```
[root@drwalbr /]# chattr +i /etc/passwd
[root@drwalbr /]# chattr +i /etc/shadow
[root@drwalbr /]# chattr +i /etc/group
[root@drwalbr /]# chattr +i /etc/gshadow
```

Если в дальнейшем потребуется добавить или удалить пользователей, пароли, группу пользователей или файлы групп, или установить rpm-пакет, который автоматически добавляет нового пользователя и/или группу пользователей, вы должны снять атрибут `immutable` с файлов `/etc/passwd`, `/etc/shadow`, `/etc/group` и `/etc/gshadow`. Для этого:

```
[root@drwalbr /]# chattr -i /etc/passwd
[root@drwalbr /]# chattr -i /etc/shadow
[root@drwalbr /]# chattr -i /etc/group
[root@drwalbr /]# chattr -i /etc/gshadow
```

Управление монтированием файловых систем

Вы можете управлять монтированием файловых систем, размещенных на отдельных разделах диска, с использованием опций монтирования файловых систем:

- `defaults` – все операции (`quota`, `read-write` и `suid`) разрешены;
- `noquota` – отсутствуют квоты для пользователей;
- `nosuid` – отсутствует доступ SUID/SGID;
- `nodev` – отсутствует доступ к символьным или специальным устройствам;
- `noexec` – запрещено выполнение любых файлов;
- `quota` – все пользователи имеют квоты;
- `ro` – разрешен доступ только для чтения;
- `rw` – разрешен доступ чтения и записи;
- `suid` – разрешен доступ SUID/SGID.

Шаг 1

Отредактируйте файл `/etc/fstab` в соответствии с вашими потребностями, например, заменив строки:

```
/dev/hda13  /usr              ext3   defaults     0     1
/dev/hda14  /tmp              ext3   defaults     0     1
/dev/hda18  /home             ext3   defaults     0     1
/dev/hda16  /var/lib          ext3   defaults     0     1
```

на:

```
/dev/hda13  /usr              ext3   Defaults, ro 0     1
/dev/hda14  /tmp              ext3   defaults, nosuid   0     1
/dev/hda18  /home             ext3   defaults, nosuid, noexec 0    1
/dev/hda16  /var/lib          ext3   defaults, nodev    0     1
```

Шаг 2

Для перемонтирования файловых систем с новыми опциями выполните:

```
[root@drwalbr /]# mount /usr -oremount
[root@drwalbr /]# mount /var/lib -oremount
[root@drwalbr /]# mount /home -oremount
[root@drwalbr /]# mount /tmp -oremount
```

Проверить правильность монтирования файловых систем можно с помощью команды:

```
[root@drwalbr/]# cat /proc/mounts
```

Полезно смонтировать каталог `/usr`, в который устанавливаются основные пользовательские программы, с опцией `ro` (только чтение). При этом устраняется возможность замены критичных, с точки зрения безопасности системы, файлов.

ЗАМЕЧАНИЕ При установке программ из исходных кодов или rpm-пакетов в указанный каталог необходимо перемонтировать его без опции `ro`. Для этого удалите из файла `/etc/fstab` опцию `ro` и перемонтируйте каталог с помощью команды `mount -oremount`.

Права доступа к файлам сценариев запуска и остановки процессов

В каталоге `/etc/init.d` находятся файлы сценариев запуска и остановки процессов, запускаемых при загрузке системы. Обычным пользователям, а также злоумышленникам, получившим права доступа обычных пользователей, совершенно не обязательно знать, что находится в этих файлах. Поэтому настоятельно рекомендуем разрешить доступ к этим файлам (чтение, запись и исполнение) только пользователю `root`:

```
[root@drwalbr /]# chmod 0700 /etc/init.d/*
```

При установке программы, использующей сценарий в каталоге `/etc/init.d`, не забывайте проверять права доступа к вновь созданному или измененному сценарию.

Специальные символы у программ, владельцем которых является root

Обычный пользователь сможет выполнить программу с правами суперпользователя `root`, если в правах доступа к файлу программы установлен, так называемый, SUID или SGID бит (символ `"s"` в правах доступа, например, `-rwsr-xr-x` или `-r-xr-sr-x` допускаемый символ). Поскольку эти программы предоставляют специальные привилегии пользователю, который их выполняет, важно удалить SUID и SGID из прав доступа файлов программ, владельцем которых является `root`, и которые не должны выполняться другими пользователями. Это делается следующим образом.

Шаг 1

Для получения списка программ, имеющих в правах доступа SUID или SGID-биты, выполните:

```
[root@drwalbr /]# find / -type f \( -perm -04000 -o -perm -02000 \) -exec
ls -l {} \;
-rwsr-xr-x    1 root     root        60104 Июл 29 20:34 /bin/mount
-rwsr-xr-x    1 root     root        30664 Июл 29 20:34 /bin/umount
-rwsr-xr-x    1 root     root        35040 Июн 19  2002 /bin/ping
-rwsr-xr-x    1 root     root        19072 Июн 10  2002 /bin/su
-r-xr-sr-x    1 root     tty          6920 Июн 10  2002 /usr/bin/wall
-rwsr-xr-x    1 root     root        34680 Июн  4  2002 /usr/bin/chage
-rwsr-xr-x    1 root     root        36032 Июн  4  2002 /usr/bin/gpasswd
-rws--x--x    1 root     root        12104 Июл 29 20:34 /usr/bin/chfn
-rws--x--x    1 root     root        11496 Июл 29 20:34 /usr/bin/chsh
-rws--x--x    1 root     root         4764 Июл 29 20:34 /usr/bin/newgrp
-rwxr-sr-x    1 root     tty          9008 Июл 29 20:34 /usr/bin/write
-rwsr-xr-x    1 root     root        21044 Июн  4  2002 /usr/bin/crontab
-rwxr-sr-x    1 root     mail        17767 Июн  4  2002 /usr/bin/lockfile
-r-s--x--x    1 root     root        15080 Июн  4  2002 /usr/bin/passwd
-rwxr-sr-x    1 root     slocate     30422 Июн  4  2002 /usr/bin/slocate
-rwsr-xr-x    1 root     root        32797 Июн 19  2002 /usr/sbin/ping6
-rwsr-xr-x    1 root     root        14033 Июн 19  2002 /usr/sbin/ trac-
eroute6
-rwsr-xr-x    1 root     root        17413 Июл 11  2002
/usr/sbin/usernetctl
-rwxr-sr-x    1 root     utmp         6372 Июн  4  2002
/usr/sbin/utempter
-rws--x--x    1 root     root        22388 Июн  4  2002
/usr/sbin/userhelper
-rwxr-sr-x    1 root     root        14609 Июл 11  2002 /sbin/netreport
-r-sr-xr-x    1 root     root       109384 Июл 29 14:12 /sbin/pwdb_chkpwd
-r-sr-xr-x    1 root     root        16072 Июл 29 14:12 /sbin/unix_chkpwd

find / -type f \( -perm -2 -o -perm -20 \) -exec ls -ldg {} \;
```

Шаг 2

Снимите SUID-биты в правах доступа к следующим файлам:

```
[root@drwalbr /]# chmod a-s /bin/mount
[root@drwalbr /]# chmod a-s /bin/umount
[root@drwalbr /]# chmod a-s /bin/ping
[root@drwalbr /]# chmod a-s /usr/bin/wall
[root@drwalbr /]# chmod a-s /usr/bin/chage
[root@drwalbr /]# chmod a-s /usr/bin/gpasswd
[root@drwalbr /]# chmod a-s /usr/bin/chfn
[root@drwalbr /]# chmod a-s /usr/bin/chsh
[root@drwalbr /]# chmod a-s /usr/bin/newgrp
[root@drwalbr /]# chmod a-s /usr/bin/write
[root@drwalbr /]# chmod a-s /usr/sbin/ping6
[root@drwalbr /]# chmod a-s /usr/sbin/traceroute6
[root@drwalbr /]# chmod a-s /usr/sbin/usernetctl
[root@drwalbr /]# chmod a-s /sbin/netreport
```

Запрещение внутренним компьютерам сообщать серверу свой MAC-адрес

Злоумышленник может легко изменить IP-адрес своего компьютера и представиться в виде другого компьютера для вашей системы. Для исключения (осложнения) реализации такого мероприятия следует запретить всем локальным компьютерам в вашей сети сообщать серверу свой MAC (Media Access Control) и IP-адрес.

Для этого необходимо сделать следующее.

Шаг 1

Для каждого компьютера в сети узнайте его MAC-адрес:

```
[root@drwalbr /]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:80:48:CB:BD:73
          inet addr:172.16.181.103  Bcast:172.16.181.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:250 (250.0 b)  TX bytes:2996 (2.9 Kb)
          Interrupt:11 Base address:0xc000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:700 (700.0 b)  TX bytes:700 (700.0 b)
```

MAC-адресом компьютера являются символы, стоящие после `HWaddr` в первой строке вывода команды `ifconfig`. В данном примере - `00:80:48:CB:BD:73`.

Шаг 2

После определения MAC-адреса, соответствующего определенному IP-адресу, их нужно добавить в ARP таблицу сервера:

```
[root@drwalbr /]# arp -s 172.16.181.103  00:80:48:CB:BD:73
```

или:

```
[root@drwalbr /]# arp -s karlnext.und 00:80:48:CB:BD:73
```

Шаг 3

Проверьте правильность внесенных изменений:

```
[root@drwalbr /]# arp
 Address     Hwtype      Hwaddress   Flags Mask  Iface
 ...
 karlnext.und      ether 00:80:48:CB:73:00 CM    eth0
```

Шаг 4

Для того, чтобы внесенные нами изменения сохранились при перезагрузке системы, добавьте в конец файла `/etc/rc.local` строку:

```
arp -s 172.16.181.103  00:80:48:CB:BD:73
```

или:

```
arp -s karlnext.und 00:80:48:CB:BD:73
```

Теперь в случае изменения IP-адреса компьютера karlnext сервер не будет отвечать на его запросы.

Необычные или скрытые файлы

Проверьте систему на предмет наличия необычных или скрытых файлов (файлы, которые начинаются с точки и обычно не отображающиеся в выводе команды `ls`), поскольку они могут использоваться для скрытия инструментальных программ, используемых для получения информации о системе.

Для поиска скрытых файлов наберите:

```
[root@drwalbr /]# find / -name ".. " -print –xdev
```

или:

```
[root@drwalbr /]# find / -name ".*" -print -xdev | cat -v
```

Обнаружение файлов и каталогов, изменяемых любым пользователем

Файлы и каталоги, изменяемые любым пользователем, особенно системные файлы, могут стать брешью в защите, если взломщик программной защиты получит доступ к вашей системе и изменит их. Кроме того, общедоступные каталоги опасны, так как они позволяют злоумышленникам добавлять или удалять файлы в этих каталогах как им вздумается. Для поиска общедоступных файлов и каталогов выполните:

```
[root@drwalbr /]# find / -type f \( -perm -2 -o -perm -20 \) -exec ls -lg
{} \;
-rw-rw-r--    1 root     utmp        92928 Янв 16 18:37 /var/log/wtmp
-rw-rw-r--    1 root     utmp         4224 Янв 16 18:37 /var/run/utmp
```

и:

```
[root@drwalbr /]# find / -type d \( -perm -2 -o -perm -20 \) -exec ls -
ldg {} \;
drwxrwxr-x   12 root     man          4096 Дек 23 16:23
/var/cache/man/X11R6
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat1
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat2
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat3
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat4
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat5
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat6
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat7
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat8
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/cat9
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/X11R6/catn
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat1
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat2
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat3
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat4
```

```
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat5
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat6
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat7
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat8
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/cat9
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/catn
drwxrwxr-x   12 root     man          4096 Дек 23 16:23
/var/cache/man/local
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat1
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat2
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat3
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat4
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat5
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat6
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat7
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat8
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/cat9
drwxrwxr-x    2 root     man          4096 Июн 11  2002
/var/cache/man/local/catn
drwxrwxr-x    3 root     lock         4096 Янв 16 18:37 /var/lock
drwxrwxr-x    2 root     root         4096 Июл 11  2002
/var/run/netreport
drwxrwxr-x    2 root     mail         4096 Янв 16 18:37 /var/spool/mail
drwxrwxrwt    2 root     root         4096 Дек 23 16:23 /var/tmp
drwxrwxrwt    4 root     root         4096 Янв 16 18:37 /tmp
drwxrwxrwt    2 root     root            0 Янв 16 18:31 /dev/shm
```

Для поиска общедоступных файлов и каталогов можно также воспользоваться и программой `tripwire`.

Файлы без владельцев

Не допускайте наличия в системе любых файлов, не имеющих владельцев, кроме находящихся в каталоге `/dev`. Появление таких файлов может также служить сигналом, что злоумышленник проник в систему. Если найден файл или каталог, не имеющий владельца, проверьте целостность системы, и если все нормально, задайте имя владельца. Иногда после удаления программы могут появиться файлы или каталоги, связанные с ней и не имеющие владельцев. В этом случае их можно просто удалить.

Для поиска файлов и каталогов без владельцев выполните:

```
[root@drwalbr /]# find / -nouser -o -nogroup
```

Поиск файлов `.rhosts`

Поиск всех существующих `.rhosts` файлов на сервере должен стать частью вашей обычной работы по администрированию системы. Наличие этих файлов недопустимо, т:к они могут использоваться для получения несанкционированного доступа к вашей системе.

Для поиска файлов `.rhosts` выполните:

```
[root@drwalbr /]# find /home -name .rhosts
```

В случае обнаружения таких файлов их нужно уничтожить.

Копии файлов регистрации на жестких носителях и удаленных системах

Одним из самых важных принципов безопасности является обеспечение целостности различных файлов регистрации в каталоге сервера `/var/log`. Критически важные сообщения могут быть также выведены на принтер с использованием программы `syslog`. Взломщик может изменить файлы, программы и т. д. на вашем сервере, но ничего не сможет сделать с реальными бумажными копиями.

Для распечатки на принтере, подключенном к вашей системе, всех telnet-соединений, почтовых сообщений, сообщений начальной загрузки и ssh-соединений сделайте следующее.

Шаг 1

На вашей системе добавьте в конец файла `/etc/syslog.conf` строку:

```
authpriv.*;mail.*;local7.*; auth.*;daemon.info /dev/lp0
```

Шаг 2

Перезапустите службу `syslog`:

```
[root@drwalbr /]# /etc/init.d/syslog restart
Останавливается служба журналирования ядра:                [OK]
Останавливается служба журналирования системы:             [OK]
Запускается служба журналирования системы:                 [OK]
Запускается служба журналирования ядра:                    [OK]
```

Для распечатки на принтере, подключенном к удаленной системе, всех telnet-соединений, почтовых сообщений, сообщений начальной загрузки и ssh-соединений сделайте следующее.

Шаг 1

Добавьте в конец файла `/etc/syslog.conf` на удаленной системе строку:

```
authpriv.*;mail.*;local7.*;auth.*;daemon.info /dev/lp0
```

Если в вашей сети нет принтера, скопируйте регистрационные файлы на другую машину. Для этого не выполняйте первый шаг, а переходите сразу ко второму.

Шаг 2

Для включения возможности получения по сети сообщений от других систем, на удаленной системе в файле `/etc/rc.d/init.d/syslog` замените строку:

```
SYSLOGD_OPTIONS="-m 0"
```

на:

```
SYSLOGD_OPTIONS="-r -m 0"
```

Шаг 3

Перезапустите службу `syslog` на удаленной системе:

```
[root@mail /]# etc/init.d/syslog restart
Останавливается служба журналирования ядра:                [OK]
Останавливается служба журналирования системы:             [OK]
Запускается служба журналирования системы:                 [OK]
Запускается служба журналирования ядра:                    [OK]
```

Шаг 4

Отредактируйте файл `/etc/syslog.conf` на локальной системе и добавьте в конец этого файла следующую строку:

```
authpriv.*;mail.*;local7.*;auth.*;daemon.info NameRemouteHost
```

Вместо `NameRemouteHost` используйте имя удаленной системы, на которую осуществляется копирование файлов регистрации.

Шаг 5

Перезапустите службу `syslog` на локальной системе:

```
[root@mail /]# etc/init.d/syslog restart
Останавливается служба журналирования ядра:                [OK]
Останавливается служба журналирования системы:             [OK]
Запускается служба журналирования системы:                 [OK]
Запускается служба журналирования ядра:                    [OK]
```

Удаление страниц руководства

Страницы руководства, также известные как man-страницы – это сжатые файлы, расположенные в каталоге `/usr/share/man` системы. Файлы документации очень полезны для получения быстрой информации о работе различных служб, программ, команд и синтаксисе различных конфигурационных файлов. Эти файлы читаются man-программой. Их место– на рабочей станции администратора сервера. Авторы рекомендуют удалить страницы руководства и программы, необходимые для их просмотра, с целью увеличения объема свободного места на дисках и некоторого увеличения безопасности системы.

Шаг 1
Удалите программу `man`:
```
[root@drwalbr /]# rpm -e man
```

Шаг 2
Удалите программу `groff`, используемую программой `man` для форматирования страниц:
```
[root@drwalbr /]# rpm -e groff
```

Шаг 3
Удалите файлы архивов, содержащие страницы руководства:
```
[root@drwalbr /]# cd /usr/share/man/
[root@drwalbr man]# rm -f man*/*.gz
```

ЗАМЕЧАНИЕ В дальнейшем инсталляцию и обновление rpm-пакетов нужно осуществлять с использованием опции `-excludedocs`. При этом страницы руководства не устанавливаются.

Глава 4

Дополнительные модули аутентификации

В этой главе:

1. Допустимая минимальная длина пароля
2. Таблица управления доступом входа в систему
3. Удаление из системы ненужных привилегированных пользователей
4. Наложение ограничений на ресурсы, выделяемые пользователям системы
5. Управление временем доступа к службам
6. Ограничение использования команды su root
7. Использование команды sudo вместо su для регистрации в качестве суперпользователя

Дополнительные модули аутентификации (PAM – Pluggable Authentication Modules) включают динамические библиотеки, которые дают администраторам возможность выбора методов подтверждения подлинности пользователей.

PAM разрешает применение различных опознавательных схем. Это достигается использованием библиотеки функций, которую используют приложения для идентификации пользователей. SSH, POP, IMAP и т. д. – приложения, использующие спецификацию PAM. Для них может быть изменен метод ввода пароля, например, не с консоли, а с голоса или по отпечаткам пальцев, путем изменения PAM-модулей без необходимости перезаписи самих кодов приложений.

Конфигурационные файлы модулей PAM расположены в каталоге `/etc/pam.d`, а сами модули (динамические библиотеки) расположены в каталоге `/lib/security`. Каталог `/etc/pam.d` содержит файлы, названные в соответствии с использующими их приложениями, например, SSH, POP, IMAP и т. д., указывающие на заданный по умолчанию конфигурационный файл `other`.

В этой главе будут рассмотрены некоторые настройки PAM, улучшающие безопасность системы.

Допустимая минимальная длина пароля

Длина пароля при использовании настройки PAM управляется пятью параметрами: `minlen`, `dcredit`, `ucredit`, `lcredit` и `ocredit`.

Параметр `minlen=N` определяет допустимое минимальное количество символов в новом пароле.

Допустимое минимальное количество символов в пароле уменьшается на величину, равную значению параметров:

- `dcredit` - используемой в пароле цифры;
- `ucredit` - для каждого используемого в пароле символа в верхнем регистре;
- `lcredit` - для каждого используемого в пароле символа в нижнем регистре;
- `ocredit` - для каждого используемого в пароле специального символа.

Значения параметров `dcredit`, `ucredit`, `lcredit` и `ocredit` равны единице.

Для задания приемлемого минимального количества символов длины пароля, например, равного 12, в файле `/etc/pam.d/system-auth` раскомментируйте строку:

```
#password    required      /lib/security/pam_cracklib.so retry=3
```

и добавьте параметр `minlen=12`:

```
password required /lib/security/pam_cracklib.so retry=3 minlen=12
```

Теперь попробуем установить пароль из девяти символов – `Wsvhl_Faz`. Пароль благополучно установится. Что и следовало ожидать. Максимально допустимая длина пароля (12 символов) уменьшилась на 3 из-за одного специального символа "_" и двух букв в верхнем регистре "W" и "F".

Таблица управления доступом входа в систему

В каталоге `/etc/security` находится файл `access.conf`, с помощью которого можно ограничить доступ для различных пользователей и IP-адресов к вашей системе. Предположим, что у нас имеется Linux-сервер, к администрированию которого допущены только два пользователя – `drwalbr` и `karlnext`.

Шаг 1

Одним из вариантов ограничения доступа к серверу является добавление в файл `/etc/security/access.conf` строки:

```
-:ALL EXCEPT root drwalbr karlnext:ALL
```

При этом доступ к консоли сервера будет запрещен с любой другой системы для всех пользователей, кроме `root`, `drwalbr` и `karlnext`. А для последних пользователей доступ будет разрешен откуда угодно.

Для разрешения только удаленного доступа к серверу пользователям `root`, `drwalbr` и `karlnext` с рабочей станции 192.168.2.99 в файл `/etc/security/access.conf` нужно добавить (подредактировать предыдущую строку):

```
-:ALL EXCEPT root drwalbr karlnext: 192.168.2.99
```

и добавить еще одну:

```
-:ALL: LOCAL
```

Последняя строка запрещает локальный доступ всех пользователей, в том числе и `root`.

Шаг 2

Для того, чтобы настройки, внесенные в файл `/etc/security/access.conf`, в последующем (когда вы установите OpenSSH) могли использоваться средствами удаленного администрирования SSH, в файлы `/etc/pam.d/system-auth` и `/etc/pam.d/sshd` необходимо добавить (проверить наличие) строки:

```
account    required     /lib/security/pam_access.so
```

Удаление из системы ненужных привилегированных пользователей

Файл безопасности `/etc/security/console.perms`, используемый модулем `pam_console.so`, предназначен для выделения привилегированным пользователям физической возможности использования консоли (виртуальных консолей и локальных xdm-управляемых X-сеансов).

ЗАМЕЧАНИЕ Обратите внимание, что привилегированные пользователи не имеют ничего общего с обычными пользователями. Это пользователи, соответствующие устройствам, подобно дисководу, CD-ROM, сканеру, и т. п., которые в среде сетевой операционной системы также считаются пользователями.

Файл `/etc/security/console.perms` устанавливаемый по умолчанию:

```
#
# This file determines the permissions that will be given to priviledged
# users of the console at login time, and the permissions to which to
# revert when the users log out.

# format is:
#   <class>=list of regexps specifying consoles or globs specifying files
#   file-glob|<class> perm dev-regex|<dev-class> \
#     revert-mode revert-owner[.revert-group]
# the revert-mode, revert-owner, and revert-group are optional, and de-
fault
# to 0600, root, and root, respectively.
#
# For more information:
# man 5 console.perms

# file classes -- these are regular expressions
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
<xconsole>=:[0-9]\.[0-9] :[0-9]

# device classes -- these are shell-style globs
<floppy>=/dev/fd[0-1]* \
  /dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
 /dev/mixer* /dev/sequencer \
 /dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
<pilot>=/dev/pilot
<jaz>=/mnt/jaz*
<zip>=/mnt/pocketzip* /mnt/zip*
<ls120>=/dev/ls120 /mnt/ls120*
<scanner>=/dev/scanner /dev/usb/scanner*
<rio500>=/dev/usb/rio500
<camera>=/mnt/camera* /dev/usb/dc2xx* /dev/usb/mdc800*
<memstick>=/mnt/memstick*
<flash>=/mnt/flash*
<diskonkey>=/mnt/diskonkey*
<rem_ide>=/mnt/microdrive*
<fb>=/dev/fb /dev/fb[0-9]* \
     /dev/fb/*
<kbd>=/dev/kbd
<joystick>=/dev/js[0-9]*
<v4l>=/dev/video* /dev/radio* /dev/winradio* /dev/vtx* /dev/vbi* \
      /dev/video/*
<gpm>=/dev/gpmctl
<dri>=/dev/3dfx*
<mainboard>=/dev/apm_bios

# permission definitions
<console>  0660 <floppy>     0660 root.floppy
<console>  0600 <sound>      0600 root
<console>  0600 <cdrom>      0660 root.disk
<console>  0600 <pilot>      0660 root.uucp
```

```
<console>  0600 <jaz>        0660 root.disk
<console>  0600 <zip>        0660 root.disk
<console>  0600 <ls120>      0660 root.disk
<console>  0600 <scanner>    0600 root
<console>  0600 <camera>     0600 root
<console>  0600 <memstick>   0600 root
<console>  0600 <flash>      0600 root
<console>  0600 <diskonkey>  0660 root.disk
<console>  0600 <rem_ide>    0660 root.disk
<console>  0600 <fb>         0600 root
<console>  0600 <kbd>        0600 root
<console>  0600 <joystick>   0600 root
<console>  0600 <v4l>        0600 root
<console>  0700 <gpm>         0700 root
<console>  0600 <mainboard>  0600 root
<console>  0600 <rio500>     0600 root
<xconsole> 0600 /dev/console 0600 root.root
<xconsole> 0600 <dri>         0600 root
```

является достаточно безопасным для правильного использования системы с интерфейсом Xwindow. Но в среде без графической оболочки пользователя (GUI – Graphical User Interface) и специальных устройств, наподобие звуковым картам, джойстикам, сканерам, Web-камерам, накопителям zip, jaz и т. д., для повышения безопасности удалите всех несуществующих или ненужных привилегированных пользователей из файла:

```
#file classes -- these are regular expressions
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
#device classes -- these are shell-style globs
<floppy>=/dev/fd[0-1]* \
/dev/floppy/* /mnt/floppy*
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
<pilot>=/dev/pilot
<fb>=/dev/fb /dev/fb[0-9]* \
/dev/fb/*
<kbd>=/dev/kbd
/dev/video/*
<gpm>=/dev/gpmctl
<mainboard>=/dev/apm_bios
# permission definitions
<console>  0660 <floppy>     0660 root.floppy
<console>  0600 <cdrom>      0660 root.disk
<console>  0600 <pilot>      0660 root.uucp
<console>  0600 <fb>         0600 root
<console>  0600 <kbd>        0600 root
<console>  0600 <v4l>        0600 root
<console>  0700 <gpm>         0700 root
<console>  0600 <mainboard>  0600 root
```

Наложение ограничений на ресурсы, выделяемые пользователям системы

Файл `/etc/security/limits.conf` может использоваться для наложения ограничений на ресурсы (число выполняемых процессов, объем памяти и т. д.), выделяемые пользователям системы. Файл, устанавливаемый по умолчанию, не накладывает никаких ограничений на объем ресурсов, выделяемых пользователям системы:

```
# /etc/security/limits.conf
#
#Each line describes a limit for a user in the form:
#
#<domain>        <type>  <item>  <value>
#
#Where:
#<domain> can be:
#        - an user name
#        - a group name, with @group syntax
#        - the wildcard *, for default entry
```

```
#
#<type> can have the two values:
#        - "soft" for enforcing the soft limits
#        - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#        - core - limits the core file size (KB)
#        - data - max data size (KB)
#        - fsize - maximum filesize (KB)
#        - memlock - max locked-in-memory address space (KB)
#        - nofile - max number of open files
#        - rss - max resident set size (KB)
#        - stack - max stack size (KB)
#        - cpu - max CPU time (MIN)
#        - nproc - max number of processes
#        - as - address space limit
#        - maxlogins - max number of logins for this user
#        - priority - the priority to run user process with
#        - locks - max number of file locks the user can hold
#
#<domain>      <type>  <item>         <value>
#

#*               soft    core            0
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#@student        -       maxlogins       4

# End of file
```

И это, не смотря на то, что указанные ограничения существенно затруднили бы со стороны пользователей системы реализацию атак типа отказа в обслуживании. В предположении, что все обычные пользователи вашей системы входят в группу `users` для установления ограничений в файл `/etc/security/limits.conf` добавьте следующие строки:

```
@users       hard    core    0
@users       hard    rss     5000
@users       hard    nproc   30
```

В результате для всех пользователей из группы `users` будет запрещено создание файлов с образами памяти приложений, объем используемой оперативной памяти ограничится 5 МБайт, а число запускаемых процессов – тридцатью.

ЗАМЕЧАНИЕ При добавлении новых пользователей не забудьте указать, что они входят в группу `users`.

Управление временем доступа к службам

С помощью файла безопасности `/etc/security/time.conf`, в случае необходимости, можно ограничить время доступа к различным службам. Файл `time.conf` может быть сконфигурирован для запрета доступа ко всем или некоторым службам сервера различным пользователям. Дополнительная селекция может осуществляться по временным интервалам, консолям, именам машин и их IP-адресам.

Шаг 1

Для регистрации на сервере в рабочее время только пользователей `karlnext` и `root` в файл `/etc/security/time.conf` добавьте следующую строку:

```
login;tty* & !ttyp*; !root & karlnext & ; !Al0900-1900
```

Шаг 2

Для реализации возможности использования настроек в предыдущем файле в файл /etc/pam.d/system-auth и /etc/pam.d/sshd (если вы используете SSH для удаленного администрирования сервера) добавьте (проверьте наличие строки):

```
account    required     /lib/security/pam_time.so
```

Ограничение использования команды su root

Команда su (substitute user) позволяет открывать сеансы под именами других пользователей системы, запускать программы и выполнять команды от их имени и с их правами доступа.

Для открытия сеанса суперпользователя root используется команда:

```
[root@drwalbr /]# su root
Password:
```

Авторы рекомендуют не использовать команду su, либо строго ограничить круг пользователей, которому использование этой команды разрешено.

Шаг 1

В файле /etc/pam.d/su раскомментируйте (добавьте строку):

```
auth       required     /lib/security/pam_wheel.so use_uid
```

В этом случае использование команды su будет разрешено только пользователям из специальной группы

Шаг 2

Для того, чтобы некоторый пользователь системы, например karlnext, мог использовать команду, ему в качестве дополнительной группы нужно добавить группу wheel:

```
[root@drwalbr /]# usermod –G wheel karlnext
```

В файле /etc/pam.d/su имеется строка:

```
#auth       sufficient   /lib/security/pam_wheel.so trust use_uid
```

раскомментировав которую, можно разрешить пользователям из группы wheel разрешить выполнять команду su root без ввода пароля. Авторы не рекомендуют использовать эту опцию.

Использование команды sudo вместо su для регистрации в качестве суперпользователя

Программа sudo, также как и команда su, позволяет выполнять команды от имени и с полномочиями другого пользователя, но более безопасным и информативным способом. Используя sudo, вы получите полную информацию о том, кто вошел в систему как суперпользователь root, а также много другой полезной информации. Инсталляция и настройка sudo рассматривается далее в отдельной главе.

Если вы планируете использовать sudo, удалите SUID-бит из файла /bin/su:

```
[root@drwalbr /]# chmod a-s /bin/su
```

Глава 5

Оптимизация операционной системы

В этой главе

1. Статические и динамические библиотеки
2. Библиотеки Linux Glibc 2.2
3. Почему Linux-программы распространяются в исходных кодах
4. Файл gcc specs
5. Удаление комментариев из исполняемых файлов и библиотек
6. Оптимизация настроек жесткого диска с IDE-интерфейсом

Если вы следовали нашим рекомендациям, то на сервере установлены пакеты программ для его функционирования, обеспечения безопасности и компиляции программ. Перед тем как начать установку необходимых служб, необходимо выполнить ряд операций, повышающих быстродействие сервера.

Статические и динамические библиотеки

Во время компиляции исходных кодов большинства программ на последней стадии осуществляется связь кода программы с кодами Linux-библиотек. Эти библиотеки поставляются в динамическом и статическом формате и содержат общий системный код, который хранится в одном месте и совместно используется различными программами. Обычно на Linux-системах файлы библиотек находятся в каталогах `/lib`, `/usr/lib` и `/usr/share`. По умолчанию Linux использует динамические библиотеки, а если он не может найти их, то статические.

При использовании статической библиотеки, компилятор находит фрагменты кода, которые требуются для модулей программы, и копирует их непосредственно в исполняемый файл. При использовании динамических библиотек компилятор вставляет ссылку, в которой указывает на необходимость загрузки определенной библиотеки перед началом выполнения программы.

С одной стороны, при статической компоновке программ в случае выявления ошибки в одной из библиотек, влияющей на безопасность системы, система будет потенциально уязвимой до тех пор, пока не будут перекомпилированы все программы, содержащие код соответствующей библиотеки. С другой стороны, при динамической компоновке программ система потенциально уязвима к атакам, направленным на модификацию библиотечных файлов, а уязвимость системы, вызванная ошибкой в библиотеке, может быть устранена путем ее замены.

Другим достоинством статической компоновки является то, что процесс инсталляции программного обеспечения упрощается и может быть осуществлен при отсутствии доступа к библиотечным файлам. На сильно загруженных системах использование статических библиотек негативно влияет на производительность системы, поэтому в этом случае использование динамических библиотек более предпочтительно.

Таким образом:

• если вы хотите компилировать программу, используя динамические библиотеки, необходимо использовать следующие флаги компилятора:

```
CFLAGS = "-O2-march=i686 -funroll-loops"; export CFLAGS
./Configure \
```

• если хотите компилировать, используя статические библиотеки, необходимо использовать следующие флаги компилятора:

```
CFLAGS="-O2 -static -march=i686 -funroll-loops"; export CFLAGS
./Configure \
--disabled-shared\
```

ЗАМЕЧАНИЕ В Linux статические библиотеки имеют имена вида libc.a, а динамические библиотеки – .libc.so.x.y.z, где x.y.z - номер версии.

Библиотеки Linux Glibc 2.2

Библиотека `Glibc 2.2` пришла на смену `libc4` и `libc5` и является последней версией GNU библиотеки языка `C` для Linux. Она содержит стандартные библиотеки, используемые различными программами. Этот специфический пакет содержит самые важные наборы динамических и статических библиотек, который обеспечивает основные функциональные возможности ядра для запуска программ `C`. Без них Linux-система не смогла бы функционировать.

По умолчанию в ASPLinux и во многих других дистрибутивах этот пакет для повышения совместимости устанавливается сконфигурированным для работы с процессором i386. Поэтому для того, чтобы наши рекомендации по повышению производительности сервера за счет использования программ, откомпилированных для конкретной версии процессора, оказались наиболее действенными, необходимо установить версию пакета `Glibc 2.2` для соответствующего процессора. Если использовать файл, устанавливаемый по умолчанию, часть кода программы, использующая код библиотек, не будет оптимизирована для работы с версией процессора, отличной от i386.

Почему Linux-программы распространяются в исходных кодах

Первоначально Linux был разработан как операционная система, предназначенная для работы на различных платформах. Поэтому наиболее простым способом распространения программного обеспечения является распространение исходного кода программы и последующая ее компиляция. Создатели программного обеспечения не всегда могут знать, на какой версии процессора (i386,i486, Pentium и т. д.) будут выпол-

няться их коды. Поэтому для обеспечения межплатформенной совместимости предварительно откомпилированное программное обеспечение поставляется в версии для процессора i386 и, естественно, не учитываются дополнительные особенности более современных процессоров, например, набор команд MMX или 3D Now! Естественно, при использовании предварительно откомпилированного программного обеспечения не может быть достигнута максимальная производительность системы, если вы, конечно, не используете процессор i386.

Опции компилятора, грамотное использование которых позволяет получить исполняемые файлы, оптимизированы для заданной архитектуры центрального процессора. Описание опций, используемых при компиляции исходных кодов программ применительно к различным процессорам, приведено ниже. Первый параметр, который необходимо установить – это тип центрального процессора. Это делается с помощью флага "`-march=cpu_type`" (архитектура процессора). Например, "`-march=i686`" или "`-march=k6`" позволяет компилятору выбирать соответствующий вариант оптимизации для конкретного процессора.

Вы можете установить значение флага "`-O`" от `1` до `3`, указав компилятору степень оптимизации. Значение "`-O3`" позволяет создавать исполняемые файлы, имеющие максимальное быстродействие.

Следующим этапом является установка флага "`-f` **,** который может принимать значение "`-funroll-loops`" и "`-fomit-frame-pointer`".

ЗАМЕЧАНИЕ Компиляция с опцией выключателя "-fomit-frame-pointer" будет использовать стек для обращения к переменным. К сожалению, отладка программ при установке этой опции, как правило, невозможна. Также, обратите внимание, что во флаге "O3" первым символом является заглавная буква "O".

Учитывая вышеизложенное, мы предлагаем компилировать программное обеспечение со следующими флагами:

```
CFLAGS = "-O2-march=i686 -funroll-loops"
```

Мы не используем флаги "`-O3`" и "`-fomit-frame-pointer`", так как они не всегда хорошо работают при компиляции некоторого программного обеспечения.

Файл gcc specs

Файл `/usr/lib/gcc-lib/i386-asplinux-linux/2.96/specs` содержит набор установок для компилятора `gcc` и будет использован нами для задания параметров компиляции.

Шаг 1

Проверьте версию компилятора, установленную на вашей системе:

```
[root@drwalbr /]# gcc -v
Reading specs from /usr/lib/gcc-lib/i386-asplinux/2.96/specs
gcc version 2.96 20000731 (ASPLinux 7.3 2.96-112)
```

Шаг 2

Для процессоров i686 или PentiumPro, Pentium II, Pentium III и Athlon откройте файл `/usr/lib/gcc-lib/i386-redhat-linux/2.96/specs`. В ниже приведенном фрагменте:

```
*cpp_cpu_default:
-D__tune_i386__

*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}

*cc1_cpu:
%{!mcpu*: %{m386:-mcpu=i386} %{m486:-mcpu=i486} %{mpentium:-mcpu=pentium}
%{mpentiumpro:-mcpu=pentiumpro}}
```

сделайте следующие исправления:

```
*cpp_cpu_default:
-D__tune_i686__
*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}

*cc1_cpu:
%{!mcpu*: -O2 –march=i686 –funroll-loops %{m386:-mcpu=i386} %{m486:-
mcpu=i486} %{mpentium:-mcpu=pentium} %{mpentiumpro:-mcpu=pentiumpro}}
```

ЗАМЕЧАНИЕ Мы используем флаг "-O2" (большая буква "O" два), а не "-02" (ноль два).

Для процессоров i586 и Pentium откройте файл `/usr/lib/gcc-lib/i386-redhat-linux/2.96/specs`. В ниже приведенном фрагменте:

```
*cpp_cpu_default:
-D__tune_i386__

*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}

*cc1_cpu:
%{!mcpu*: %{m386:-mcpu=i386} %{m486:-mcpu=i486} %{mpentium:-mcpu=pentium}
%{mpentiumpro:-mcpu=pentiumpro}}
```

сделайте следующие исправления:

```
*cpp_cpu_default:
-D__tune_i586__
*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}
```

```
*cc1_cpu:
%{!mcpu*: -O2 –march=i586 –funroll-loops %{m386:-mcpu=i386} %{m486:-
mcpu=i486} %{mpentium:-mcpu=pentium} %{mpentiumpro:-mcpu=pentiumpro}}
```

ЗАМЕЧАНИЕ Мы используем флаг "-O2" (большая буква "O" два), а не "-02" (ноль два).

Для процессоров i486 откройте файл `/usr/lib/gcc-lib/i386-redhat-linux/2.96/specs`. В ниже приведенном фрагменте:

```
*cpp_cpu_default:
-D__tune_i386__

*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}

*cc1_cpu:
%{!mcpu*: %{m386:-mcpu=i386} %{m486:-mcpu=i486} %{mpentium:-mcpu=pentium}
%{mpentiumpro:-mcpu=pentiumpro}}
```

сделайте следующие исправления:

```
*cpp_cpu_default:
-D__tune_i486__

*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}

*cc1_cpu:
%{!mcpu*: -O2 –march=i486 –funroll-loops %{m386:-mcpu=i386} %{m486:-
mcpu=i486} %{mpentium:-mcpu=pentium} %{mpentiumpro:-mcpu=pentiumpro}}
```

ЗАМЕЧАНИЕ Мы используем флаг "-O2" (большая буква "O" два), а не "-02" (ноль два).

Для процессоров AMD K6 или K6-2 откройте файл `/usr/lib/gcc-lib/i386-redhat-linux/2.96/specs`. В ниже приведенном фрагменте:

```
*cpp_cpu_default:
-D__tune_i386__

*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
```

```
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}

*cc1_cpu:
%{!mcpu*: %{m386:-mcpu=i386} %{m486:-mcpu=i486} %{mpentium:-mcpu=pentium}
%{mpentiumpro:-mcpu=pentiumpro}}
```

сделайте следующие исправления:

```
*cpp_cpu_default:
-D__tune_k6__

*cpp_cpu:
-Acpu(i386) -Amachine(i386) %{!ansi:-Di386} -D__i386 -D__i386__
%{march=i386:%{!mcpu*:-D__tune_i386__ }}%{march=i486:-D__i486 -D__i486__
%{!mcpu*:-D__tune_i486__ }}%{march=pentium|march=i586:-D__pentium -
D__pentium__   %{!mcpu*:-D__tune_pentium__
}}%{march=pentiumpro|march=i686:-D__pentiumpro -D__pentiumpro__
%{!mcpu*:-D__tune_pentiumpro__ }}%{march=k6:-D__k6 -D__k6__ %{!mcpu*:-
D__tune_k6__ }}%{march=athlon:-D__athlon -D__athlon__ %{!mcpu*:-
D__tune_athlon__ }}%{m386|mcpu=i386:-D__tune_i386__ }%{m486|mcpu=i486:-
D__tune_i486__ }%{mpentium|mcpu=pentium|mcpu=i586:-D__tune_pentium__
}%{mpentiumpro|mcpu=pentiumpro|mcpu=i686:-D__tune_pentiumpro__
}%{mcpu=k6:-D__tune_k6__ }%{mcpu=athlon:-D__tune_athlon__
}%{!march*:%{!mcpu*:%{!m386:%{!m486:%{!mpentium*:%(cpp_cpu_default)}}}}}

*cc1_cpu:
%{!mcpu*: -O2 –march=k6 –funroll-loops %{m386:-mcpu=i386} %{m486:-
mcpu=i486} %{mpentium:-mcpu=pentium} %{mpentiumpro:-mcpu=pentiumpro}}
```

ЗАМЕЧАНИЕ Мы используем флаг "-O2" (большая буква "O" два), а не "-02" (ноль два).

Шаг 3

Для проверки работоспособности внесенных изменений выполните следующие команды:

```
[root@drwalbr /]# touch cpu.c
[root@drwalbr /]# gcc cpu.c –S –fverbose-sam
[root@drwalbr /]# less cpu.c
```

Если на экран будет выведено нечто подобное:

```
  .file "cc9xBgp3.i"
  .version    "01.01"
# GNU C version 2.96 20000731 (ASPLinux 7.3 2.96-112) (i386-asplinux-
linux) compiled by GNU C version 2.96 20000731 (ASPLinux 7.3 2.96-112).
# options passed:  -O2 -march=i686 -funroll-loops -fverbose-asm
# options enabled:  -fdefer-pop -foptimize-sibling-calls -fcse-follow-
jumps
# -fcse-skip-blocks -fexpensive-optimizations -fthread-jumps
# -fstrength-reduce -funroll-loops -fpeephole -fforce-mem -ffunction-cse
# -finline -fkeep-static-consts -fcaller-saves -fpcc-struct-return -fgcse
# -frerun-cse-after-loop -frerun-loop-opt -fdelete-null-pointer-checks
# -fschedule-insns2 -fsched-interblock -fsched-spec -fbranch-count-reg
# -fnew-exceptions -fcommon -fverbose-asm -fgnu-linker -fregmove
# -foptimize-register-move -fargument-alias -fstrict-aliasing
# -fmerge-constants -fident -fpeephole2 -fmath-errno -m80387 -mhard-float
# -mno-soft-float -mieee-fp -mfp-ret-in-387 -march=i686

gcc2_compiled.:
  .ident      "GCC: (GNU) 2.96 20000731 (ASPLinux 7.3 2.96-112)"
```

то внесенные вами изменения работают.

Удаление комментариев из исполняемых файлов и библиотек

На этапе компиляции программы в нее добавляется много различных комментариев. Это делается для удобства отладки программного обеспечения. Для повышения быстродействия системы и сокращения размера исполняемых и библиотечных файлов эти комментарии необходимо удалить. Что может быть выполнено при помощи команды `strip` Linux. При использовании команды необходимо соблюдать некоторые меры предосторожности, о которых мы расскажем ниже. Неаккуратное использование команды `strip` может привести к непредсказуемым последствиям. Важно помнить, что не все бинарные файлы, особенно файлы библиотек, должны быть отредактированы с использованием этой команды, а только часть из них. Этот метод повышения производительности системы может быть применен на серверах, на которых не осуществляется компиляция программного обеспечения, либо на сервере, на котором откомпилировано и установлено все необходимое для его работы программное обеспечение.

Шаг 1

Прежде всего, необходимо убедиться, что команда `strip` доступна на вашем сервере. Если она не установлена, то необходимо установить пакет `binutils`, входящий в дистрибутив ASPLinux, используя рекомендации раздела «Как использовать команды rpm» главы 2.

Шаг 2

Для очистки исполняемых файлов в директориях `/bin`, `/sbin`, `/usr/bin` и `/usr/sbin` необходимо выполнить следующие команды:

```
[root@drwalbr /]# strip /bin/*
[root@drwalbr /]# strip /sbin/*
[root@drwalbr /]# strip /usr/bin/*
[root@drwalbr /]# strip /usr/sbin/*
```

ЗАМЕЧАНИЕ При выполнении этих команд вы увидите несколько сообщений об ошибках:
"File format not recognized".
Это обусловлено тем, что в директориях /bin, /sbin, /usr/bin и /usr/sbin содержатся не только исполняемые файлы, но и символьные ссылки на них, а программа strip не умеет их обрабатывать.

Шаг 3

Для очистки файлов библиотек необходимо выполнить следующие команды:

```
[root@drwalbr /]# strip –R .comment /usr/lib/*.so.*
[root@drwalbr /]# strip –R .comment /lib/*.so.*
```

ЗАМЕЧАНИЕ Опция "-R" в команде strip позволяет нам задавать названия фрагментов, удаляемых из библиотек. С помощью ".comment" мы сообщаем команде, что необходимо удалять любые строки, содержащие ".comment"

Оптимизация настроек жесткого диска с IDE-интерфейсом

Доступ к информации на жестком диске осуществляется в 50…100 раз медленнее, чем к данным в оперативной памяти. Именно поэтому настройка быстродействия жесткого диска является критичной, с точки зрения обеспечения максимальной производительности сервера

Настройки ASPLinux по умолчанию позволяют обеспечить максимум совместимости. Вы же, хорошо зная особенности диска и материнской платы, можете изменить настройки, обеспечив максимум производительности. Для оптимизации настроек жесткого диска с интерфейсом IDE используется команда `hdparm`. Ускорение в работе на операции ввода-вывода достигается путем специализированных IDE драйверов, использования прямого доступа к памяти, 32-разрядного обмена и блочных режимов передачи данных.

Следует отметить, что диски IDE/ATA разных производителей по-разному подвержены ускорению с помощью рассматриваемой утилиты. Так, лучше всего ускоряются диски Quantum (ныне Maxtor), чуть хуже – Western Digital, и совсем плохо – Fujitsu.

Перед началом оптимизации диска проверьте, установлен ли пакет `hdpram`:

```
[root@drwalbr /]#  rpm -q hdparm
package hdparm is not installed
```

Для установки пакета необходимо вставить первый компакт-диск дистрибутива ASPLinux в дисковод и выполнить следующие команды:

```
[root@drwalbr /]# mount /mnt/cdrom
[root@drwalbr /]# cd /mnt/cdrom/ASPLinux/RPMS
[root@drwalbr RPMS]# rpm –Uhv hdparm-5.1-1.asp.i386.rpm
hdparm       ########################################################## 100%
```

После установки пакета необходимо размонтировать компакт диск:

```
[root@drwalbr /]# cd
[root@drwalbr /]# umount /mnt/cdrom
```

В зависимости от моделей производителей диска и системной платы будут устанавливаться различные параметры оптимизации. Неправильный выбор этих параметров может привести к полному выходу диска из строя. Поэтому перед началом оптимизации необходимо изучить параметры системы.

Необходимо так же проверить параметры настройки BIOS, выяснить, поддерживает ли ваша система режим DMA и включены ли параметры, обеспечивающие поддержку этого режима.

Шаг 1

Этот шаг применим к большинству дисков – включает 32-разрядный ввод-вывод по PCI-шинам. Эта опция – одна из самых важных и может удвоить скорость вашего диска:

```
[root@drwalbr /]# /sbin/hdparm -c3 /dev/hda
```

Здесь и далее предполагается, что мы оптимизируем диск `/dev/hda`. Опция "`-c3`" работает почти со всеми 32-разрядными наборами микросхем IDE. Более подробно использование этой опции описано на man-странице `hdparm`:

```
[root@drwalbr /]# /sbin/man 8 hdparm -c3 /dev/hda
```

Шаг 2

Второй параметр применяется только для дисков стандарта DMA и активизирует обычный режим DMA. Такой режим поддерживается старыми DMA дисками. Для включения режима DMA выполните:

```
[root@drwalbr /]# /sbin/hdparm –d1 /dev/hda
```

Эта команда не только включает поддержку DMA (только для интерфейсов, поддерживающих этот режим), но и в зависимости от набора микросхем, поддерживаемых ядром системы, вдвое сокращает время считывания информации с диска.

Шаг 3

Протокол `Multiword DMA mode 2` (максимальная скорость передачи данных - 16,6 МБ/с), также известный как ATA-2 интерфейс – более скоростной преемник DMA. Если у вас жесткий диск, поддерживающий этот режим, для включения режима DMA-2 выполните команду:

```
[root@drwalbr /]# /sbin/hdparm –d1 –X34 /dev/hda
```

Шаг 4

Протокол `multiword DMA mode 3`, названный UltraDMA, также известный как ATA/ATAPI-4 – это дальнейшее развитие технологии DMA (максимальная скорость пакетной передачи данных - 33 МБ/с). Если у вас такой диск, то выбирайте этот режим:

```
[root@drwalbr /]# /sbin/hdparm –d1 –X66 /dev/hda
```

Шаг 5

Протокол UltraDMA с пропускной способностью 66 МБ/с, также известный как ATA/ATAPI-5. Жесткие диски, поддерживающие такой интерфейс, появились начиная с 1999 года. Включение поддержки протокола осуществляется командой:

```
[root@drwalbr /]# /sbin/hdparm –d1 –X12 –X68 /dev/hda
```

Шаг 6

Протокол UltraDMA с пропускной способностью 100 МБ/с – один из распространенных сейчас интерфейсов, также известен как ATA/ATAPI-6. Производители представили такие жесткие диски уже в середине 2000 года, т. е. еще до официального утверждения ATA/ATAPI-5. Фактически, их объявление было приурочено к объявлению 5 июня первого чипсета, поддерживающего протокол UltraATA/100 – i820E. Мы думаем, что у большинства из вас именно такие жесткие диски. Включение поддержки протокола осуществляется командой:

```
[root@drwalbr /]# /sbin/hdparm –d1 –X12 –X70 /dev/hda
```

Шаг 7

Режим `Multiple sector mode` (IDE Block Mode) поддерживается большинством современных жестких дисков с IDE-интерфейсом. Этот режим позволяет сокращать количество обращений к жесткому диску на 30…50 % , увеличивая скорость передачи данных на 5…50%. Для включения режима выполните команду:

```
[root@drwalbr /]# /sbin/hdparm –mXX  /dev/hda
```

Параметр "XX" представляет максимальное значение, поддерживаемое IDE/ATA диском. Для определения величины этого параметра используется опция "-i". Посмотрите вывод значения MaxMultSect в тексте:

```
[root@drwalbr /]# /sbin/hdparm –i  /dev/hda
/dev/hda:
Model=QUANTUM FIREBALLP LM15, FwRev=A35.0700, SerialNo=737909725840
Config={ HardSect NotMFM HdSw>15uSec Fixed DTR>IOMbs }
RawCHS=16383/16/63, TrkSize=32256, SectSize=21298, ECCbytes=4
BuffType=3(DualPortCache), BuffSize=1900kB, MaxMultSect=16, MultSect=16
DblWordIO=no, OldPIO=2, DMA=yes, OldDMA=2
CurCHS=16383/16/63, CurSects=-66060037, LBA=yes, LBAsects=29336832
tDMA={min:120,rec:120}, DMA modes: mword0 mword1 mword2
IORDY=on/off, tPIO={min:120,w/IORDY:120}, PIO modes: mode3 mode4
UDMA modes: mode0 mode1 mode2 mode3 *mode4
```

Шаг 8

Число секторов get/set влияет на быстродействие многократного обращения к большим файлам. Значение этого параметра по умолчанию – 8 секторов (4 кБайт). Мы советуем увеличить его вдвое, для этого выполните команду:

```
[root@drwalbr /]# /sbin/hdparm -a16 /dev/hda .
```

Шаг 9

Флаг get/set interrupt-unmask несколько увеличивает скорость обмена с жестким диском и устраняет ошибки переполнения последовательного порта. Для установки флага выполните команду:

```
[root@drwalbr /]# /sbin/hdparm -u1 /dev/hda
```

Шаг 10

Кэширование записи также несколько увеличивает скорость обмена с жестким диском. Для включения кэширования выполните команду:

```
[root@drwalbr /]# /sbin/hdparm –W1 /dev/hda
```

Шаг 11

Эти опции позволяют сохранять параметры настройки диска при перезагрузке системы. К сожалению, не все диски их поддерживают. Для включения опций выполните команду:

```
[root@drwalbr /]# /sbin/hdparm -K1 -k1 /dev/hda
```

Шаг 12

Протестировать настройки можно с помощью команды:

```
[root@drwalbr /]# /sbin/hdparm -vtT /dev/hda
/dev/hda:
multcount       = 16 (on)
I/O support     = 3 (32-bit w/sync)
unmaskirq       = 1 (on)
using_dma       = 1 (on)
keepsettings    = 1 (on)
nowerr          = 0 (off)
readonly        = 0 (off)
readahead       = 16 (on)
geometry        - 1826/255/63, sectors = 29336832, start = 0
Timing buffer-cache reads: 128 MB in 0.85 seconds = 150.59 MB/sec
Timing buffered disk reads: 64 MB in 2.54 seconds = 25.20 MB/sec
```

ЗАМЕЧАНИЕ Использование всех перечисленных выше опций должно осуществляться с максимальной осторожностью, т. к. может привести к повреждению жесткого диска.

После того, как выполнена установка и проверка опции hdparm в конец файла /etc/rc.local логично добавить строку, запускающую hdparm с выбранными опциями, например:

```
/sbin/hdparm -c3 -d1 -X12 -X68 -m16 -a16 -u1 -W1 -k1 -K1 /dev/hda
```

Это позволит устанавливать требуемые опции при каждой перезагрузке системы.

Глава 6

Безопасность и оптимизация ядра

Содержание главы:

Самая главная часть системы – ядро. Оно сконфигурировано поставщиком дистрибутива, исходя из соображений максимальной совместимости. В него включена поддержка как можно большего числа устройств и функций и, по мнению авторов, ориентирована в основном на пользователей, использующих Linux в качестве настольной операционной системы. Это обстоятельство, конечно, упрощает установку системы на рабочих станциях и компьютерах домашних пользователей, способствует росту популярности Linux, но ни коим образом не удовлетворяет специфичным требованиям, предъявляемым к ядру сервера. В этой главе описана технология создания уникальной версии ядра, включающей только те фрагменты кода, которые необходимы для использования системы в качестве оптимизированного и безопасного Linux-сервера. Это достаточно простая задача, потому, что код ядра 2.4 был написан специально для серверных систем, и многие из ограничений, присущих старым версиям ядра, были сняты. Ядро, созданное в соответствии с изложенными ниже рекомендациями позволит:

- повысить производительность системы и устойчивость к хакерским атакам за счет уменьшения объема исполняемого кода ядра, удаления неиспользуемых фрагментов кода ядра и применения патча `Grsecurity`;
- дополнительно увеличить производительность системы за счет отказа от модульной архитектуры ядра (по мнению авторов, ядро с модульной архитектурой работают несколько медленнее);
- увеличить объем свободной оперативной памяти (ядро не использует раздел `Swap`);

Ниже описаны процедуры конфигурирования и инсталляции ядра с модульной и монолитной архитектурой. Основное отличие этих процедур состоит в том, что при конфигурировании ядра с монолитной архитектурой на вопросы о включении той или иной опции вы должны отвечать только "`y`" или "`n`" (при модульной архитектуре возможен ответ "`m`" – включить в качестве модуля). При монолитной архитектуре исключены шаги, связанные с компиляцией и инсталляцией модулей, т. е. команды `make modules` и `make modules_install`.

ЗАМЕЧАНИЕ Процесс компиляции ядра оброс слухами, приводящими в ужас начинающих пользователей. Например, авторы сталкивались с ситуацией, в которой пользователь отказывался от компиляции ядра потому, что для этого «нужно знать в совершенстве языки `C` и `C++`". Другой пользователь жаловался, что «в результате компиляции ядра вышел из строя CD-RW". По этому поводу хотелось бы заметить, что знание C и других языков программирования никогда не помешает, но для компиляции ядра в этом нет необходимости. По поводу CD-RW выяснилось, что его владелец пытался что-то дописать на лицензионный штампованный инсталляционный диск MS Windows. Ниже описана процедура, с помощью которой вы всегда можете вернуться к старой работоспособной версии ядра. Отбрасываем все страхи и сомнения и переходим к делу.

Различия между ядрами с модульной и монолитной архитектурами

Одной из причин использования ядра с модульной архитектурой является то, что оно должно быть совместимо с конфигурацией множества систем (тип процессора, чипсет материнской платы, тип жесткого диска и т. д.). Различия между этими системами заставляют разработчиков непрерывно разрабатывать и включать в состав ядра все новые и новые драйверы, поддерживающие соответствующие устройства. Если бы коды всех драйверов непосредственно включались в код ядра, оно стало бы очень большим, что негативно отразилось бы на производительности системы. Кроме того, не все драйверы устройств являются совместимыми. Поэтому была предложена модульная архитектура ядра, которая предполагает загрузку только тех драйверов, которые необходимы для поддержки устройств, используемых в системе.

В ядро с монолитной архитектурой на этапе конфигурирования включаются те, и только те драйверы, которые необходимы для нормального его функционирования.

Таким образом, ядро с модульной архитектурой позволяет фрагментам откомпилированного кода модулей, которые находятся в каталоге ядра `/lib/modules/2.4.18-5asp/` (для дистрибутива ASPLinux 7.3), при необходимости загружаться и удаляться из кода ядра. Ядро же с монолитной архитектурой содержит в своем коде все драйверы.

Преимущества и недостатки каждой из архитектур мы рассмотрели выше. Выбор за вами. Мы же советуем для использования в серверной системе, где решается постоянная или редко изменяемая номенклатура задач и используется постоянная аппаратная конфигурация, использовать ядро с монолитной архитектурой.

Ограничения и допущения

Все операции выполняются пользователем с учетной записью `root`.

Используется ядро версии 2.4.18-5asp.

Используется дистрибутив ASPLinux 7.3 (Vostok). На других дистрибутивах возможно успешное выполнение подобной процедуры, но авторы этого не проверяли.

Пакеты

Последующие шаги описаны в соответствии с информацией, представленной на `http://www.kernel.orq`. Мы использовали две версии ядра: 2.4.18 (на ней основан рассматриваемый дистрибутив ASPLinux 7.3) и 2.4.19 (последняя доступная на момент написания главы версия). В обоих случаях выполняемые операции идентичны.

Необходимые исходные коды ядра – пакеты `linux-2.4.18.tar.gz` или `linux-2.4.19.tar.gz`, можно получить с `http://www.kernel.orq` или `ftp://204.152.189.116`.

Дополнительно устанавливаемые пакеты

Если в системе предполагается использовать систему сетевой защиты (Firewall), поддержку ограничений использования дискового пространства quota, SCSI или RAID контроллеры, перед компиляцией ядра необходима установка соответствующих пакетов:

- для реализации системы сетевой защиты необходима установка пакета `iptables`;
- для реализации поддержки ограничений использования дискового пространства пользователями необходима установка пакета `quota`;
- при использовании SCSI или RAID контроллеров необходима установка пакета `mkinitrd`;
- при использовании модульной архитектуры ядра следует установить пакеты `mkbootdisk` и `dosfstools`.
-

ЗАМЕЧАНИЕ Процесс установки пакетов `iptables` и `quota` подробно описан в соответствующих главах этой книги.

Создание аварийной загрузочной дискеты для ядра с модульной архитектурой

Перед началом конфигурирования, компиляции и инсталляции нового ядра необходимо создать аварийную загрузочную дискету. Исходя из предположения, что вы используете модульное ядро, устанавливаемое в ASPLinux 7.3, ниже описывается процесс создания загрузочной дискеты для ядра с модульной архитектурой.

ЗАМЕЧАНИЕ Процесс создания аварийной загрузочной дискеты для ядра с монолитной архитектурой описан в конце этой главы.

Шаг 1

Выполните команду:

```
[root@drwalbr /]# uname -a
Linux drwalbr.und 2.4.18-5asp #1 Sat Jul 6 20:16:12 EEST 2002 i686 un-
known
```

Версия ядра на рассматриваемой системе – 2.4.18-5asp. Эта информация используется при создании загрузочной дискеты.

Шаг 2

Вставьте в дисковод чистую дискету и выполните команду:

```
[root@drwalbr /]# mkbootdisk --device /dev/fd0H1440 2.4.18-5asp
Insert a disk in /dev/fd0. Any information on the disk will be lost.
Press <Enter> to continue or ^C to abort:
```

ЗАМЕЧАНИЕ В этом примере в качестве опции команды `mkbootdisk` используется версия ядра, установленного в системе, т. е. 2.4.18-5asp. Если установлена другая версия ядра, например, 2.4.19-1, которую мы рекомендуем, то, естественно, нужно указывать именно ее опции, для надежности проверив ядро командой `uname -a`.

Загрузочная дискета может быть использована для загрузки системы в случае возникновения проблем во время обновления ядра. Вы всегда сможете загрузить систему, установив в настройках BIOS загрузку с дискеты, и продолжить настройку ядра. Для большей уверенности загрузите систему с дискеты. Если все прошло успешно, можно переходить к следующим шагам.

Подготовка ядра к инсталляции

Прежде всего, необходимо скопировать архив с исходными кодами ядра в директорию `/usr/src` и удалить старое ядро.

ЗАМЕЧАНИЕ Удаление старого ядра не вызовет остановки компьютера, потому что ядро Linux постоянно находится в оперативной памяти. В случае аварийного отключения питания, окончания рабочего дня и т. п. вы можете загрузить ядро с дискеты и продолжить работу.

Шаг 1

Поместите архив с исходными кодами ядра в каталог `/usr/src`:

```
[root@drwalbr /]# cp linux-2.4.18.tar.gz /usr/src/
```

Шаг 2

Если ядро системы было установлено с использованием rpm-пакетов (в случае выполнения установки системы в соответствии с рекомендациями главы 2, это действительно так), вам необходимо их удалить:

```
[root@drwalbr /]# rpm –q  kernel
kernel-2.4.18-5asp.i386.rpm

[root@drwalbr /]# rpm –q glibc-kernheaders
glibc-kernheaders-2.4-7.14.asp.i386.rpm

[root@drwalbr /]# rpm –e  --nodeps kernel  glibc-kernheaders
```

ЗАМЕЧАНИЕ Если вы получите сообщения об ошибках, подобно такой: "`cannot remove /lib/modules/2.4.x directory, directory not empty`", удалите каталог вручную:

```
rm -rf /lib modules/2.4.18-5asp/.
```

Этот каталог предназначен для хранения модулей старого ядра и больше вам не понадобится.

Если необходимо удалить старое ядро, установленное из исходных кодов tar-архива (например, ядро, созданное в результате выполнения рекомендаций этой главы), то необходимо выполнить следующие действия.

Перейдите в каталог `/usr/src`:

```
[root@drwalbr /]# cd /usr/src
```

Удалите каталог заголовков ядра:

```
[root@drwalbr src]# rm –rf linux-2.4.x/
```

Удалите ядро:

```
[root@drwalbr src]# rm –f /boot/vmlinuz-2.4.x
```

Удалите файл `system.map`:

```
[root@drwalbr src]# rm -f /boot/System.map-2.4.x
```

Если в системе установлена модульная версия ядра, удалите каталог модулей ядра Linux:

```
[root@drwalbr src]# rm -rf /lib/modules/2.4.x/
```

Шаг 3

Распакуйте и удалите архив с исходными кодами ядра:

```
[root@drwalbr src]# tar xzpf linux-version.tar.gz
[root@drwalbr src]# rm -f linux-version.tar.gz
```

ЗАМЕЧАНИЕ Мы советуем вам перенести в надежное место и сохранить архив с кодами ядра до окончания обновления ядра и успешной перезагрузки системы. Он может понадобиться в случае неудачи при обновлении ядра.

Применение патча Grsecurity

Grsecurity – патч, предназначенный для улучшения безопасности устойчивых версий ядра Linux. Существует много других подобных проектов, например, rsbac (`http://www.rsbac.org/`), lids (`http://www.lids.org/`), SELinux (`http://www.nsa.gov/selinux/`) и OpenWall (`http://www.openwall.com/linux/`), которые рассматривают лишь частные вопросы обеспечения безопасности. Проект Grsecurity, на наш взгляд, наиболее комплексно учитывает различные аспекты обеспечения безопасности ядра Linux-системы и имеет механизмы защиты, не реализованные в других проектах. Патч Grsecurity адаптируется применительно к различным версиям ядер, поэтому необходимо использовать патч, соответствующий версии ядра, используемого в системе. Для версии ядра 2.4.18 используется патч Grsecurity для версии ядра 2.4.18, для версии ядра 2.4.19 – патч Grsecurity для версии ядра 2.4.19 и т. д. При конфигурации ядра, использующего патч Grsecurity, в настройках ядра будет добавлен новый раздел, позволяющий конфигурировать настройки безопасности.

Необходимый патч для версии ядра 2.4.18 или 2.4.19 можно получить с узла `http://www.grsecurity.org`. Применение патча и дальнейшие операции по созданию и установке нового ядра рассматриваются применительно к версии 2.4.18.

```
[root@drwalbr /]# cp grsecurity-1.9.4-2.4.18.patch /usr/src/
[root@drwalbr /]# cd /usr/src/linux/
[root@drwalbr linux]# patch -p1 < ../grsecurity-1.9.4-2.4.18.patch
[root@drwalbr linux]# cd ..
[root@drwalbr src]# rm -f grsecurity-1.9.4-2.4.18.patch
```

Настройка ядра

Переходим к конфигурированию (т. е. определению номенклатуры драйверов и функциональных возможностей, включаемых в код) нового ядра.

Шаг 1

В файле `/usr/src/linux-2.4.x/include/linux/sem.h` измените параметр:

```
#define SEMMNI 128 /* <= IPCMNI max # of semaphore identifiers */
```

на параметр:

```
#define SEMMNI 512 /* <= IPCMNI max # of semaphore identifiers */
```

В файле `/usr/src/linux-2.4.x/include/linux/limits.h` измените следующие параметры:

```
#define NR_OPEN                 1024
```

на:

```
#define NR_OPEN                 8192
```

и

```
#define OPEN_MAX          256   /* # open files a process may have */
```

на:

```
#define OPEN_MAX         8192   /* # open files a process may have */
```

В файле `/usr/src/linux-2.4.x/include/linux/posix_types.h` измените параметр:

```
#define __FD_SETSIZE   1024
```

на:

```
#define __FD_SETSIZE   8192
```

Шаг 2

Теперь необходимо задать параметры оптимизации ядра применительно к имеющейся архитектуре процессора.

В файле `usr/src/linux-2.4.x/Makefile` измените строку:

```
HOSTCFLAGS = -Wall -Wstrict-prototypes -O2 -fomit-frame-pointer
```

на:

HOSTCFLAGS = -Wall -Wstrict-prototypes -O2 **-march=i686 -funroll-loops** -fomit-frame-pointer

и

```
CFLAGS := $(CPPFLAGS) -Wall -Wstrict-prototypes - O2 -fomit-frame-pointer
-fno-strict-aliasing
```

на:

```
CFLAGS := $(CPPFLAGS) -Wall -Wstrict-prototypes - O2  -march=i686 –fun-
roll -loops -fomit-frame-pointer –fno -strict-aliasing
```

ЗАМЕЧАНИЕ В последних примерах проведена оптимизация для процессора i686. Для систем с процессорами i586, i486 или AMD K6 или K6-2 параметр `-march-i686` должен быть изменен, соответственно, на `-march-i586`, `-march-i486` или `-march-k6`. Компиляция ядра с опцией `-O3` (прописная буква "О" *три*) не повышает его производительности и в некоторых случаях приводит к нестабильности ядра. Поэтому при компиляции ядра используется параметр `-O2` (прописная буква "О" *два*).

Очистка ядра

Для выполнения дальнейших операций необходимо обеспечить правильность ссылок `/usr/include/asm` и `/usr/include/linux`. Для этого необходимо сделать следующее.

Шаг 1

Удалите старые и создайте новые ссылки `asm` и `linux`:

```
[root@drwalbr /]# cd /usr/include/
[root@drwalbr include] # rm -f asm linux
[root@drwalbr include] # ln -s /usr/src/linux-2.4.x/include/asm-i386 asm
[root@drwalbr include] # ln -s /usr/src/linux-2.4.x/include/linux linux
```

Это очень важная часть конфигурирования. В ней удаляются каталоги `asm` и `linux` в `/usr/include`, содержащие файлы заголовков старой версии ядра, и создаются новые ссылки на те же каталоги для новой версии исходного кода ядра.

ЗАМЕЧАНИЕ Если ранее установленное ядро было создано из rpm-пакетов, то ссылок `asm` и `linux` не будет, т. к. при удалении пакета `glibc-kernheaders` они будут удаляться автоматически.

Шаг 2

Удалите старые объектные файлы и зависимости:

```
[root@drwalbr include] # cd /usr/src/linux-2.4.x/
[root@drwalbr linux-2.4.x]# make mrproper
```

Шаг 3

Для конфигурирования ядра можно воспользоваться одной из нескольких программ:

- `make config`, позволяющей последовательно вводить требуемые параметры конфигурации ядра путем ответа на вопросы в текстовой консоли;
- `make menuconfig`, позволяющей вводить параметры настройки ядра с использованием меню в текстовом режиме;
- `make xconfig`, позволяющей вводить параметры настройки ядра с использованием меню в графическом режиме.

Авторы рекомендуют осуществлять конфигурирование ядра программой `make config` или `make menuconfig`, чтобы не устанавливать лишних пакетов, наличие которых может негативно повлиять на безопасность системы:

```
[root@drwalbr /]# cd /usr/src/linux-2.4.x/
[root@drwalbr linux-2.4.x] # make config
rm -f include/asm
( cd include ; In -sf asm-i386 asm)
/bin/sh scripts/Configure  arch/i386/config.in
#
# Using defaults found in arch/i386/defconfig
#
```

Конфигурирование ядра

После запуска программы `make config` на экране последовательно отображаются вопросы о включении различных опций конфигурации ядра, отвечая на которые можно определить, какие функциональные возможности и драйверы устройств будут включены в ядро системы. На большинство вопросов, задаваемых `make config`, можно дать три варианта ответа:

- `Y` – включить в ядро соответствующий опции фрагмент кода;
- `m` – использовать модуль для размещения соответствующего опции фрагмента кода и загружать его при необходимости;
- `n` – не включать поддержку соответствующей опции.

ЗАМЕЧАНИЕ Значение, указанное в квадратных скобках первым, соответствует заданному по умолчанию выбору ответа. Для выбора значения по умолчанию необходимо нажать клавишу <Enter>. Среди предлагаемых вариантов ответа может оказаться символ "?". Это означает, что, нажав последовательно клавиши <?> и <Enter>, можно получить более подробную информацию о возможных вариантах ответа на вопрос.

Для осуществления правильного конфигурирования ядра необходимо иметь достоверную информацию о комплектующих устройствах системы. Начинать конфигурирование ядра можно, зная точные ответы, по крайней мере, на следующие вопросы.

1. Какой тип процессора используется?
2. Сколько процессоров?
3. Какой тип жесткого диска и контроллеров жесткого диска?
4. Сколько жестких дисков?

5. Предполагается ли создание RAID-массива?
6. Каков объем оперативной памяти?
7. Какой используется тип сетевых карт (производитель, модель, чипсет)?
8. Имеется ли SCSI-адаптер и, если да, то какой?
9. Имеется ли RAID-контроллер и, если да, то какой?
10. Каков тип мыши?
11. Какая используется видеокарта (производитель, модель, чипсет, объем видеопамяти)?

Ответы на эти вопросы можно получить, изучив имеющуюся документацию, визуально определив марку установленных комплектующих устройств, посетив веб-ресурсы производителей и дистрибьюторов оборудования.

Конфигурирование ядра с монолитной архитектурой

В качестве примера рассмотрим конфигурирование ядра с монолитной архитектурой в следующей системе:

- процессор Pentium II 400 МГЦ (i686);
- системная плата SCSI;
- жесткий диск SCSI;
- SCSI ControlerAdaptecAIC 7xxx;
- CD-ROM ATAPI IDE;
- дисковод для гибкого диска;
- сетевая карта Ethernet Intel EtherExpressPro 10/100;
- мышь PS/2.

Наберите с консоли:

```
[root@drwalbr /]# cd /usr/src/linux-2.4.x/
[root@drwalbr linux-2.4.x]# make config
rm -f include/asm
( cd include ; In -sf asm-i386 asm) /bin/sh scripts/Configure
arch/i386/config.in
#
#Using defaults found in arch/1386/defconfig
#
...
*
Code maturity level options
*Prompt for development and/or incomplete code/drivers
(CONFIG_EXPERIMENTAL) [N/y/?] <Enter>
```

Эта опция позволяет использовать настройки и драйверы, которые в настоящее время находятся в стадии тестирования. Настоятельно рекомендуем не включать ее.

ЗАМЕЧАНИЕ Здесь и далее <Enter> означает нажатие клавиши Enter, при котором вводится значение по умолчанию, обозначенное прописной буквой (в данном случае N).

```
*
* Loadable module support
* Enable loadable module support (CONFIG_MODULES) [Y/n/?] <n>
```

Эта опция включает/отключает поддержку ядра с модульной архитектурой.

```
* Processor type and features
Processor family (386, 486, 586/K5/5x86/6x86/6x86MX, Pentium-Classic,
Pentium-MMX, Pentium-Pro/Celeron/Pentium-ll, Pentium-
lll/Celeron(Coppermine), Pentium-4, K6/K6-11/K6-111, Athlon/Duron/K7,
Crusoe, Winchip-C6, Winchip-2, Winchip-2A/Winchip-3, Cyrixlll/C3)
[Pentium-lll/Celeron(Coppermine)] Pentium-II
```

Здесь задается тип процессора.

```
Toshiba Laptop support (CONFIG_TOSHIBA) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку драйвера Toshiba в переносных или настольных компьютерах.

```
Dell Inspiron 8000 support (CONFIG_18K) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку драйвера Dell Inspiron 8000 для переносных или настольных компьютеров.

```
/dev/cpu/microcode - Intel IA32 CPU microcode support (CONFIG MICROCODE)
[N/y/?] <Enter>
```

Эта опция включает/отключает модификацию микропрограмм на процессорах Intel семейства IA32, например, Pentium Pro, Pentium II, Pentium III, Pentium 4, Xeon и т. д. В большинстве случаев эта опция просто не нужна.

```
/dev/cpu/*/msr - Model-specific register support (CONFIG_X86_MSR) [N/y/?]
<y>
```

Эта опция включает/отключает поддержку устройства, которое дает возможность приоритетным процессам обращаться к x86 Model-Specific Registers (MSRs). На многопроцессорных системах доступ к MSR адресован к определенному процессору. Эту опцию можно включить и для однопроцессорной системы.

```
/dev/cpu/*/cpuid - CPU information support (CONFIG_X86_CPUID) [N/y/?] <y>
```

Эта опция включает/отключает поддержку устройства, обеспечивающего доступ к командам x86 CPUID.

```
High Memory Support (off, 4GB, 64GB) [off] <Enter>
```

Эта опция позволяет использовать до 64 гигабайтов физической памяти на x86 системах.

```
Math emulation (CONFIG_MATH_EMULATION) [N/y/?] <Enter>
```

Эта опция позволяет использовать не встроенный математический сопроцессор.

```
MTRR (Memory Type Range Register) support (CONFIG_MTRR) [N/y/?] <Enter>
```

Эта опция на процессорах семейства Intel (Pentium Pro, Pentium II и старше) используется для повышения производительности при использовании графического интерфейса XFree86 на многопроцессорных системах. Она не работает с процессорами AMD и Cyrix.

```
Symmetric multi-processing support (CONFIG_SMP) [Y/n/?] <n>
```

Эта опция включает/отключает поддержку многопроцессорного режима.

```
Local APIC support on uniprocessors (CONFIG_X86_UP_APIC) [N/y/?] (NEW)
<y>
```

Эта опция включает/отключает контроллер прерываний (APIC) на системе с одним процессором. Эта опция не поддерживается процессорами AMD и Cyrix.

```
*
* General setup
* Networking support (CONFIG_NET) [Y/n/?] <Enter>
```

Эта опция необходима и включает/отключает поддержку работы в сети.

```
PCI support (CONFIG_PCI) [Y/n/?] <Enter>
```

Эта опция включает/отключает поддержку PCI-шины.

```
PCI access mode (BIOS, Direct, Any) [Any] <Enter>
```

Эта опция определяет способ обнаружения и диагностики устройств на шине PCI. Обычно для обнаружения и определения конфигурации PCI-устройств используются BIOS. Некоторые старые системы с шиной PCI имеют ошибки в BIOS и могут выйти из строя, если эта опция отключена. Современные встраиваемые системы могут не иметь BIOS вообще. В этом случае Linux может обнаружить аппаратные средства на шине PCI, не используя BIOS. При выборе "Any" ядро будет пробовать метод прямого доступа и BIOS.

```
PCI device name database (CONFIG_PCI_NAMES) [Y/n/?] <n>
```

Эта опция включает/отключает поддержку базы данных, содержащей название многих PCI-устройств, увеличивая размер ядра на 80 кБайт.

```
EISA support (CONFIG_EISA) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку шины EISA.

```
MCA support (CONFIG_MCA) [N/y/?] <Enter>
```

Эта опция позволяет включить поддержку ядром шины MCA.

```
Support for hot-pluggable devices (CONFIG_HOTPLUG) [Y/n/?] <n>
```

Эта опция используется только в переносных или настольных компьютерах с PCMCIA или PC-платами, которые подключаются к системе без ее остановки и перезагрузки.

`System V I PC (CONFIG_SYSVIPC) [Y/n/?]` **<Enter>**

Эта опция позволяет реализовать поддержку взаимодействия между процессами, протекающими в IPC (Inter Process Communication) – наборе библиотечных функций и системных вызовов, которые позволяют процессам синхронизироваться и обмениваться информацией. Некоторые программы не будут работать без включения этой опции.

`BSD Process Accounting (CONFIG_BSD_PROCESS_ACCT) [N/y/?]` **<Enter>**

Эта опция позволяет/запрещает пользовательским программам инициировать запись процесса, считывающего информацию в специальный файл. Совсем необязательно разрешать эту опцию.

`Sysctl support (CONFIG_SYSCTL) [Y/n/?]` **<Enter>**

Эта очень важная опция – она позволяет/запрещает изменять некоторые параметры ядра в процессе функционирования системы с использованием файловой системы `/proc` и файла `/etc/sysctl.conf`.

`Kernel core (/proc/kcore) format (ELF, A.OUT) [ELF]` **<Enter>**

Эта опция позволяет/запрещает в файле `kcore` файловой системы `/proc` содержать образ ядра в одном из двух форматов: ELF (Executable and Linkable Format) или A.OUT.

`Kernel support for a.out binaries (CONFIG_BINFMT_AOUT) [Y/n/?]` **<n>**

Эта опция включает/отключает поддержку устаревшего формата A. OUT, который представляет собой набор форматов для библиотек и выполняемых программ, используемых в самых ранних версиях UNIX.

`Kernel support for ELF binaries (CONFIG_BINFMT_ELF) [Y/n/?]` **<Enter>**

Эта опция включает/отключает поддержку исполняемых файлов и файлов библиотек в формате ELF.

`Kernel support for MISC binaries (CONFIG_BINFMT_MISC) [Y/n/?]` **<Enter>**

Эта опция позволяет/запрещает обращение исполняемых файлов к ядру. Эта настройка требуется программам, которые запускаются с использованием интерпретаторов (Perl, Java, Python, Emacs-Lisp…).

`Power Management support (CONFIG_PM) [Y/n/?]` **<n>**

Эта опция включает/отключает поддержку управления питанием, применяемых в основном на ноутбуках.

```
*
* Memory Technology Devices (MXD)
* Memory Technology Device (MTD) support (CONFIG_MTD) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку MTD (Memory Technology Devices), предназначенной для создания файловых систем в оперативной памяти.

```
*
*Parallel port support
* Parallel port support (CONFIG_PARPORT) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку параллельных портов. Ее включение необходимо только, если предполагается использование периферийных устройств, подключаемых через порт подобного типа (принтер, съемные накопители и т. д.).

```
*
* Plug and Play configuration
*
* Plug and Play support (CONFIG_PNP) [Y/n/?] <n>
```

Эта опция позволяет включать/отключает поддержку стандарта Plug and Play (PnP) для автоматического конфигурирования периферийных устройств.

```
*
* Block devices
* Normal PC floppy disk support (CONFIG_BLK_DEV_FD) [Y/n/?] <Enter>
```

Эта опция включает/отключает поддержку накопителей на гибких магнитных дисках.

`XT hard disk support (CONFIG_BLK_DEV_XD) [N/y/?]` **<Enter>**

Эта опция включает/отключает поддержку контроллеров жесткого диска устаревшего стандарта XT.

`Compaq SMART2 support (CONFIG_BLK_CPQ_DA) [N/y/?]` **<Enter>**

Эта опция включает/отключает поддержку контроллеров Compaq Smart Array.

`Compaq Smart Array 5xxx support (CONFIG_BLK_CPQ_CISS_DA) [N/y/?]` **<Enter>**

Эта опция включает/отключает поддержку контроллеров Compaq Smart Array 5xxx.

```
Mylex DAC960/DACIIOO PCI RAID Controller support (CONFIG_BLK_DEV_DAC960)
[N/y/?] <Enter>
```

Эта опция включает поддержку RAID контроллеров Mylex DAC960, AcceleRAID, и eXtremeRAID PCI.

```
Loopback device support (CONFIG_BLK_DEV_LOOP) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку «петлевого интерфейса" и необходима при наличии в системе устройств с SCSI-интерфейсом. Включение этой опции Также необходимо при наличии в системе устройств, эмулирующих SCSI-интерфейс, например, CD-RW.

```
Network block device support (CONFIG_BLK_DEV_NBD) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку клиента блочных устройств.

```
RAM disk support (CONFIG_BLK_DEV_RAM) [N/y/?] <Enter>
```

Эта опция позволит использовать часть вашей оперативной памяти в качестве блочного устройства, создавать в ней файловые системы.

```
*
* Multi-device support (RAID and LVM)
* Multiple devices driver support (RAID and LVM) (CONFIG_MD) [N/y/?] <En-
ter>
```

Эта опция требуется только для RAID и управления логическим томом (LVM)

```
*
* Networking options
* Packet socket (CONFIG__PACKET) [Y/n/?] <Enter>
```

Эта опция включает/отключает поддержку приложений, которые связываются непосредственно с сетевыми устройствами без использования промежуточного сетевого протокола, осуществленного в ядре, подобно программе tcpdump.

```
Packet socket: mmapped IO (CONFIG_PACKET_MMAP) [N/y/?] <y>
```

Эта опция включает/отключает ускорение работы драйвера пакетов.

```
Kernel/User netlink socket (CONFIG_NETLINK) [N/y/?] <y>
```

Эта опция позволяет разрешать/запрещать двухстороннюю связь между пользовательскими процессами и процессами ядра.

```
Routing messages (CONFIG_RTNETLINK) [N/y/?] (NEW) <y>
```

Эта опция необходима для нормальной работы предыдущей.

```
Netlink device emulation (CONFIG_NETLINK_DEV) [N/y/?] (NEW) <y>
```

Эта опция обеспечивает обратную совместимость.

```
Network packet filtering (replaces ipchains) (CONFIG_NETFILTER) [N/y/?]
<y>
```

Эта опция включает/отключает поддержку Firewall.

```
Network packet filtering debugging (CONFIG_NETFILTER_DEBUG) [N/y/?] (NEW)
<y>
```

Эта опция включает/отключает поддержку отладки кода netfilter.

```
Socket Filtering (CONFIG_FILTER) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку фильтра Linux Socket Filter, необходимого для реализации фильтрации PPP-пакетов.

```
Unix domain sockets (CONFIG_UNIX) [Y/n/?] <Enter>
```

Опция включает/отключает поддержку работы с сетями TCP/IP.

```
TCP/IP networking (CONFIG_INET) [Y/n/?] <Enter>
```

Опция включает/отключает поддержку работы с сетями TCP/IP.

```
IP: multicasting (CONFIG_IP_MULTICAST) [Y/n/?] <n>
```

Эта опция необходима для реализации сетевых мультимедийных технологий.

```
IP: advanced router (CONFIG_IP_ADVANCED_ROUTER) [N/y/?] <n>
```

Эта опция позволяет конфигурировать систему как шлюз. В случае включения этой опции необходимо ответить на ряд дополнительных вопросов.

```
IP: kernel level autoconfiguration (CONFIG IP_PNP) [N/y/?] <Enter>
```

Включение этой опции необходимо только для бездисковых рабочих станций, требующих доступа к сети для загрузки.

```
IP: tunneling (CONFIG_NET_IPIP) [N/y/?] <Enter>
```

Эта опция включает поддержку туннелирования.

```
IP: GRE tunnels over IP (CONFIG_NET_IPGRE) [N/y/?] <Enter>
```

Другой вид настройки туннелирования. Её использование необходимо, например, при подключении сервера к сети через VPN-подключение.

```
IP: TCP Explicit Congestion Notification support (CONFIG_INET_ECN)
[N/y/?] <Enter>
```

Опция включает/отключает поддержку уведомления клиентов о перегрузке системы. К сожалению, многие сервера отказывают в доступе тем системам, на которых включена эта опция, из соображений безопасности.

```
IP: TCP syncookie support (disabled per default) (CONFIG_SYN_COOKIES)
[N/y/?] Y
```

Эта опция включает/отключает поддержку защиты от атак типа "SYN flooding".

```
*
*IP: Netfilter Configuration
*
Connection tracking (required for masq/NAT) (CONFIG_IP_NF_CONNTRACK)
[N/y/?] (NEW) <y>
FTP protocol support (CONFIG_IP_NF_FTP) [N/y/?] (NEW) <y>
IRC protocol support (CONFIG_IP_NF_IRC) [N/y/?] (NEW) <y>
IP tables support (required for filtering/masq/NAT)
(CONFIG_IP_NF_IPTABLES) [N/y/?] (NEW) <y>
limit match support (CONFIG_IP_NF_MATCH_LIMIT) [N/y/?] (NEW) <y>
MAC address match support (CONFIG_IP_NF_MATCH_MAC) [N/y/?] (NEW) <y>
netfilter MARK match support (CONFIG_IP_NF_MATCH_MARK) [N/y/?] (NEW) <y>
Multiple port match support (CONFIG_IP_NF_MATCH_MULTIPORT) [N/y/?] (NEW)
<y>
TOS match support (CONFIG_IP_NF_MATCH_TOS) [N/y/?] (NEW) <y>
LENGTH match support (CONFIG_IP_NF_MATCH_LENGTH) [N/y/?] (NEW) <y>
TTL match support (CONFIG_IP_NF_MATCH_TTL) [N/y/?] (NEW) <y>
tcpmss match support (CONFIG_IP_NF_MATCH_TCPMSS) [N/y/?] (NEW) <y>
Connection state match support (CONFIG_IP_NF_MATCH_STATE) [N/y/?] (NEW)
<y>
Packet filtering (CONFIG_IP_NF_FILTER) [N/y/?] (NEW) <y>
REJECT target support (CONFIG_IP_NF_TARGET_REJECT) [N/y/?] (NEW) <y>
Full NAT (CONFIG_IP_NF_NAT) [N/y/?] (NEW) <y>
Packet mangling (CONFIG_IP_NF_MANGLE) [N/y/?] (NEW) <y>
TOS target support (CONFIG_IP_NF_TARGET_TOS) [N/y/?] (NEW) <y>
MARK target support (CONFIG_IP_NF_TARGET_MARK) [N/y/?] (NEW) <y>
LOG target support (CONFIG_IP_NF_TARGET_LOG) [N/y/?] (NEW) <y>
TCPMSS target support (CONFIG IP NF_TARGET_TCPMSS) [N/y/?] (NEW) <y>
```

На все вопросы в разделе конфигурации ядра `IP: Netfilter Configuration` следует отвечать положительно, т. к. они связаны с поддержкой Firewall.

```
*
*
*he IPX protocol (CONFIG_IPX) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку сетевого протокола Novell.

```
Appletalk protocol support (CONFIG_ATALK) [N/y/?] <Enter>
```

Эта опция включает/отключает протокол AppleTalk, используемый для связи с системами на платформе Apple.

```
DECnet Support (CONFIG_DECNET) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку сетевого протокола DECnet, используемого в программных продуктах компании Digital (в настоящее время Compaq).

```
802.1d Ethernet Bridging (CONFIG_BRIDGE) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку моста Ethernet (в соответствии со стандартом IEEE 802.1).

```
* QoS and/or fair queueing
* QoS and/or fair queueing (CONFIG_NET_SCHED) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку QoS, предназначенной для оптимизации порядка отсылки пакетов на сетевые устройства. Включение этой опции желательно в случаях, если система используется в качестве маршрутизатора.

```
*
* Telephony Support
* Linux telephony support (CONFIG PHONE) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку использования карт для IP-телефонии.

```
*
* ATA/IDE/MEM/RLL support
* ATA/IDE/MFM/RLL support (CONFIG_IDE) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку управления модулями запоминающих устройств большой емкости типа ATA/(E) IDE и ATAPI.

```
*
* ZDB, ATA and ATARI Block devices
* Enhanced IDE/MFM/RLL disk/cdrom/tape/floppy support
(CONFIG_BLK_DEV_IDE) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку расширенного драйвера для IDE/MFM/RLL. Если в системе имеется хотя бы одно устройство, использующее IDE контроллер, необходимо включить эту опцию.

```
Use old disk-only driver on primary interface (CONFIG_BLK_DEV_HD_IDE)
[N/y/?] <Enter>
```

Эта опция включает/выключает поддержку старого драйвера для IDE/MFM/RLL.

```
Include IDE/ATA-2 DISK support (CONFIG_BLK_DEV_IDEDISK) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку еще одного варианта драйвера для mfm/rll/ide.

```
Use multi-mode by default (CONFIG_IDEDISK_MULTI_MODE) [Y/n/?] <n>
```

Эта опция включает/выключает поддержку вывода сообщений вида:

```
hda: set_multmode: status=0x51 { DriveReady SeekCompiete Error }
hda: set multmode: error=0x04 { DriveStatusError }
```

об ошибках ввода-вывода в системах с IDE-интерфейсом. При использовании исправных и надежных дисков и системных плат нет необходимости в выводе отладочных сообщений.

```
Include IDE/ATAPI CDROM support (CONFIG_BLK_DEV_IDECD) [Y/n/?] <n>
```

Эта опция включает включает/выключает поддержку более чем одного привода CD-ROM.

```
Include IDE/ATAPI TAPE support (CONFIG_BLK_DEV_IDETAPE) [N/y/?] <Enter>
```

Эта опция включает включает/выключает поддержку ATAPI протокола для накопителей на магнитной ленте с IDE интерфейсом.

```
Include IDE/ATAPI FLOPPY support (CONFIG_BLK_DEV_IDEFLOPPY) [N/y/?] <En-
ter>
```

Эта опция включает включает/выключает поддержку ATAPI протокола для накопителей на гибких магнитных дисках с IDE интерфейсом.

```
SCSI emulation support (CONFIG_BLK_DEV_IDESCSI) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку эмуляции SCSI-контроллера для IDE ATAPI-устройств и позволяет использовать SCSI драйвер устройства вместо штатного ATAPI-драйвера. Это необходимо при наличии в системе устройств CD-RW.

```
*
* XDB chipsetc supporfe/bugfixes
* CMD640 chipset bugfix/support (CONFIG_BLK_DEV_CMD640) [Y/n/?] <n>
```

Эта опция включает/выключает поддержку исправления ошибок чипсета CMD640.

```
RZ1000 chipset bugfix/support (CONFIG_BLK_DEV_RZIOOO) [Y/n/?] <n>
```

Эта опция включает/выключает поддержку исправления ошибок чипсета RZ1000.

```
Generic PCI IDE chipset support (CONFIG_BLK_DEV_IDEPCI) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку обнаружения и конфигурирования IDE интерфейсов в системах с шиной PCI.

```
Sharing PCI IDE interrupts support (CONFIG_IDEPCI_SHARE_IRQ) [Y/n/?] <En-
ter>
```

Эта опция включает/выключает поддержку совместного использования IDE контроллера другими устройствами.

```
Generic PCI bus-master DMA support (CONFIG_BLK_DEV_IDEDMA_PCI) [Y/n/?]
<Enter>
```

Включение этой опции позволяет снизить загрузку центрального процессора в системе с дисками IDE на шине PCI, поддерживающей операцию bus-master DMA. При наличии в системе дисков, поддерживающих IDE ATA/33/66/100, рекомендуется использование этой опции.

```
Boot off-board chipsets first support (CONFIG_BLK_DEV_OFFBOARD) [N/y/?]
<Enter>
```

Эта опция включает/выключает поддержку изменения порядка просмотра устройств при загрузке системы.

```
Use PCI DMA by default when available (CONFIG_IDEDMA_PCI_AUTO) [Y/n/?]
<Enter>
```

Эта опция включает/выключает поддержку настроек DMA, которые могут быть использованы для повышения производительности дисковой подсистемы.

```
AEC62XX chipset support (CONFIG_BLK_DEV_AEC62XX) [N/y/?] <Enter>
ALI M15x3 chipset support (CONFIG_BLK_DEV_AL115X3) [N/y/?] <Enter>
CMD64X chipset support (CONFIG_BLK_DEV_CMD64X) [N/y/?] <Enter>
CY82C693 chipset support (CONFIG_BLK_DEV_CY82C693) [N/y/?] <Enter>
Cyrix CS5530 MediaGX chipset support (CONFIG_BLK_DEV_CS5530) [N/y/?] <En-
ter>
HPT34X chipset support (CONFIG_BLK_DEV_HPT34X) [N/y/?] <Enter>
HPT366 chipset support (CONFIG_BLK_DEV_HPT366) [N/y/?] <Enter>
Intel PIIXn chipsets support (CONFIG_BLK_DEV_PIIX) [Y/n/?] <Enter>
PIIXn Tuning support (CONFIG_PIIX_TUNING) [Y/n/?] <Enter>
NS87415 chipset support (EXPERIMENTAL) (CONFIG_BLK_DEV_NS87415) [N/y/?]
<Enter>
PROMISE PDC202{46162165167168} support (CONFIG_BLK_DEV_PDC202XX) [N/y/?]
<Enter>
ServerWorks OSB4/CSB5 chipsets support (CONFIG_BLK_DEV_SVWKS) [N/y/?]
<Enter>
SiS5513 chipset support (CONFIG_BLK_DEV_SIS5513) [N/y/?] <Enter>
SLC90E66 chipset support (CONFIG_BLK__DEV_SLC90E66) [N/y/?] <Enter>
Tekram TRM290 chipset support (EXPERIMENTAL) (CONFIG_BLK_DEV_TRM290)
[N/y/?] <Enter>
VIA82CXXX chipset support (CONFIG_BLK_DEV_VIA82CXXX) [N/y/?] <Enter>
Other IDE chipset support (CONFIG_IDE_CHIPSETS) [N/y/?] <Enter>
IGNORE word93 Validation BITS (CONFIG_IDEDMA_IVB) [N/y/?] <Enter>
```

Эти опции включают/выключают поддержку различных типов чипсетов, используемых в материнской плате. Отсутствие чипсета в перечне может означать, что он автоматически поддерживается ядром.

ЗАМЕЧАНИЕ В двух вариантах есть ответы по умолчанию, установленные как Y (Intel PIIxn chipsets support (CONFIG_BLK_DEV_PIIX) [Y/n/?] и PIIXn Tuning support (CONFIG_PIIX_TUNING) [Y/n/?]). При использовании процессоров Pentium II или более поздних моделей необходимо сохранить значение по умолчанию.

```
*
```

```
* SCSI support
* SCSI support (CONFIG_SCSI) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку устройств SCSI. Использование опции необходимо на системах, использующих SCSI жесткие диски, SCSI накопители на магнитной ленте, SCSI CD-ROM или CD-RW с любым типом интерфейса.

```
*
* SCSI support type (disk, tape, CD-ROM) * SCSI disk support
(CONFIG_BLK_DEV_SD) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку SCSI жесткого диска.

```
Maximum number of SCSI disks that can be loaded as modules
(CONFIG_SD_EXTRA_DEVS) [40] <Enter>
```

Эта опция позволяет управлять количеством дополнительного пространства в таблицах драйверов, которые загружены как модули. Так как создается ядро с монолитной архитектурой, принимается значение по умолчанию.

```
SCSI tape support (CONFIG_CHR_DEV_ST) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку SCSI накопителя на магнитной ленте для Linux.

```
SCSI OnStream SC-xO tape support (CONFIG_CHR_DEV_OSST) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку SCSI-накопителей на магнитной ленте OnStrea.

```
SCSI CD-ROM support (CONFIG_BLK_DEV_SR) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку CD-ROM.

```
SCSI generic support (CONFIG_CHR_DEV_SG) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку использования SCSI сканеров, устройств записи компакт-дисков и других устройств.

```
*
* Some SCSI devices (e.g. CD jukebox) support multiple LUNs
* Enable extra checks in new queueing code (CONFIG_SCSI_DEBUG_QUEUES)
[Y/n/?] <Enter>
```

Эта опция включает/выключает большую дополнительную последовательность, проверяющую новый код организации очереди на SCSI-устройствах.

```
Probe all LUNs on each SCSI device (CONFIG_SCSI_MULTI_LUN) [Y/n/?] <n>
```

Эта опция негативно влияет на производительность системы и в большинстве случаев должна быть отключена.

```
Verbose SCSI error reporting (kernel size +=12K) (CONFIG_SCSI_CONSTANTS)
[Y/n/?] <n>
```

Эта опция включает/выключает поддержку более подробного формата вывода сообщений об ошибках аппаратных средств SCSI и негативно влияет на производительность системы.

```
SCSI logging facility (CONFIG_SCSI_LOGGING) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку дополнительных средств регистрации SCSI и негативно влияет на производительность системы.

```
*
* SCSI low-level drivers
*
3ware Hardware ATA-RAID support (CONFIG_BLK_DEV_3W_XXXX_RAID) [N/y/?]
<Enter>
7000FASST SCSI support (CONFIG_SCSI_7000FASST) [N/y/?] <Enter>
ACARD SCSI support (CONFIG_SCSI_ACARD) [N/y/?] <Enter>
Adaptec AHA152X/2825 support (CONFIG_SCSI_AHA152X) [N/y/?] <Enter>
Adaptec AHA1542 support (CONFIG_SCSI_AHAl542) [N/y/?] <Enter>
Adaptec AHA1740 support (CONFIG_SCSI_AHA1740) [N/y/?] <Enter>
Adaptec AIC7xxx support (CONFIG_SCSI_AIC7XXX) [N/y/?] <y>
Maximum number of TCQ commands per device
(CONFIG_AIC7XXX_CMDS_PER_DEVICE) [253] (NEW) <Enter>
```

```
Initial bus reset delay in milli-seconds (CONFIG_AIC7XXX_RESET_DELAY_MS)
[15000] (NEW) <Enter>
Build Adapter Firmware with Kernel Build (CONFIG_AIC7XXX_BUILD_FIRMWARE)
[N/y/?] (NEW) <Enter>
Adaptec 120 RAID support (CONFIG_SCSI_DPT_120) [N/y/?] <Enter>
AdvanSys SCSI support (CONFIG_SCSI_ADVANSYS) [N/y/?] <Enter>
Always IN2000 SCSI support (CONFIG_SCSI_IN2000) [N/y/?] <Enter>
AM53/79C974 PCI SCSI support (CONFIG_SCSI_AM53C974) [N/y/?] <Enter>
AMI MegaRAID support (CONFIG_SCSI_MEGARAID) [N/y/?] <Enter>
BusLogic SCSI support (CONFIG_SCSI_BUSLOGIC) [N/y/?] <Enter>
Compaq Fibre Channel 64-bit/66Mhz HBA support (CONFIG_SCSI_CPQFCTS)
[N/y/?] <Enter>
DMX3191D SCSI support (CONFIG_SCSI_DMX3191D) [N/y/?] <Enter>
DTC3180/3280 SCSI support (CONFIG_SCSI_DTC3280) [N/y/?] <Enter>
EATA ISA/EISA/PCI (DPT and generic EATA/DMA-compliant boards) support
(CONFIG_SCSI_EATA) [N/y/?] <Enter>
EATA-DMA [Obsolete] (DPT, NEC, AT&T, SNI, AST, Olivetti, Alphatronix)
support (CONFIG_SCSI_EATA_DMA) [N/y/?] <Enter>
EATA-PIO (old DPT PM2001, PM2012A) support (CONFIG_SCSI_EATA_PIO) [N/y/?]
<Enter>
Future Domain 16xx SCSI/AHA-2920A support (CONFIG_SCSI_FUTURE_DOMAIN)
[N/y/?] <Enter>
Intel/ICP (former GDT SCSI Disk Array) RAID Controller support
(CONFIG_SCSI_GDTH) [N/y/?] <Enter>
Generic NCR5380/53c400 SCSI support (CONFIG_SCSI_GENERIC_NCR5380) [N/y/?]
<Enter>
IBM ServeRAID support (CONFIG_SCSI__IPS) [N/y/?] <Enter>
Initio 9100U(W) support (CONFIG_SCSI_INITIO) [N/y/?] <Enter>
Initio INI-AIOOU2W support (CONFIG_SCSI_INIAIOO) [N/y/?] <Enter>
NCR53c406a SCSI support (CONFIG_SCSI_NCR53C406A) [N/y/?] <Enter>
NCR53c7,8xx SCSI support (CONFIG_SCSI_NCR53C7xx) [N/y/?] <Enter>
 SYM53C8XX Version 2 SCSI support (CONFIG_SCSI_SYM53C8XX_2) [N/y/?] <En-
ter>
NCR53C8XX SCSI support (CONFIG_SCSI_NCR53C8XX) [N/y/?] <Enter>
SYM53C8XX SCSI support (CONFIG_SCSI_SYM53C8XX) [Y/n/?] <n>
PAS16 SCSI support (CONFIG_SCSI_PAS16) [N/y/?] <Enter>
PC12000 support (CONFIG_SCSI_PC12000) [N/y/?] <Enter>
PC12220i support (CONFIG_SCSI_PC12220l) [N/y/?] <Enter>
PS1240i support (CONFIG_SCSI_PS12401) [N/y/?] <Enter>
Qlogic FAS SCSI support (CONFIG_SCSI_QLOGIC_FAS) [N/y/?] <Enter>
Qlogic ISP SCSI support (CONFIG_SCSI_QLOGIC_ISP) [N/y/?] <Enter>
Qlogic ISP FC SCSI support (CONFIG_SCSI_QLOGIC_FC) [N/y/?] <Enter>
Qlogic QLA 1280 SCSI support (CONFIG_SCSI_QLOGIC_1280) [N/y/?] <Enter>
Seagate ST-02 and Future Domain TMC-8xx SCSI support
(CONFIG_SCSI_SEAGATE) [N/y/?] <Enter>
Simple 53c710 SCSI support (Compaq, NCR machines) (CONFIG_SCSI_SIM710)
[N/y/?] <Enter>
Symbios 53c416 SCSI support (CONFIG_SCSI_SYM53C416) [N/y/?] <Enter>
Tekram DC390(T) and Am53/79C974 SCSI support (CONFIG_SCSI_DC390T) [N/y/?]
<Enter>
Trantor T128/T128F/T228 SCSI support (CONFIG_SCSI_T128) [N/y/?] <Enter>
UltraStor 14F/34F support (CONFIG_SCSI_U14_34F) [N/y/?] <Enter>
UltraStor SCSI support (CONFIG_SCSI_ULTRASTOR) [N/y/?] <Enter>
```

Эти опции включают/выключают поддержку SCSI-контроллеров. Необходимо выбрать только один тип контроллера, соответствующий контроллеру, установленному в системе. В рассматриваемом примере используется Adaptec AIC7080.

```
*
* Fusion MPT device support
* Fusion MPT (base + SCSIHost) drivers (CONFIG_FUSION) [N/y/?] <Enter>
*
* 120 device support
* 120 support (CONFIG_120) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку архитектуры для большого числа (120) SCSI контроллеров.

```
*
* Network device support
* Network device support (CONFIG_NETDEVICES) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку сетевых карт.

```
*
* ARCnet devices
* ARCnet support (CONFIG_ARCNET) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку чипсета ARCnet.

```
Dummy net driver support (CONFIG_DUMMY) [Y/n/?] <n>
```

Использование этой опции необходимо в системах с доступом в Интернет по протоколам PPP и SLIP.При использовании VPN-соединения по протоколу PPTP также необходимо использование этой опции.

```
Bonding driver support (CONFIG BONDING) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку объединения нескольких каналов Ethernet.

```
EQL (serial line load balancing) support (CONFIG_EQUALIZER) [N/y/?] <En-
ter>
```

Эта опция, по аналогии с предыдущей, включает/выключает поддержку нескольких модемных каналов.

```
Universal TUN/TAP device driver support (CONFIG_TUN) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку виртуального устройства, обеспечивающего обмен сетевыми пакетами между пользовательскими программами.

```
*
* Ethernet (10 or 100Mbit)
* Ethernet (10 or 100Mbit) (CONFIG_NET_ETHERNET) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку сетевых карт. Если более точно, позволяет включить в ядро только те фрагменты кода, которые непосредственно отвечают за поддержку сетевых карт, используемых в рассматриваемой системе.

```
Sun Happy Meal 10/IOObaseT support (CONFIG_HAPPYMEAL) [N/y/?] <Enter>
Sun GEM support (CONFIG_SUNGEM) [N/y/?] <Enter>
3COM cards (CONFIG_NET_VENDOR_3COM) [N/y/?] <Enter>
AMD LANCE and PCnet (AT1500 and NE2100) support (CONFIG_LANCE) [N/y/?]
<Enter>
Western Digital/SMC cards (CONFIG_NET_VENDOR_SMC) [N/y/?] <Enter>
Racal-interlan (Micom) Nl cards (CONFIG_NET_VENDOR_RACAL) [N/y/?] <Enter>
DEPCA, DElOx, DE200, DE201, DE202, DE422 support (CONFIG_DEPCA) [N/y/?]
<Enter>
HP 10/IOOVG PCLAN (ISA, EISA, PCI) support (CONFIG_HPIOO) [N/y/?] <Enter>
Other ISA cards (CONFIG_NET_ISA) [N/y/?] <Enter>
EISA, VLB, PCI and on board controllers (CONFIG_NET_PCI) [Y/n/?] <Enter>
AMD PCnet32 PCI support (CONFIG_PCNET32) [N/y/?] <Enter>
Apricot Xen-II on board Ethernet (CONFIG_APRICOT) [N/y/?] <Enter>
CS89xO support (CONFIG_CS89xO) [N/y/?] <Enter>
DECchip Tulip (dc21x4x) PCI support (CONFIG_TULIP) [N/y/?] <Enter>
Generic DECchip & DIGITAL EtherWORKS PCI/EISA (CONFIG_DE4X5) [N/y/?] <En-
ter>
Digi Intl. RightSwitch SE-X support (CONFIG_DGRS) [N/y/?] <Enter>
Davicom DM910x/DM980x support (CONFIG_DM9102) [N/y/?] <Enter>
EtherExpressPro/100 support (CONFIG_EEPROIOO) [Y/n/?] <Enter>
Myson MTD-8xx PCI Ethernet support (CONFIG_FEALNX) [N/y/?] <Enter>
National Semiconductor DP8381x series PCI Ethernet support
(CONFIG_NATSEMI) [N/y/?] <Enter>
PCI NE2000 and clones support (see help) (CONFIG_NE2K_PCI) [N/y/?] <En-
ter>
RealTek RTL-8139 PCI Fast Ethernet Adapter support (CONFIG_8139TOO)
[N/y/?] <Enter>
SiS 900/7016 PCI Fast Ethernet Adapter support (CONFIG_SIS900) [N/y/?]
<Enter>
SMC EtherPower II (CONFIG_EPICIOO) [N/y/?] <Enter>
```

```
Sundance Alta support (CONFIG_SUNDANCE) [N/y/?] <Enter>
TI ThunderLAN support (CONFIG_TLAN) [N/y/?] <Enter>
VIA Rhine support (CONFIG_VIA_RHINE) [N/y/?] <Enter>
Winbond W89c840 Ethernet support (CONFIG_WINBOND_840) [N/y/?] <Enter>
Pocket and portable adapters (CONFIG_NET_POCKET) [N/y/?] <Enter>
* Ethernet (1000 Mbit)
* Alteon AceNIC/3Com 3C985/NetGear GA620 Gigabit support (CONFIG_ACENIC)
[N/y/?] <Enter>
D-Link DL2000-based Gigabit Ethernet support (CONFIG_DL2K) [N/y/?] <En-
ter>
National Semiconduct DP83820 support (CONFIG_NS83820) [N/y/?] <Enter>
Packet Engines Hamachi GNIC-II support (CONFIG_HAMACHI) [N/y/?] <Enter>
SysKonnect SK-98xx support (CONFIG_SK98LIN) [N/y/?] <Enter>
```

С использованием приведенной опции включается поддержка сетевой карты "EtherExpressPro/100", используемой в рассматриваемой системе.

```
FDDI driver support (CONFIG_FDDI) [N/y/?] <Enter>
```

Эта опция включает поддержку карт FDDI (интерфейс передачи данных по оптико-волоконным линиям связи).

```
PPP (point-to-point protocol) support (CONFIG_PPP) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку протокола PPP. При использовании для подключения к Интернет VPN-соединения по протоколу PPTP также необходимо использование этой опции.

```
SLIP (serial line) support (CONFIG_SLIP) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку протоколов SLIP и CSLIP.

```
*
* Wireless LAN (non-hamradio)
* Wireless LAN (non-hamradio) (CONFIG_NET_RADIO) [N/y/?] <Enter>
```

Эта опция включает поддержку беспроводных локальных сетей.

```
*
* Token Ring devices
* Token Ring driver support (CONFIG_TR) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку "Token Ring" – способа организации связи между компьютерами сети, предложенного и иногда используемого компанией IBM.

```
Fibre Channel driver support (CONFIG_NET_FC) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку специальных волоконно-оптических каналов, предназначенных для связи внешних запоминающих устройств с компьютером.

```
*
* Wan interfaces
* Wan interfaces support (CONFIG_WAN) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку Wan-интерфейса, предназначенного для объединения систем, находящихся на больших расстояниях, в локальную сеть.

```
*
* Amateur Radio support
* Amateur Radio support (CONFIGJHAMRADIO) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку Web-радио.

```
*
* lrDA (infrared) support
* lrDA subsystem support (CONFIG_IRDA) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку инфракрасного порта.

```
*
* ISDN subsystem
* ISDN support (CONFIG_ISDN) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку ISDN – цифровой сети, предоставляющей доступ к Интернет и сервисам цифровой телефонии.

```
* Old CD-ROM drivers (not SCSI, not IDE)
* Support non-SCSI/IDE/ATAPI CDROM drives (CONFIG_CD_NO_IDESCSI) [N/y/?]
<Enter>
```

Эта опция включает/выключает поддержку устаревших приводов CD-ROM.

```
*
* Input core support
* Input core support (CONFIG_INPUT) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку USB-устройств.

```
*
* Character devices
* Virtual terminal (CONFIG_VT) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку оконечных устройств с клавиатурой и дисплеем.

```
Support for console on virtual terminal (CONFIG_VT_CONSOLE) [Y/n/?] <En-
ter>
```

Эта опция включает/выключает поддержку клавиатур на виртуальных консолях.

```
Standard/generic (8250/16550 and compatible UARTs) serial support
(CONFIG_SERIAL) [Y/n/?] n
```

Эта опция включает/выключает поддержку мыши, модемов и других устройств, подключаемых через последовательный порт.

```
Non-standard serial port support (CONFIG_SERIAL_NONSTANDARD) [N/y/?] <En-
ter>
```

Эта опция включает/выключает поддержку нестандартных последовательных портов.

```
Unix98 PTY support (CONFIGJJNIX98_PTYS) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку псевдоконсолей.

```
Maximum number of Unix98 PTYs in use (0-2048) (CONFIG_UNIX98_PTY_COUNT)
[256] 128
```

Эта опция позволяет устанавливать максимальное число виртуальных консолей с целью увеличения производительности. В примере уменьшается до 128.

```
*
* I2C support
* I2C support (CONFIG_I2C) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку протоколов последовательной шины I2C и SMBus.

```
Bus Mouse Support (CONFIG_BUSMOUSE) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку bus-мыши.

```
Mouse Support (not serial and bus mice) (CONFIG_MOUSE) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку мыши, отличной от последовательной или bus-мыши, например, PS/2.

```
PS/2 mouse (aka "auxiliary device") support (CONFIG_PSMOUSE) [Y/n/?] <En-
ter>
```

Эта опция включает/выключает поддержку мыши PS/2.

```
C&T 82C710 mouse port support (as on TI Travelmate)
(CONFIG__82C710_MOUSE) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку некоторых видов мыши PS/2, используемых на TI Travelmate.

```
PCIIO digitizer pad support (CONFIG_PCIIO_PAD) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку управления клавиатурой цифрового преобразователя на IBM PCIIO palmtop. С помощью этой опции можно настроить клавиатуру цифрового преобразователя для эмуляции мыши PS/2 или обычной клавиатуры.

```
QIC-02 tape support (CONFIG_QIC02_TAPE) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку накопителя на магнитной ленте QIC-02.

```
*
* Watchdog Cards
* Watchdog Timer Support (CONFIG_WATCHDOG) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку Watchdog Timer для Linux (см. файл `Documentation/watchdog.txt` в исходном коде ядра).

```
Intel i8x0 Random Number Generator support (CONFIG_INTEL_RNG) [N/y/?]
<Enter>
```

Эта опция включает/выключает поддержку драйвера встроенного в некоторые материнские платы (Intel i8xx) генератора случайных чисел.

```
/dev/nvram support (CONFIG_NVRAM) [N/y/?] <Enter>
```

Эта опция позволяет получить доступ чтения-записи к 50 байтам энергонезависимой памяти в часах реального времени (RTC).

ЗАМЕЧАНИЕ Если установка Linux осуществляется на многопроцессорной системе, и на вопрос "`Symmetric Multi Processing`" был дан утвердительный ответ, здесь также необходимо дать утвердительный ответ.

```
Double Talk PC internal speech card support (CONFIG_DTLK) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку DoubleTalk PC для Linux.

```
Siemens R3964 line discipline (CONFIG_R3964) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку синхронной передачи данных устройствами, используя протокол Siemens R3964.

```
Applicom intelligent fieldbus card support (CONFIG_APPLICOM) [N/y/?] <En-
ter>
```

Эта опция включает/выключает поддержку плат fieldbus производства Applicom International.

```
*
* ftape, the floppy tape device driver
* Ftape (QIC-80/Travan) support (CONFIG_FTAPE) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку некоторых хорошо известных накопителей на магнитной ленте. В последующем необходимо будет выбрать соответствующий накопитель из предложенного списка.

```
/dev/agpgart (AGP Support) (CONFIG_AGP) [Y/n/?] <n>
```

Эта опция включает/выключает поддержку AGP для оптимизации работы XFree86.

```
Direct Rendering Manager (XFree86 4.1.0 and higher DRI support) (CONFIG
DRM) [Y/n/?] <n>
```

Эта опция непосредственно связана с оптимизацией использования XFree86 и графического интерфейса.

```
ACP Modem (Mwave) support (CONFIG_MWAVE) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку WinModem.

```
*
* Multimedia devices
* Video For Linux (CONFIG_VIDEO_DEV) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку специализированных видеокарт.

```
* File systems
* Quota support (CONFIG_QUOTA) [N/y/?] <y>
```

Эта опция включает/выключает поддержку ограничений на использование дискового пространства пользователями системы.

```
Kernel automounter support (CONFIG_AUTOFS_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку устаревшей версии программы automounter, предназначенной для автоматического монтирования файловых систем на удаленных компьютерах.

```
Kernel automounter version 4 support (also supports v3) (CONFIG_AUTOFS4
FS) [Y/n/?] <n>
```

Эта опция включает/выключает поддержку обновленной версии automounter.

```
Ext3 journalling file system support (EXPERIMENTAL) (CONFIG_EXT3_FS)
[N/y/?] <y>
```

Эта опция включает/выключает поддержку журнализируемой файловой системы Ext3.

```
JBD (ext3) debugging support (CONFIG_JBD_DEBUG) [N/y/?] <y>
```

Эта опция включает/выключает поддержку вывода отладочных сообщений, касающихся работы файловой системы Ext3.

```
DOS FAT fs support (CONFIG_FAT_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку FAT-подобных файловых систем (MS DOS, VFAT (Windows 95) и UMSDOS).

```
Compressed ROM file system support (CONFIG_CRAMFS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы CramFs, используемой на встраиваемых системах.

```
Virtual memory file system support (former shm fs) (CONFIG_TMPFS) [Y/n/?]
<Enter>
```

Эта опция включает/выключает поддержку файловой системы Tmpfs. Tmpfs - файловая система, предназначенная для сохранения файлов в виртуальной памяти.

```
Simple RAM-based file system support (CONFIG_RAMFS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы Ramfs. Ramfs – система, предназначенная для хранения в оперативной памяти файлов.

```
ISO 9660 CDROM file system support (CONFIG_IS09660_FS) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы IS09660, используемой на компакт-дисках.

```
Microsoft Joliet CDROM extensions (CONFIG_JOLLET) [N/y?] <Enter>
```

Эта опция включает/выключает т поддержку расширения Microsoft для файловой системы ISO 9660 CD-ROM -Joliet, которая понимает длинные имена файлов в формате Unicode.

```
Transparent decompression extension (CONFIG_ZISOFS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку специфического расширения к RockRidge, которое позволяет осуществлять сжатие и распаковку данных при чтении и записи на компакт-диски.

```
Minix fs support (CONFIG_MINIX_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку устаревшей файловой системы Minix fs.

```
FreeVxFS file system support (VERITAS VxFS(TM) compatible)
(CONFIG_VXFS_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает драйвер FreeVxFS, который поддерживает формат файловой системы Veritas vxfs (tm), используемой в Sunsoft Solaris, HEWLETT-PACKARD-UX.

```
NTFS file system support (read only) (CONFIG_NTFS_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы NTFS, используемой в Microsoft Windows NT.

```
OS/2 HPFS file system support (CONFIG_HPFS_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы OS/2.

```
/proc file system support (CONFIG_PROC_FS) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку виртуальной файловой системы `/proc`, используемой для отображения информации о состоянии системы и изменения ее некоторых параметров.

```
/dev/pts file system for Unix98 PTYs (CONFIG_DEVPTS_FS) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку виртуальной файловой системы `/dev/pts`, используемой многими программами.

```
ROM file system support (CONFIG_ROMFS_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы ROM. Включение этой опции необходимо, если используется модульное ядро на системе со SCSI-устройствами.

```
Second extended fs support (CONFIG_EXT2_FS) [Y/n/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы Ext2, являющейся стандартом для Linux.

```
System V/Xenix/V7/Coherent file system support (config_sysv_fs) [N/y/?]
<Enter>
```

Эта опция включает/выключает поддержку коммерческих файловых систем SCO, Xenix и Coherent.

```
UDF file system support (read only) (CONFIG_UDF_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы UDF, используемой на некоторых CD-ROM и видеодисках DVD.

```
UFS file system support (read only) (CONFIG_UFS_FS) [N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы UFS, используемую в SunOS, FreeBSD, NetBSD, OpenBSD и NeXTStep.

```
*
* Network File Systems
* Coda file system support (advanced network fs) (CONFIG_CODA_FS) [N/y/?]
<Enter>
```

Эта опция включает/выключает поддержку сетевой файловой системы Coda, которая, подобно NFS, позволяет монтировать файловые системы на удаленных компьютерах.

```
NFS file system support (CONFIG_NFS_FS) [Y/n/?] <n>
```

Эта опция включает/выключает поддержку файловой системы NFS, позволяющей монтировать файловые системы на удаленном компьютерах.

```
NFS server support (CONFIG_NFSD) [Y/n/?] n
```

Эта опция включает/выключает поддержку сервера NFS.

```
SMB file system support (to mount Windows shares etc.) (CONFIG_SMB FS)
[N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы SMB, используемой для монтирования файловых систем удаленных компьютеров с операционными системами Windows 95/98, Windows NT, 2000, XP.

```
NCP file system support (to mount NetWare volumes) (CONFIG_NCP_FS)
[N/y/?] <Enter>
```

Эта опция включает/выключает поддержку файловой системы NCP, используемой для монтирования томов файлового сервера `Novell NetWare.`

```
*
* Partition Types
* Advanced partition selection (CONFIG_PARTITION_ADVANCED) [N/y/?]
<Enter>
```

Эта опция позволяет выбрать типы локальных файловых систем других операционных систем, используемых на рассматриваемом компьютере.

```
*
* Console drivers
VGA text console (CONFIG_VGA_CONSOLE) [Y/n/?] <Enter>
```

Эта опция включает поддержку текстового режима SVGA.

```
Video mode selection support (CONFIG_VIDEO_SELECT) [N/y/?] <Enter>
```

Эта опция не используется в текстовом режиме SVGA (см. файл `Documentation/svga.txt`).

```
*
* Sound
* Sound card support (CONFIG_SOUND) [Y/n/?] <n>
```

Эта опция позволяет выбрать тип поддерживаемой звуковой карты.

```
*
* USB support
```

Support for USB (CONFIG_USB) [Y/n/?] **<n>**
Эта опция включает/выключает поддержку USB.

```
*
* Kernel hacking
* Kernel debugging (CONFIG_DEBUG_KERNEL) [N/y/?] <Enter>
```
Эта опция используется только разработчиками ядра при его тестировании и отладке.

```
*
* Grsecurity
*
```
Этот раздел появляется только, если к исходным кодам ядра был применен патч Grsecurity, и позволяет осуществить настройки, связанные с обеспечением безопасности ядра.

```
Grsecurity (CONFIG_GRKERNSEC) [N/y/?] <y>
```
Эта опция включает поддержку патча Grsecurity.

```
Security level (Low, Medium, High, Customized) [Customized] <Enter>
```
Эта опция позволяет выбрать требуемый вариант конфигурации Grsecurity.

```
*
* Buffer Overflow Protection
*
Openwall non-executable stack (CONFIG_GRKERNSEC_STACK) [N/y/?] <y>
```
Включение этой опции запрещает выполнение кода в стеке, делая переполнение буфера невозможным.

```
Gcc trampoline support (CONFIG_GRKERNSEC_STACK_GCC) [N/y/?] <Enter>
```
Отключение этой опции не позволяет держать в стеке исполняемый код.

```
Read-only kernel memory (CONFIG_GRKERNSEC_KMEM) [N/y/?] <y>
```
Включение этой опции разрешает доступ к памяти ядра в режиме «только чтение". В сочетании с использованием ядра с монолитной архитектурой это полностью (даже для хакера, получившего права доступа `root`) исключает возможность модификации кода ядра.

```
*
* Access Control Lists
*
Grsecurity ACL system (CONFIG_GRKERNSEC_ACL) [N/y/?] <y>
```
Эта опция включает/отключает поддержку списка контроля доступа (ACL) для Grsecurity, определяющего, кому и какие действия разрешены в защищаемой системе.

```
ACL Debugging Messages (CONFIG_GR_DEBUG) [N/y/?] <y>
```
Включение этой опции разрешает вывод отладочных сообщений об ошибках в конфигурации ACL.

```
Extra ACL Debugging Messages (CONFIG_GR_SUPERDEBUG) [N/y/?] <Enter>
```
Включение этой опции разрешает вывод дополнительных отладочных сообщений об ошибках в конфигурации списков ACL.

```
Denied capability logging (CONFIG_GRKERNSEC_ACL_CAPLOG) [N/y/?] <y>
```
Включение этой опции разрешает запись в файлы регистрации отклоненной возможности, это очень полезно при отладке конфигураций списков ACL.

```
Path to gradm (CONFIG_GRADM_PATH) [/sbin/gradm] <Enter>
```
Эта опция Grsecurity задает путь к установленныv исполняемым файлам программы gradm, используемой для управления Grsecurity ACL. Установка gradm описана ниже.

```
Maximum tries before password lockout (CONFIG_GR_MAXTRIES) [3] 2
```
Эта опция определяет максимальное количество попыток авторизации пользователя перед временной блокировкой доступа.

```
Time to wait after max password tries, in seconds (CONFIG GR TIMEOUT)
[30] <Enter>
```

Эта опция определяет продолжительность паузы, в течение которой пользователь должен ждать доступа к ACL, после введения определенного выше числа недопустимых паролей.

```
*
* Pilesysfcem Protections
*
Proc restrictions (CONFIG_GRKERNSEC_PROC) [N/y/?] <y>
```

Эта опция ограничивает права доступа к файловой системе `/proc`.

```
Restrict to user only (CONFIG_GRKERNSEC_PROC_USER) [N/y/?] <y>
```

Эта опция Grsecurity ограничивает права непривилегированных пользователей. При ее включении пользователи смогут выполнять только свои собственные процессы, не имея доступа к информации о сети, модулях, версии ядра и т. п.

```
Additional restrictions (CONFIG_GRKERNSEC_PROC_ADD) [N/y/?] <y>
```

Эта опция включает/отключает поддержку дополнительных ограничений на доступ к файловой системе `/proc`, препятствующих просмотру обычными пользователями сведений об устройствах и центральном процессоре.

```
Linking restrictions (CONFIG_GRKERNSEC_LINK) [N/y/?] <y>
```

Эта опция включает/отключает поддержку запрета использования символьных ссылок, принадлежащих другим пользователям.

```
FIFO restrictions (CONFIG_GRKERNSEC_FIFO) [N/y/?] <y>
```

Эта опция Grsecurity позволяет разрешить защиту ограничений FIFO на системе.

```
Secure file descriptors (CONFIG_GRKERNSEC_FD) [N/y/?] <y>
```

Эта опция включает/отключает поддержку использования дескрипторов безопасности исполняемых файлов и повышает стойкость системы к хакерским атакам, основанным на подмене данных в сетевых пакетах (data spoofing atack).

```
Chroot-jail restrictions (CONFIG_GRKERNSEC_CHROOT) [N/y/?] <y>
```

Эта опция включает/отключает поддержку выбора дополнительных опций, усложняющих взлом окружения chroot-jail.

```
Restricted signals (CONFIG_GRKERNSEC_CHROOT_SIG) [N/y/?] <y>
```

Эта опция включает/отключает поддержку запрета на отправку сигналов от процессов, работающих в окружении chroot-jail за его пределы.

```
Deny mounts (CONFIG_GRKERNSEC_CHROOT_MOUNT) [N/y/?] <y>
```

Эта опция включает/отключает поддержку запрета на монтирование файловых систем внутри окружения chroot-jail.

```
Deny double-chroots (CONFIG_GRKERNSEC_CHROOT_DOUBLE) [N/y/?] <y>
```

Эта опция включает/отключает поддержку запрета на повторное использование команды chroot процессами, работающими в среде chroot.

```
Enforce chdir("/") on all chroots (CONFIG_GRKERNSEC_CHROOT_CHDIR) [N/y/?]
<y>
```

Эта опция позволяет установить корневой каталог среды chroot в качестве рабочего каталога всех вновь запускаемых приложений в среде chroot.

```
Deny (f)chmod +s (CONFIG_GRKERNSEC_CHROOT_CHMOD) [N/y/?] <y>
```

Эта опция позволяет установить запрет на обращение процессов, работающих в среде chroot, к командам `chmod` или `fchmod`. Эти команды нужны для установки SUID или SGID-битов в правах доступа к файлам.

```
Deny mknod (CONFIG_GRKERNSEC_CHROOT_MKNOD) [N/y/?] <y>
```

Эта опция позволяет установить запрет на создание устройств процессами, работающими в среде chroot.

```
Deny ptraces (CONFIG_GRKERNSEC_CHROOT_PTRACE) [N/y/?] <y>
```

Эта опция Grsecurity позволяет разрешить защиту ptraces на системе. Если вы отвечаете здесь "y", процессы внутри chroot не смогут обратиться к ptrace других процессов.

```
Restrict priority changes (CONFIG_GRKERNSEC_CHROOT_NICE) [N/y/?] <y>
```

Эта опция позволяет установить запрет на изменение приоритетов процессов. При этом процессы, работающие внутри chroot, не смогут поднять приоритет процессов в среде chroot или изменить приоритет процессов вне chroot.

```
Capability restrictions within chroot (CONFIG_GRKERNSEC_CHROOT_CAPS)
[N/y/?] <Enter>
```

Включение этой опции сделает невозможным запуск ряда широко используемых приложений.

```
Secure keymap loading (CONFIG_GRKERNSEC_KBMAP) [N/y/?] <y>
```

Эта опция позволяет установить запрет на изменение раскладки консоли непривилегированными пользователями.

```
*
*
* Kernel Auditing
*
Single group for auditing (CONFIG_GRKERNSEC_AUDIT_GROUP) [N/y/?] <Enter>
Exec logging (CONFIG_GRKERNSEC_EXECLOG) [N/y/?] <Enter>
Log execs within chroot (CONFIG_GRKERNSEC_CHROOT_EXECLOG) [N/y/?] <y>
Chdir logging (CONFIG_GRKERNSEC_AUDIT_CHDIR) [N/y/?] <Enter>
(Un) Mount logging (CONFIG_GRKERNSEC_AUDIT_MOUNT) [N/y/?] <Enter>
IPC logging (CONFIG_GRKERNSEC_AUDIT_]:PC) [N/y/?] <y>
Ptrace logging (CONFIG_GRKERNSEC_AUDIT_PTRACE) [N/y/?] <y>
 Signal logging (CONFIG_GRKERNSEC_SIGNAL) [N/y/?] <y>
Fork failure logging (CONFIG_GRKERNSEC_FORKFAIL) [N/y/?] <y>
Set*id logging (CONFIG_GRKERNSEC_SUID) [N/y/?] <Enter>
Log set*ids to root (CONFIG_GRKERNSEC_SUID_ROOT) [N/y/?] <y>
Time change logging (CONFIG_GRKERNSEC_TIME) [N/y/?] <y>
```

Эти опции позволяют установить разумный компромисс между объемом и информативностью файлов регистрации, создаваемых системой.

```
*
* Executable Protections
*
Exec process limiting (CONFIG_GRKERNSEC_EXECVE) [N/y/?] <y>
```

Эта опция позволяет установить ограничения на использование ресурсов для определенной группы пользователей.

```
Dmesg(8) restriction (CONFIG_GRKERNSEC_DMESG) [N/y/?] <y>
```

Эта опция позволяет установить запрет на просмотр непривилегированными пользователями последних 4 кБайт сообщений в буфере регистрационного файла ядра.

```
Randomized PIDs (CONFIG_GRKERNSEC_RANDPID) [N/y/?] <y>
```

Эта опция включает поддержку псевдослучайных значений идентификаторов процессов, что затрудняет прогнозирование хакерами указанных значений для демонов, функционирующих в системе.

```
Altered default IPC permissions (CONFIG_GRKERNSEC_IPC) [N/y/?] <Enter>
```

Эта опция нарушает работу популярных приложений, например, сервера Apache.

```
Limit uid/gid changes to root (CONFIG_GRKERNSEC_TTYROOT) [N/y/?] <y>
```

Эта опция ограничивает доступ непривилегированных пользователей к учетной записи суперпользователя `root`.

```
Deny physical consoles (tty) (CONFIG_GRKERNSEC_TTYROOT_PHYS) [N/y/?] <En-
ter>
```

Эта опция позволяет установить запрет доступа суперпользователя `root` с физических консолей.

```
Deny serial consoles (ttyS) (CONFIG_GRKERNSEC_TTYROOT_SERIAL) [N/y/?] <y>
```

Эта опция позволяет установить запрет доступа суперпользователя `root` с консолей `ttyS`. В настоящее время этот вариант доступа к системе практически не используется.

```
Deny pseudo consoles (pty) (CONFIG_GRKERNSEC_TTYROOT_PSEUDO) [N/y/?] <En-
ter>
```

Эта опция позволяет установить запрет доступа суперпользователя `root` с псевдоконсолей (`pty`) в системе. Это необходимо для удаленного администрирования системы, например, с использованием SSH.

```
Fork-bomb protection (CONFIG_GRKERNSEC_FORKBOMB) [N/y/?] <y>
```

Эта опция Grsecurity позволяет выбрать различные варианты защиты системы от атак, основанных на инициализации ветвления процессов.

```
GID for restricted users (CONFIG_GRKERNSEC_FORKBOMB_GID) [1006] <Enter>
```

Эта опция устанавливает значения идентификатора группы пользователей ("не доверенной группы"), для которой вводятся ниже рассматриваемые ограничения. Значение 1006 задается по умолчанию.

```
Forks allowed per second (CONFIG_GRKERNSEC_FORKBOMB_SEC) [40] <Enter>
```

Эта опция задает максимально допустимое количество ветвлений пользовательского процесса в секунду.

```
Maximum processes allowed (CONFIG_GRKERNSEC_FORKBOMB_MAX) [20] 33
```

Здесь задается максимальное число процессов, которое может быть запущено пользователем из "не доверенной группы".

ЗАМЕЧАНИЕ Введенное здесь значение максимального количества процессов должно совпадать со значением в файле `/etc/security/limit.conf`.

```
Trusted path execution (CONFIG_GRKERNSEC_TPE) [N/y/?] <y>
```

Эта опция позволяет ввести дополнительные ограничения на путь к программам, которые могут выполнять пользователи из "не доверенной группы". Далее необходимо ввести идентификатор группы.

```
Glibc protection (CONFIG_GRKERNSEC_TPE_GLIBC) [N/y/?] <y>
```

Эта опция позволяет ограничить доступ пользователей из "не доверенной группы" к библиотекам glibc.

```
Partially restrict non-root users (CONFIG_GRKERNSEC_TPE_ALL) [N/y/?] <y>
```

Эта опция разрешает обычным, не входящих в группу GID (см. ниже), пользователям выполнять файлы только в принадлежащих им каталогах.

```
GID for untrusted users: (CONFIG_GRKERNSEC_TPE_GID) [1005] <Enter>
```

Эта опция задает GID группы, к которой не применяются описанные выше три ограничения.

```
Restricted ptrace (CONFIG_GRKERNSEC_PTRACE) [N/y/?] <y>
```

Эта опция позволяет разрешить запуск ptrace только суперпользователю `root`.

```
Allow ptrace for group (CONFIG_GRKERNSEC_PTRACE_GROUP) [N/y/?] <Enter>
```

Эта опция позволяет разрешить запуск программы ptrace пользователям группы с GID=[1005] или другой указанной группы.

```
*
*Network Protecions
*
Randomized IP IDs (CONFIG_GRKERNSEC_RANDID) [N/y/?] <y>
Randomized TCP source ports (CONFIG_GRKERNSEC_RANDSRC) [N/y/?] <y>
Randomized RPC XIDs (CONFIG_GRKERNSEC_RANDRPC) [N/y/?] <y>
Altered Ping IDs (CONFIG_GRKERNSEC_RANDPING) [N/y/?] <y>
Randomized TTL (CONFIG_GRKERNSEC_RANDTTL) [N/y/?] <y>
```

Эти опции включают/отключают поддержку выбора соответствующих числовых параметров, используемых системой, по случайному закону, что затрудняет прогнозирование поведения системы при попытке ее взлома.

```
Socket restrictions (CONFIG_GRKERNSEC_SOCKET) [N/y/?] <y>
```

Эта опция включает/отключает поддержку сетевых соединений, устанавливаемых системой. Необходимо выбрать один из трех доступных способов введения ограничений на сетевые соединения.

```
Deny any sockets to group (CONFIG_GRKERNSEC_SOCKET_ALL) [N/y/?] <y>
GID to deny all sockets for: (CONFIG_GRKERNSEC_SOCKET_ALI_GID) [1004]
<Enter>
```

Эта опция позволяет запретить установку сетевых соединений и запуск серверных приложений с рассматриваемой системы для группы пользователей со значением GID=1004 (задано по умолчанию).

```
Deny client sockets to group (CONFIG_GRKERNSEC_SOCKET_CLIENT) [N/y/?]
<Enter>
```

Эта опция позволяют запретить установку сетевых соединений системы для определенной группы пользователей.

```
Deny server sockets to group (CONFIG_GRKERNSEC_SOCKET_SERVER) [N/y/?]
<Enter>
```

Эта опция позволяет запретить запуск с системы серверных приложений для определенной группы пользователей.

```
*
*Sysctl support
*
Sysctl support (CONFIG_GRKERNSEC_SYSCTL) [N/y/?] <Enter>
```

Эта опция позволяет разрешить изменения параметров настройки Grsecurity без перекомпиляции ядра путем модификации файла `/proc/sys/kernel/grsecurity`.

```
*
* Miscellaneous Features
*
Seconds in between log messages (minimum) (CONFIG GRKERNSEC FLOODTIME)
[30] <Enter>
```

Эта опция определяет минимальный интервал времени между сообщениями в файл журнала.

```
BSD-style coredumps (CONFIG_GRKERNSEC_COREDUMP) [N/y/?] <y>
```

Эта опция не влияет на безопасность системы, а только позволяет использовать более удобный, на наш взгляд, BSD-стиль для отображения сообщений coredumps.

```
*** End of Linux kernel configuration.
*** Check the top-level Makefile for additional configuration.
*** Next, you must run 'make dep'
```

Конфигурация ядра с модульной архитектурой

Осуществим конфигурирование ядра с модульной архитектурой для следующей системы:

- процессор Pentium-III 600 МГЦ (i686);
- системная плата Asus P3V4XPro 133Mhz EIDE;
- жесткий диск Ultra ATA/100 EIDE;
- микросхемы Apollo Pro 133A;
- CD-ROM ATAPI IDE;
- дисковод для гибкого диска;
- Сетевые карты 3COM 3c597 PCI 10/100;
- мышь PS/2.

С этой целью выполните следующие действия:

```
[root@drwalbr /]# cd /usr/src/linux-2.4.x/
[root@drwalbr linux-2.4.x]# make config
rm -f include/asm
( cd include ; In -sf asm-i386 asm) /bin/sh scripts/Configure
arch/i386/config.in
…
#
#Using defaults found in arch/1386/defconfig
#
*
*Code maturity level options
*
Prompt for development and/or incomplete code/drivers
(CONFIG_EXPERIMENTAL) [N/y/?] <Enter>
*
*Loadable nodule support:
```

```
*
Enable loadable module support (CONFIG_MODULES) [Y/n/?] <Enter>
Set version information on all module symbols (CONFIG_MODVERSIONS)
[Y/n/?] <n>
Kernel module loader (CONFIG_KMOD) [Y/n/?] <Enter>
* Processor type and features
*
Processor family (386, 486, 586/K5/5x86/6x86/6x86MX, Pentium-Classic,
Pentium-MMX, Pentium-Pro/Celeron/Pentium-II, Pentium-
III/Celeron(Coppermine), Pentium-4, K6/K6-11/K6-III, Athlon/Duron/K7,
Elan, Crusoe, Winchip-06, Winchip-2, Winchip-2A/Winchip-3, CyrixIII/C3)
[Pentium-III/Celeron(Coppermine)] <Enter>
Toshiba Laptop support (CONFIG_TOSHIBA) [N/y/m/?] <Enter>
Dell laptop support (CONFIG_18K) [N/y/m/?] <Enter>
/dev/cpu/microcode - Intel IA32 CPU microcode support (CONFIG_MICROCODE)
[N/y/m/?] <m>
/dev/cpu/*/msr - Model-specific register support (CONFIG_X86_MSR)
[N/y/m/?] <m>
/dev/cpu/*/cpuid - CPU information support (CONFIG_X86_CPUID) [N/y/m/?]
<m>
High Memory Support (off, 4GB, 64GB) [off] <Enter>
Math emulation (CONFIG_MRTH_EMULATION) [N/y/?] <Enter>
MTRR (Memory Type Range Register) support (CONFIG_MTRR) [N/y/?] <Enter>
Symmetric multi-processing support (CONFIG_SMP) [Y/n/?] <n>
Local APIC support on uniprocessors (CONFIG_X86_UP_APIC) [N/y/?] (NEW)
<y>
IO-APIC support on uniprocessors (CONFIG_X86_UP_IOAPIC) [N/y/?] (NEW) <y>
*
* General setup
*
Networking support (CONFIG_NET) [Y/n/?] <Enter>
PCI support (CONFIG_PCI) [Y/n/?] <Enter>
PCI access mode (BIOS, Direct, Any) [Any] <Enter>
PCI device name database (CONFIG_PCI_NAMES) [Y/n/?] <n>
EISA support (CONFIG_EISA) [N/y/?] <Enter>
MCA support (CONFIG_MCA) [N/y/?] <Enter>
Support for hot-pluggable devices (CONFIG_HOTPLUG) [Y/n/?] <n>System V
IPC (CONFIG_SYSVIPC) [Y/n/?] <Enter>
BSD Process Accounting (CONFIG_BSD_PROCESS_ACCT) [N/y/?]
<Enter>
Sysctl support (CONFIG_SYSCTL) [Y/n/?] <Enter>
Kernel core (/proc/kcore) format (ELF, A.OUT) [ELF] <Enter>
Kernel support for a.out binaries (CONFIG_BINFMT_AOUT) [Y/m/n/?] <n>
Kernel support for ELF binaries (CONFIG_BINFMT_ELF) [Y/m/n/?] <Enter>
Kernel support for MISC binaries (CONFIG_BINFMT_MISC) [Y/m/n/?] <m>
Power Management support (CONFIG_PM) [Y/n/?] <n>
*
* Memory Technology Devices (MTD)
*
Memory Technology Device (MTD) support (CONFIG_MTD) [N/y/m/?] <Enter>
*
* Parallel port support
*
Parallel port support (CONFIG_PARPORT) [N/y/m/?] <Enter>
*
* Plug and Play configuration
*
Plug and Play support (CONFIG_PNP) [Y/m/n/?] <n>
*
* Block devices
*
Normal PC floppy disk support (CONFIG_BLK_DEV_FD) [Y/m/n/?] <Enter>
XT hard disk support (CONFIG_BLK_DEV_XD) [N/y/m/?] <Enter>
Compaq SMART2 support (CONFIG_BLK_CPQ_DA) [N/y/m/?] <Enter>
```

```
Compaq Smart Array 5xxx support (CONFIG_BLK_CPQ_CISS_DA) [N/y/m/?] <En-
ter>
Mylex DAC960/DACIIOO PCI RAID Controller support (CONFIG_BLK_DEV_DAC960)
[N/y/m/?] <Enter>
Loopback device support (CONFIG_BLK_DEV_LOOP) [N/y/m/?] <Enter>
Network block device support (CONFIG_BLK_DEV_NBD) [N/y/m/?] <Enter>
RAM disk support (CONFIG_BLK_DEV_RAM) [N/y/m/?] <Enter>
*
* Multi-device support (RAID and LVM)
*
Multiple devices driver support (RAID and LVM) (CONFIG_MD) [N/y/?] <En-
ter>
*
* Networking options
*
Packet socket (CONFIG_PACKET) [Y/m/n/?] <Enter>
Packet socket: mmapped 10 (CONFIG_PACKET_MMAP) [N/y/?] <y>
Netlink device emulation (CONFIG_NETLINK_DEV) [N/y/m/?] (NEW) <m>
Network packet filtering (replaces ipchains) (CONFIG_NETFILTER) [N/y/?]
<y>
Network packet filtering debugging (CONFIG_NETFILTER_DEBUG) [N/y/?] (NEW)
<y>
Socket Filtering (CONFIG_FILTER) [N/y/?] <Enter>
Unix domain sockets (CONFIGJJNIX) [Y/m/n/?] <Enter>
TCP/IPnetworking (CONFIG_INET) [Y/n/?] <Enter>
IP: multicasting (CONFIG_IP_MULTICAST) [Y/n/?] <n>
IP: advanced router (CONFIG_IP_ADVANCED_ROUTER) [N/y/?] <Enter>
IP: kernel level autoconfiguration (CONFIG_IP_PNP) [N/y/?] <Enter>
IP: tunneling (CONFIG_NET_IPIP) [N/y/m/?] <Enter>
IP: GRE tunnels over IP (CONFIG_NET_IPGRE) [N/y/m/?] <Enter>
IP: TCP Explicit Congestion Notification support (CONFIG_INET_ECN)
[N/y/?] <Enter>
IP: TCP syncookie support (disabled default) (CONFIG_SYN_COOKIES) [N/y/?]
<y>
*
*   IP: Netfilter Configuration
*
Connection tracking (required for masq/NAT) (CONFIG_IP_NF_CONNTRACK)
[N/y/m/?] (NEW) <m>
FTP protocol support (CONFIG__IP_NF_FTP) [N/m/?] (NEW) <m>
IRC protocol support (CONFIG_IP_NF_IRC) [N/m/?] (NEW) <m>
IP tables support (required for filtering/masq/NAT)
(CONFIG_IP_NF_IPTABLES) [N/y/m/?] (NEW) <m>
limit match support (CONFIG_IP NF_MATCH LIMIT) [N/m/?] (NEW) <m>
MAC address match support (CONFIG_IP_NF_MATCH_MAC) [N/m/?] (NEW) <m>
netfilter MARK match support (CONFIG_IP_NF_MATCH_MARK) [N/m/?] (NEW) <m>
Multiple port match support (CONFIG_IP_NF_MATCH_MULTIPORT) [N/m/?] (NEW)
<m>
TOS match support (CONFIG_IP_NF_MATCH_TOS) [N/m/?] (NEW) <m>
AH/ESP match support (CONFIG_IP_NF_MATCH_AH_ESP) [N/m/?] (NEW) <m>
LENGTH match support (CONFIG_IP_NF_MATCH_LENGTH) [N/m/?] (NEW) <m>
TTL match support (CONFIG_IP_NF_MATCH_TTL) [N/m/?] (NEW) <m>
tcpmss match support (CONFIG_IP_NF_MATCH_TCPMSS) [N/m/?] (NEW) <m>
Connection state match support (CONFIG_IP_NF_MATCH_STATE) [N/m/?] (NEW)
<m>
Packet filtering (CONFIG_IP_NF_FILTER) [N/m/?] (NEW) <m>
REJECT target support (CONFIG_IP_NF_TARGET_REJECT) [N/m/?] (NEW) <m>
Full NAT (CONFIG_IP_NF_NAT) [N/m/?] (NEW) <m>
MASQUERADE target support (CONFIG_IP_NF_TARGET_MASQUERADE) [N/m/?] (NEW)
<m>
REDIRECT target support (CONFIG_IP_NF_TARGET_REDIRECT) [N/m/?] (NEW) <m>
Packet mangling (CONFIG_IP_NF_MANGLE) [N/m/?] (NEW) <m>
TOS target support (CONFIG_IP_NF_TARGET_TOS) [N/m/?] (NEW) <m>
MARK target support (CONFIG_IP_NF_TARGET_MARK) [N/m/?] (NEW) <m>
```

```
LOG target support (CONFIG_IP_NF_TARGET_LOG) [N/m/?] (NEW) <m>
TCPMSS target support (CONFIG_IP_NF_TARGET_TCPMSS) [N/m/?] (NEW) <m>
ipchains (2.2-styie) support (CONFIG_IP_NF_COMPAT_IPCHAINS) [N/y/m/?]
(NEW) <Enter>
ipfwadm (2.0-style) support (CONFIG IP NF COMPAT IPFWADM) [N/y/m/?] (NEW)
<Enter>
*
*
*
The IPX protocol (CONFIG_IPX) [N/y/m/?] <Enter>
Appletalk protocol support (CONFIG_ATALK) [N/y/m/?] <Enter>
DECnet Support (CONFIG_DECNET) [N/y/m/?] <Enter> 802.Id Ethernet Bridging
(CONFIG_BRIDGE) [N/y/m/?] <Enter>
* QoS and/or fair queueing
QoS and/or fair queueing (CONFIG_NET_SCHED) [N/y/?] <Enter>
*
* Telephony Support
*
Linux telephony support (CONFIG_PHONE) [N/y/m/?] <Enter>
*
* ATA/IDE/MEM/RLI. support
*
RTA/IDE/MFM/RLL support (CONFIG_IDE) [Y/m/n/?] <Enter>
*
IDE, ATA and ATAPI Block devices
*
Enhanced IDE/MFM/RLL disk/cdrom/tape/floppy support (CONFIG_BLK_DEV IDE)
[Y/m/n/?] <Enter>
*
* Please see Documentation/ide.txt for help/info on IDE drives
*
Use old disk-only driver on primary interface (CONFIG_BLK_DEV_HD_IDE)
[N/y/?] <Enter>
 Include IDE/ATA-2 DISK support (CONFIG_BLK_DEV_IDEDISK) [Y/m/n/?] <En-
ter>
Use multi-mode by default (CONFIG_IDEDISK_MULTI_MODE) [Y/n/?] <n>
Include IDE/ATAPI CDROM support (CONFIG_BLK_DEV_IDECD) [Y/m/n/?] <Enter>
Include IDE/ATAPI TAPE support (CONFIG_BLK_DEV_IDETAPE) [N/y/m/?] <Enter>
Include IDE/ATAPI FLOPPY support (CONFIG_BLK_DEV_IDEFLOPPY) [N/y/m/?]
<Enter>
SCSI emulation support (CONFIG_BLK_DEV_IDESCSI) [N/y/m/?] <Enter>
*
*IDB chipset support/bugfixes
*
CMD640 chipset bugfix/support (CONFIG_BLK_DEV_CMD640) [Y/n/?] <n>
RZIOOO chipset bugfix/support (CONFIG_BLK_DEV_RZIOOO) [Y/n/?] <n>
Generic PCI IDE chipset support (CONFIG_BI.K_DEV_IDEPCI) [Y/n/?] <Enter>
Sharing PCI IDE interrupts support (CONFIG_IDEPCI_SHARE_IRQ) [Y/n/?] <En-
ter>
Generic PCI bus-master DMA support (CONFIG_BLK_DEV_IDEDMA_PCI) [Y/n/?]
<Enter>
Boot off-board chipsets first support (CONFIG_BLK_DEV_OFFBOARD) [N/y/?]
<Enter>
Use PCI DMA by default when available (CONFIG_IDEDMA_PCI_AUTO) [Y/n/?]
<Enter>
AEC62XX chipset support (CONFIG_BLK_DEV_AEC62XX) [N/y/?] <Enter>
ALI M15x3 chipset support (CONFIG_BLK DEV_AL115X3) [N/y/?] <Enter>
AMD Viper support (CONFIG_BLK_DEV_AMD74XX) [N/y/?] <Enter>
CMD64X chipset support (CONFIG_BLK_DEV_CMD64X) [N/y/?] <Enter>
CY82C693 chipset support (CONFIG_BLK_DEV_CY82C693) [N/y/?] <Enter>
Cyrix CS5530 MediaGX chipset support (CONFIG_BLK_DEV_CS5530) [N/y/?] <En-
ter>
HPT34X chipset support (CONFIG_BLK_DEV_HPT34X) [N/y/?] <Enter>
HPT366 chipset support (CONFIG_BLK_DEV_HPT366) [M/y/?] <Enter>
```

```
Intel PIIXn chipsets support (CONFIG_BLK_DEV__PIIX) [Y/n/?] <Enter>
PIIXn Tuning support (CONFIG_PIIX_TUNING) [Y/n/?] <Enter>
NS87415 chipset support (EXPERIMENTAL) (CONFIG_BLK_DEV_NS87415) [N/y/?]
<Enter>
PROMISE PDC202(46162165167168} support (CONFIG_BLK_DEV_PDC202XX) [N/y/?]
<Enter>
ServerWorks OSB4/CSB5 chipsets support (CONFIG_BLK_DEV_SVWKS) [N/y/?]
<Enter>
SiS5513 chipset support (CONFIG_BLK_DEV_SIS5513) [N/y/?] <Enter>
SLC90E66 chipset support (CONFIG_BLK_DEV_SLC90E66) [N/y/?] <Enter>
Tekram TRM290 chipset support (EXPERIMENTAL) (CONFIG_BLK_DEV TRM290)
[N/y/?] <Enter>
VIA82CXXX chipset support (CONFIG_BLK_DEV_VIA82CXXX) [N/y/?] <y>
Other IDE chipset support (CONFIG_IDE_CHIPSETS) [N/y/?] <Enter>
IGNORE word93 Validation BITS (CONFIG_IDEDMA_IVB) [N/y/?] <Enter>
*
SCSI support
*
SCSI support (CONFIG_SCSI) [Y/m/n/?] <n>
* Fusion MPT device support
*
120 device support
*
120 support (CONFIG_120) [N/y/m/?] <Enter>
*
* Network device support
*
Network device support (CONFIG_NETDEVICES) [Y/n/?] <Enter>
*
*ARCnet devices
*
ARCnet support (CONFIG_ARCNET) [N/y/m/?] <Enter>
Dummy net driver support (CONFIG_DUMMY) [M/n/y/?] <Enter>
Bonding driver support (CONFIG_BONDING) [N/y/m/?] <Enter>
EQL (serial line load balancing) support (CONFIG_EQUALIZER) [N/y/m/?]
<Enter>
Universal TUN/TAP device driver support (CONFIG_TUN) [N/y/m/?] <Enter>
*
*Ethernet (10 or lOOMbit)
*
Ethernet (10 or 100Mbit) (CONFIG_NET_ETHERNET) [Y/n/?] <Enter>
Sun Happy Meal 10/100baseT support (CONFIG_HAPPYMEAL) [N/y/m/?] <Enter>
Sun GEM support (CONFIG_SUNGEM) [N/y/m/?] <Enter>
3COM cards (CONFIG_NET_VENDOR_3COM) [N/y/?] <y>
3c501 "EtherLink" support (CONFIG_ELI) [N/y/m/?] (NEW) <Enter>
3c503 "EtherLink II" support (CONFIG_EL2) [N/y/m/?] (NEW) <Enter>
3c505 "EtherLink Plus" support (CONFIG_ELPLUS) [N/y/m/?] (NEW) <Enter>
3c509/3c529 (MCA)/3c579 "EtherLink III" support (CONFIG_EL3) [N/y/m/?]
(NEW) <Enter>
3c515 ISA "Fast EtherLink" (CONFIG_3C515) [N/y/m/?] (NEW) <Enter>
3c590/3c900 series (592/595/597) "Vortex/Boomerang" support
(CONFIG_VORTEX) [N/y/m/?] (NEW) <y>
AMD LANCE and PCnet (AT1500 and NE2100) support (CONFIG_LANCE) [N/y/m/?]
<Enter>
Western Digital/SMC cards (CONFIG_NET_VENDOR_SMC) [N/y/?] <Enter>
Racai-interlan (Micom) Nl cards (CONFIG_NET_VENDOR_RACAL) [N/y/?] <Enter>
DEPCA, DElOx, DE200, DE201, DE202, DE422 support (CONFIG_DEPCA) tN/y/m/?]
<Enter>
HP 10/100VG PCLAN (ISA, EISA, PCI) support (CONFIG_HPIOO) [N/y/m/?] <En-
ter>
Other ISA cards (CONFIG_NET_ISA) [N/y/?] <Enter>
EISA, VLB, PCI and on board controllers (CONFIG_NET_PCI) [Y/n/?] <n>
Pocket and portable adapters (CONFIG_NET_POCKET) [N/y/?] <Enter>
*
```

```
Ethernet (1000 Mbit)
*
Alteon AceNIC/3Com 3C985/NetGear GA620 Gigabit support (CONFIG ACENIC)
[N/y/m/?] <Enter>
D-Link DL2000-based Gigabit Ethernet support (CONFIG_DL2K) [N/y/m/?] <En-
ter>
National Semiconduct DP83820 support (CONFIG_NS83820) [N/y/m/?] <Enter>
Packet Engines Hamachi GNIC-II support (CONFIG_HAMACHI) tN/y/m/?] <Enter>
SysKonnect SK-98xx support (CONFIG_SK98LIN) tN/y/m/?] <Enter>
FDDI driver support (CONFIG_FDDI) [N/y/?] <Enter>
PPP (point-to-point protocol) support (CONFIG_PPP) [N/y/m/?] <Enter>
SLIP (serial line) support (COHFIG_SLIP) [N/y/m/?] <Enter>
*
* Wiraless LAN (non-hamradio)
*
Wireless LAN (non-hamradio) (CONFIG_NET_RADIO) [N/y/?] <Enter>
*
*Token Ring devices
*
Token Ring driver support (CONFIG_TR) [N/y/?] <Enter>
Fibre Channel driver support (CONFIG_NET_FC) [N/y/?] <Enter>
*
* Wan interfaces
*
Wan interfaces support (CONFIG_WAN) [N/y/?] <Enter>
*
* Jbnateur Radio support
*
Amateur Radio support (CONFIG_HAMRADIO) [N/y/?] <Enter>
*
* lrDA (infrared) support
*
lrDA subsystem support (CONFIG_IRDA) [N/y/m/?] <Enter>
*
* ISDN subsystem
*
ISDN support (CONFIG_ISDN) [N/y/m/?] <Enter>
*
*Old CD-ROM drivers (not SCSI, not IDE)
*
Support non-SCSI/IDE/ATAPI CDROM drives (CONFIG_CD_NO_IDESCSI) [N/y/?]
<Enter>
*
* Input core support
*
Input core support (CONFIG_INPUT) [N/y/m/?] <Enter>
*
*Character devices
*
Virtual terminal (CONFIG_VT) [Y/n/?] <Enter>
Support for console on virtual terminal (CONFIG_VT_CONSOLE) [Y/n/?] <En-
ter>
Standard/generic (8250/16550 and compatible UARTs) serial support
(CONFIG_SERIAL) [Y/m/n/?] <Enter>
Support for console on serial port (CONFIG_SERIAL_CONSOLE) [N/y/?] <En-
ter>
Extended dumb serial driver options (CONFIG_SERIAL_EXTENDED) [N/y/?] <En-
ter>
Non-standard serial port support (CONFIG_SERIAL_NONSTANDARD) [N/y/?] <En-
ter>
Hnix98 PTY support (CONFIG_UNIX98_PTYS) [Y/n/?] <Enter>
Maximum number of Unix98 PTYs in use (0-2048) (CONFIG_UNIX98 PTY_COUNT)
[256] 128
*
```

```
* I2C support
*
I2C support (CONFIG_12C) [N/y/m/?] <Enter>
*
* Mice
*
Bus Mouse Support (CONFIG_BUSMOUSE) [N/y/m/?] <Enter>
Mouse Support (not serial and bus mice) (CONFIG_MOUSE) [Y/m/n/?] <n>
*
* Joysticks
*
* Input core support is needed for gameports
* Input core support is needed for joysticks
*
QIC-02 tape support (CONFIG_QIC02_TAPE) [N/y/m/?] <Enter>
*
* Watchdog Cards
*
Watchdog Timer Support (CONFIG_WATCHDOG) [N/y/?] <Enter>
Intel i8x0 Random Number Generator support (CONFIG_INTEL_RNG) [N/y/m/?]
<Enter>
/dev/nvram support (CONFIG_NVRAM) [N/y/m/?] <Enter>
Enhanced Real Time Clock Support (CONFIG_RTC) [N/y/m/?] <Enter>
Double Talk PC internal speech card support (CONFIG_DTLK) [N/y/m/?] <En-
ter>
Siemens R3964 line discipline (CONFIG_R3964) [N/y/m/?] <Enter>
Applicom intelligent fieldbus card support (CONFIG_APPLICOM) [N/y/m/?]
<Enter>
*
* Ftape, the floppy tape device driver
*
Ftape (QIC-80/Travan) support (CONFIG_FTAPE) [N/y/m/?] <Enter>
/dev/agpgart (AGP Support) (CONFIG_AGP) [Y/m/n/?] n
Direct Rendering Manager (XFree86 DRI support) (CONFIG_DRM) [Y/n/?] <n>
ACP Modem (Mwave) support (CONFIG_MWAVE) [N/y/m/?] <Enter>
*
* Multimedia devices
*
Video For Linux (CONFIG_VIDEO_DEV) [N/y/m/?] <Enter>
*
* File systems
*
Quota support (CONFIG_QUOTA) [N/y/?] <y>
Kernel automounter support (CONFIG_AUTOFS_FS) [N/y/m/?] <Enter>
Kernel automounter version 4 support (also supports v3)
(CONFIG_AUTOFS4_FS) [Y/m/n/?] <n>
Reiserfs support (CONFIG_REISERFS_FS) [N/y/m/?] <Enter>
Ext3 journalling file system support (EXPERIMENTAL) (CONFIG_EXT3_FS)
[N/y/m/?] <y>
JBD (ext3) debugging support (CONFIG_JBD_DEBUG) [N/y/?] <y>
DOS FAT fs support (CONFIG_FAT_FS) [N/y/m/?] <m>
MSDOS fs support (CONFIG_MSDOS_FS) [N/y/m/?] <m>
VFAT (Windows-95) fs support (CONFIG_VFAT_FS) [N/y/m/?] <m>
Compressed ROM file system support (CONFIG_CRAMFS) [N/y/m/?] <Enter>
Virtual memory file system support (former shm fs) (CONFIG_TMPFS) [Y/n/?]
<Enter>
Simple RAM-based file system support (CONFIG_RAMFS) [N/y/m/?] <Enter>
ISO 9660 CDROM file system support (CONFIG_IS09660_FS) [Y/m/n/?] <m>
Microsoft Joliet CDROM extensions (CONFIG_JOLIET) [N/y/?] <y>
Transparent decompression extension (CONFIG_ZISOFS) [N/y/?] <Enter>
Minix fs support (CONFIG_MINIX_FS) [N/y/m/?] <Enter>
FreeVxFS file system support (VERITAS VxFS(TM) compatible)
(CONFIG_VXFS_FS) [N/y/m/?] <Enter>
NTFS file system support (read only) (CONFIG_NTFS_FS) [N/y/m/?] <Enter>
```

```
OS/2 HPFS file system support (CONFIG_HPFS_FS) [N/y/m/?] <Enter>
/proc file system support (CONFIG_PROC_FS) [Y/n/?] <Enter>
/dev/pts file system for Unix98 PTYs (CONFIG_DEVPTS_FS) [Y/n/?] <Enter>
ROM file system support (CONFIG_ROMFS_FS) [N/y/m/?] <Enter>
Second extended fs support (CONFIG_EXT2_FS) [Y/m/n/?] <Enter>
System V/Xenix/V7/Coherent file system support (CONFIG_SYSV_FS) [N/y/m/?]
<Enter>
UDF file system support (read only) (CONFIG_UDF_FS) [N/y/m/?] <Enter>
UFS file system support (read only) (CONFIG_UFS_FS) [N/y/m/?] <Enter>
*
* Network File Systems
*
Coda file system support (advanced network fs) (CONFIG_CODA_FS) [N/y/m/?]
<Enter>
NFS file system support (CONFIG_NFS_FS) [Y/m/n/?] <n>
NFS server support (CONFIG_NFSD) [Y/m/n/?] n
SMB file system support (to mount Windows shares etc.) (CONFIG_SMB_FS)
[N/y/m/?] <Enter>
NCP file system support (to mount NetWare volumes) (CONFIG_NCP_FS)
[N/y/m/?] <Enter>
*
* Partition Types
*
Advanced partition selection (CONFIG_PARTITION_ADVANCED) [N/y/?] <Enter>
*
Native Language Support
*
Default NLS Option (CONFIG_NLS_DEFAULT) [ISO8859-l] (NEW) <Enter>
Codepage 437 (United States, Canada) (CONFIG_NLS_CODEPAGE_437) [N/y/m/'?]
(NEW) <Enter>
Codepage 737 (Greek) (CONFIG_NLS_CODEPAGE_737) [N/y/m/?] (NEW) <Enter>
Codepage 775 (Baltic Rim) (CONFIG_NLS_CODEPAGE_775) [N/y/m/?] (NEW) <En-
ter>
Codepage 850 (Europe) (CONFIG_NLS_CODEPAGE_850) [N/y/m/?] (NEW) <Enter>
Codepage 852 (Central/Eastern Europe) (CONFIG_NLS_CODEPAGE_852) [N/y/m/?]
(NEW) <Enter>
Codepage 855 (Cyrillic) (CONFIG_NLS_CODEPAGE_855) [N/y/m/?] (NEW) <Enter>
Codepage 857 (Turkish) (CONFIG_NLS_CODEPAGE_857) [N/y/m/?] (NEW) <Enter>
Codepage 860 (Portuguese) (CONFIG_NLS_CODEPAGE_860) [N/y/m/?] (NEW) <En-
ter>
Codepage 861 (Icelandic) (CONFIG_NLS_CODEPAGE_861) [N/y/m/?] (NEW) <En-
ter>
Codepage 862 (Hebrew) (CONFIG_NLS_CODEPAGE_862) [N/y/m/?] (NEW) <Enter>
Codepage 863 (Canadian French) (CONFIG_NLS_CODEPAGE_863) [N/y/m/?] (NEW)
<Enter>
Codepage 864 (Arabic) (CONFIG_NLS_CODEPAGE_864) [N/y/m/?] (NEW) <Enter>
Codepage 865 (Norwegian, Danish) (CONFIG_NLS_CODEPAGE_865) [N/y/m/?]
(NEW) <Enter>
Codepage 866 (Cyrillic/Russian) (CONFIG_NLS_CODEPAGE_866) [N/y/m/?] (NEW)
<y>
Codepage 869 (Greek) (CONFIG_NLS_CODEPAGE_869) [N/y/m/?] (NEW) <Enter>
Simplified Chinese charset (CP936, GB2312) (CONFIG_NLS_CODEPAGE_936)
[N/y/m/?] (NEW) <Enter>
Traditional Chinese charset (Big5) (CONFIG_NLS_CODEPAGE_950) [N/y/m/?]
(NEW) <Enter>
Japanese charsets (Shift-JIS, EUC-JP) (CONFIG_NLS_CODEPAGE_932) [N/y/m/?]
(NEW) <Enter>
Korean charset (CP949, EUC-KR) (CONFIG_NLS_CODEPAGE_949) [N/y/m/?] (NEW)
<Enter>
Thai charset (CP874, TIS-620) (CONFIG_NLS_CODEPAGE_874) [N/y/m/?] (NEW)
<Enter>
Hebrew charsets (ISO-8859-8, CP1255) (CONFIG_NLS_IS08859_8) [N/y/m/?]
(NEW) <Enter>
```

```
Windows CP1250 (Slavic/Central European Languages)
(CONFIG_NLS_CODEPAGE_1250) [N/y/m/?] (NEW) <Enter>
Windows CP1251 (Bulgarian, Belarusian) (CONFIG_NLS_CODEPAGE_1251)
[N/y/m/?] (NEW) <y>
NLS ISO 8859-1 (Latin 1; Western European Languages) (CONFIG_NLS_IS08859
1) [N/y/m/?] (NEW) <Enter>
NLS ISO 8859-2 (Latin 2; Slavic/Central European Languages)
(CONFIG_NLS_IS08859_2) [N/y/m/?] (NEW) <Enter>
NLS ISO 8859-3 (Latin 3; Esperanto, Galician, Maltese, Turkish)
(CONFIG_NLS_IS08859 3) [N/y/m/?] (NEW) <Enter>
NI.S ISO 8859-4 (Latin 4; old Baltic charset) (CONFIG_NLS_IS08859_4)
[N/y/m/?] (NEW) <Enter>
NLS ISO 8859-5 (Cyrillic) (CONFIG_NLS_IS08859_5) [N/y/m/?] (NEW) <y>
HIS ISO 8859-6 (Arabic) (CONFIG_NLS_IS08859_6) [N/y/m/?] (NEW) <Enter>
NLS ISO 8859-7 (Modern Greek) (CONFIG_NLS_IS08859_7) [N/y/m/?] (NEW) <En-
ter>
NLS ISO 8859-9 (Latin 5; Turkish) (CONFIG_NLS_IS08859_9) [N/y/m/?] (NEW)
<Enter>
NLS ISO 8859-13 (Latin 7; Baltic) (CONFIG_NLS_IS08859_13) [N/y/m/?] (NEW)
<Enter>
NLS ISO 8859-14 (Latin 8; Celtic) (CONFIG_NLS_IS08859_14) [N/y/m/?] (NEW)
<Enter>
NLS ISO 8859-15 (Latin 9; Western European Languages with Euro)
(CONFIG_NLS IS08859 15) [N/y/m/?] (NEW) <Enter>
NLS K018-R (Russian) (CONFIG_NLS_K018_R) [N/y/m/?] (NEW) <Enter>
NLS K018-D/RU (Ukrainian, Belarusian) (CONFIG_NLS_K018_U) [N/y/m/?] (NEW)
<Enter>
 NLS UTF8 (CONFIG_NLS_UTF8) [N/y/m/?] (NEW) <Enter>
*
* Console drivers
*
VGA text console (CONFIG_VGA_CONSOLE) [Y/n/?] <Enter>
Video mode selection support (CONFIG_VIDEO_SELECT) [N/y/?] <Enter>
*
*Sound
*
Sound card support (CONFIG_SOUND) [Y/m/n/?] <n>
*
*USB support
*
Support for USB (CONFIG_USB) [Y/m/n/?] <n>
*
*USB Controllers
*
*
*USB Device Class drivers
*
* SCSI support is needed for USB Storage
*
*
* USB Human Interface Devices (HID)
*
*
* Input core support is needed for USB HID
*
*
* USB Imaging devices
*
* USB Multimedia devices
*
*
* Video4Linux support is needed for USB Multimedia device support
*
*
```

```
* USB Network adapters
*
*
* USB port drivers
*
*
* USB Serial Converter support
*
*
* USB Miscellaneous drivers
*
*
* Kernel hacking
*
Kernel debugging (CONFIG_DEBUG_KERNEL) [N/y/?] <Enter>
*
*Graecurity
*
Grsecurity (CONFIG_GRKERNSEC) [N/y/?] <y>
Security level (Low, Medium, High, Customized) [Customized] <Enter>
*
* Buffer Overflow Protection
*
Openwall non-executable stack (CONFIG_GRKERNSEC_STACK) [N/y/?] <y>
Gee trampoline support (CONFIG_GRKERNSEC_STACK_GCC) [N/y/?] <Enter>
Read-only kernel memory (CONFIG_GRKERNSEC_KMEM) [N/y/?] <y>
*
Access Control Lists
*
Grsecurity ACL system (CONFIG_GRKERNSEC_ACL) [N/y/?] <y>
ACL Debugging Messages (CONFIG_GR_DEBUG) [N/y/?] <y>
Extra ACL Debugging Messages (CONFIG_GR_SUPERDEBUG) [N/y/?] <Enter>
Denied capability logging (CONFIG_GRKERNSEC_ACL_CAPLOG) [N/y/?] <y>
Path to gradm (CONFIG_GRADM_PATH) [/sbin/gradm] <Enter>
Maximum tries before password lockout (CONFIG_GR_MAXTRIES) [3] 2
Time to wait after max password tries, in seconds (CONFIG_GR_TIMEOUT)
[30] <Enter>
*
Filesystem Protections
*
Proc restrictions (CONFIG_GRKERNSEC_PROC) [N/y/?] <y>
Restrict to user only (CONFIG_GRKERNSEC_PROC_USER) [N/y/?] <y>
Additional restrictions (CONFIG_GRKERNSEC_PROC_ADD) tN/y/?] <y>
Linking restrictions (CONFIG_GRKERNSEC_LINK) [N/y/?] <y>
FIFO restrictions (CONFIG_GRKERNSEC_FIFO) [N/y/?] <y>
Secure file descriptors (CONFIG_GRKERNSEC_FD) [N/y/?] <y>
Chroot-jail restrictions (CONFIG_GRKERNSEC_CHROOT) [N/y/?] <y>
Restricted signals (CONFIG_GRKERNSEC_CHROOT_SIG) [N/y/?] <y>
Deny mounts (CONFIG_GRKERNSEC_CHROOT_MOUNT) [N/y/?] <y>
Deny double-chroots (CONFIG_GRKERNSEC_CHROOT_DOUBLE) [N/y/?] <y>
Enforce chdir("/") on all chroots (CONFIG_GRKERNSEC_CHROOT_CHDIR) [N/y/?]
<y>
Deny (f)chmod +s (CONFIG_GRKERNSEC_CHROOT_CHMOD) [N/y/?] <y>
Deny mknod (CONFIG_GRKERNSEC_CHROOT_MKNOD) [N/y/?] <y>
Deny ptraces (CONFIG_GRKERNSEC_CHROOT_PTRACE) [N/y/?] <y>
Restrict priority changes (CONFIG_GRKERNSEC_CHROOT_NICE) [N/y/?] <y>
Capability restrictions within chroot (CONFIG_GRKERNSEC_CHROOT_CAPS)
[N/y/?] <Enter>
Secure keymap loading (CONFIG_GRKERNSEC_KBMAP) [N/y/?] <y>
*
Kernel Auditing
*
Single group for auditing (CONFIG_GRKERNSEC_AUDIT_GROUP) [N/y/?] <Enter>
Exec logging (CONFIG_GRKERNSEC_EXECLOG) [N/y/?] <Enter>
```

```
Log execs within chroot (CONFIG_GRKERNSEC_CHROOT_EXECLOG) [N/y/?] <y>
Chdir logging (CONFIG_GRKERNSEC_AUDIT_CHDIR) [N/y/?] <Enter>
(Un)Mount logging (COHFIG_GRKERNSEC_AUDIT_MOUNT) [N/y/?] <Enter>
IPC logging (CONFIG_GRKERNSEC_AUDIT_IPC) [N/y/?] <y>
Ptrace logging (CONFIG_GRKERNSEC_AUDIT_PTRACE) [N/y/?] <Enter>
Signal logging (CONFIG_GRKERNSEC_SIGNAL) [N/y/?] <y>
Fork failure logging (CONFIG_GRKERNSEC_FORKFAIL) [N/y/?] <y>
Set*id logging (CONFIG_GRKERNSEC_SUID) [N/y/?] <Enter>
Log set*ids to root (CONFIG_GRKERNSEC_SUID_ROOT) [N/y/?] <y>
Time change logging (CONFIG_GRKERNSEC_TIME) [N/y/?] <y>
*
*Executable Protections
*
Exec process limiting (CONFIG_GRKERNSEC_EXECVE) [N/y/?] <y>
Dmesg(8) restriction (CONFIG_GRKERNSEC_DMESG) [N/y/?] <y>
Randomized PIDs (CONFIG_GRKERNSEC_RANDPID) [N/y/?] <y>
Altered default IPC permissions (CONFIG_GRKERNSEC_IPC) [N/y/?] <Enter>
imit uid/gid changes to root (CONFIG_GRKERNSEC_TTYROOT) [N/y/?] <y>
Deny physical consoles (tty) (CONFIG_GRKERNSEC_TTYROOT_PHYS) [N/y/?] <En-
ter>
Deny serial consoles (ttyS) (CONFIG_GRKERNSEC_TTYROOT_SERIAL) [N/y/?] <y>
Deny pseudo consoles (pty) (CONFIG_GRKERNSEC_TTYROOT_PSEUDO) [N/y/?] <En-
ter>
Fork-bomb protection (CONFIG_GRKERNSEC_FORKBOMB) [N/y/?] <y>
GID for restricted users (CONFIG_GRKERNSEC_FORKBOMB_GID) [1006] <Enter>
Forks allowed per second (CONFIG_GRKERNSEC_FORKBOMB_SEC) [40] <Enter>
Maximum processes allowed (CONFIG_GRKERNSEC_FORKBOMB_MAX) [20] 33
Trusted path execution (CONFIG_GRKERNSEC_TPE) [N/y/?] <y>
Glibc protection (CONFIG_GRKERNSEC_TPE_GLIBC) [N/y/?] <y>
Partially restrict non-root users (CONFIG_GRKERNSEC_TPE_ALL) [N/y/?] <y>
GID for untrusted users: (CONFIG_GRKERNSEC_TPE_GID) [1005] <Enter>
Restricted ptrace (CONFIG_GRKERNSEC_PTRACE) [N/y/?] <y>
Allow ptrace for group (CONFIG_GRKERNSEC_PTRACE_GROUP) [N/y/?] <Enter>
*
*Network Protections
*
Randomized IP IDs (CONFIG_GRKERNSEC_RANDID) [N/y/?] <y>
Randomized TCP source ports (CONFIG_GRKERNSEC_RANDSRC) [N/y/?] <y>
Randomized RPC XIDs (CONFIG_GRKERNSEC_RANDRPC) [N/y/?] <y>
Altered Ping IDs (CONFIG_GRKERNSEC_RANDPING) [N/y/?] <y>
Randomized TTL (CONFIG_GRKERNSEC_RANDTTL) [N/y/?] <y>
Socket restrictions (CONFIG_GRKERNSEC_SOCKET) [N/y/?] <y>
Deny any sockets to group (CONFIG_GRKERNSEC_SOCKET_ALL) [N/y/?] <y>
GID to deny all sockets for: (CONFIG_GRKERNSEC_SOCKET_ALI_GID) [1004]
<Enter>
Deny client sockets to group (CONFIG_GRKERNSEC_SOCKET_CLIENT) [N/y/?]
<Enter>
Deny server sockets to group (CONFIG_GRKERNSEC_SOCKET_SERVER) [N/y/?]
<Enter>
*
Syactl support
*
Sysctl support (CONFIG_GRKERNSEC_SYSCTL) [N/y/?] <Enter>
*
*Miscellaneous Features
*
Seconds in between log messages (minimum) (CONFIG_GRKERNSEC_FLOODTIME)
[30] <Enter>
BSD-style coredumps (CONFIG_GRKERNSEC_COREDUMP) [N/y/?] <y>
*** End of Linux kernel configuration.
*** Check the top-level Makefile for additional configuration.
*** Next, you must run 'make dep'.
```

Компиляция ядра

Компиляция ядра с монолитной и модульной архитектурами осуществляется следующим образом.

Шаг 1

Перейдите в каталог, где находятся исходные коды ядра:

```
[root@drwalbr /]# cd /usr/src/linux-2.4.x/
```

Шаг 2

Сформируйте дерево зависимостей в соответствии с выбранными параметрами конфигурации, т. е. определите, что нужно компилировать, а что нет:

```
[root@drwalbr linux-2.4.x]# make dep
```

Шаг 3

Удалите старые объектные модули:

```
[root@drwalbr linux-2.4.x]# make clean
```

ЗАМЕЧАНИЕ Команда `make clean` удаляет все объектные модули и заставляет пересобираться ядро «с нуля», т. е. с заново создаваемыми объектными модулями. Использование этой команды необходимо, если ядро компилируется впервые после замены объектной библиотеки, транслятора или компоновщика. Если вы путем перебора нескольких вариантов конфигурации ядра пытаетесь получить ядро, надежно работающее с некоторым экзотическим оборудованием, в использовании команды `make clean` нет необходимости. Ее использование только увеличит время, затраченное на поиск оптимальной конфигурации ядра.

Шаг 4

Скомпилируйте новое ядро:

```
[root@drwalbr linux-2.4.x]# make bzImage
```

Шаг 5

Если вы используете ядро с модульной архитектурой, скомпилируйте новые модули ядра:

```
[root@drwalbr linux-2.4.x]# make modules
[root@drwalbr linux-2.4.x]# make modules_install
```

Инсталляция ядра

Инсталляция нового ядра осуществляется следующим образом.

Шаг 1

Скопируйте файл `/usr/src/linux-2.4.x/arch/i386/boot/bzlmage` из исходного дерева ядра в каталог`/boot` и переименуйте его:

```
[root@drwalbr linux-2.4.x]# cd /usr/src/linux/
[root@drwalbr linux]# cp arch/i386/boot/bzlmage /boot/vmlinuz-2.4.x
```

Шаг 2

При компиляции ядра в каталоге `/usr/src/linux-2.4.x` создан новый файл `System.map`, используемый рядом программ (`klog`, `ps` и `lsof`). Для того, чтобы эти программы могли найти и использовать информацию, содержащуюся в файле, необходимо скопировать его в каталог `/boot`:

```
[root@drwalbr linux]# cp System.map /boot/System.map-2.4.x
```

Шаг 3

Восстановите ранее удаленные символьные ссылки `vmlinuz` и `System.map`:

```
[root@drwalbr linux]# cd /boot/
[root@drwalbr /boot]# ln -fs vmlinuz-2.4.x vmlinuz
[root@drwalbr /boot]# ln -fs System.map-2.4.x System.map
```

Шаг 4

Удалите ссылку на каталог, в котором находились модули старого ядра:

```
[root@drwalbr /boot] # rm -f module-info
```

Удалите файл `initrd.2.4.18-5asp.img`:

```
[root@drwalbr /boot] # rm -f initrd.2.4.18-5asp.img
```

Этот файл содержит начальный образ загрузочного диска и используется системой до того, как диск станет доступным. Он используется на системах со SCSI дисками. В нашем случае он может быть удален,

т. к. все опции поддержки SCSI жестко «вкомпилированы» в ядро с монолитной конфигурацией, а на системе, где установлено ядро с модульной архитектурой – диск с IDE контроллером.

Шаг 5

Создайте каталог, в котором будут храниться заголовочные файлы ядра, необходимые для последующей компиляции программ-приложений:

```
[root@drwalbr /]# mkdir -p /usr/src/linux/include
[root@drwalbr /]# cd /usr/src/linux-2.4.x/
[root@drwalbr linux-2.4.x]# cp -r include/asm-i386 ../linux/include/
[root@drwalbr linux-2.4.x]# cp -r include/linux ../linux/include/
[root@drwalbr linux-2.4.x]# cd ../
[root@drwalbr /]# rm -rf /usr/src/linux-2.4.x/
```

Настройка загрузчика

После инсталляции нового ядра необходимо настроить загрузчик LILO, чтобы он мог загружать новое ядро.

Настройка загрузчика осуществляется следующим образом.

Шаг 1

В файле `lilo.conf` необходимо отредактировать строки "`image=…`" и "`label=…`". Для этого выполните следующие действия:

```
[root@drwalbr /]# vi /etc/lilo.conf
boot=/dev/sda
map=/boot/map
install=/boot/boot.b
timeout=00
default=linux
restricted
password=SecReTn0e_Sl0V0
image=/boot/vmlinuz
label=linux-2.4.x-grsec
read-only
root=/dev/sda5
```

Шаг 2

Для того, что бы внесенные изменения вступили в силу, выполните команду:

```
[root@drwalbr /]# /sbin/lilo
Added linux *
```

Загрузчик GRUB после инсталляции нового ядра не нуждается в настройках. Для проверки правильности настройки загрузчика выполните:

```
[root@drwalbr /]# vi /boot/grub/grub.conf
default 0
timeout 00
title linux-2.4.18
kernel (hd0,0)/vmlinuz ro root=/dev/sda5
```

Файл `/etc/modules.conf`

Файл `/etc/modules.conf` является дополнительным конфигурационным файлом, влияющим на процессы загрузки модулей ядра. Он используется программами depmod и modprobe. После каждого обновления ядра с модульной архитектурой необходимо проверить, правильно ли отражена в этом конфигурационном файле необходимая информация о модулях, загружаемых ядром.

В рассматриваемом примере файл `modules.conf` был создан автоматически. В него были записаны следующие строки:

```
alias SCSI_hostadapter aic7xxx
alias eth0 eepro100
alias eth1 eepro100
alias parport_lowlevel parport_pc alias usb-controller uhci
```

Указанный файл может быть использован для передачи параметров и присвоения загружаемым модулям алиасов (альтернативных имен).

Если конфигурационный файл /etc/modules.conf отсутствует или если любая директива в нем не переопределена (значение по умолчанию можно посмотреть в каталоге /lib/modules, содержащем модули, откомпилированные для текущей версии ядра), то файл /etc/modules.conf можно удалить:

```
[root@drwalbr /]# rm -f /etc/modules.conf
```

Проверка работоспособности нового ядра

Шаг 1

Для проверки работоспособности нового ядра перезагрузите систему:

```
[root@drwalbr /]# reboot
```

Шаг 2

После перезагрузки проверьте версию нового ядра:

```
[root@drwalbr /]# uname -a
Linux dev 2.4.18-grsec-1.9.4 #l Mon Dec 23 17:14:55 EDT 2002 i686 unknown
```

ЗАМЕЧАНИЕ Если система не загрузилась или ядро не поддерживает необходимые возможности и/или нужные устройства, то анализируются и исправляются допущенные ошибки, система загружается с помощью загрузочной дискеты, и повторяются все операции по конфигурированию, компиляции и инсталляции нового ядра.

Создание аварийной загрузочной дискеты для ядра с монолитной архитектурой

Сразу же после первой удачной загрузки системы необходимо создать аварийную загрузочную дискету для новой конфигурации ядра.

ЗАМЕЧАНИЕ Создание аварийной загрузочной дискеты для ядра с модульной архитектурой описано в начале главы.

Аварийная загрузочная дискета для ядра с монолитной архитектурой создается следующим образом.

Шаг 1

Вставьте в дисковод и отформатируйте дискету с помощью следующей команды:

```
[root@drwalbr /]# fdformat /dev/fd0H1440
Double-sided, 80 tracks, 18 sec/track. Total capacity 1440 kB
Formatting . . . done
Verifying . . . done
```

Шаг 2

Скопируйте существующий файл vmlinuz из /boot каталога на дискету:

```
[root@drwalbr /]# cp /boot/vmlinuz /dev/fd0H1440
cp: overwrite '/dev/fdOH1440'? <y>
```

Шаг 3

Определите корневой раздел:

```
[root@drwalbr /]# rdev
/dev/sda5/
```

Шаг 4

Установите корневой раздел (в примере это /dev/sda5/, определенный на предыдущем шаге):

```
[root@drwalbr /]# rdev /dev/fd0H1440 /dev/sda5
```

Шаг 5

Установите к корневому разделу доступ "только для чтения":

```
[root@drwalbr /]# rdev -R /dev/fd0H1440
```

Шаг 6

Если в системе используется ядро с монолитной архитектурой, можно удалить пакеты mkbootdisk и dosfstools, предназначенные для создания аварийных загрузочных дискет в системах с модульной архитектурой ядра:

```
[root@drwalbr /]# rpm -e mkbootdisk dosfstools
```

Шаг 7

После установки в BIOS загрузки с дискеты система перезагружается:

```
[root@drwalbr /]# reboot
```

Глава 7

Псевдофайловая система /proc

В этой главе:

1. Утилита sysctl
2. Настройка параметров подсистемы виртуальной памяти
3. Настройка параметров подсистемы IPv4
4. Установка запрета ответа на ping-запросы
5. Установка запрета ответа на широковещательные ping-запросы
6. Запрет на использование сервером информации об источнике пакета
7. Включение защиты от SYN-атак
8. ICMP-переадресация
9. Сообщения об ошибках сети
10. Включение защиты от атак, основанных на фальсификации IP-адреса
11. Включение регистрации Spoofed, Source Routed и Redirect пакетов
12. Включение пересылки пакетов

Псевдофайловая система /proc используется как интерфейс для доступа к структурам данных ядра. Большинство каталогов в каталоге /proc имеют названия в виде десятичных чисел, совпадающих с идентификатором соответствующего процесса, выполняемого в системе. Файловая система /proc отображает информацию о центральном процессоре, IDE и SCSI-устройствах, прерываниях, портах ввода-вывода, памяти, модулях, разделах, PCI-платах и др. При этом следует учитывать, что, на самом деле, не существует ни подкаталогов /proc, ни файлов в них. В этом легко убедится, посмотрев каталог /proc на машине, в которой установлены две операционные системы Linux и Windows с помощью программы для просмотра файловых систем Ext2 и Ext3, например, ext2viewer из Windows. Каталог /proc будет пустым. Содержимое этого каталога можно рассматривать как некоторые временные файлы, существующие только во время работы системы. Большинство из этих файлов доступны только для чтения и, следовательно, не могут быть изменены. Изменение параметров ядра осуществляется путем редактирования конфигурационного файла /etc/sysctl.conf, используемого утилитой sysctl, либо непосредственным вызовом утилиты. В этой главе рассматриваются некоторые параметры, конфигурирующие виртуальную память и TCP/IP.

Утилита sysctl

Утилита sysctl – интерфейс, который позволяет изменять некоторые параметры ядра без его перекомпиляции. Более подробная информация об этой утилите может быть получена с помощью команды:

```
[root@karlnext /]# man 8 sysctl
```

Эта утилита позволяет считывать и изменять параметры настройки ядра.

Для просмотра всех переменных выполните:

```
[root@karlnext /]# sysctl –a
```

Для просмотра некоторой переменной, например, fs.file-max, выполните:

```
[root@karlnext /]# sysctl fs.file-max
fs.file-max = 8192
```

Для установки значения некоторой переменной, например, fs.file-max, выполните:

```
[root@karlnext /]# sysctl -w fs.file-max=16384
fs.file-max = 16384
```

Изменения, внесенные с помощью команды sysctl, действуют только до перезагрузки системы. Для того, чтобы внесенные изменения сохранились после перезагрузки, необходимо изменить соответствующие параметры в конфигурационном файле /etc/sysctl.conf.

Настройка параметров подсистемы виртуальной памяти

В каталоге /proc/sys/vm находятся файлы, используемые для настройки и отображения подсистемы виртуальной памяти ядра. Будьте очень осторожны и внимательны при выполнении приведенных ниже рекомендаций.

Приведенных здесь примеры протестированы и прекрасно работают на серверах с объемом оперативной памяти 256, 384 и 512 МБайт. При меньшем объеме памяти мы не гарантируем работоспособности приведенных ниже настроек и рекомендуем использовать настройки по умолчанию.

Для просмотра файлов в каталоге /proc/sys/vm выполните:

```
[root@karlnext /]# ls –l /proc/sys/vm
-rw-r--r--    1 root     root            0 Янв 12 10:38 bdflush
-rw-r--r--    1 root     root            0 Янв 12 10:38 kswapd
-rw-r--r--    1 root     root            0 Янв 12 10:38 max_map_count
-rw-r--r--    1 root     root            0 Янв 12 10:38 max-readahead
-rw-r--r--    1 root     root            0 Янв 12 10:38 min-readahead
-rw-r--r--    1 root     root            0 Янв 12 10:38 overcommit_memory
-rw-r--r--    1 root     root            0 Янв 12 10:38 page-cluster
-rw-r--r--    1 root     root            0 Янв 12 10:38 pagetable_cache
```

Файл /proc/sys/vm/bdflush содержит настройки демона ядра bdflush и может быть использован для повышения производительности файловой системы. Файл /proc/sys/vm/bdflush содержит значения (приведены значения по умолчанию) следующих 9 параметров:

```
[root@karlnext /]# cat /proc/sys/vm/bdflush
30      500   0     0     500   3000  60    20    0
```

Первый параметр – `nfract` – в конечном итоге определяет процент заполнения буфера, при достижении которого осуществляется запись на диск. Значение по умолчанию – 30 %, минимальное – 0 % и максимальное – 100 %. Установка высокого значения параметра приводит к тому, что задержка записи на диск осуществляется в течение более длительного времени, но при этом увеличивается загрузка памяти из-за операций ввода - вывода фрагментами большего размера. Рекомендуем установить значение параметра, равное 40.

Второй параметр – `dummy1` пока не используется, сохраните значение по умолчанию.

Третий параметр – `dummy2` тоже пока не используется, сохраните значение по умолчанию.

О четвертом параметре – `dummy3` – можно сказать то же самое.

Параметр `interval` определяет минимальный интервал, в течение которого осуществляется очистка буфера. Значение по умолчанию – 5 секунд, минимальное – 0 секунд и максимальное – 600 секунд. Мы сохраняем здесь значение по умолчанию.

Шестой параметр – `age_buffer` определяет максимальный интервал времени, по истечении которого информация из буфера записывается на диск. Значение по умолчанию – 30 секунд, минимальное – 1 секунда и максимальное – 6 000 секунд. Рекомендуем оставить значение по умолчанию.

Седьмой параметр – `nfract_sync` управляет размером буферного кэша, выраженным в процентах, который заполняется до начала активизации `bdflush`. Его можно рассматривать как жесткое ограничение буфера прежде, чем `bdflush` начнет запись на диск. Значение по умолчанию – 60 %, минимальное – 0 % и максимальное – 100 %. Рекомендуем оставить значение по умолчанию.

Восьмой и девятые параметры – `dummy4` и `dummy5` - пока не используется, сохраните значения по умолчанию.

Установка рекомендуемых нами или любых других значений параметров осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` строку:

```
#Увеличение производительности файловой системы
vm.bdflush = 40    500   0     0     500   3000  60    20    0
```

Шаг 2

Для того, чтобы внесенные нами изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w vm.bdflush="40 500 0 0 500 3000 60 20 0"
```

Файл `/proc/sys/vm/kswapd` содержит параметры настройки операций с виртуальной памятью системы (очистка, дефрагментирование). Очистка производится, когда виртуальная память сильно дефрагментированна или заполнена. Файл `/proc/sys/vm/kswapd` содержит значения (приведены значения по умолчанию) следующих 3 параметров:

```
[root@karlnext /]# /proc/sys/vm/kswapd
512     32    8
```

Первый параметр – `tries_base` определяет максимальное количество страниц `kswapd`, которые должны очищаться за один цикл. Увеличив это число, можно заставить виртуальную память работать быстрее. Сохраните значение по умолчанию.

Второй параметр – `tries_min` определяет минимальное количество страниц, которые `kswapd` должен очищать каждый раз при вызове. В основном этот параметр служит для того, чтобы удостовериться, что `kswapd` очищает страницы, даже когда программа работает с минимальным приоритетом. Значение по умолчанию – 32 страницы. Сохраните значение по умолчанию.

Третий параметр – `swap_cluster` определяет количество страниц, которые `kswapd` записывает за одну итерацию. Естественно стремление повысить производительность за счет проведения операций ввода - вывода большими фрагментами и уменьшения времени поиска нужного сектора диска. Однако фрагменты не должны быть слишком большими, иначе может произойти переполнение очереди запроса. Значение по умолчанию – 8 страниц. Установите значение этого параметра, равное 32.

Установка значений параметров осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` строки:

```
#Увеличение производительности swap
vm.kswapd = 512    32    32
```

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w vm.kswapd = "512 32 32"
```

Настройка параметров подсистемы IPv4

Файлы, соответствующие всем описываемым ниже параметрам, находятся в каталоге `/proc/sys/net/ipv4` и используются для настройки подсистемы ядра IPv4. Для просмотра файлов в каталоге `/proc/sys/net/ipv4` наберите команду:

```
[root@karlnext /]# ls -l /proc/sys/net/ipv4
dr-xr-xr-x    6 root     root            0 Янв 25 13:18 conf
-rw-r--r--    1 root     root            0 Янв 25 13:18
icmp_echo_ignore_all
-rw-r--r--    1 root     root            0 Янв 25 13:18
icmp_echo_ignore_broadcasts
-rw-r--r--    1 root     root            0 Янв 25 13:18
icmp_ignore_bogus_error_responses
-rw-r--r--    1 root     root            0 Янв 25 13:18 icmp_ratelimit
-rw-r--r--    1 root     root            0 Янв 25 13:18 icmp_ratemask
-rw-r--r--    1 root     root            0 Янв 25 13:18
inet_peer_gc_maxtime
-rw-r--r--    1 root     root            0 Янв 25 13:18
inet_peer_gc_mintime
-rw-r--r--    1 root     root            0 Янв 25 13:18 inet_peer_maxttl
-rw-r--r--    1 root     root            0 Янв 25 13:18 inet_peer_minttl
-rw-r--r--    1 root     root            0 Янв 25 13:18
inet_peer_threshold
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip_autoconfig
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip_conntrack_max
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip_default_ttl
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip_dynaddr
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip_forward
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip-
frag_high_thresh
-rw-r--r--    1 root     root            0 Янв 25 13:18 ipfrag_low_thresh
-rw-r--r--    1 root     root            0 Янв 25 13:18 ipfrag_time
-rw-r--r--    1 root     root            0 Янв 25 13:18
ip_local_port_range
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip_nonlocal_bind
-rw-r--r--    1 root     root            0 Янв 25 13:18 ip_no_pmtu_disc
dr-xr-xr-x    5 root     root            0 Янв 25 13:18 neigh
dr-xr-xr-x    2 root     root            0 Янв 25 13:18 route
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_abort_on_overflow
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_adv_win_scale
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_app_win
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_dsack
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_ecn
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_fack
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_fin_timeout
```

```
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_keepalive_intvl
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_keepalive_probes
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_keepalive_time
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_max_orphans
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_max_syn_backlog
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_max_tw_buckets
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_mem
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_orphan_retries
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_reordering
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_retrans_collapse
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_retries1
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_retries2
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_rfc1337
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_rmem
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_sack
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_stdurg
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_synack_retries
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_syncookies
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_syn_retries
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_timestamps
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_tw_recycle
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_tw_reuse
-rw-r--r--    1 root     root            0 Янв 25 13:18
tcp_window_scaling
-rw-r--r--    1 root     root            0 Янв 25 13:18 tcp_wmem
```

Приведенный вывод с экрана получен для версии ядра 2.4.19, в другой системе он может выглядеть несколько по-другому.

Установка запрета ответа на ping-запросы

Предотвращение возможности ответов вашей системы на запросы утилиты `ping` может значительно улучшить сетевую безопасность, так как никто не сможет «пропинговать» ваш сервер. Установка запрета осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` следующие строки:

```
# Игнорирование ответов на  ping
net.ipv4.icmp_echo_ignore_all=1
```

ЗАМЕЧАНИЕ Установку значения параметра `net.ipv4.icmp_echo_ignore_all=1` рекомендуется устанавливать только в случае осуществления атак, основанных на использовании ICMP-пакетов. В других случаях этого делать не рекомендуется, т. к. это существенно ограничивает функциональные возможности системы, которая использует ICMP-пакеты для установки такого важного параметра, как MTU. Многие владельцы Web-серверов используют эту опцию, забывая при этом, что MS Windows-98/Me имеет в установках по умолчанию автоматический выбор значения MTU. В этом случае Web-сервера становятся недоступными для большинства пользователей.

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
```

```
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w net.ipv4.icmp_echo_ignore_all=1
```

Установка запрета ответа на широковещательные ping-запросы

Когда запрос утилиты `ping` посылается на широковещательный адрес (например, 172.16.255.255 или 192.168.1.255), то соответствующие пакеты доставляются всем машинам этой сети. После этого все машины в сети отвечают на посланный широковещательный запрос. В результате может возникнуть перегрузка сети, и ваша система может оказаться невольным участником DoS-атаки. Более подробную информацию по этому вопросу можно получить в RFC 2644. Установка запрета осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` следующие строки:

```
#Игнорирование широковещательных запросов
net.ipv4.icmp_e_cho_ignore_broadcasts = 1
```

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts =1
```

Запрет на использование сервером информации об источнике пакета

Маршрутизация и протоколы маршрутизации также содержат источник потенциальной опасности для системы. Заголовки IP-пакетов содержат полный путь между источником и получателем пакета. В соответствии с RFC 1122 получатель пакета должен ответить по адресу источника, содержащегося в пакете. Таким образом, злоумышленник может получить возможность перехватить ответ вашей системы и представиться доверенной системой. Авторы настоятельно рекомендуют отключить возможность использования сервером информации об источнике пакета. Установка запрета осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` следующие строки:

```
# Установка запрета на использование информации об источнике пакета
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
```

Шаг 2

Для того, чтобы внесенные нами изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w net.ipv4.conf.all.accept_source_route = 0
[root@karlnext /]# sysctl -w net.ipv4.conf.default.accept_source_route =
0
```

Включение защиты от SYN-атак

SYN-атаки используют следующие особенности TCP/IP соединений. Обычно при установке соединения клиент посылает серверу пакет с SYN-битом (первого типа), в ответ на который сервер посылает клиенту пакет-подтверждение (второго типа). После получения подтверждения клиент отправляет серверу пакет, который завершает установку соединения (третьего типа). При этом сервер сохраняет в очереди данные первого пакета и использует их для идентификации клиента. Посылая серверу пакеты, содержащие SYN-бит и случайные IP-адреса источников и не высылая соответствующие им завершающие пакеты (третьего типа), злоумышленник может реализовать DoS-атаку, исчерпав ресурсы для хранения информации, содержащейся в пакетах первого типа. Для исключения такой возможности на сервере устанавливается такой алгоритм функционирования, при котором пакеты, содержащие SYN-бит не сохраняются вообще, а сервер идентифицирует клиента, выполняя соответствующие операции над информацией, содержащейся в пакетах третьего типа. Включение защиты осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` следующие строки:

```
#Включение защиты от TCP SYN атак
net.ipv4.tcp_syncookies = 1
```

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl –w net.ipv4.tcp_syncookies = 1
```

ICMP-переадресация

Когда компьютеры, находящиеся в сети, используют для пересылки пакетов неоптимальный или несуществующий маршрут, ICMP-переадресация используется маршрутизаторами для того, чтобы сообщить компьютерам правильный маршрут. В сетях со сложной топологией рекомендуется разрешение ICMP-переадресации. В небольших сетях ее следует отключить. При этом исключается возможность изменения злоумышленником таблиц маршрутизации на компьютерах сети путем отправки им поддельных ICMP-сообщений. Установка запрета на ICMP-переадресацию осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` следующие строки:

```
# Установка запрета  на ICMP переадресацию
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
```

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl –w net.ipv4.conf.all.accept_redirects = 0
[root@karlnext /]# sysctl –w net.ipv4.conf.default.accept_redirects = 0
```

Сообщения об ошибках сети

Шаг 1

Для получения информации об ошибках сети добавьте или откорректируйте в файле /etc/sysctl.conf следующие строки:

```
# Включение сообщений об ошибках сети
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w net.ipv4.icmp_ignore_bogus_error_responses =
1
```

Включение защиты от атак, основанных на фальсификации IP-адреса

При реализации атак, основанных на фальсификации IP-адреса (IP spoofing), злоумышленник отправляет в сеть пакеты с ложным обратным адресом, пытаясь переключить на свой компьютер соединения, установленные между другими компьютерами. При этом он может получить удаленный доступ к системе с правами доступа, равным правам доступа того пользователя, чье соединение с сервером было переключено на компьютер злоумышленника. Включение защиты осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле /etc/sysctl.conf следующие строки:

```
# Включение защиты от IP-spoofing
# Усиленная проверка
ipv4.conf.all.rp_filter = 2
net.ipv4.conf.default.rp_f liter = 2
# Простая проверка
#ipv4.conf.all.rp_filter = 1
#net.ipv4.conf.default.rp_f liter = 2
```

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w ipv4.conf.all.rp_filter = 2
[root@karlnext /]# sysctl -w net.ipv4.conf.default.rp_f liter = 2
```

Включение регистрации Spoofed, Source Routed и Redirect пакетов

Для получения информации о Spoofed, Source Routed и Redirect пакетах, которая может быть использована для анализа выявления попыток и механизмов взлома системы, необходимо установить следующие параметры.

Шаг 1

Добавьте или откорректируйте в файле /etc/sysctl.conf следующие строки:

```
# Включение регистрации Spoofed, Source Routed и Redirect пакетов
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
```

Шаг 2

Для того чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без ее перезагрузки:

```
[root@karlnext /]# sysctl -w net.ipv4.conf.all.log_martians = 1
[root@karlnext /]# sysctl -w net.ipv4.conf.all.log_martians = 1
```

Включение пересылки пакетов

Если система используется в качестве шлюза, прокси-сервера, VPN-сервера и т. п., необходимо включить пересылку пакетов с одной сети в другую. Это осуществляется следующим образом.

Шаг 1

Добавьте или откорректируйте в файле `/etc/sysctl.conf` следующие строки:

```
# Разрешаем пересылку пакетов
net.IPv4.IP_forward = 1
```

Шаг 2

Для того, чтобы внесенные изменения вступили в силу, перезагрузите сеть:

```
[root@karlnext /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@karlnext /]# sysctl -w IP_forward =1
```

ЗАМЕЧАНИЕ К включению этой опции нужно относиться с определенной степенью осторожности и использовать ее только в случае крайней необходимости, т. е. только если предполагается использование системы в качестве сервера, обеспечивающего пересылку пакетов. Подключать систему с включенной опцией `IP_forward` к сетям общего пользования можно только после настройки и тщательной проверки правильности настроек системы сетевой защиты и серверов, ограничивающих пересылку пакетов, например SQUID, FreeS/WAN VPN и т. п.

Авторы столкнулись с анекдотичной ситуацией, в которой некоторая московская фирма жаловалась на завышение объема трафика провайдером. Можно понять возмущение ее владельцев, когда в период с 02.00 до 07.00 1января провайдер выставил счет на несколько сотен мегабайт трафика. В это время все компьютеры (кроме шлюза, Web-сервера и почтового сервера), естественно, были выключены, а у единственного сотрудника службы безопасности, который в это время находился в офисе, было, на наш взгляд, железное алиби: «Я не умею включать компьютеры, и денег у вашего Интернета я не брал!..».

Детальный анализ ситуации (проверка настроек и включение дополнительных опций служб регистрации) показал, что сервера этой компании используются в качестве анонимного прокси-сервера для просмотра ресурсов эротического содержания пользователями из страны, в которой это делать, по-видимому, запрещено. В итоге деньги за трафик получали два провайдера – из далекой страны и московский. Последнему, естественно, платила московская фирма.

Глава 8

Настройка сети

В этой главе:

1. Конфигурационные файлы /etc/sysconfig/network-scripts/ifcfg-ethN
2. Конфигурационный файл /etc/resolv.conf
3. Конфигурационный файл /etc/hosts
4. Конфигурационный файл /etc/host.conf
5. Конфигурационный файл /etc/sysconfig/network
6. Проверка работоспособности сетевых настроек

В этой главе рассматриваются вопросы, связанные с конфигурационными файлами сетевых устройств и основными командами, используемыми для настройки сети. Перед продолжением работ по созданию оптимизированной и безопасной системы необходимо проверить все конфигурационные файлы, связанные с настройкой сети и убедиться, что все сконфигурировано правильно. И если в дальнейшем что-то не будет получаться, то будет твердая уверенность, что это уж точно не связано с настройками сети.

Конфигурационные файлы /etc/sysconfig/network-scripts/ifcfg-ethN

Файлы `/etc/sysconfig/network-scripts/ifcfg-ethN` используются системой для инициализации и настройки сетевых карт. Содержимое файла `/etc/sysconfig/network-scripts/ifcfg-eth0`, установленного по умолчанию можно посмотреть с помощью команды:

```
[root@dymatel /]#cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
IPADDR=172.16.181.100
NETMASK=255.255.255.0
NETWORK=172.16.181.0
BROADCAST=172.16.181.255
BOOTPROTO=static
DSERCTL=no
```

Вы можете изменить параметры сети для данного сетевого интерфейса, добавив или изменив в файле `/etc/sysconfig/network-scripts/ifcfg-eth0` соответствующие строки. Наиболее часто для конфигурации сетевых устройств используются следующие параметры.

Параметр `DEVICE=devicename`
определяет название физического сетевого устройства, в данном примере – eth0.

Параметр `ONBOOT=yes/no` о
определяет, активизируется ли сетевое устройство при загрузке или нет (`yes`-активизируется, `no` -нет).

Параметр `BOOTPROTO=proto`
определяет способ установки IP-адреса при загрузке системы. Например:

- `static` – при загрузке системы устанавливается статический IP-адрес (значение по умолчанию);
- `none` – при загрузке не используется никакой протокол;
- `bootp` – при загрузке системы используется протокол bootp;
- `dhcp` – при загрузке используется протокол dhcp.

Параметр `IPADDR=Ipaddr`
определяет IP-адрес, в данном примере 172.16.181.100.

Параметр `NETMASK=netmask`
определяет маску сети, в данном примере 255.255.255.0.

Параметр `NETWORK=network`
определяет адрес сети, в данном примере 172.16.181.0.

Параметр `BROADCAST=broadcast`
определяет широковещательный адрес, в данном примере 172.16.181.255.

Параметр `DSERCTL=yes/no`
определяет, разрешено ли обычным пользователям управлять сетевым интерфейсом (`yes`-разрешено, `no` - запрещено).

Предположим, что нам необходимо присвоить сетевому интерфейсу дополнительный IP-адрес – 172.16.181.101. Это можно реализовать следующим образом.

Шаг 1
Создайте копию файла `/etc/sysconfig/network-scripts/ifcfg-eth0`:

```
[root@dymatel /]# cp /etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/ifcfg-eth0:0
```

Шаг 2
Измените строку:

```
IPADDR=172.16.181.100
```

на:

```
IPADDR=172.16.181.101
```

Шаг 3
Перезагрузите сеть:

```
[root@dymatel /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Конфигурационный файл /etc/resolv.conf

Конфигурационный файл `/etc/resolv.conf` содержит IP-адреса DNS-серверов, используемых вашей системой для выполнения преобразований имени хостов в IP-адрес и обратно:

```
[root@dymatel /]# cat /etc/resolv.conf
search und
nameserver 172.16.181.200
nameserver 212.111.78.3
nameserver 212.111.80.3
```

Запросы к серверам имен делаются в том порядке, в котором они указаны в файле `/etc/resolv.conf`. То есть в рассматриваемом примере сначала осуществляется обращение к DNS-серверу 172.16.181.200, который находится внутри локальной сети, и только в случае, если он не дает ответа на запрос, обращение осуществляется к первичному и вторичному DNS-серверам провайдера. Наличие внутреннего DNS-сервера упрощает администрирование локальной сети, повышает быстродействие и несколько сокращает затраты на трафик.

Конфигурационный файл /etc/hosts

Конфигурационный файл `/etc/hosts` предназначен для установления взаимно однозначного соответствия между именами хостов и их IP-адресами без использования обращения к DNS-серверам. Этот файл имеет очень простую структуру:

```
[root@dymatel /]# cat /etc/hosts/
#IP- Адрес          Полное имя хоста         Псевдоним
127.0.0.1           localhost.localdomain    localhost
…
172.16.181.100      www.dymatel.und          dymatel
172.16.181.103      drwalbr.und              walbr
172.16.181.105      karlnext.und             karlnext
…
213.180.194.129     www.yandex.ru            y
…
```

Этот файл пришел к нам в качестве наследства из тех времен, когда сетевых ресурсов было очень мало, и на каждом компьютере содержалась информация о всех хостах. В настоящее время этот файл может использоваться для организации преобразования имен в IP-адреса в небольших сетях, не имеющих DNS-серверов (при этом копия файла должна быть установлена на каждом из компьютеров сети), для снижения загрузки DNS-серверов при обращении к часто запрашиваемым ресурсам и для организации возможности обращении к ресурсам по псевдонимам. Например, при предложенной конфигурации файла `/etc/hosts` обращение к ресурсам `www.dymatel.und` и `www.yandex.ru` возможно по их псевдонимам, соответственно – `dymatel` и `y`.

Конфигурационный файл /etc/host.conf

Конфигурационный файл `/etc/host.conf` используется для установки порядка, в котором осуществляются обращения к различным типам ресурсов, используемых для установки соответствия между именами хостов и их IP-адресами. Пример файла `/etc/host.conf`:

```
[root@dymatel /]# cat /etc/hosts.conf
#сначала осуществляется обращение к файлу
#/etc/hosts а затем к DNS-серверам
order hosts,bind
#Разрешена поддержка хостов с несколькими IP-адресами
multi on
```

Конфигурационный файл /etc/sysconfig/network

В файле `/etc/sysconfig/network` содержатся основные параметры настройки сети:

```
[root@dymatel /]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=www.dymatel.und
GATEWAY=172.16.181.200
GATEWAYDEV=eth0
DNS1=212.111.78.3
DNS2=212.111.80.3
```

Вы можете изменять настройки сети, варьируя следующие параметры:

- `NETWORKING=yes/no` – включает/выключает поддержку сетевых функций системы;
- `HOSTNAME=hostname` – устанавливает сетевое имя системы, в данном примере `www.dymatel.und`;
- `GATEWAY=IP_gw` – устанавливает IP-адрес шлюза;
- `GATEWAYDEV=dev_gv` - определяет физическое устройство, через которое осуществляется доступ к шлюзу, в данном примере – eth0.

Проверка работоспособности сетевых настроек

Шаг 1

Проверьте в соответствии с рекомендациями этой и предыдущей главы правильность установки параметров в следующих файлах:

- `/etc/sysctl.conf`;
- `/etc/sysconfig/network-scripts/ifcfg-ethN`;
- `/etc/resolv.conf`;
- `/etc/hosts` и `/etc/sysconfig/network`.

Шаг 2

Проверьте состояние сетевых интерфейсов:

```
[root@dymatel /]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:C0:26:AA:35:0C
          inet       addr:172.16.181.100             Bcast:172.16.181.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13152266 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13130468 errors:0 dropped:0 overruns:0 carrier:0
          collisions:56228 txqueuelen:100
          RX  bytes:4209088620  (4014.0  Mb)   TX  bytes:2575418894  (2456.1
Mb)
          Interrupt:11 Base address:0xd000

eth0:0    Link encap:Ethernet  HWaddr 00:C0:26:AA:35:0C
          inet       addr:172.16.181.102             Bcast:172.16.181.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:11 Base address:0xd000

eth1      Link encap:Ethernet  HWaddr 00:C0:26:AA:47:38
          inet       addr:192.168.14.85             Bcast:192.168.255.255
Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21285840 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10510 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1755892233 (1674.5 Mb)  TX bytes:2386737 (2.2 Mb)
          Interrupt:10 Base address:0xf000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:39809472 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:39809472 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3988297410 (3803.5 Mb)   TX bytes:3988297410 (3803.5
Mb)
```

В рассматриваемом примере на системе установлены две сетевых карты eth0 и eth1, причем eth0 имеет два IP-адреса – 172.16.181.100 и 172.16.181.102, а eth1 один – 192.168.14.85. Все сетевые интерфейсы активны.

Шаг 3
Проверьте связь с другими системами.
С системой в сети 172.16.181.103:

```
[root@www root]# ping -c 3 172.16.181.103
PING 172.16.181.103 (172.16.181.103) from 172.16.181.100 : 56(84) bytes
of data.
64 bytes from 172.16.181.103: icmp_seq=1 ttl=64 time=280 usec
64 bytes from 172.16.181.103: icmp_seq=2 ttl=64 time=287 usec
64 bytes from 172.16.181.103: icmp_seq=3 ttl=64 time=295 usec

--- 172.16.181.103 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 1998ms
rtt min/avg/max/mdev = 0.280/0.287/0.295/0.015 ms
```

С системой в сети 192.168.10.5:

```
[root@www root]# ping -c 3 192.168.10.5
PING 192.168.10.5 (192.168.10.5) from 192.168.14.85 : 56(84) bytes of
data.
64 bytes from 192.168.10.5: icmp_seq=1 ttl=64 time=1.625 msec
64 bytes from 192.168.10.5: icmp_seq=2 ttl=64 time=742 usec
64 bytes from 192.168.10.5: icmp_seq=3 ttl=64 time=671 usec

--- 192.168.10.5 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2004ms
rtt min/avg/max/mdev = 0.671/1.012/1.625/0.435 ms
```

С системой в Интернете:

```
[root@www root]# ping -c 3 213.180.194.129
PING 213.180.194.129 (213.180.194.129) from 172.16.181.100 : 56(84) bytes
of data.
64 bytes from 213.180.194.129: icmp_seq=1 ttl=56 time=15.627 msec
64 bytes from 213.180.194.129: icmp_seq=2 ttl=56 time=12.886 msec
64 bytes from 213.180.194.129: icmp_seq=3 ttl=56 time=12.207 msec

--- 213.180.194.129 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2023ms
rtt min/avg/max/mdev = 12.207/13.573/15.627/1.481 ms
```

Если вы получили отклики от других систем, аналогичные приведенным выше, то связь работает. В противном случае, т. е. при появлении вывода аналогичного этому:

```
[root@www root]# ping -c 3 192.168.10.5
PING 192.168.10.5 (192.168.10.5) from 192.168.14.85 : 56(84) bytes of
data.
From 192.168.14.85: icmp_seq=3 Destination Host Unreachable
From 192.168.14.85: icmp_seq=3 Destination Host Unreachable
From 192.168.14.85: icmp_seq=2 Destination Host Unreachable
From 192.168.14.85: icmp_seq=1 Destination Host Unreachable

--- 192.168.10.5 ping statistics ---
3 packets transmitted, 0 received, +4 errors, 100% loss, time 2018ms
, pipe 3
```

убедитесь, что выбранные для тестирования системы включены и в них не установлен запрет на ответ на ping-запросы. Если системы, используемые для тестирования, включены и способны отвечать на ping-

запросы, проверьте еще раз сетевые настройки (шаг 1), правильность подключения концентраторов и маршрутизаторов, кабели т. д.

Шаг 4
Проверьте правильность настроек DNS.
Работоспособность настроек в файле `/etc/hosts`:

```
[root@www root]# ping -c 3 drwalbr.und
PING drwalbr.und (172.16.181.103) from 172.16.181.100 : 56(84) bytes of
data.
64 bytes from drwalbr.und (172.16.181.103): icmp_seq=1 ttl=64 time=395
usec
64 bytes from drwalbr.und (172.16.181.103): icmp_seq=2 ttl=64 time=344
usec
64 bytes from drwalbr.und (172.16.181.103): icmp_seq=3 ttl=64 time=296
usec

--- drwalbr.und ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 1998ms
rtt min/avg/max/mdev = 0.296/0.345/0.395/0.040 ms

[root@www root]# ping -c 3 walbr
PING drwalbr.und (172.16.181.103) from 172.16.181.100 : 56(84) bytes of
data.
64 bytes from drwalbr.und (172.16.181.103): icmp_seq=1 ttl=64 time=392
usec
64 bytes from drwalbr.und (172.16.181.103): icmp_seq=2 ttl=64 time=293
usec
64 bytes from drwalbr.und (172.16.181.103): icmp_seq=3 ttl=64 time=292
usec

--- drwalbr.und ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 1999ms
rtt min/avg/max/mdev = 0.292/0.325/0.392/0.051 ms
```

Работоспособность настроек в файле `/etc/resolv.conf`:

```
[root@www root]# ping -c 3 www.yandex.ru
PING www.yandex.ru (213.180.194.129) from 172.16.181.100 : 56(84) bytes
of data.
64 bytes from yandex.ru (213.180.194.129): icmp_seq=1 ttl=56 time=16.812
msec
64 bytes from yandex.ru (213.180.194.129): icmp_seq=2 ttl=56 time=91.939
msec
64 bytes from yandex.ru (213.180.194.129): icmp_seq=3 ttl=56 time=17.107
msec

--- www.yandex.ru ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2019ms
rtt min/avg/max/mdev = 16.812/41.952/91.939/35.346 ms
```

Если вы получили отклики от удаленных систем в Интернет и локальных сетях, аналогичные приведенным выше, то настройки DNS – правильные. В противном случае, т. е. при появлении вывода аналогичного этому:

```
[root@www root]# ping –c 3 www.yandex.ru
ping: unknown host www.yandex.ru
```

проверьте содержимое файлов `/etc/hosts` и `/etc/resolv.conf`.

Шаг 5
Проверьте таблицу маршрутизации:

```
[root@www root]# route -n
Destination  Gateway      Genmask    Flags Metric Ref Use Iface
172.16.181.0 0.0.0.0      255.255.255.0 U     0   0   0   eth0
192.168.0.0  0.0.0.0      255.255.0.0   U     0   0   0   eth1
```

```
127.0.0.0    0.0.0.0      255.0.0.0     U     0   0   0   lo
0.0.0.0      172.16.181.1 0.0.0.0       UG    0   0   0   eth0
```

Шаг 6

Проверьте статистику TCP/IP соединений:

```
[root@dymatel /]# netstat –vat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address   Foreign Address   State
tcp        0      0 *:http          *:*               LISTEN
tcp        0      0 *:https         *:*               LISTEN
```

Шаг 7

Проверьте правильность установки сетевого имени системы:

```
[root@dymatel /]# hostname
www.dymatel.und
```

Часть 2

Система сетевой защиты

Глава 9

Основные положения системы сетевой защиты (Firewall)

В этой главе:

1. Концепция безопасности системы сетевой защиты
2. Порты
3. Ограничения и допущения
4. Пакеты
5. Компиляция оптимизация и инсталляция IPTables из rpm -пакетов
6. Компиляция оптимизация и инсталляция IPTables из исходных кодов
7. Настройка системы сетевой защиты IPTables
8. Проверка настроек сетевой защиты

В этой главе рассматриваются основные принципы и понятия, связанные с системой сетевой защиты (Firewall). К настоящему времени разработаны и активно развиваются системы сетевой защиты, основанные на следующих технологиях.

Первый тип – фильтрация пакетов(packet filtering) – тип встроенной в ядро сетевой защиты, работающей на сетевом уровне. Пакеты фильтруются в соответствии с их типом, исходным адресом, адресом назначения и информацией о порте, содержащейся в заголовке пакета. Такой тип сетевой защиты основан на анализе небольшого объема информации, поэтому мало влияет на загрузку центрального процессора и не создает заметных задержек в работе сети.

Первое поколение данного типа фильтрации, известное в Linux как IPCHAINS, реализовывало статическую схему сетевой защиты, при которой соединения между внутренними и внешними сетями всегда оставались открытыми для портов, используемых работающими на системе службами. Такая система сетевой защиты реализована в ядрах версий 2.2.x. Основной недостаток этого типа защиты состоит в том, что для нормального функционирования системы необходимо все время держать открытыми ряд портов.

Второе поколение – так называемые динамические пакетные фильтры (Dynamic Packet Filters), известные в Linux, как программа сетевой защиты IPTables, используемая в версиях ядра 2.4.x. При такой системе фильтрации соответствующий порт открывается только на время прохождения легитимного исходящего пакета, либо для приема ожидаемого системой пакета. Ядра Linux версии 2.4.x поддерживают новый механизм для формирования системы сетевой защиты, называемый сетевой пакетной фильтрацией (netfilter). Он более сложен, чем предыдущий механизм (IPCHAINS), но более безопасен. Блокирует большинство DoS-атак. В случае, если инородный пакет пытается проникнуть в защищаемую систему или сеть под видом пакета, принадлежащего существующему соединению, IPTables может свериться со своим хранящимся в памяти списком открытых соединений, обнаружить, что пакет не соответствует ни одному из них, и запретить его пропуск.

Общими недостатками систем сетевой защиты, основанных на фильтрации пакетов, являются:

- возможность подключения систем, находящихся за пределами локальной сети, к системам внутри неё;
- отсутствие возможности селекции пакетов по пользователям с реализацией соответствующей идентификации.

Второй тип систем сетевой защиты, так называемые прокси-программы (application gateway), известные в Linux как Squid. Это программное обеспечения детально анализирует информацию, заключенную в теле пакетов, перед тем, как разрешить доступ в сеть пользователю из внешней сети. Запрещает прямые соединения между внутренними и внешними системами, поддерживает идентификацию пользователей.

Концепция безопасности системы сетевой защиты

Существует два подхода к концепции безопасности.

«Все, что не разрешено – то запрещено». При таком подходе блокируется весь трафик между внешней и внутренней сетями, за исключением трафика, генерируемого разрешенными службами и приложениями. Такая концепция безопасности наиболее эффективна, однако создает определенные неудобства для пользователей и требует больших трудозатрат на администрирование сети для реализации конкретных требований пользователей (у меня не работает «мирка», «аська», не могу скачать последнюю версию программы с неправильно настроенного FTP-сервера, не слышу Web-радио и т. п.).

«Все, что не запрещено – то разрешено». При таком подходе разрешается весь трафик между двумя сетями, за исключением некоторого перечня служб и приложений. Это очень удобно для пользователей, но с точки зрения авторов, не обеспечивает приемлемый уровень безопасности.

Поэтому авторы настоятельно рекомендуют использовать именно первый вариант концепции системы сетевой защиты.

Порты

IANA (Internet Assigned Numbers Authority) образован международными организациями ISOC (Internet Society) и FNC (Federal Network Council) как центр обмена информацией для определения и координирования использования параметров протоколов Интернет. Одним из таких параметров являются номера портов, закрепленные за определенной службой. Например, если вы разработали новый (ранее не существующий) тип службы, например, службу управления специфичными бытовыми устройствами в вашем доме, IANA должна будет зарегистрировать и обслуживать уникальный номер порта, выделенный для этой программы.

Понятие «порт» было введено для организации одновременного соединения с многочисленными службами Интернет. Каждый компьютер имеет 65535 доступных портов. Так называемые «хорошо известные» (well known) порты имеют номера в диапазоне от 0 до 1023. Эти порты, в большинстве случаев, используются системными процессами или программами, выполняемыми привилегированными пользователями в фоновом режиме (службами). Зарегистрированные (registered) порты имеют номера в диапазоне от

1024 до 49151, но на большинстве систем могут использоваться любыми приложениями. Динамические порты (dynamic или private) имеют номера в диапазоне 49152…65535.

Все открытые порты должны иметь службу (демон), которая на нем выполняется, т. е. обслуживает обращающихся к этому порту пользователей. Если служба на некотором порту не выполняется, то он должен быть закрыт.

Ограничения и допущения

Все операции выполняются пользователем с учетной записью `root`.

Используется ядро версии 2.4.x.

Используется дистрибутив ASPLinux 7.3 (Vostok). На других дистрибутивах возможно успешное выполнение подобной процедуры, но авторы этого не проверяли.

Пакеты

В дистрибутив ASPLinux 7.3 (Vostok) входит пакет `iptables-1.2.6a-1.asp`, используемый для установки системы сетевой защиты. Ее поддержка также включена в ядро, устанавливаемое по умолчанию. Если вы следовали рекомендациям по инсталляции нового ядра, то пакет, поставляемый с дистрибутивом, сохраняет свою работоспособность и не требует перекомпиляции ядра. Однако, используя новое ядро с персональной конфигурацией, из-за наличия неудовлетворенных зависимостей, вы не сможете установить пакет `iptables-1.2.6a-1.asp`, входящий в состав дистрибутива, или обновленный пакет, который может быть выпущен поставщиком дистрибутива. В этом случае придется устанавливать IPTables из исходных кодов.

Последующие рекомендации основаны на информации с домашней страницы проекта NetFilter/IPTables, полученной 01.02.2003. Пожалуйста, регулярно посещайте домашнюю страницу проекта `http://www.iptables.org/` или `http://www.iptables.org/` для отслеживания обновлений. Основная часть кода, используемая для системы сетевой защиты, включается в состав ядра. Разработчики IPTables не могут гарантировать, что последние изменения внесены в официальный релиз ядра, размещаемый на `http://www.kernel.org.` Поэтому все необходимые для нормальной работы системы сетевой защиты изменения в код ядра содержатся в пакете `patch-o-matic-YYYYMMDD.tar.bz2` (последний, доступный на момент написания книги, - `patch-o-matic-20030107.tar.bz2`). Часть кода, не входящая в ядро, содержится в пакете `iptables-version.tar.bz2` (последний, доступный на момент написания книги, - `iptables-1.2.7a.tar.bz2`).

Необходимые пакеты доступны с домашней страницы разработчиков `http://www.iptables.org` или `http://www.iptables.org`, `а также` FTP-сервера `ftp://ftp.netfilter.org.`

Компиляция оптимизация и инсталляция IPTables из rpm-пакетов

Если вы используете пакет `iptables-1.2.6a-1.asp`, входящий в состав дистрибутива ASPLInux 7.3 (Vostok), то вам необходимо сделать следующее.

Шаг 1

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет `iptables` с помощью следующей команды:

```
[root@bastion /]# rpm –iq iptables
```

Если вы следовали нашим рекомендациям, то он должен быть уже установлен.

Если пакет не установлен, перейдите в каталог, где находится пакет `iptables-1.2.6a-1.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@bastion /]# cd /home/distrib
```

и установите:

```
[root@bastion distrib]# rpm –ihv iptables-1.2.6a-1.asp.i386.rpm
```

или обновите пакет:

```
[root@bastion distrib]# rpm –Uhv iptables-1.2.6a-1.asp.i386.rpm
```

Шаг 2

Как уже отмечалось, поддержка системы сетевой защиты осуществляется на уровне ядра. Для того, чтобы она могла функционировать на вашей системе, необходимо при настройке ядра установить или проверить правильность установки опций, связанных с функционированием системы сетевой защиты, в соответствии с рекомендациями, приведенными ниже в главе 6.

Для всех серверов, кроме шлюзов и прокси-серверов:

```
* Packet socket (CONFIG__PACKET) [Y/n/?] <Enter>
```

Эта опция включает/отключает поддержку приложений, которые связываются непосредственно с сетевыми устройствами без использования промежуточного сетевого протокола, осуществленного в ядре, подобно программе tcpdump.

```
Packet socket: mmapped IO (CONFIG_PACKET_MMAP) [N/y/?] <y>
```

Эта опция включает/отключает ускорение работы драйвера пакетов.

```
Netlink device emulation (CONFIG_NETLINK_DEV) [N/y/?] (NEW) <y>
```

Эта опция обеспечивает обратную совместимость.

```
Network packet filtering (replaces ipchains) (CONFIG_NETFILTER) [N/y/?]
<y>
```

Эта опция включает/отключает поддержку Firewall.

```
Network packet filtering debugging (CONFIG_NETFILTER_DEBUG) [N/y/?] (NEW)
<y>
```

Эта опция включает/отключает поддержку отладки кода netfilter.

```
Socket Filtering (CONFIG_FILTER) [N/y/?] <Enter>
```

Эта опция включает/отключает поддержку фильтра Linux Socket Filter, необходимого для реализации фильтрации пакетов PPP соединений.

```
Unix domain sockets (CONFIG_UNIX) [Y/n/?] <Enter>
```

Опция включает/отключает поддержку работы с сетями TCP/IP.

```
TCP/IP networking (CONFIG_INET) [Y/n/?] <Enter>
```

Опция включает/отключает поддержку работы с сетями TCP/IP.

```
IP: multicasting (CONFIG_IP_MULTICAST) [Y/n/?] <n>
```

Эта опция необходима для реализации сетевых мультимедийных технологий.

```
IP: advanced router (CONFIG_IP_ADVANCED_ROUTER) [N/y/?] <n>
```

Эта опция позволяет конфигурировать систему как шлюз. В случае включения этой опции необходимо ответить на ряд дополнительных вопросов.

```
IP: kernel level autoconfiguration (CONFIG IP_PNP) [N/y/?] <Enter>
```

Включение этой опции необходимо только для бездисковых рабочих станций, требующих доступа к сети для загрузки.

```
IP: tunneling (CONFIG_NET_IPIP) [N/y/?] <Enter>
```

Эта опция включает поддержку туннелирования. Её использование необходимо, например, при подключении сервера к сети через VPN-подключение.

```
IP: GRE tunnels over IP (CONFIG_NET_IPGRE) [N/y/?] <Enter>
```

Другой вид настройки туннелирования. Её использование необходимо, например, при подключении сервера к сети через VPN-подключение.

```
IP: TCP Explicit Congestion Notification support (CONFIG_INET_ECN)
[N/y/?] <Enter>
```

Опция включает/отключает поддержку уведомления клиентов о перегрузке системы. К сожалению, многие сервера отказывают в доступе тем системам, на которых включена эта опция, из соображений безопасности.

```
IP: TCP syncookie support (disabled per default) (CONFIG_SYN_COOKIES)
[N/y/?] Y
```

Эта опция включает/отключает поддержку защиты от SYN-атак.

```
*
*IP: Netfilter Configuration
*
Connection tracking (required for masq/NAT) (CONFIG_IP_NF_CONNTRACK)
[N/y/?] (NEW) <y>
FTP protocol support (CONFIG_IP_NF_FTP) [N/y/?] (NEW) <y>
IRC protocol support (CONFIG_IP_NF_IRC) [N/y/?] (NEW) <Enter>
IP tables support (required for filtering/masq/NAT)
(CONFIG_IP_NF_IPTABLES) [N/y/?] (NEW) <y>
limit match support (CONFIG_IP_NF_MATCH_LIMIT) [N/y/?] (NEW) <y>
MAC address match support (CONFIG_IP_NF_MATCH_MAC) [N/y/?] (NEW) <y>
netfilter MARK match support (CONFIG_IP_NF_MATCH_MARK) [N/y/?] (NEW) <y>
Multiple port match support (CONFIG_IP_NF_MATCH_MULTIPORT) [N/y/?] (NEW)
<y>
TOS match support (CONFIG_IP_NF_MATCH_TOS) [N/y/?] (NEW) <y>
LENGTH match support (CONFIG_IP_NF_MATCH_LENGTH) [N/y/?] (NEW) <y>
TTL match support (CONFIG_IP_NF_MATCH_TTL) [N/y/?] (NEW) <y>
tcpmss match support (CONFIG_IP_NF_MATCH_TCPMSS) [N/y/?] (NEW) <y>
Connection state match support (CONFIG_IP_NF_MATCH_STATE) [N/y/?] (NEW)
<y>
Packet filtering (CONFIG_IP_NF_FILTER) [N/y/?] (NEW) <y>
REJECT target support (CONFIG_IP_NF_TARGET_REJECT) [N/y/?] (NEW) <y>
Full NAT (CONFIG_IP_NF_NAT) [N/y/?] (NEW) <Enter>
Packet mangling (CONFIG_IP_NF_MANGLE) [N/y/?] (NEW) <y>
TOS target support (CONFIG_IP_NF_TARGET_TOS) [N/y/?] (NEW) <y>
MARK target support (CONFIG_IP_NF_TARGET_MARK) [N/y/?] (NEW) <y>
LOG target support (CONFIG_IP_NF_TARGET_LOG) [N/y/?] (NEW) <y>
TCPMSS target support (CONFIG IP NF_TARGET_TCPMSS) [N/y/?] (NEW) <y>
```

Для шлюзов и прокси-серверов.

```
* Packet socket (CONFIG__PACKET) [Y/n/?] <Enter>
```

Эта опция включает/отключает поддержку приложений, которые связываются непосредственно с сетевыми устройствами без использования промежуточного сетевого протокола, осуществленного в ядре, подобно программе tcpdump.

```
Packet socket: mmapped IO (CONFIG_PACKET_MMAP) [N/y/?] <y>
```

Эта опция включает/отключает ускорение работы драйвера пакетов.

```
Netlink device emulation (CONFIG_NETLINK_DEV) [N/y/?] (NEW) <y>
```

Эта опция обеспечивает обратную совместимость.

```
Network packet filtering (replaces ipchains) (CONFIG_NETFILTER) [N/y/?]
<y>
```

Эта опция включает/отключает поддержку Firewall.

```
Network packet filtering debugging (CONFIG_NETFILTER_DEBUG) [N/y/?] (NEW)
<y>
```

Эта опция включает/отключает поддержку отладки кода netfilter.

```
Socket Filtering (CONFIG_FILTER) [N/y/?] <y>
```

Эта опция включает/отключает поддержку фильтра Linux Socket Filter, необходимого для реализации фильтрации пакетов PPP-соединений.

```
Unix domain sockets (CONFIG_UNIX) [Y/n/?] <y>
```

Опция включает/отключает поддержку работы с сетями TCP/IP.

```
TCP/IP networking (CONFIG_INET) [Y/n/?] <Enter>
```

Опция включает/отключает поддержку работы с сетями TCP/IP.

```
IP: multicasting (CONFIG_IP_MULTICAST) [Y/n/?] <Y>
```

Эта опция необходима для реализации сетевых мультимедийных технологий.

```
IP: advanced router (CONFIG_IP_ADVANCED_ROUTER) [N/y/?] <y>
```

Эта опция позволяет конфигурировать систему как шлюз. В случае включения этой опции необходимо ответить на ряд дополнительных вопросов.

```
IP: policy router (CONFIG_IP_MULTIPLE_TABLES) [N/y/?] <y>
IP: use netfilter MARK value as routing key (CONFIG_IP_ROUTE_FWMARK)
[N/y/?] <y>
IP: fast network address translation (CONFIG_IP_ROUTE_NAT) [N/y/?] <y>
IP: equal cost multipath (CONFIG_IP_ROUTE_MULTIPATH) [N/y/?] <y>
IP: use TOS value as routing key(CONFIG_IP_ROUTE_TOS) [N/y/?] <y>
IP: verbose route monitoring (CONFIG_IP_ROUTE_VERBOSE) [N/y/?] <y>
IP: large routing tables (CONFIG_IP_ROUTE_LARGE_TABLES) [N/y/?] <y>
IP: kernel level autoconfiguration (CONFIG_IP_PNP) [N/y/?] <Enter>
```

Включение этой опции необходимо только для бездисковых рабочих станций, требующих доступа к сети для загрузки.

```
IP: tunneling (CONFIG_NET_IPIP) [N/y/?] <y>
```

Эта опция включает поддержку туннелирования. Её использование необходимо, например, при подключении сервера к сети через VPN-подключение.

```
IP: GRE tunnels over IP (CONFIG_NET_IPGRE) [N/y/?] <y>
```

Другой вид настройки туннелирования. Её использование необходимо, например, при подключении сервера к сети через VPN-подключение.

```
IP: TCP Explicit Congestion Notification support (CONFIG_INET_ECN)
[N/y/?] <Enter>
```

Опция включает/отключает поддержку уведомления клиентов о перегрузке системы. К сожалению, многие сервера отказывают в доступе тем системам, на которых включена эта опция, из соображений безопасности.

```
IP: TCP syncookie support (disabled per default) (CONFIG_SYN_COOKIES)
[N/y/?] Y
```

Эта опция включает/отключает поддержку защиты от атак типа "SYN-flood".

```
*
*IP: Netfilter Configuration
*
Connection tracking (required for masq/NAT) (CONFIG_IP_NF_CONNTRACK)
[N/y/?] (NEW) <y>
FTP protocol support (CONFIG_IP_NF_FTP) [N/y/?] (NEW) <y>
IRC protocol support (CONFIG_IP_NF_IRC) [N/y/?] (NEW) <y>
IP tables support (required for filtering/masq/NAT)
(CONFIG_IP_NF_IPTABLES) [N/y/?] (NEW) <y>
limit match support (CONFIG_IP_NF_MATCH_LIMIT) [N/y/?] (NEW) <y>
MAC address match support (CONFIG_IP_NF_MATCH_MAC) [N/y/?] (NEW) <y>
netfilter MARK match support (CONFIG_IP_NF_MATCH_MARK) [N/y/?] (NEW) <y>
Multiple port match support (CONFIG_IP_NF_MATCH_MULTIPORT) [N/y/?] (NEW)
<y>
TOS match support (CONFIG_IP_NF_MATCH_TOS) [N/y/?] (NEW) <y>
LENGTH match support (CONFIG_IP_NF_MATCH_LENGTH) [N/y/?] (NEW) <y>
TTL match support (CONFIG_IP_NF_MATCH_TTL) [N/y/?] (NEW) <y>
tcpmss match support (CONFIG_IP_NF_MATCH_TCPMSS) [N/y/?] (NEW) <y>
Connection state match support (CONFIG_IP_NF_MATCH_STATE) [N/y/?] (NEW)
<y>
Packet filtering (CONFIG_IP_NF_FILTER) [N/y/?] (NEW) <y>
REJECT target support (CONFIG_IP_NF_TARGET_REJECT) [N/y/?] (NEW) <y>
Full NAT (CONFIG_IP_NF_NAT) [N/y/?] (NEW) <y>
MASQURADE target support (CONFIG_IP_NF_TARGET_MARK) [N/y/?] (NEW) <y>
REDIRECT target support (CONFIG_IP_NF_TARGET_REDIRECT) [N/y/?] (NEW) <y>
Packet mangling (CONFIG_IP_NF_MANGLE) [N/y/?] (NEW) <y>
TOS target support (CONFIG_IP_NF_TARGET_TOS) [N/y/?] (NEW) <y>
MARK target support (CONFIG_IP_NF_TARGET_MARK) [N/y/?] (NEW) <y>
LOG target support (CONFIG_IP_NF_TARGET_LOG) [N/y/?] (NEW) <y>
TCPMSS target support (CONFIG_IP_NF_TARGET_TCPMSS) [N/y/?] (NEW) <y>
ipchains (2.2 style) support (CONFIG_IP_NF_COMPAT_IPCHAINS) [N/y/?] (NEW)
<y>
ipchains (2.0 style) support (CONFIG_IP_NF_COMPAT_IPWADM) [N/y/?] (NEW)
<y>
```

Шаг 3

Настройте, перекомпилируйте и инсталлируйте ядро в соответствии с одним из приведенных выше вариантов конфигурации и инструкциями, изложенными в главе 6.

ЗАМЕЧАНИЕ Если вы следовали инструкциям, изложенным в главе 6, то в настройке, перекомпиляции и инсталляции ядра нет необходимости. В этом случае достаточно лишь проверить правильность установки опций, связанных с настройкой подсистемы сетевой безопасности ядра.

Компиляция оптимизация и инсталляция IPTables из исходных кодов

Для установки IPTables из исходных кодов необходимо сделать следующее. Авторы протестировали работоспособность приведенных ниже рекомендаций для ядра версии 2.4.19 с наложенным на исходные коды патчем `grsecurity-1.9.7d-2.4.19`.

Шаг 1

Распакуйте архив с патчем `patch-o-matic-20030107.tar.bz2` (этот патч применим к ядрам версии 2.4.18…2.4.20) в каталоге `/var/tmp`:

```
[root@bastion tmp]# /usr/bin/bunzip2 patch-o-matic-20030107.tar.bz2
[root@bastion tmp]# tar –xpf patch-o-matic-20030107.tar
```

Шаг 2

Примените патч к исходным кодам ядра:

```
[root@bastion tmp]# cd  patch-o-matic-20030107
[root@bastion patch-o-matic-20030107]# make
KERNEL_DIR=path_to_kernel_source patching_option
```

Параметр `path_to_kernel_source`
задает путь к каталогу, в который распакованы исходные коды ядра, инсталлированного в вашей системе. В рассматриваемом примере – `KERNEL_DIR=/usr/src/linux-2.4.19`.

Параметр `patching_option`
определяет степень модификации исходных кодов ядра.

Параметр `pending-patches`
означает, что при применении патча будут изменены только те фрагменты кодов ядра, которые содержат наиболее существенные ошибки и в любом случае будут учтены группой разработчиков кода ядра.

Параметр `most-of-pom`
внесет все из наиболее существенных, не противоречащих друг другу изменений, предлагаемых группой разработчиков IPTables.

Параметр `patch-o-matic`
предназначен для экспертов в области сетевой безопасности и позволяет самостоятельно добавлять, удалять и получать информацию о каждом из патчей, применяемом к исходным кодам ядра. Если вы эксперт в области сетевой безопасности, то вряд ли вы будете читать этот раздел и книгу в целом. Для остальных читателей, желающих поэкспериментировать с различными вариантами модификации исходных кодов ядра, может оказаться полезным ознакомление, по крайней мере, с Netfilter Hacking HOWTO и Netfilter Extensions HOWTO, которые можно найти по адресу `http://www.netfilter.org/documentation/index.html#HOWTO`.

Шаг 3

Распакуйте архив с пакетом `iptables-1.2.7a.tar.bz2` в каталоге `/var/tmp`:

```
[root@bastion tmp]# /usr/bin/bunzip2 iptables-1.2.7a.tar.bz2
[root@bastion tmp]# tar –xpf iptables-1.2.7a.tar
```

Шаг 4

Удалите старую версию пакета `iptables`, если она установлена. Если `iptables` был установлен из rpm-пакета, например, при первичной установке с поставляемого дистрибутива, выполните:

```
[root@bastion tmp]# rpm -e iptables
```

Если пакет устанавливался из исходных текстов, то наберите:

```
[root@bastion tmp]# rm –rf list_installed_files
```

Параметр `list_of_installed_files` представляет собой список файлов, установленных в системе при инсталляции `iptables` из исходных кодов, разделенных пробелами. Описание команд для создания перечня установленных файлов приведено ниже.

Шаг 5

Перейдите в каталог `/var/tmp/iptables-1.2.7a`:

```
[root@bastion tmp]# cd  iptables-1.2.7a.tar
```

Откомпилируйте исходный код `iptables-1.2.7a`:

```
[root@bastion iptables-1.2.7a]# make KERNEL_DIR=/usr/src/linux-2.4.19.
BINDIR=/sbin LIBDIR=/lib/iptables MANDIR=/usr/share/man/man8
```

Установите `iptables-1.2.7a`:

```
[root@bastion iptables-1.2.7a]# find /* > /var/tmp/iptables.1.txt
[root@bastion iptables-1.2.7a]# make KERNEL_DIR=/usr/src/linux-2.4.19.
BINDIR=/sbin LIBDIR=/lib/iptables MANDIR=/usr/share/man/man8
```

Создайте и сохраните в надежном месте список файлов IPTables, установленных на системе:

```
[root@bastion iptables-1.2.7a]# find /* > /var/tmp/iptables.2.txt
[root@bastion iptables-1.2.7a]# diff /var/tmp/iptables.1.txt
/var/tmp/iptables.2.txt > /var/tmp/iptables.installed.txt
[root@bastion iptables-1.2.7a]# mv iptables.installed.txt
/very_reliable_place/iptables.installed.YYYYMMDD.txt /
```

Шаг 6

Осуществите в соответствии с назначением системы и рекомендациями, изложенными выше, настройку, компиляцию и инсталляцию нового ядра, к исходным кодам которого был применен патч `patch-o-matic-20030107`. Инструкции по настройке компиляции и инсталляции ядра содержатся в главе 6.

Шаг 7

Удалите каталоги с исходными кодами ядра, патча `patch-o-matic-20030107` и `iptables-1.2.7a` и их архивы**:**

```
[root@bastion iptables-1.2.7a]# rm –rf /usr/src/linux-2.4.19
[root@bastion iptables-1.2.7a]# rm –rf /var/tmp/patch-o-matic-20030107
[root@bastion iptables-1.2.7a]# rm –rf /var/tmp/iptables-1.2.7a
[root@bastion iptables-1.2.7a]# rm –f /var/tmp/ iptables-1.2.7a.tar
[root@bastion iptables-1.2.7a]# rm –f /var/tmp/ patch-o-matic-
20030107.tar
```

Настройка системы сетевой защиты IPTables

IPTables используется для отправки, переадресации, организации маскарадинга (masquarade) и фильтрации пакетов, входящих в сеть или исходящих из нее. В настоящее время существуют четыре главных подсистемы, но только три действительно важны для работы IPTables:

- подсистема классификации пакетов;
- подсистема мониторинга подключений (connection-tracking system);
- подсистема трансляции адресов (network address translation).

Обычно правила, определяющие, что же должна делать система сетевой защиты, передаются ей в виде команд:

```
[root@bastion /]# /sbin/iptables RULE
```

Параметр `RULE` представляет собой некоторое правило в виде набора опций команды `iptables`. Набор правил также может быть оформлен в виде скрипта командного интерпретатора, содержащего команды, аналогичные приведенной выше. Подробное описание настроек сетевой защиты, применительно даже к типовым вариантам ее конфигурации, может являться темой для отдельной книги и не может быть рассмотрено в пределах одной главы.

Ниже приведены три примера, демонстрирующие возможность управления подсистемами классификации пакетов, мониторинга подключений и трансляции адресов. Для желающих детально изучить систему сетевой защиты рекомендуем, по крайней мере, ознакомиться с документом Iptables Tutorial, автором которого является Оскар Андреассон (Oskar Andreasson). Последнюю версию этого документа можно получить с `http://www.netfilter.org/documentation/tutorials/blueflux/` или воспользоваться одной из версий перевода на русский язык этого документа, сделанного Андреем Киселевым. Для тех, кто не жела-

ет или не имеет времени на детальное изучение системы сетевой безопасности, настоятельно рекомендуем изучить материалы следующей главы, где рассматриваются вопросы, связанные с установкой и настройкой GIPTables Firewall. Этот программный продукт прост в установке и настройке, и позволяет автоматически генерировать правила IPTables для систем различного целевого назначения с одной или двумя сетевыми картами.

Правила IPTables используются для определения того, что вы хотите сделать с входящими и исходящими пакетами. По умолчанию существуют три цепочки правил:

- для входящих пакетов используется цепочка правил `INPUT`;
- для исходящих – `OUTPUT`;
- для перенаправляемых – `FORWARD`.

Для изменения концепции безопасности используйте команду:

```
[root@bastion /]# /sbin/iptables –policy CHAIN TARGET
```

Параметр `CHAIN` содержит имя цепочки правил (например, `INPUT`, `OUTPUT` или `FORWARD`), для которой изменяется концепция безопасности. `TARGET` – имя концепции (например, `ACCESS` или `DROP`).

Для добавления нового правила к цепочке используется опция `–A`. Для определения протокола, к которому относится опция, используется опция `–p`. Для определения IP-адреса отправителя и получателя – опции `–s` и `–d`, соответственно. Для ограничения диапазона портов отправителя и получателя, к которым применимо правило – опции `--sport` и `--dport`, соответственно. Определение, какие сетевые устройства используются для входящих и исходящих пакетов, осуществляется с помощью опций `–i` и `–o`, соответственно.

Для работы подсистемы классификации соединений создайте правила, запрещающие доступ входящих и исходящих пакетов через внешний интерфейс к Web-серверу. Для этого добавьте к цепочке правил для входящих пакетов (`-A INPUT`) новое правило, которое запретит доступ всех пакетов (`-J DROP`) через интерфейс eth0 (`-i eth0`) с использованием протокола TCP (`-p tcp`) со всех адресов (`-s 0.0.0.0`) в диапазоне номеров портов 1024…65535 (`--sport 1024:65535`) на IP-адрес внешнего интерфейса 212.45.28.122 (`-d 212.45.28.122`) к порту службы `httpd` (`--dport 80`):

```
[root@bastion /]# /sbin/iptables -A INPUT -i eth0 -p TCP -s 0.0.0.0 --
sport 1024:65535 -d 212.45.28.122 --dport 80 -j DROP
```

Добавьте к цепочке правил для исходящих пакетов (`-A OUTPUT`) новое правило, которое запретит отправку всех пакетов (`-J DROP`) через интерфейс eth0 (`-i eth0`) с использованием протокола TCP (`-p tcp`), с адреса (`-s 212.45.28.122`) порта 80 (`--sport 80`) на любой IP-адрес (`-d 0.0.0.0`) в диапазоне портов 1024…65535 (`--dport 1024:65535`):

```
[root@bastion /]# /sbin/iptables -A OUTPUT -o eth0 -p tcp -s
212.45.28.122 --sport 80 -d 0.0.0.0 --dport 1024:65535  -j DROP
```

Подсистема мониторинга подключений отслеживает соединения и позволяет селектировать принадлежность пакетов к следующим типам соединений:

- вновь устанавливаемым;
- уже установленным;
- создаваемым с уже установленными соединениями;
- не установленной принадлежности.

В правилах IPTables для характеристики каждого из типов пакетов, соответственно, используются опции `NEW`, `ESTABLISH`, `RELATED` и `INVALID`.

Для иллюстрации работы подсистемы мониторинга соединений создайте правила:

- разрешающие прием пакетов для устанавливаемых новых соединений;
- разрешающие прием пакетов, принадлежащих уже установленным соединениям;
- разрешающие отправку исходящих пакетов только для уже существующих соединений.

Для этого добавьте к цепочке правил для входящих пакетов (`-A INPUT`) новое правило, которое разрешает прием всех пакетов (`–J ACCEPT`), которые устанавливают новые соединения, инициализируемые вашей системой, или уже связаны с установленными соединениями (`-m state --state NEW, ESTABLISHED`) через интерфейс eth0 (`-i eth0`) с использованием протокола TCP (`-p tcp`) со всех адресов (`-s 0.0.0.0`) в диапазоне номеров портов 1024…65535 (`--sport 1024:65535`) на IP-адрес внешнего интерфейса 212.45.28.122 (`-d 212.45.28.122`) к порту службы `httpd` (`--dport 80`):

```
[root@bastion /]# /sbin/iptables -A INPUT -i eth0 -p TCP -s 0.0.0.0 --
sport 1024:65535 -d 212.45.28.122 --dport 80 -m state --state NEW,
ESTABLISHED -j ACCEPT
```

Добавьте к цепочке правил для входящих пакетов (`-A OUTPUT`) новое правило, которое разрешает отправление всех пакетов (`-J ACCEPT`), которые связаны с существующими соединениями (`-m state --state ESTABLISHED`) с интерфейса eth0 (`-i eth0`) с использованием протокола TCP (`-p tcp`) с адреса 212.45.28.122 (`-s 212.45.28.122`) порта 80 (`--sport 1024:65535`) на любой IP-адрес (`-d 0.0.0.0`) в диапазоне номеров портов 1024…65535 (`--sport 1024:65535`):

```
[root@bastion /]# /sbin/iptables -A OUTPUT -o eth0 -p TCP -s
212.45.28.122 --sport 80 -d 0.0.0.0 --dport 1024:65535 -m state --state
ESTABLISHED -j ACCEPT
```

Подсистема трансляции сетевых адресов транслирует IP-адреса локальной сети в адреса внешней сети. Например, она используется для организации шлюзов, в том числе, и поддерживающих, так называемый, маскарадинг, для более эффективного распределения нагрузки на системы сети и т. п. Подсистема трансляции адресов содержит две цепочки правил `PREROUTING` и `POSTROUTING`. Первая из них содержит набор правил для входящих пакетов, вторая для исходящих.

Для иллюстрации работы подсистемы трансляции адресов создайте правило, которое маскирует все пакеты, исходящие из вашей внутренней сети под пакеты, якобы отправленные с наружного интерфейса. Для наружного интерфейса – сетевой карты (eth0) – в таблицу NAT (`-t nat`) добавьте к цепочке правил исходящих пакетов (`-A POSTROUTING`) через сетевой интерфейс eth0 (`–o eth0`) маскарадинг (`–j MASQUERADE`):

```
[root@bastion /]# /sbin/iptables –t nat –A POSTROUTING –o eth0 –j
MASQUERADE
```

Для наружного интерфейса – ppp0 (создаваемого при установке VPN-соединения по протоколу PPTP или модемном соединении со шлюзом провайдера) – в таблицу NAT (`-t nat`) добавьте к цепочке правил исходящих пакетов (`-A POSTROUTING`) через сетевой интерфейс ppp0 (`–o ppp0`) маскарадинг (`–j MASQUERADE`):

```
[root@bastion /]# /sbin/iptables –t nat –A POSTROUTING –o ppp0 –j
MASQUERADE
```

Для перенаправления входящих пакетов на компьютер, находящийся во внутренней сети, создайте правило в таблицу NAT (`-t nat`), добавьте к цепочке правил входящих пакетов (`-A PREROUTING`) на IP-адрес 212.45.28.122 (`-d 212.45.28.122`) для протокола TCP (`-p tcp`) порта 80 (`--dport 80`) перенаправление (`-j DNAT`) на IP-адрес 172.16.181.102 порта 8001(`--to 172.16.181.102:8001`):

Теперь, если вы хотите отправить информацию о порте, например, его значении, с TCP-пакетами, входящими на внешний интерфейс по IP-адресу 207.35.78.2 на порту 8080 так, чтобы их отображение адресата на локальный интерфейс было по IP-адресу 192.168.1.1 на порту 80, тогда вы могли бы использовать следующие правила:

```
[root@bastion /]# /sbin/iptables -t nat -A PREROUTING -d 212.45.28.122 -p
tcp --dport 80 -j DNAT --to 172.16.181.102:8001
```

Проверка настроек сетевой защиты

Для просмотра всех правил во всех цепочках используйте команду:

```
[root@bastion /]# iptables -L
```

Для вывода всех правил в некоторой цепочке используйте, например, команду `INPUT`:

```
[root@bastion/ ] # iptables -L INPUT
```

Если вы предпочитаете числовой формат отображения информации, то используйте опцию `–n`, например:

```
[root@bastion /]# iptables –nL
```

ЗАМЕЧАНИЕ Команда `iptables` имеет большое число опций, которые позволяют создавать правила, удовлетворяющие практически любым требованиям пользователей к системе сетевой защиты, и осуществлять диагностику работы этой системы. Описание всех возможных и даже типовых конфигураций системы сетевой защиты выходит за рамки этой главы и книги. Поэтому перед применением на практике рекомендаций, изложенных в настоящей главе, авторы рекомендуют изучить страницы руководства, связанные с IPTables, и документ IPTables Tutorial.

Глава 10

GIPTables Firewall - программное обеспечение для настройки IPTables

В этой главе:

Программный продукт GIPTables Firewall, разработанный Адрианом Паскалау (Adrian Pascalau), представляет собой свободно распространяемые скрипты, позволяющие автоматически создавать правила для сетевой защиты IPTables на Linux-системах с ядром версии 2.4.x с одной или двумя сетевыми картами. Программа проста в установке и конфигурировании.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Используется ядро версии 2.4.x., настроенное и откомпилированное в соответствии с рекомендациями глав 6 и 9.

Установлена система сетевой защиты IPTables.

Процедуры, описанные в этой главе, могут оказаться применимыми для других дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта GIPTables Firewal от 01.02.2003. Регулярно посещайте домашнюю страницу проекта `http://www.giptables.org` и отслеживайте обновления.

Исходные коды GIPTables Firewall содержатся в архиве `gip-tables-version.tar.gz` (последняя доступная на момент написания главы версия `gip-tables-1.1.tar.gz`).

Компиляция, оптимизация и инсталляция GIPTables Firewall

Шаг 1

Распакуйте архив с пакетом `gip-tables-1.1.tar.gz` в каталоге `/var/tmp`:

```
[root@bastion tmp]# tar -xzpf gip-tables-1.1.tar.gz
```

Шаг 2

Перейдите в каталог `/var/tmp/gip-tables-1.1`:

```
[root@bastion tmp]# cd /var/tmp/gip-tables-1.1
```

Установите `gip-tables-1.1`:

```
[root@bastion gip-tables-1.1]# find /* > /root/gip-tables1.txt
[root@bastion gip-tables-1.1]# ./install.sh
```

Создайте и сохраните в надежном месте список файлов `gip-tables-1.1`, установленных на системе:

```
[root@bastion gip-tables-1.1]# find /* > /root/gip-tables2.txt
[root@bastion gip-tables-1.1]# diff /root/gip-tables1.txt /root/gip-
tables2.txt > /root/gip-tables.installed.txt
[root@bastion gip-tables-1.1]# mv gip-tables.installed.txt /very reli-
able_place/gip-tables.installed.YYYYMMDD.txt
```

Шаг 3

Удалите каталоги с исходными кодами `gip-tables-1.1` и архив:

```
root@bastion gip-tables-1.1]# rm –rf /var/tmp/gip-tables-1.1/
root@bastion gip-tables-1.1]# rm –f /var/tmp/gip-tables-1.1.tar.gz
```

Настройка GIPTables

В процессе установки GIPTables Firewall в каталог `/lib/giptables/conf` устанавливаются следующие конфигурационные файлы. В настоящее время в комплект поставки входят:

- `giptables.conf.dns1` и `giptables.conf.dns2` – конфигурационные файлы для первичного и вторичного DNS-серверов, соответственно;
- `giptables.conf.ftpserver` – конфигурационный файл для сервера;
- `giptables.conf.gateway` – конфигурационный файл для шлюза;
- `giptables.conf.mailserver` – конфигурационный файл для почтового сервера;
- `giptTables.conf.ppp` – конфигурационный файл для PPP-сервера;

- `giptables.conf.virtual` – для виртуального сервера;
- `giptables.conf.workstation` – для рабочей станции;
- `giptables.conf.README` – демонстрационный файл, включающий все возможные опции конфигурирования с достаточно подробными комментариями.

В каталог `/etc/rc.d` устанавливается файл `rc.giptables.blocked`, в который можно внести перечень IP-адресов, для которых доступ к системе следует закрыть. В каталог `/etc/init.d` устанавливается файл инициализации `giptables`.

Конфигурационный файл /etc/giptables.conf

Файл `/etc/giptables.conf` – основной конфигурационный файл GIPTables. При инсталляции программы он не создается. Для его создания необходимо выполнить определенные действия.

Шаг 1

Выберите один из файлов `/lib/giptables/conf/giptables.conf.*`, наиболее соответствующий вашим требованиям к системе сетевой защиты, например, `/lib/giptables/conf/giptables.conf.gateway`, и скопируйте его в файл `/lib/giptables/conf/giptables.conf`:

```
[root@bastion /]# cd /lib/giptables/conf/
[root@bastion conf]# cp giptables.conf.gateway giptables.conf
```

Создайте символьную ссылку:

```
[root@bastion conf]# ln -sf /lib/gip-tables/conf/giptables.conf
/etc/giptables.conf
```

Шаг 2

Установите необходимые для реализации ваших требований к системе сетевой защиты значения опций в файле `/lib/giptables/conf/giptables.conf`, о чем будет подробно рассказано чуть позже.

Шаг 3

Запустите GIPTables Firewall:

```
[root@bastion conf]# /etc/init.d./giptables start
```

Для автоматизированного запуска GIPTables Firewall при загрузке системы, выполните:

```
[root@bastion conf]# chkconfig --add giptables
```

Рассмотрим некоторые из наиболее важных параметров, содержащихся в конфигурационном файле `/lib/giptables/conf/giptables.conf`.

В разделе `DEBUG` содержится единственный конфигурационный параметр – `DEBUG`.

```
# DEBUG
#

    DEBUG="off"
```

Параметр `DEBUG` включает/выключает режим отладки. При установленном по умолчанию значении "off" режим отладки выключен. При включении режима отладки на экран будут выведены все правила, применяемые системой сетевой защиты. При этом никакие действия (фильтрация, перенаправление и т. п.) с пакетами совершаться не будут. Для удобства при включенном режиме отладки можно переадресовать вывод с экрана в файл:

```
[root@bastion /]# /etc/init.d/giptables start > giptables-dump.txt
```

ЗАМЕЧАНИЕ Это очень удобная опция, позволяющая сгенерировать свод правил, которые легко могут быть преобразованы в скрипт IPTables, запускаемый при старте системы. При этом правила могут быть сгенерированы и отлажены на одной системе (рабочей станции администратора сервера, оснащенной графическим интерфейсом и необходимым для отладки программным обеспечением), а установлены на другой, где по каким либо причинам отладка может быть затруднена или не возможна.

В следующем разделе определяются основные параметры системы.

```
# Some definitions for easy maintenance
# Edit these to suit your system
#

    MONOLITIC_KERNEL="no"
```

```
# Interface 0: This is our external network interface
# It is directly connected to Internet

    INTERFACE0="eth0"
    INTERFACE0_IPADDR="x.x.x.x"
    ANY_IPADDR="0/0"

# Interface 1: This is our internal network interface
# It is directly connected to our internal Network 1

    INTERFACE1="eth1"
    INTERFACE1_IPADDR="192.168.1.254"
    NETWORK1="192.168.1.0/24"

# Do you need Network Address Translation for your internal network?

    NETWORK1_NAT="yes"

# Your name servers ip address

    ISP_PRIMARY_DNS_SERVER="a.a.a.a"
    ISP_SECONDARY_DNS_SERVER="b.b.b.b"

# SYSLOG server ip address

    SYSLOG_SERVER="c.c.c.c"

# SYSLOG client ip address

    SYSLOG_CLIENT="d.d.d.d"

# Loopback interface

    LOOPBACK_INTERFACE="lo"                    # Loopback interface

# Port declarations, do not change them

    PRIV_PORTS="0:1023"
    UNPRIV_PORTS="1024:65535"

# ------------------------------------------------------------------------
# Loading custom firewall rules from /etc/rc.d/rc.giptables.custom
#

    LOAD_CUSTOM_RULES="yes"
```

Параметр `MONOLITIC_KERNEL`
определяет не архитектуру ядра в целом, а только способ включения в него кодов IPTables. Мы рекомендуем во всех случаях, когда это возможно, использовать ядро с монолитной архитектурой и включать код, реализующий систему сетевой защиты, непосредственно в код ядра. Если вы следуете нашим рекомендациям, значение параметра, установленное по умолчанию "no", нужно изменить на "yes".

Параметры `INTERFACE0="eth0"` и `INTERFACE0_IPADDR="x.x.x.x"`
определяют внешний (ориентированный в сторону Интернет) сетевой интерфейс и его IP-адрес, соответственно.

Параметр `ANY_IPADDR="0/0"`
определяет параметры сети, с которыми данный компьютер может устанавливать соединения. Учитывая, что этот параметр соответствует внешнему интерфейсу, ему присвоено значение, позволяющее устанавливать соединение с компьютером, имеющим любой адрес – "`0/0`". Не изменяйте значение опции. Ограничение доступа со стороны нежелательных хостов осуществляется другим способом и описано ниже.

Если ваша система получает IP-адрес с DHCP-сервера провайдера, то параметру `INTERFACE0` должно быть присвоено значение "`/lib/giptabies/if_ipaddr $INTERFACE0`":

```
INTERFACE0_IPADDR="/lib/giptabies/if_ipaddr $INTERFACE0"
```

В этом случае в файле инициализации `/etc/init.d/giptabies` также необходимо изменить вторую строку:

```
# chkconfig: 2345 08 92
```

на:

```
# chkconfig: 2345 11 92
```

После внесения изменений система сетевой защиты будет запускаться после инициализации сети, и компьютер сможет получить динамический IP-адрес от DHCP-сервера провайдера.

Опции `INTERFACE1="eth1"`, `INTERFACE1_IPADDR="y.y.y.y"` и `NETWORK1="s.s.s.0/24"` определяют сетевой интерфейс, IP-адрес компьютера во внутренней сети и внутреннюю подсеть, соответственно.

Если компьютер не имеет интерфейса, ориентированного во внутреннюю сеть – т. е. имеет только один сетевой интерфейс, например, являясь рабочей станцией с одним сетевым интерфейсом, ориентированным в локальную сеть офиса, или сервером с одним сетевым интерфейсом, ориентированным в Интернет – закомментируйте или удалите параметры `INTERFACE1="eth1"`, `INTERFACE1_IPADDR="y.y.y.y"` и `NETWORK1="s.s.s.0/24"`.

Параметры

```
ISP_PRIMARY_DNS_SERVER="a.a.a.a"
ISP_SECONDARY_DNS_SERVBR="b.b.b.b"
```

предназначены для определения IP-адресов первичного и вторичного DNS-серверов.

Параметр `SYSLOG_SERVER="c.c.c.c"` определяет IP-адрес сервера, на котором осуществляется запись файлов регистрации.

Параметр `LOOPBACK_INTERFACE="lo"` определяет петлевой интерфейс.

Параметры

```
PRIV_PORTS="0:1023"
UNPRIV_PORTS="1024:65535"
```

определяют диапазон привилегированных портов.

Параметр `LOAD_CUSTOM_RULES="yes"` предназначен для добавления дополнительных правил, включаемых в файл `/etc/rc.d/rc.GIPTables.custom`. Если установлено значение "no", то правила, содержащиеся в этом файле, игнорируются.

В разделе `Logging` конфигурируется регистрация пакетов, задерживаемых системой сетевой защиты:

```
# ------------------------------------------------------------------
# Logging
# Limit the amount of incoming dropped packets that gets sent to the logs
#

# We log & drop all the packets that are not expected. In order to avoid
# our logs beeing flooded, we rate limit the logging

# Interface 0 log dropped packets

    INTERFACE0_LOG_DROPPED_PACKETS="yes"
    INTERFACE0_LOG_LIMIT="5/m"
    INTERFACE0_LOG_LIMIT_BURST="7"

# Interface 1 log dropped packets

    INTERFACE1_LOG_DROPPED_PACKETS="yes"
    INTERFACE1_LOG_LIMIT="7/m"
    INTERFACE1_LOG_LIMIT_BURST="9"

# Network 1 log forwarded dropped packets

    NETWORK1_LOG_DROPPED_PACKETS="yes"
    NETWORK1_LOG_LIMIT="9/m"
    NETWORK1_LOG_LIMIT_BURST="11"
```

Если в системе нет внутреннего сетевого интерфейса, удалите или закомментируйте строки, относящиеся к внутреннему сетевому интерфейсу и локальной сети (`INTERFACE1` и `NETWORK1`). При выбранной нами концепции сетевой безопасности система сетевой защиты исключает все пакеты, кроме разрешенных.

В случае прихода нежелательных пакетов они задерживаются и регистрируются. Если система будет подвергнута атаке путем отправки на ее сетевые интерфейсы большого числа нежелательных пакетов, файл регистрации быстро заполнит все свободное дисковое пространство. Чтобы избежать этого, мы устанавливаем ограничение на количество сообщений в файлы регистрации с помощью параметров `LOG_LIMIT` и `LOG_LIMIT_BURST`.

Параметр `LOG_LIMIT_BURST`
определяет максимальное число нежелательных пакетов, информация о которых заносится в файл регистрации в течение интервала времени, величина которого определяется числом, стоящим перед знаком `"/"`, а единица измерения ключом, стоящим после (секунда - `/second` или `/s`, минута - `/minute` или `/m`, час - `/hour` или `/h` и день - `/day` или `/d`). Таким образом, пара значений параметров `NETWORK1_LOG_LIMIT="9/m"` и `NETWORK1_LOG_LIMIT_BURST="11"` в рассмотренном примере означает, что в течение 9 минут в файл регистрации будут внесена информация не более чем об 11 первых нежелательных пакетах.

Регистрационная информация посылается в файл `/var/log/messages`.

Параметры, с помощью которых устанавливается запрет на установку любых соединений с определенных IP-адресов, содержатся в секции `Network Ghouls`:

```
# Network Ghouls
# Refuse any connection from problem sites
#

# The /etc/rc.d/rc.giptables.blocked file contains a list of ip addresses
that
# will be blocked from having any kind of access to your server on all
your
# interfaces if the next option is "yes"

    NETWORK_GHOULS="yes"


# If you would like to block an ip address from having any kind of access
to
# your server on a specific interface, please use the options below

    REFUSE_CONNECTION_IPADDR[0]="1.1.1.1"
    INTERFACE0_REFUSE_CONNECTION[0]="yes"
    INTERFACE1_REFUSE_CONNECTION[0]="yes"
    NETWORK1_REFUSE_CONNECTION[0]="yes"

    REFUSE_CONNECTION_IPADDR[1]="2.2.2.2"
    INTERFACE0_REFUSE_CONNECTION[1]="yes"
    INTERFACE1_REFUSE_CONNECTION[1]="yes"
    NETWORK1_REFUSE_CONNECTION[1]="yes"
```

Для включения или отключения блокирования сетевых подключений с определенных IP-адресов используется параметр `NETWORK_GHOULS="yes"/"no"`. Если установлено значение параметра – "yes", то установка любых сетевых соединений с IP-адресов, перечисленных в файле `/etc/rc.d/rc.giptables.blocked`, запрещается. Если установлено значение параметра "no", то список запрещенных IP-адресов игнорируется.

Параметры
`REFUSE_CONNECTION_IPADDR[0]`
`INTERFACE0_REFUSE_CONNECTION[0]`
`NTERFACE1_REFUSE_CONNECTION[0]`
`NETWORK1_REFUSE_CONNECTION[0]`
используются для ограничения установки сетевых соединений с нежелательными адресами только для определенных сетевых интерфейсов.

Для конфигурирования системы защиты от одного из видов DoS-атак – "SYN-flood" – используются параметры секции `Syn-flood protection`:

```
# Syn-flood protection
# Limit the number of incoming tcp connections
#

    SYN_FLOOD_PROTECTION="yes"
```

```
# Interface 0 incoming syn-flood protection

    INTERFACE0_IN_SYN_FLOOD_PROTECTION="yes"
    INTERFACE0_IN_TCP_CONN_LIMIT="1/s"
    INTERFACE0_IN_TCP_CONN_LIMIT_BURST="3"

# Interface 1 incoming syn-flood protection

    INTERFACE1_IN_SYN_FLOOD_PROTECTION="yes"
    INTERFACE1_IN_TCP_CONN_LIMIT="3/s"
    INTERFACE1_IN_TCP_CONN_LIMIT_BURST="5"

# Network 1 forwarded incoming syn-flood protection

    NETWORK1_IN_SYN_FLOOD_PROTECTION="yes"
    NETWORK1_IN_TCP_CONN_LIMIT="5/s"
    NETWORK1_IN_TCP_CONN_LIMIT_BURST="7"
```

Установка значения параметра `SYN_FLOOD_PROTECTION="yes"` включает защиту от SYN-атак.

Параметры

```
INTERFACE0_IN_TCP_CONN_LIMIT="1/s"
INTERFACE0_IN_TCP_CONN_LIMIT_BURST="3"
```

ограничивают минимально допустимое число пакетов (в рассматриваемом примере – три), пропускаемых через сетевой интерфейс в единицу времени (в рассматриваемом примере – за 1 секунду).

Для включения и конфигурирования проверки потенциально опасных входящих пакетов используются параметры раздела `Sanity check`:

```
# Sanity check
#

    SANITY_CHECK="yes"

# Make sure NEW incoming tcp connections are SYN packets

    INTERFACE0_IN_DROP_NEW_WITHOUT_SYN="yes"
    INTERFACE1_IN_DROP_NEW_WITHOUT_SYN="yes"
    NETWORK1_IN_DROP_NEW_WITHOUT_SYN="yes"

# Drop all incoming fragments

    INTERFACE0_IN_DROP_ALL_FRAGMENTS="yes"
    INTERFACE1_IN_DROP_ALL_FRAGMENTS="yes"
    NETWORK1_IN_DROP_ALL_FRAGMENTS="yes"

# Drop all incoming malformed XMAS packets

    INTERFACE0_IN_DROP_XMAS_PACKETS="yes"
    INTERFACE1_IN_DROP_XMAS_PACKETS="yes"
    NETWORK1_IN_DROP_XMAS_PACKETS="yes"

# Drop all incoming malformed NULL packets

    INTERFACE0_IN_DROP_NULL_PACKETS="yes"
    INTERFACE1_IN_DROP_NULL_PACKETS="yes"
    NETWORK1_IN_DROP_NULL_PACKETS="yes"
```

Установка значения параметра `SANITY_CHECK="yes"` включает проверку.

Параметры `INTERFACE0_IN_DROP_NEW_WITHOUT_SYN="yes"`

```
INTERFACE1_IN_DROP_NEW_WITHOUT_SYN ="yes"
NETWORK1_IN_DROP_NEW_WITHOUT_SYN="yes"
```

используются для включения режима, в котором проверяется наличие SYN-бита у всех новых входящих пакетов, новые пакеты без SYN-бита фильтруются, информация о них запоминается в файле регистрации.

Параметры

```
INTERFACE0_IN_DROP_ALL_FRAGMENTS="yes"
```

```
INTERFACE1_IN_DROP_ALL_FRAGMENTS="yes"
NETWORK1_IN_DROP_ALL_FRAGMENTS="yes"
```

используются для включения режима, в котором отфильтровываются и регистрируются все некорректные пакеты.

Параметры

```
INTERFACE0_IN_DROP_XMAS_PACKETS="yes"
INTERFACE1_IN_DROP_XMAS_PACKETS="yes"
NETWORK1_IN_DROP_XMAS_PACKETS="yes"
```

используются для включения режима, в котором отфильтровываются и регистрируются все некорректные XMAS-пакеты.

Параметры

```
INTERFACE0_IN_DROP_NULL_PACKETS="yes"
INTERFACE1_IN_DROP_NULL_PACKETS="yes"
NETWORK1_IN_DROP_NULL_PACKETS="yes"
```

используются для включения режима, в котором отфильтровываются и регистрируются все NULL-пакеты, обычно генерируемые программами-сканерами портов.

В заголовках пакетов содержатся исходный адрес, адрес назначения и тип протокола сообщения (ICMP, UDP или TCP). Наличие в заголовках пакетов исходного адреса и использование его для идентификации отправителя может быть использовано и для получения несанкционированного доступа к системе. Существует, по крайней мере, семь разновидностей исходных адресов, которые должны отфильтровываться внешним (ориентированным в сторону Интернет) интерфейсом (адреса, зарезервированные для локальных сетей, интерфейса возвратной петли и неиспользуемые Интернет адреса).

Для включения и конфигурирования фильтрации пакетов на внешнем интерфейсе системы используйте параметры секции `Spoofing and bad addresses`.

```
# Spoofing and bad addresses
#

    REFUSE_SPOOFING="yes"

# Refuse incoming packets claiming to be from the ip addresses of our in-
terfaces

    REFUSE_SPOOFING_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_IN_REFUSE_SPOOFING[0]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[0]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[0]="yes"

    REFUSE_SPOOFING_IPADDR[1]=$INTERFACE1_IPADDR
    INTERFACE0_IN_REFUSE_SPOOFING[1]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[1]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[1]="yes"

# Refuse incoming packets claiming to be from broadcast-src address range

    REFUSE_SPOOFING_IPADDR[2]="0.0.0.0/8"

# If you provide DHCP services on one of your interfaces, do not forget
to
# set the following option related to that interface to "no"

    INTERFACE0_IN_REFUSE_SPOOFING[2]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[2]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[2]="yes"

# Refuse incoming packets claiming to be from reserved loopback address
range

    REFUSE_SPOOFING_IPADDR[3]="127.0.0.0/8"
    INTERFACE0_IN_REFUSE_SPOOFING[3]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[3]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[3]="yes"

# Refuse incoming packets claiming to be from class A private network
```

```
    REFUSE_SPOOFING_IPADDR[4]="10.0.0.0/8"
    INTERFACE0_IN_REFUSE_SPOOFING[4]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[4]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[4]="yes"

# Refuse incoming packets claiming to be from class B private network

    REFUSE_SPOOFING_IPADDR[5]="172.16.0.0/12"
    INTERFACE0_IN_REFUSE_SPOOFING[5]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[5]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[5]="yes"

# Refuse incoming packets claiming to be from class C private network

    REFUSE_SPOOFING_IPADDR[6]="192.168.0.0/16"
    INTERFACE0_IN_REFUSE_SPOOFING[6]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[6]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[6]="yes"

# Refuse incoming packets claiming to be from class D, E, and unallocated

    REFUSE_SPOOFING_IPADDR[7]="224.0.0.0/3"
    INTERFACE0_IN_REFUSE_SPOOFING[7]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[7]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[7]="yes"
```

Параметры:
`REFUSE_SPOOFING_IPADDR[0]`,
`INTERFACE0_IN_REFUSE_SPOOFING[0]`,
`INTERFACE1_IN_REFUSE_SPOOFING[0]`,
`NETWORK1_IN_REFUSE_SPOOFING[0]`,
`REFUSE_SPOOFING_IPADDR[1]`,
`INTERFACE0_IN_REFUSE_SPOOFING[1]`,
`INTERFACE1_IN_REFUSE_SPOOFING[1]`,
`NETWORK1_IN_REFUSE_SPOOFING[1]`
используются для регистрации и фильтрации входящих пакетов, отправленных якобы с нашего IP-адреса на внутренний и внешние сетевые интерфейсы системы.

Параметры:
`REFUSE_SPOOFING_IPADDR[2]`,
`INTERFACE0_IN_REFUSE_SPOOFING[2]`,
`INTERFACE1_IN_REFUSE_SPOOFING[2]`,
`NETWORK1_IN_REFUSE_SPOOFING[2]`
используются для регистрации и фильтрации входящих пакетов, адресуемых на широковещательные адреса. Если вы используете DHCP-сервер для автоматического распределения IP-адресов в локальной сети, или ваш провайдер выделяет динамический адрес при подключении к Интернет, не следует включать фильтрацию пакетов, адресуемых на широковещательные адреса.

Параметры:
`REFUSE_SPOOFING_IPADDR[3]`,
`INTERFACE0_IN_REFUSE_SPOOFING[3]`,
`INTERFACE1_IN_REFUSE_SPOOFING[3]`,
`NETWORK1_IN_REFUSE_SPOOFING[3]`
используются для регистрации и фильтрации входящих пакетов, отправляемых якобы из диапазона адресов возвратной петли.

Параметры:
`REFUSE_SPOOFING_IPADDR[4]`,
`INTERFACE0_IN_REFUSE_SPOOFING[4]`,
`INTERFACE1_IN_REFUSE_SPOOFING[4]`,
`NETWORK1_IN_REFUSE_SPOOFING[4]`,
`REFUSE_SPOOFING_IPADDR[5]`,
`INTERFACE0_IN_REFUSE_SPOOFING[5]`,
`INTERFACE1_IN_REFUSE_SPOOFING[5]`,
`NETWORK1_IN_REFUSE_SPOOFING[5]`,

```
REFUSE_SPOOFING_IPADDR[6],
INTERFACE0_IN_REFUSE_SPOOFING[6],
INTERFACE1_IN_REFUSE_SPOOFING[6],
NETWORK1_IN_REFUSE_SPOOFING[6],
REFUSE_SPOOFING_IPADDR[7],
INTERFACE0_IN_REFUSE_SPOOFING[7],
INTERFACE1_IN_REFUSE_SPOOFING[7],
NETWORK1_IN_REFUSE_SPOOFING[7]
```

используются для регистрации и фильтрации входящих пакетов, отправляемых якобы с адресов, зарезервированных для сетей класса A,B,C,D,E и неиспользуемых IP-адресов.

Конфигурирование совместной работы GIPTables Firewall с различными службами

В GIPTables Firewall имеются модули, обеспечивающие нормальное функционирование типовых служб. Эти файлы находятся в каталоге `/lib/giptables/modules` и имеют имя вида `giptaples-service`. Модули загружаются только, если это предусмотрено (т. е. строки, разрешающие использование соответствующих служб, имеются в наличии и раскомментированы) в файле `giptables.conf`. Вы можете определить, на каком сетевом интерфейсе, в какой сети и с какими соединениями будет работать служба. Для получения списка модулей, наберите:

```
[root@bastion /]# ls -l /lib/giptables/modules
-rw-------    1 root     root          7230 Фев  3 11:16 giptables-ANY
-rw-------    1 root     root          9199 Фев  3 11:16 giptables-AUTH
-rw-------    1 root     root          5465 Фев  3 11:16 giptables-DHCP
-rw-------    1 root     root         13936 Фев  3 11:16 giptables-DNS
-rw-------    1 root     root          7833 Фев  3 11:16 giptables-FINGER
-rw-------    1 root     root         12626 Фев  3 11:16 giptables-FTP
-rw-------    1 root     root          7639 Фев  3 11:16 giptables-HTTP
-rw-------    1 root     root          7746 Фев  3 11:16 giptables-HTTPS
-rw-------    1 root     root         10299 Фев  3 11:16 giptables-ICMP
-rw-------    1 root     root          7651 Фев  3 11:16 giptables-IMAP
-rw-------    1 root     root          7755 Фев  3 11:16 giptables-IMAPS
-rw-------    1 root     root          7596 Фев  3 11:16 giptables-LDAP
-rw-------    1 root     root          7755 Фев  3 11:16 giptables-LDAPS
-rw-------    1 root     root          7537 Фев  3 11:16 giptables-LPD
-rw-------    1 root     root          7763 Фев  3 11:16 giptables-MSSQL
-rw-------    1 root     root          7748 Фев  3 11:16 giptables-MYSQL
-rw-------    1 root     root          6145 Фев  3 11:16 giptables-NETBIOS
-rw-------    1 root     root          7652 Фев  3 11:16 giptables-NNTP
-rw-------    1 root     root          7755 Фев  3 11:16 giptables-NNTPS
-rw-------    1 root     root          7525 Фев  3 11:16 giptables-NTP
-rw-------    1 root     root          7945 Фев  3 11:16 giptables-ORACLE
-rw-------    1 root     root          7636 Фев  3 11:16 giptables-POP3
-rw-------    1 root     root          7748 Фев  3 11:16 giptables-POP3S
-rw-------    1 root     root          8108 Фев  3 11:16 giptables-
POSTGRES
-rw-------    1 root     root          7608 Фев  3 11:16 giptables-SMTP
-rw-------    1 root     root          7761 Фев  3 11:16 giptables-SMTPS
-rw-------    1 root     root          7719 Фев  3 11:16 giptables-SNMP
-rw-------    1 root     root          7761 Фев  3 11:16 giptables-SOCKS
-rw-------    1 root     root          7787 Фев  3 11:16 giptables-SQUID
-rw-------    1 root     root          7569 Фев  3 11:16 giptables-SSH
-rw-------    1 root     root          7834 Фев  3 11:16 giptables-SYSLOG
-rw-------    1 root     root          7832 Фев  3 11:16 giptables-TELNET
-rw-------    1 root     root          7953 Фев  3 11:16 giptables-TELNETS
-rw-------    1 root     root          7367 Фев  3 11:16 giptables-
TRACEROUTE
-rw-------    1 root     root          7476 Фев  3 11:16 giptables-VNC
-rw-------    1 root     root          8152 Фев  3 11:16 giptables-
WEBCACHE
-rw-------    1 root     root          7728 Фев  3 11:16 giptables-WHOIS
-rw-------    1 root     root          7529 Фев  3 11:16 giptables-X11
```

GIPTables Firewall по умолчанию реализует концепцию безопасности «все, что не разрешено – то запрещено". Поэтому для обеспечения нормальной работы службы необходимо внести соответствующие изменения в конфигурационный файл `giptables.conf`. В качестве примера разрешим работу MySQL-сервера на системе с одним внешним сетевым интерфейсом.

Шаг 1

Разрешите использования модуля для MySQL, для этого добавьте или раскомментируйте строку:

```
ACCEPT_MYSQL="yes"
```

Шаг 2

Добавьте или раскомментируйте строки, разрешающие клиентские запросы к MySQL-серверу:

```
INTERFACE0_MYSQL_SERVER="yes"
INTERFACE0_MYSQL_IN_SRC_IPADDR[0]=$ANY_IPADDR
INTERFACE0_MYSQL_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR
```

Шаг 3

Для того, чтобы изменения вступили в силу, перегрузите GIPTables Firewall:

```
[root@bastion /]# /etc/init.d/giptables restart
```

Настройка GIPTables Firewall для шлюза (прокси-сервера)

Практика показывает, что наибольшее количество вопросов у начинающих пользователей возникает при настройке шлюза. Ниже приведены пошаговые инструкции его настройки и пример конфигурационного файла для GIPTables Firewall, за основу которого взят конфигурационный файл `/lib/giptables/conf/giptables.conf.gateway` (комментарии на русском языке добавлены авторами). Предложенная конфигурация шлюза организует, так называемый маскарадинг (masquerading), при реализации которого компьютеры из внутренней сети имеют доступ в Интернет, но полностью скрыты для внешней сети и не имеют официально зарегистрированных интернет-адресов.

Шаг 1

Разрешите пересылку пакетов между внутренним и внешним интерфейсом (по умолчанию эта опция отключена). Для этого в файле `/etc/sysctl.conf` замените строку:

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

на:

```
net.ipv4.ip_forward = 1
```

Для вступления изменений в силу перезагрузите сеть:

```
[root@bastion /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

Тот же самый эффект может быть достигнут и без перезагрузки сети:

```
[root@bastion /]# sysctl -w net.ipv4.ip_forward = 1
```

Шаг 2

Скопируйте файл `/lib/giptables/conf/giptables.conf.gateway` в `/lib/giptables/conf/giptables.conf` и создайте ссылку:

```
[root@bastion /]# cp /lib/giptables/conf/giptables.conf.gateway
/lib/giptables/conf/giptables.conf
[root@bastion /]# ln -s /lib/giptables/conf/giptables.conf
etc/giptables.conf
```

Шаг 3

Отредактируйте файл `/lib/giptables/conf/giptables.conf` в соответствии с рекомендациями приведенного ниже примера, вашими потребностями и конфигурацией сети. Особое внимание обратите на корректировку фрагментов, выделенных жирным шрифтом.

Для этого можно воспользоваться командой:

```
[root@bastion /]# vi /etc/giptables.conf
# ------------------------------------------------------------------------
# GIPTables Firewall v1.1 http://www.giptables.org
```

```
# Copyright (C) 2002 Adrian Pascalau <apascalau@openna.com>
# GATEWAY main configuration file
#
# ------------------------------------------------------------------------
-
# This file is part of GIPTables Firewall
#
# GIPTables Firewall is free software; you can redistribute it and/or
modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307
USA

# ------------------------------------------------------------------------
-----
# DEBUG
#

    DEBUG="off"

# ------------------------------------------------------------------------
-----
# Some definitions for easy maintenance
# Edit these to suit your system
# Если вы следовали нашим рекомендациям, то код iptables включен в код
ядра.

    MONOLITIC_KERNEL="yes"

# Interface 0: This is our external network interface
# It is directly connected to Internet
# Установите параметры внешнего интерфейса.
    INTERFACE0="eth0"
    INTERFACE0_IPADDR="x.x.x.x"
    ANY_IPADDR="0/0"

# Interface 1: This is our internal network interface
# It is directly connected to our internal Network 1
# Проверьте, правильно ли указаны параметры внутренней сети.
    INTERFACE1="eth1"
    INTERFACE1_IPADDR="192.168.1.254"
    NETWORK1="192.168.1.0/24"

# Do you need Network Address Translation for your internal network?

    NETWORK1_NAT="yes"

# Your name servers ip address
# Установите правильные значения IP-адресов ваших DNS-серверов.
# Использование чужих DNS-серверов - плохой тон !!!
    ISP_PRIMARY_DNS_SERVER="a.a.a.a"
    ISP_SECONDARY_DNS_SERVER="b.b.b.b"

# SYSLOG server ip address
```

```
# Если для хранения файлов регистрации используется шлюз - что не очень
# хорошо с точки зрения безопасности - укажите IP-адрес внутреннего
# интерфейса. Если же файлы регистрации хранятся на другой системе внутри
# локальной сети, то укажите ее IP-адрес.
    SYSLOG_SERVER="c.c.c.c"

# Loopback interface

    LOOPBACK_INTERFACE="lo"                    # Loopback interface

# Port declarations, do not change them

    PRIV_PORTS="0:1023"
    UNPRIV_PORTS="1024:65535"

# ------------------------------------------------------------------------
# Loading custom firewall rules from /etc/rc.d/rc.giptables.custom
#
# Если вы следовали нашим рекомендациям, то /etc/rc.d/rc.giptables.custom
# не содержит никаких дополнительных правил. Если в последующем они будут
# созданы и добавлены, не забудьте изменить значение параметра на "yes".
    LOAD_CUSTOM_RULES="no"

# ------------------------------------------------------------------------
# Logging
# Limit the amount of incoming dropped packets that gets sent to the logs
# Ниже выставляются параметры, устанавливающие разумный компромисс
# между объемом файлов регистрации и информативностью. Не советуем
# изменять значения этих параметров.
# We log & drop all the packets that are not expected. In order to avoid
# our logs beeing flooded, we rate limit the logging

# Interface 0 log dropped packets

    INTERFACE0_LOG_DROPPED_PACKETS="yes"
    INTERFACE0_LOG_LIMIT="5/m"
    INTERFACE0_LOG_LIMIT_BURST="7"

# Interface 1 log dropped packets

    INTERFACE1_LOG_DROPPED_PACKETS="yes"
    INTERFACE1_LOG_LIMIT="7/m"
    INTERFACE1_LOG_LIMIT_BURST="9"

# Network 1 log forwarded dropped packets

    NETWORK1_LOG_DROPPED_PACKETS="yes"
    NETWORK1_LOG_LIMIT="9/m"
    NETWORK1_LOG_LIMIT_BURST="11"

# ------------------------------------------------------------------------
-
# Network Ghouls
# Refuse any connection from problem sites
#

# The /etc/rc.d/rc.giptables.blocked file contains a list of ip addresses
that
# will be blocked from having any kind of access to your server on all
your
# interfaces if the next option is "yes"
# Если вы следовали нашим рекомендациям, то
/etc/rc.d/rc.giptables.blocked
```

```
# не содержит никаких IP-адресов, доступ с которых к вашей системе запре-
щен.
# Если в последующем они будут добавлены, не забудьте изменить значение
# параметра на "yes".
    NETWORK_GHOULS="no"

# ------------------------------------------------------------------------
# Syn-flood protection
# Limit the number of incoming tcp connections
# Защита от Syn-flood атак. Не советуем изменять значения этих
# параметров.


    SYN_FLOOD_PROTECTION="yes"

# Interface 0 incoming syn-flood protection

    INTERFACE0_IN_SYN_FLOOD_PROTECTION="yes"
    INTERFACE0_IN_TCP_CONN_LIMIT="1/s"
    INTERFACE0_IN_TCP_CONN_LIMIT_BURST="3"

# Interface 1 incoming syn-flood protection

    INTERFACE1_IN_SYN_FLOOD_PROTECTION="yes"
    INTERFACE1_IN_TCP_CONN_LIMIT="3/s"
    INTERFACE1_IN_TCP_CONN_LIMIT_BURST="5"

# Network 1 forwarded incoming syn-flood protection

    NETWORK1_IN_SYN_FLOOD_PROTECTION="yes"
    NETWORK1_IN_TCP_CONN_LIMIT="5/s"
    NETWORK1_IN_TCP_CONN_LIMIT_BURST="7"

# ------------------------------------------------------------------------
---
# Sanity check
# Фильтрация «некорректных» пакетов. Не советуем изменять значения этих
# параметров.

    SANITY_CHECK="yes"

# Make sure NEW incoming tcp connections are SYN packets

    INTERFACE0_IN_DROP_NEW_WITHOUT_SYN="yes"
    INTERFACE1_IN_DROP_NEW_WITHOUT_SYN="yes"
    NETWORK1_IN_DROP_NEW_WITHOUT_SYN="yes"

# Drop all incoming fragments

    INTERFACE0_IN_DROP_ALL_FRAGMENTS="yes"
    INTERFACE1_IN_DROP_ALL_FRAGMENTS="yes"
    NETWORK1_IN_DROP_ALL_FRAGMENTS="yes"

# Drop all incoming malformed XMAS packets

    INTERFACE0_IN_DROP_XMAS_PACKETS="yes"
    INTERFACE1_IN_DROP_XMAS_PACKETS="yes"
    NETWORK1_IN_DROP_XMAS_PACKETS="yes"

# Drop all incoming malformed NULL packets

    INTERFACE0_IN_DROP_NULL_PACKETS="yes"
    INTERFACE1_IN_DROP_NULL_PACKETS="yes"
    NETWORK1_IN_DROP_NULL_PACKETS="yes"
```

```
#--------------------------------------------------------------------
# Spoofing and bad addresses
#

    REFUSE_SPOOFING="yes"

# Refuse incoming packets claiming to be from the ip addresses of our
interfaces
# Разрешаем пересылку пакетов между наружным и внешним интерфейсом,
# локальной и внешней сетями.
    REFUSE_SPOOFING_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_IN_REFUSE_SPOOFING[0]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[0]="no"
    NETWORK1_IN_REFUSE_SPOOFING[0]="yes"

    REFUSE_SPOOFING_IPADDR[1]=$INTERFACE1_IPADDR
    INTERFACE0_IN_REFUSE_SPOOFING[1]="no"
    INTERFACE1_IN_REFUSE_SPOOFING[1]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[1]="no"

# Refuse incoming packets claiming to be from broadcast-src address range
    REFUSE_SPOOFING_IPADDR[2]="0.0.0.0/8"

# If you provide DHCP services on one of your interfaces, do not forget
to
# set the following option related to that interface to "no"

    INTERFACE0_IN_REFUSE_SPOOFING[2]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[2]="no"
    NETWORK1_IN_REFUSE_SPOOFING[2]="yes"

# Refuse incoming packets claiming to be from reserved loopback address
range

    REFUSE_SPOOFING_IPADDR[3]="127.0.0.0/8"
    INTERFACE0_IN_REFUSE_SPOOFING[3]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[3]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[3]="yes"
# Фильтруем пакеты, отправленные якобы с адресов, зарезервированных
# для локальных сетей. Очень важно не отфильтровать пакеты, приходящие
# из локальной сети на внутренний сетевой интерфейс.

# Refuse incoming packets claiming to be from class A private network
# Если вы используете локальную сеть класса A, то измените значения
# параметров:
#    INTERFACE0_IN_REFUSE_SPOOFING[4]="yes"
#    INTERFACE1_IN_REFUSE_SPOOFING[4]="no"
#    NETWORK1_IN_REFUSE_SPOOFING[4]="no"
REFUSE_SPOOFING_IPADDR[4]="10.0.0.0/8"
    INTERFACE0_IN_REFUSE_SPOOFING[4]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[4]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[4]="yes"

# Refuse incoming packets claiming to be from class B private network
# Если вы используете локальную сеть класса B, то измените значения
# параметров:
#    INTERFACE0_IN_REFUSE_SPOOFING[5]="yes"
#    INTERFACE1_IN_REFUSE_SPOOFING[5]="no"
#    NETWORK1_IN_REFUSE_SPOOFING[5]="no"

    REFUSE_SPOOFING_IPADDR[5]="172.16.0.0/12"
    INTERFACE0_IN_REFUSE_SPOOFING[5]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[5]="yes"
```

```
    NETWORK1_IN_REFUSE_SPOOFING[5]="yes"

# Refuse incoming packets claiming to be from class C private network
# Если вы не используете локальную сеть класса C, то измените значения
# параметров:
#    INTERFACE0_IN_REFUSE_SPOOFING[4]="yes"
#    INTERFACE1_IN_REFUSE_SPOOFING[4]="yes"
#    NETWORK1_IN_REFUSE_SPOOFING[4]="yes"

    REFUSE_SPOOFING_IPADDR[6]="192.168.0.0/16"
    INTERFACE0_IN_REFUSE_SPOOFING[6]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[6]="no"
    NETWORK1_IN_REFUSE_SPOOFING[6]="no"

# Refuse incoming packets claiming to be from class D, E, and unallocated

    REFUSE_SPOOFING_IPADDR[7]="224.0.0.0/3"
    INTERFACE0_IN_REFUSE_SPOOFING[7]="yes"
    INTERFACE1_IN_REFUSE_SPOOFING[7]="yes"
    NETWORK1_IN_REFUSE_SPOOFING[7]="yes"
# Далее приведены настройки, разрешающие работу служб. Если вам
# необходимо отключить какую-нибудь службу, измените значения
# соответствующих параметров с "yes" на "no", или просто закомментируйте
# фрагмент. Для разрешения служб, запрещенных в приведенном примере,
# используйте соответствующие фрагменты из файла
# /lib/giptables/conf/giptables.conf.README
#*********************************************************************
#                                                                    *
#                                  A N Y                             *
#                                                                    *
#  *******************************************************************

    ACCEPT_ANY="no"

#*********************************************************************
#                                                                    *
#                                D N S                               *
#                                                                    *
#*********************************************************************

    ACCEPT_DNS="yes"

#--------------------------------------------------------------------
# DNS outgoing client request
#

# Interface 0 DNS outgoing client request

    INTERFACE0_DNS_CLIENT="yes"

    INTERFACE0_DNS_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_DNS_OUT_DST_IPADDR[0]=$ISP_PRIMARY_DNS_SERVER
    INTERFACE0_DNS_OUT_UDP_REQUEST[0]="yes"
    INTERFACE0_DNS_OUT_TCP_REQUEST[0]="yes"
    INTERFACE0_DNS_OUT_SPORT53_REQUEST[0]="no"

    INTERFACE0_DNS_OUT_SRC_IPADDR[1]=$INTERFACE0_IPADDR
    INTERFACE0_DNS_OUT_DST_IPADDR[1]=$ISP_SECONDARY_DNS_SERVER
    INTERFACE0_DNS_OUT_UDP_REQUEST[1]="yes"
    INTERFACE0_DNS_OUT_TCP_REQUEST[1]="yes"
    INTERFACE0_DNS_OUT_SPORT53_REQUEST[1]="no"

# Network 1 DNS forwarded outgoing client request
```

```
    NETWORK1_DNS_CLIENT="yes"

    NETWORK1_DNS_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_DNS_OUT_DST_IPADDR[0]=$ISP_PRIMARY_DNS_SERVER
    NETWORK1_DNS_OUT_UDP_REQUEST[0]="yes"
    NETWORK1_DNS_OUT_TCP_REQUEST[0]="yes"
    NETWORK1_DNS_OUT_SPORT53_REQUEST[0]="no"

    NETWORK1_DNS_OUT_SRC_IPADDR[1]=$NETWORK1
    NETWORK1_DNS_OUT_DST_IPADDR[1]=$ISP_SECONDARY_DNS_SERVER
    NETWORK1_DNS_OUT_UDP_REQUEST[1]="yes"
    NETWORK1_DNS_OUT_TCP_REQUEST[1]="yes"
    NETWORK1_DNS_OUT_SPORT53_REQUEST[1]="no"

# ------------------------------------------------------------------
# DNS incoming client request
#

# Interface 1 DNS incoming client request

    INTERFACE1_DNS_SERVER="no"

    INTERFACE1_DNS_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_DNS_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE1_DNS_IN_UDP_REQUEST[0]="yes"
    INTERFACE1_DNS_IN_TCP_REQUEST[0]="yes"
    INTERFACE1_DNS_IN_SPORT53_REQUEST[0]="no"

    INTERFACE1_DNS_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_DNS_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR
    INTERFACE1_DNS_IN_UDP_REQUEST[1]="yes"
    INTERFACE1_DNS_IN_TCP_REQUEST[1]="yes"
    INTERFACE1_DNS_IN_SPORT53_REQUEST[1]="no"

#*****************************************************************
#                                                               *
#                          F T P                                *
#                                                               *
#*****************************************************************

    ACCEPT_FTP="yes"

#-----------------------------------------------------------------
# FTP outgoing client request
#

# Interface 0 FTP outgoing client request

    INTERFACE0_FTP_CLIENT="yes"

    INTERFACE0_FTP_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_FTP_OUT_DST_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_FTP_OUT_PASIVE[0]="yes"
    INTERFACE0_FTP_OUT_ACTIVE[0]="no"

# Interface 1 FTP outgoing client request

    INTERFACE1_FTP_CLIENT="yes"

    INTERFACE1_FTP_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_FTP_OUT_DST_IPADDR[0]=$NETWORK1
    INTERFACE1_FTP_OUT_PASIVE[0]="yes"
    INTERFACE1_FTP_OUT_ACTIVE[0]="yes"
```

```
# Network 1 FTP forwarded outgoing client request

    NETWORK1_FTP_CLIENT="yes"

    NETWORK1_FTP_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_FTP_OUT_DST_IPADDR[0]=$ANY_IPADDR
    NETWORK1_FTP_OUT_PASIVE[0]="yes"
    NETWORK1_FTP_OUT_ACTIVE[0]="no"

#-------------------------------------------------------------------
# FTP incoming client request
#

# Interface 1 FTP incoming client request

    INTERFACE1_FTP_SERVER="yes"

    INTERFACE1_FTP_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_FTP_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE1_FTP_IN_PASIVE[0]="yes"
    INTERFACE1_FTP_IN_ACTIVE[0]="yes"

    INTERFACE1_FTP_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_FTP_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR
    INTERFACE1_FTP_IN_PASIVE[1]="yes"
    INTERFACE1_FTP_IN_ACTIVE[1]="yes"

#*******************************************************************
#                                                                  *
#                           S S H                                  *
#                                                                  *
#*******************************************************************

    ACCEPT_SSH="yes"

#-------------------------------------------------------------------
# SSH outgoing client request
#

# Interface 0 SSH outgoing client request

    INTERFACE0_SSH_CLIENT="yes"

    INTERFACE0_SSH_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_SSH_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 SSH outgoing client request

    INTERFACE1_SSH_CLIENT="yes"

    INTERFACE1_SSH_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_SSH_OUT_DST_IPADDR[0]=$NETWORK1

# Network 1 SSH forwarded outgoing client request

    NETWORK1_SSH_CLIENT="yes"

    NETWORK1_SSH_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_SSH_OUT_DST_IPADDR[0]=$ANY_IPADDR

#-------------------------------------------------------------------
# SSH incoming client request
#
```

```
# Interface 0 SSH incoming client request

    INTERFACE0_SSH_SERVER="yes"

    INTERFACE0_SSH_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_SSH_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 SSH incoming client request

    INTERFACE1_SSH_SERVER="yes"

    INTERFACE1_SSH_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_SSH_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_SSH_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_SSH_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR

#*********************************************************************
#                                                                    *
#                       T E L N E T                                  *
#                                                                    *
#*********************************************************************

    ACCEPT_TELNET="no"

#---------------------------------------------------------------------
# TELNET outgoing client request
#

# Interface 0 TELNET outgoing client request

    INTERFACE0_TELNET_CLIENT="yes"

    INTERFACE0_TELNET_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_TELNET_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 TELNET outgoing client request

    INTERFACE1_TELNET_CLIENT="yes"

    INTERFACE1_TELNET_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_TELNET_OUT_DST_IPADDR[0]=$NETWORK1

# Network 1 TELNET forwarded outgoing client request

    NETWORK1_TELNET_CLIENT="yes"

    NETWORK1_TELNET_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_TELNET_OUT_DST_IPADDR[0]=$ANY_IPADDR

#---------------------------------------------------------------------
# TELNET incoming client request
#

# Interface 1 TELNET incoming client request

    INTERFACE1_TELNET_SERVER="no"

    INTERFACE1_TELNET_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_TELNET_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_TELNET_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_TELNET_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR
```

```
#*********************************************************************
#                                                                    *
#                        T E L N E T S                               *
#                                                                    *
#*********************************************************************

    ACCEPT_TELNETS="no"

#*********************************************************************
#                                                                    *
#                          S M T P                                   *
#                                                                    *
#*********************************************************************

    ACCEPT_SMTP="yes"

#_--------------------------------------------------------------------
# SMTP outgoing client request
#

# Interface 0 SMTP outgoing client request

    INTERFACE0_SMTP_CLIENT="yes"
    INTERFACE0_SMTP_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_SMTP_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Network 1 SMTP forwarded outgoing client request

    NETWORK1_SMTP_CLIENT="yes"

    NETWORK1_SMTP_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_SMTP_OUT_DST_IPADDR[0]=$ANY_IPADDR

#--------------------------------------------------------------------
# SMTP incoming client request
#

# Interface 0 SMTP incoming client request

    INTERFACE0_SMTP_SERVER="no"

    INTERFACE0_SMTP_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_SMTP_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 SMTP incoming client request

    INTERFACE1_SMTP_SERVER="no"

    INTERFACE1_SMTP_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_SMTP_IN_DST_IPADDR[0]=$INTERFACE1_IPADDR

#*********************************************************************
#                                                                    *
#                          S M T P S                                 *
#                                                                    *
#*********************************************************************

    ACCEPT_SMTPS="no"

#*********************************************************************
#                                                                    *
#                          P O P 3                                   *
#                                                                    *
#*********************************************************************
```

```
    ACCEPT_POP3="yes"

#-----------------------------------------------------------------------
# POP3 outgoing client request
#

# Network 1 POP3 forwarded outgoing client request

    NETWORK1_POP3_CLIENT="yes"

    NETWORK1_POP3_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_POP3_OUT_DST_IPADDR[0]=$ANY_IPADDR

#-----------------------------------------------------------------------
# POP3 incoming client request
#

# Interface 0 POP3 incoming client request

    INTERFACE0_POP3_SERVER="no"

    INTERFACE0_POP3_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_POP3_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 POP3 incoming client request

    INTERFACE1_POP3_SERVER="no"

    INTERFACE1_POP3_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_POP3_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_POP3_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_POP3_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR

#**********************************************************************
*
#
*
#                               P O P 3 S
*
#
*
#**********************************************************************
*

    ACCEPT_POP3S="no"

#-----------------------------------------------------------------------
-
# POP3S outging client request
#

# Network 1 POP3S forwarded outging client request

    NETWORK1_POP3S_CLIENT="yes"

    NETWORK1_POP3S_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_POP3S_OUT_DST_IPADDR[0]=$ANY_IPADDR

#-----------------------------------------------------------------------
-
# POP3S incoming client request
#
```

```
# Interface 0 POP3S incoming client request

    INTERFACE0_POP3S_SERVER="no"

    INTERFACE0_POP3S_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_POP3S_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 POP3S incoming client request

    INTERFACE1_POP3S_SERVER="no"

    INTERFACE1_POP3S_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_POP3S_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_POP3S_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_POP3S_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR

#*********************************************************************
#                                                                    *
#                            I M A P                                 *
#                                                                    *
#*********************************************************************

    ACCEPT_IMAP="yes"

#--------------------------------------------------------------------
# IMAP outgoing client request
#

# Network 1 IMAP forwarded outgoing client request

    NETWORK1_IMAP_CLIENT="yes"

    NETWORK1_IMAP_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_IMAP_OUT_DST_IPADDR[0]=$ANY_IPADDR

#_--------------------------------------------------------------------
-
# IMAP incoming client request
#

# Interface 0 IMAP incoming client request

    INTERFACE0_IMAP_SERVER="no"

    INTERFACE0_IMAP_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_IMAP_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 IMAP incoming client request

    INTERFACE1_IMAP_SERVER="no"

    INTERFACE1_IMAP_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_IMAP_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_IMAP_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_IMAP_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR
#*********************************************************************
#                                                                    *
#                            I M A P S                               *
#                                                                    *
#*********************************************************************
```

```
    ACCEPT_IMAPS="no"

#-----------------------------------------------------------------------
# IMAPS outgoing client request
#

# Network 1 IMAPS forwarded outgoing client request

    NETWORK1_IMAPS_CLIENT="yes"

    NETWORK1_IMAPS_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_IMAPS_OUT_DST_IPADDR[0]=$ANY_IPADDR

#-----------------------------------------------------------------------
# IMAPS incoming client request
#

# Interface 0 IMAPS incoming client request

    INTERFACE0_IMAPS_SERVER="no"

    INTERFACE0_IMAPS_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_IMAPS_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 IMAPS incoming client request

    INTERFACE1_IMAPS_SERVER="no"

    INTERFACE1_IMAPS_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_IMAPS_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_IMAPS_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_IMAPS_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR
#**********************************************************************
*
#
*
#                               H T T P
*
#
*
#**********************************************************************
*

    ACCEPT_HTTP="yes"

#-----------------------------------------------------------------------
-
# HTTP outgoing client request
#

# Network 1 HTTP forwarded outgoing client request

    NETWORK1_HTTP_CLIENT="yes"

    NETWORK1_HTTP_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_HTTP_OUT_DST_IPADDR[0]=$ANY_IPADDR

#-----------------------------------------------------------------------
-
# HTTP incoming client request
#

# Interface 0 HTTP incoming client request
```

```
    INTERFACE0_HTTP_SERVER="no"

    INTERFACE0_HTTP_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_HTTP_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 HTTP incoming client request

    INTERFACE1_HTTP_SERVER="no"

    INTERFACE1_HTTP_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_HTTP_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_HTTP_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_HTTP_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR
#*********************************************************************
#                                                                     *
#                              H T T P S                              *
#                                                                     *
#*********************************************************************

    ACCEPT_HTTPS="yes"

#---------------------------------------------------------------------
# HTTPS outgoing client request
#

# Network 1 HTTPS forwarded outgoing client request

    NETWORK1_HTTPS_CLIENT="yes"

    NETWORK1_HTTPS_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_HTTPS_OUT_DST_IPADDR[0]=$ANY_IPADDR

#---------------------------------------------------------------------
# HTTPS incoming client request
#

# Interface 0 HTTPS incoming client request

    INTERFACE0_HTTPS_SERVER="no"

    INTERFACE0_HTTPS_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_HTTPS_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 HTTPS incoming client request

    INTERFACE1_HTTPS_SERVER="no"

    INTERFACE1_HTTPS_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_HTTPS_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_HTTPS_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_HTTPS_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR
#*********************************************************************
*
#
*
#                               S Q U I D
*
#
*
#(*********************************************************************
*
```

```
    ACCEPT_SQUID="no" # Squid in Proxy-Caching Mode

#*********************************************************************
#                                                                     *
#                          W E B C A C H E                            *
#                                                                     *
#*********************************************************************

    ACCEPT_WEBCACHE="no" # Squid in HTTPD-Accelerator Mode

#---------------------------------------------------------------------
# WEBCACHE outgoing client request
#

# Network 1 WEBCACHE forwarded outgoing client request

    NETWORK1_WEBCACHE_CLIENT="yes"

    NETWORK1_WEBCACHE_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_WEBCACHE_OUT_DST_IPADDR[0]=$ANY_IPADDR

#---------------------------------------------------------------------
# WEBCACHE incoming client request
#

# Interface 0 WEBCACHE incoming client request

    INTERFACE0_WEBCACHE_SERVER="no"

    INTERFACE0_WEBCACHE_IN_SRC_IPADDR[0]=$ANY_IPADDR
    INTERFACE0_WEBCACHE_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

# Interface 1 WEBCACHE incoming client request

    INTERFACE1_WEBCACHE_SERVER="no"

    INTERFACE1_WEBCACHE_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_WEBCACHE_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_WEBCACHE_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_WEBCACHE_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR

#*********************************************************************
#                                                                     *
#                            S O C K S                                *
#                                                                     *
#*********************************************************************

    ACCEPT_SOCKS="no"

#*********************************************************************
*
#
*
#                             N N T P
*
#
*
#*********************************************************************
*

    ACCEPT_NNTP="yes"
```

```
#-------------------------------------------------------------------------
-
# NNTP outgoing client request
#

# Network 1 NNTP forwarded outgoing client request

    NETWORK1_NNTP_CLIENT="yes"

    NETWORK1_NNTP_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_NNTP_OUT_DST_IPADDR[0]=$ANY_IPADDR

#*************************************************************************
**
#
*
#                               N N T P S
*
#
*
#*************************************************************************
**

    ACCEPT_NNTPS="no"

#*************************************************************************
**
#
*
#                               M Y S Q L
*
#
*
#*************************************************************************
**

    ACCEPT_MYSQL="no"

#
*************************************************************************
**
#
*
#                           P O S T G R E S
*
#
*
#
**********************************************************************

    ACCEPT_POSTGRES="no"

#*************************************************************************
**
#
*
#                             O R A C L E
*
#
*
#*************************************************************************
**

    ACCEPT_ORACLE="no"
```

```
#*****************************************************************************
**
#
*
#                               M S S Q L
*
#
*
#*****************************************************************************
**

    ACCEPT_MSSQL="no"

#*****************************************************************************
**
#
*
#                               L D A P
*
#
*
#*****************************************************************************
**

    ACCEPT_LDAP="no"

#*****************************************************************************
**
#
*
#                               L D A P S
*
#
*
#*****************************************************************************
**

    ACCEPT_LDAPS="no"

#*****************************************************************************
#                                                                            *
#                             A U T H                                        *
#                                                                            *
#*****************************************************************************

    ACCEPT_AUTH="no"

#-----------------------------------------------------------------------------
# AUTH outgoing client request
#

# Reject, rather than deny, the outgoing auth client packets (Net-HOWTO)

    INTERFACE0_AUTH_OUT_REJECT="yes"
    INTERFACE1_AUTH_OUT_REJECT="yes"
    NETWORK1_AUTH_OUT_REJECT="yes"

#-----------------------------------------------------------------------------
# AUTH incoming client request
#

# Reject, rather than deny, the incoming auth client packets (Net-HOWTO)
```

```
    INTERFACE0_AUTH_IN_REJECT="yes"
    INTERFACE1_AUTH_IN_REJECT="yes"
    NETWORK1_AUTH_IN_REJECT="yes"

#-----------------------------------------------------------------------
# AUTH outgoing client request
#

# Interface 0 AUTH outgoing client request

    INTERFACE0_AUTH_CLIENT="yes"

    INTERFACE0_AUTH_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_AUTH_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 AUTH outgoing client request

    INTERFACE1_AUTH_CLIENT="yes"

    INTERFACE1_AUTH_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_AUTH_OUT_DST_IPADDR[0]=$NETWORK1

# Network 1 AUTH forwarded outgoing client request

    NETWORK1_AUTH_CLIENT="yes"

    NETWORK1_AUTH_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_AUTH_OUT_DST_IPADDR[0]=$ANY_IPADDR

#***********************************************************************
#                                                                      *
#                            W H O I S                                 *
#                                                                      *
#***********************************************************************

    ACCEPT_WHOIS="no"

#-----------------------------------------------------------------------
# WHOIS outgoing client request
#

# Interface 0 WHOIS outgoing client request

    INTERFACE0_WHOIS_CLIENT="yes"

    INTERFACE0_WHOIS_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_WHOIS_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 WHOIS outgoing client request

    INTERFACE1_WHOIS_CLIENT="yes"

    INTERFACE1_WHOIS_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_WHOIS_OUT_DST_IPADDR[0]=$NETWORK1

# Network 1 WHOIS forwarded outgoing client request

    NETWORK1_WHOIS_CLIENT="yes"

    NETWORK1_WHOIS_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_WHOIS_OUT_DST_IPADDR[0]=$ANY_IPADDR

#***********************************************************************
#                                                                      *
```

```
#                            F I N G E R                                      *
#                                                                             *
#*****************************************************************************

    ACCEPT_FINGER="no"

#-----------------------------------------------------------------------------
# FINGER outgoing client request
#

# Interface 0 FINGER outgoing client request

    INTERFACE0_FINGER_CLIENT="yes"

    INTERFACE0_FINGER_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_FINGER_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 FINGER outgoing client request

    INTERFACE1_FINGER_CLIENT="yes"

    INTERFACE1_FINGER_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_FINGER_OUT_DST_IPADDR[0]=$NETWORK1

# Network 1 FINGER forwarded outgoing client request

    NETWORK1_FINGER_CLIENT="yes"

    NETWORK1_FINGER_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_FINGER_OUT_DST_IPADDR[0]=$ANY_IPADDR

#*****************************************************************************
#                                                                             *
#                               N T P                                         *
#                                                                             *
#*****************************************************************************

    ACCEPT_NTP="no"

#-----------------------------------------------------------------------------
# NTP outgoing client request
#

# Interface 0 NTP outgoing client request

    INTERFACE0_NTP_CLIENT="yes"

    INTERFACE0_NTP_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_NTP_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 NTP outgoing client request

    INTERFACE1_NTP_CLIENT="yes"

    INTERFACE1_NTP_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_NTP_OUT_DST_IPADDR[0]=$NETWORK1

# Network 1 NTP forwarded outgoing client request

    NETWORK1_NTP_CLIENT="yes"

    NETWORK1_NTP_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_NTP_OUT_DST_IPADDR[0]=$ANY_IPADDR
```

```
#*************************************************************************
#                                                                        *
#                              S N M P                                   *
#                                                                        *
#*************************************************************************

    ACCEPT_SNMP="no"

#*************************************************************************
#                                                                        *
#                               X 1 1                                    *
#                                                                        *
#*************************************************************************

    ACCEPT_X11="no"

#*************************************************************************
#                                                                        *
#                               V N C                                    *
#                                                                        *
#*************************************************************************

    ACCEPT_VNC="no"

#*************************************************************************
*
#
*
#                                L P D
*
#
*
#*************************************************************************
*

    ACCEPT_LPD="no"

#*************************************************************************
*
#
*
#                            N E T B I O S
*
#
*
#*************************************************************************
*

    ACCEPT_NETBIOS="no"

#-------------------------------------------------------------------------
-
# NETBIOS outgoing client request
#

# Interface 1 NETBIOS outgoing client request

    INTERFACE1_NETBIOS_CLIENT="yes"

    INTERFACE1_NETBIOS_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_NETBIOS_OUT_DST_IPADDR[0]=$NETWORK1

#-------------------------------------------------------------------------
-
```

```
# NETBIOS incoming client request
#

# Interface 1 NETBIOS incoming client request

    INTERFACE1_NETBIOS_SERVER="no"

    INTERFACE1_NETBIOS_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_NETBIOS_IN_DST_IPADDR[0]=$INTERFACE1_IPADDR

#*********************************************************************
*
#
*
#                            S Y S L O G
*
#
*
#*********************************************************************
*

    ACCEPT_SYSLOG="no"

#---------------------------------------------------------------------
-
# SYSLOG outgoing client request
#

# Interface 1 SYSLOG outgoing client request

    INTERFACE1_SYSLOG_CLIENT="yes"

    INTERFACE1_SYSLOG_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_SYSLOG_OUT_DST_IPADDR[0]=$SYSLOG_SERVER

#*********************************************************************
#
*
#                        T R A C E R O U T E
*
#
*
#*********************************************************************
*

    ACCEPT_TRACEROUTE="yes"

#---------------------------------------------------------------------
# TRACEROUTE outgoing client request
#

# Interface 0 TRACEROUTE outgoing client request

    INTERFACE0_TRACEROUTE_CLIENT="yes"

    INTERFACE0_TRACEROUTE_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_TRACEROUTE_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 TRACEROUTE outgoing client request

    INTERFACE1_TRACEROUTE_CLIENT="yes"

    INTERFACE1_TRACEROUTE_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_TRACEROUTE_OUT_DST_IPADDR[0]=$NETWORK1
```

```
# Network 1 TRACEROUTE forwarded outgoing client request

    NETWORK1_TRACEROUTE_CLIENT="yes"

    NETWORK1_TRACEROUTE_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_TRACEROUTE_OUT_DST_IPADDR[0]=$ANY_IPADDR

#-------------------------------------------------------------------------
-
# TRACEROUTE incoming client request
#

# Interface 1 TRACEROUTE incoming client request

    INTERFACE1_TRACEROUTE_SERVER="yes"

    INTERFACE1_TRACEROUTE_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_TRACEROUTE_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_TRACEROUTE_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_TRACEROUTE_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR

#************************************************************************
#                                                                       *
#                            I C M P                                    *
#                                                                       *
#************************************************************************

    ACCEPT_ICMP="yes"

#-------------------------------------------------------------------------
# ICMP outgoing client request
#

# Interface 0 ICMP outgoing client request

    INTERFACE0_ICMP_CLIENT="yes"

    INTERFACE0_ICMP_OUT_SRC_IPADDR[0]=$INTERFACE0_IPADDR
    INTERFACE0_ICMP_OUT_DST_IPADDR[0]=$ANY_IPADDR

# Interface 1 ICMP outgoing client request

    INTERFACE1_ICMP_CLIENT="yes"

    INTERFACE1_ICMP_OUT_SRC_IPADDR[0]=$INTERFACE1_IPADDR
    INTERFACE1_ICMP_OUT_DST_IPADDR[0]=$NETWORK1

# Network 1 ICMP forwarded outgoing client request

    NETWORK1_ICMP_CLIENT="yes"

    NETWORK1_ICMP_OUT_SRC_IPADDR[0]=$NETWORK1
    NETWORK1_ICMP_OUT_DST_IPADDR[0]=$ANY_IPADDR

#-------------------------------------------------------------------------
# ICMP incoming client request
#

# Interface 1 ICMP incoming client request

    INTERFACE1_ICMP_SERVER="yes"
```

```
    INTERFACE1_ICMP_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_ICMP_IN_DST_IPADDR[0]=$INTERFACE0_IPADDR

    INTERFACE1_ICMP_IN_SRC_IPADDR[1]=$NETWORK1
    INTERFACE1_ICMP_IN_DST_IPADDR[1]=$INTERFACE1_IPADDR

#*********************************************************************
#                                                                     *
#                           D H C P                                   *
#                                                                     *
#*********************************************************************

    ACCEPT_DHCP="yes"

#---------------------------------------------------------------------
# DHCP incoming client request
#

# Interface 1 DHCP incoming client request

    INTERFACE1_DHCP_SERVER="yes"

# If above option is "yes", do not forget to configure the following
# lines in the "Spoofing and bad addresses" section
# REFUSE_SPOOFING_IPADDR[2]="0.0.0.0/8"
# INTERFACE1_IN_REFUSE_SPOOFING[2]="no"

    INTERFACE1_DHCP_IN_SRC_IPADDR[0]=$NETWORK1
    INTERFACE1_DHCP_IN_DST_IPADDR[0]=$INTERFACE1_IPADDR

#*********************************************************************
*
#
*
#                               E N D
*
#
*
#*********************************************************************
*

    DROP_EVERYTHING_FROM_HERE="yes"

#---------------------------------------------------------------------
-
# LOG & DROP everything from here... just in case.
#

    INTERFACE0_IN_DROP_EVERYTHING_FROM_HERE="yes"
    INTERFACE1_IN_DROP_EVERYTHING_FROM_HERE="yes"
    NETWORK1_IN_DROP_EVERYTHING_FROM_HERE="yes"

#---------------------------------------------------------------------
-
# End of file
```

Шаг 4

Перезагрузите GIPTables Firewall:

```
[root@bastion /]# /etc/init.d./giptables restart
```

Часть 3

Криптографическое программное обеспечение, используемое для безопасной передачи данных и проверки подлинности и целостности электронных документов

Глава 11

GnuPG – утилита для безопасного хранения и передачи данных

В этой главе

GnuPG – утилита для безопасной передачи и хранения данных. Используется для шифрования данных и создания цифровых подписей, включает управления базой данных ключей и соответствует стандарту OpenPGP. GnuPG – свободно распространяемая утилита, не использующая запатентованных алгоритмов, поэтому она, к сожалению, не совместима с PGP2.

Одной из наиболее важных областей применения утилиты является проверка подлинности получаемых программ. GnuPG позволяет с высокой степенью достоверности установить, что коды устанавливаемого программного обеспечения не были модифицированы при транспортировке от разработчика к вам по сетям общего пользования.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

ЗАМЕЧАНИЕ В некоторых странах ввоз, распространение и использование программного обеспечения для криптографии запрещено.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта GnuPG по состоянию на 19.03.2003. Регулярно посещайте домашнюю страницу проекта `http://www.gnupg.org/` и отслеживайте обновления.

Исходные коды GnuPG содержатся в архиве `gnupg-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `gnupg-1.2.1.tar.gz`).

Для нормальной инсталляции и работы программного обеспечения необходимо, чтобы в системе были установлены пакеты `gettext-0.11.1-2.i386.rpm`, `python-1.5.2-38.3asp.i386.rpm`, `expat-1.95.2-2.i386.rpm` и `gmp-4.0.1-3.i386.rpm`.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет `gnupg` с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq gnupg
```

Если вы следовали нашим рекомендациям, то пакет не установлен.

Шаг 2

Перейдите в каталог, где находится пакет `gnupg-1.0.6-5.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

и установите:

```
[root@drwalbr distrib]# rpm –ihv gnupg-1.0.6-5.asp.i386.rpm
```

или обновите пакет:

```
[root@drwalbr distrib]# rpm –Uhv gnupg-1.0.6-5.asp.i386.rpm
```

После установки пакета перейдите к тестированию утилиты GnuPG, описанной ниже.

Компиляция, оптимизация и инсталляция GnuPG

Для конфигурирования, компилирования и оптимизации GnuPG из исходных кодов выполните следующие действия.

Шаг 1

Проверьте подлинность полученного архива с исходными кодами GnuPG. Для этого необходимо сравнить контрольную сумму MD5 пакета:

```
[root@drwalbr /]# md5sum gnupg-1.2.1.tar.gz
83e02b4905dab34c4dc25652936022f9  gnupg-1.2.1.tar.gz
```

с контрольной суммой, указанной на сервере разработчика:

```
[root@drwalbr /]# lynx http://www.gnupg.org/download/index.html
#                            Download - GnuPG.org (p4 of 9)

   We suggest that you download the GNU Privacy Guard from a mirror site
   close to you. See our list of mirrors. To locate a source package
…
GnuPG 1.2.1 source compressed using gzip. 2.5MB S FTP HTTP
Signature and MD5 checksum for previous file.
83e02b4905dab34c4dc25652936022f9  gnupg-1.2.1.tar.gz    FTP HTTP
…
```

Шаг 2

Разархивируйте исходные коды в каталоге `/var/tmp`:

```
[root@drwalbr /]# cd /var/tmp
[root@drwalbr tmp]# tar xzpf gnupg-1.2.1.tar.gz
```

Шаг 3

Сконфигурируйте исходные коды программы:

```
[root@drwalbr tmp]# cd gnupg-1.2.1/
[root@drwalbrgnupg-1.2.1]# CFLAGS="-O2 -march=i686 -funroll-loops"; ex-
port CFLAGS
./configure \
--prefix=/usr \
--mandir=/usr/share/man \
--infodir=/usr/share/info \
--disable-nls
```

При таких параметрах конфигурации осуществляется оптимизация применительно к архитектуре процессора i686, определяются каталоги для размещения соответствующих файлов и отключается поддержка языков, отличных от английского.

Шаг 4

Откомпилируйте исходные коды, проверьте правильность компиляции и наличие соответствующих библиотек, проинсталлируйте файлы GnuPG, создайте и сохраните список инсталлированных файлов:

```
[root@drwalbr gnupg-1.2.1]# make
[root@drwalbr gnupg-1.2.1]# make check
Making check in intl
make[1]: Вход в каталог `/home/gnupg/gnupg-1.2.1/intl`
make[1]: Цель `check` не требует выполнения команд.
make[1]: Выход из каталог `/home/gnupg/gnupg-1.2.1/intl`
…
home: .
Supported algorithms:
Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA, ELG
Cipher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
Hash: MD5, SHA1, RIPEMD160
Compress: Uncompressed, ZIP, ZLIB
PASS: version.test
Hash algorithm TIGER/192 is not installed
```

ЗАМЕЧАНИЕ TIGER – является экспериментальным алгоритмом, поэтому мы не включили его в число устанавливаемых компонентов. Для его включения на этапе конфигурирования исходных кодов необходимо использовать опции `--enable-tiger` и `--enable-new-tiger`.

```
PASS: mds.test
PASS: decrypt.test
PASS: decrypt-dsa.test
PASS: sigs.test
PASS: sigs-dsa.test
PASS: encrypt.test
PASS: encrypt-dsa.test
PASS: seat.test
PASS: clearsig.test
PASS: encryptp.test
PASS: detach.test
PASS: armsigs.test
PASS: armencrypt.test
PASS: armencryptp.test
PASS: signencrypt.test
PASS: signencrypt-dsa.test
PASS: armsignencrypt.test
PASS: armdetach.test
PASS: armdetachm.test
PASS: detachm.test
PASS: genkey1024.test
PASS: conventional.test
PASS: conventional-mdc.test
PASS: multisig.test
==================
All 25 tests passed
==================
make[2]: Выход из каталог `/home/gnupg/gnupg-1.2.1/checks`
make[1]: Выход из каталог `/home/gnupg/gnupg-1.2.1/checks`
make[1]: Вход в каталог `/home/gnupg/gnupg-1.2.1`
make[1]: Цель `check-am` не требует выполнения команд.
make[1]: Выход из каталог `/home/gnupg/gnupg-1.2.1`

[root@drwalbr gnupg-1.2.1]# find /* > /root/gnupg1
[root@drwalbr gnupg-1.2.1]# make install
[root@drwalbr gnupg-1.2.1]# strip /usr/bin/gpg
[root@drwalbr gnupg-1.2.1]# strip /usr/bin/gpgv
[root@drwalbr gnupg-1.2.1]# find /* > /root/gnupg2
[root@drwalbr   gnupg-1.2.1]#   diff   /root/gnupg1   /root/gnupg2   >
/root/gnupg.installed
[root@drwalbr gnupg-1.2.1]# mv /root/gnupg.installed
/very_reliable_place/gnupg.installed.YYYYMMDD
```

Шаг 5

Удалите архив с исходными кодами и каталог `gnupg-1.2.1`:

```
[root@drwalbr gnupg-1.2.1]# cd /var/tmp
[root@drwalbr tmp]# rm -rf gnupg-1.2.1/
[root@drwalbr tmp]# rm -f gnupg-1.2.1.tar.gz
```

Тестирование GnuPG

Для тестирования GnuPG создайте, как минимум, для двух пользователей вашей системы секретную пару ключей (открытый и закрытый ключ), проверьте возможность шифрования сообщения одним из пользователей и возможность расшифровки другим.

Шаг 1

Установите права доступа к файлу `/usr/bin/gpg`:

```
[root@drwalbr tmp]# chmod 4755 /usr/bin/gpg
```

Шаг 2

Зарегистрируйтесь в системе в качестве обычного пользователя, например, sergey.

```
[sergey@drwalbr sergey]$ cd
```

Шаг 3

Если вы впервые создаете ключи для пользователя sergey, наберите:

```
[sergey@drwalbr sergey]$ gpg --gen-key
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
gpg: /home/sergey/.gnupg: directory created
gpg: new configuration file `/home/sergey/.gnupg/gpg.conf' created
gpg: keyblock resource `/home/sergey/.gnupg/secring.gpg': file open error
gpg: keyring `/home/sergey/.gnupg/pubring.gpg' created
Please select what kind of key you want:
(1) DSA and ElGamal (default)
(2) DSA (sign only)
(5) RSA (sign only)
Your selection?
```

и прервите выполнение программы:

```
<Ctrl>+C
```

Это необходимо для того, чтобы программа gpg создала необходимые файлы и каталоги в домашнем каталоге пользователя. Если ключи для пользователя уже создавались ранее, перейдите к следующему шагу.

Шаг 4

Запустите gpg:

```
[sergey@drwalbr sergey]$ gpg --gen-key
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
gpg: keyring `/home/sergey/.gnupg/secring.gpg' created
Please select what kind of key you want:
(1) DSA and ElGamal (default)
(2) DSA (sign only)
(5) RSA (sign only)
```

Выберите тип ключа, предлагаемый по умолчанию:

```
Your selection? 1
DSA keypair will have 1024 bits.
About to generate a new ELG-E keypair.
minimum keysize is 768 bits
default keysize is 1024 bits
highest suggested keysize is 2048 bits
```

Выберите длину ключа, предлагаемую по умолчанию:

```
What keysize do you want? (1024)<Enter>
Requested keysize is 1024 bits
Please specify how long the key should be valid.
0 = key does not expire
<n> = key expires in n days
<n>w = key expires in n weeks
<n>m = key expires in n months
<n>y = key expires in n years
```

Выберите срок действия ключа (1 год):

```
Key is valid for? (0) 1y
Key expires at Чтв 18 Мар 2004 15:43:18 MSK
```

Подтвердите правильность введенных данных:

```
Is this correct (y/n)? y
```

```
You need a User-ID to identify your key; the software constructs the user
id
from Real Name, Comment and Email Address in this form:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
```

Введите имя пользователя:

```
Real name: Sergey Karlov
```

Введите имя e-mail пользователя:

```
Email address: sergey@drwalbr.und
```

Введите, если хотите, какие-либо комментарии, касающиеся пользователя, в противном случае:

```
Comment:<Enter>
You selected this USER-ID:
"Sergey Karlov <sergey@drwalbr.und>"
```

Вам предоставляется возможность отредактировать ID пользователя, по которому будет идентифицироваться ключи. В рассматриваемом примере – это **"Sergey Karlov <sergey@drwalbr.und>"**. Если все правильно, то:

```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

В противном случае используйте опции `N`, `C` и `E` для изменения имени пользователя, комментария и адреса электронной почты, соответственно.

```
You need a Passphrase to protect your secret key.
```

Введите пароль для защиты секретного ключа.

```
Passphrase:$ecretnoe_$lovo_Sergeya
```

Далее система в автоматическом режиме осуществит генерацию ключей. В это время следует подвигать мышку, понажимать кнопки на клавиатуре для повышения степени энтропии в вашей системе.

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.+++++.+++++..+++++++++++++++++++++++++++++...++++++++++.++++++++++.++++
+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++.++++++++++>++
++++++++.........+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++.+++++..++++++++++>+++++.....+
++++^^^
gpg: /home/sergey/.gnupg/trustdb.gpg: trustdb created
public and secret key created and signed.
key marked as ultimately trusted.
pub 1024D/5BC241B3 2003-03-19 Sergey Karlov <sergey@drwalbr.und>
Key fingerprint = D155 D3C4 F19A 5859 3A66 9108 99E5 5EBA 5BC2 41B3
sub 1024g/69CADC7B 2003-03-19 [expires: 2004-03-18]
```

Шаг 5

Экспортируйте открытый ключ:

```
[sergey@drwalbr sergey]$ gpg --export -ao sergey.asc
```

В результате в домашнем каталоге пользователя `sergey` будет создан файл `sergey.asc`:

```
[sergey@drwalbr sergey]$ cat sergey.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (GNU/Linux)

mQGiBD54ZjQRBADBezMOEg0kncSEcIV7F47AfAXXz1WtR3y/cY38o2ZeiLTo0POF
qS0aescQaU5/MU0CT7ipcD91rbcKbNLzgz4xf4jMBl3rr/qXn9xAKogPAwTvZYZL
t15ouGuAQTU25E1OAp5C/71Ro9kOK9ZBxkuWz+kfp5Ctc5t0UdMIOewBawCg7Tq7
```

```
/z7yrIUj0TpBGOpua8M32QsD/2ZhcUDTTBO6WBYMbTbWOoMrNxYfUqB4f3H24h9h
uw3e+K9wP2HFCq1BxnDO6+IBYQLntscH2kQ4hYuipEFq+iZIDrPvUfDeNs9bR33z
B+cEkGUsbE4auuQ9iD5fu3va4EJolM5EGvwp9LZBpz82i3H/2kgdTrlK3YFT7UQT
IWk4A/4nKzDomsEmm6SAkz6gpxorkTTedHXXv8E7Z+4cwjWH1h/LKKzGG2IwqpyN
liQiUHvLdQJ/fOQMiF907eWk3c/WWiMCQo1sAEJO8Y2yS5+iFzuKFisbIOmAHWMD
dWdkB6+iSz3iZkk7wlfYG2zCLt5ET834u+dAWQwc8VN2VlpE7LQiU2VyZ2V5IEth
cmxvdiA8c2VyZ2V5QGRyd2FsYnIudW5kPohfBBMRAgAfBQI+eGY0BQkB4TOABAsH
AwIDFQIDAxYCAQIeAQIXgAAKCRCZ5V66W8JBsy/jAKCrGteDpQ45JcEzgxACnBAI
vPF/3QCgpgeS3u5BBOAA1ZcsaJ0k8tnuMEG5AQ0EPnhmNRAEAOC+GW3G5FOp1aHJ
cVF+zuRRZ+oeaPRoWJwGfZ+KR5L3YYO8kP/3eeRZ5Gnp0KyJ80VCeilaJpepjot6
lrqwpRbF/oGY4qHn/a6ubPmqza+sq2ttYSDx0QkTLMiI6qbekrUxa2jNgEcXr6gJ
ig92U8cQWO+wXT4xtxMLldnhZAO3AAMFBACaH6pNG7zAT/QIgFgwNTT+roBUJGze
lFb4eUMzSSBtEi3o3NgHt6gHqkglYOZeo8wBR+lzr69Aoq8zLpSSWzY/iHjcc/p7
XflKlaiL6yqZNwSjO6aki/Hqlq9pTrxyuSIhz2jWfuzvEqoJHp1pLXbd0DbZvNs5
Wc93PcctqRx/64hMBBgRAgAMBQI+eGY1BQkB4TOAAAoJEJnlXrpbwkGzRSgAoOLL
N9siEQqzYa1ujl9y/GEQmHwbAJ9smVzY7PaLOGUIWA2Zxe+XXy0cjw==
=o1IS
-----END PGP PUBLIC KEY BLOCK-----
```

Файл `sergey.asc`, содержащий открытый ключ пользователя `sergey`, нужно передать всем пользователям, с которыми он предполагает обмениваться зашифрованными файлами. Файл может быть выложен на Web -сервере пользователя или разослан по электронной почте.

Шаг 6

Зарегистрируйтесь в системе в качестве другого пользователя, например `valentine` и повторите шаги 1…5.

Шаг 7

Поместите открытый ключ пользователя `sergey` в домашний каталог пользователя `valentine`, а открытый ключ пользователя `valentine` в домашний каталог пользователя `sergey`.

Шаг 8

Подпишите открытые ключи.

Для пользователя `sergey`:

```
[sergey@drwalbr sergey]$ gpg --sign valentine.asc

You need a passphrase to unlock the secret key for
user: "Sergey Karlov <sergey@drwalbr.und>"
1024-bit DSA key, ID 5BC241B3, created 2003-03-19
```

Введите пароль, который использовался для защиты закрытого ключа в шаге 4:

```
Enter passphrase: $ecretnoe_$lovo_Sergeya
```

Для пользователя `valentine`:

```
[valentine@drwalbr valentine]$ gpg --sign sergey.asc

You need a passphrase to unlock the secret key for
user: "Valentine Bruy <valentine@drwalbr.und>"
1024-bit DSA key, ID F3238EE5, created 2003-03-19
```

Введите пароль, который использовался для защиты закрытого ключа в шаге 4:

```
Enter passphrase: $ecretnoe_$lovo_Valentine
```

Шаг 9

От имени пользователя `valentine` создайте сообщение для пользователя `sergey`:

```
[valentine@drwalbr valentine]$ echo Привет, Сергей ! = Валентин > mes-
sage_to_sergey
```

Шаг 10

Зашифруйте сообщение:

```
[valentine@drwalbr valentine]$ gpg -sear sergey@drwalbr.und mes-
sage_to_sergey
You need a passphrase to unlock the secret key for
```

```
user: "Valentine Bruy <valentine@drwalbr.und>"
1024-bit DSA key, ID F3238EE5, created 2003-03-19
```

Введите пароль для секретного ключа:

```
Enter passphrase: $ecretnoe_$lovo_Valentine

gpg: checking the trustdb
gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: next trustdb check due at 2004-03-18
gpg: 69CADC7B: There is no indication that this key really belongs to the
owner
1024g/69CADC7B 2003-03-19 "Sergey Karlov <sergey@drwalbr.und>"
Primary key fingerprint: D155 D3C4 F19A 5859 3A66 9108
99E5 5EBA 5BC2 41B3
Subkey fingerprint: 456F C70F 8F64 38B3 B6F4 E900
70C3 B3B8 69CA DC7B

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes
```

Подтвердите использования ключа:

```
Use this key anyway? yes
```

В результате в домашнем каталоге появился файл `message_to_sergey.asc`. Следует отметить, что вместо указания адреса электронной почты, используемого при шифровании сообщения, можно использовать имя пользователя (первую часть идентификатора пользователя), т. е. команды:

```
[valentine@drwalbr valentine]$ gpg -sear sergey@drwalbr.und mes-
sage_to_sergey
```

и

```
[valentine@drwalbr valentine]$ gpg -sear "Sergey Karlov" mes-
sage_to_sergey
```

приводят к одинаковым результатам. Переместите файл `message_to_sergey` в домашний каталог пользователя `sergey`.

Шаг 11

Файл `message_to_sergey` содержит зашифрованное сообщение. Если бы вы передавали его по сетям общего пользования, то в случае перехвата сообщения третьими лицами, они смогли бы ознакомится со следующим текстом:

```
[sergey@drwalbr sergey]$ cat message_to_sergey.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.1 (GNU/Linux)

hQEOA3DDs7hpytx7EAQA3+zuXyc4ckZhS3fbKsV+vcPp9wJmbYE0BF8qFYP8KQAo
lRlbl1tz7l2HlAKqGrbnyTtuVqRw1RPz/vMo4IQCqL1/YHVz6KhYYbXsFIqFYXGb
vB9PqgEMfRCpAJK63WFj3oyX2EL1Q9qAc9v/9Ru5SY2D1bqM3dHdneWbjJvhBcAD
/iF5qWnlpex3FTTwtmvrobrKuuFzZQNIZl3AQpOL7b5EWyM5RfjKPqaG4+FVaAyd
dSRvKNpeTNA4s+OgShTp8bRpNcwZ72Fy35pkwxTTRqcD7QWVaisn/Q3EnC78T3Md
0ESCEHT/tkZmGhnQHBN3vA0PvC32SXTHFRoa+aiO09Ou0rYBc2D9KJPu7VMWUuSq
MZ4YYkF5GUOKivURAkWbrOBztHunipgbbG6QxdeaL1eSJPkq58Ob4rtgErD8tL2M
nrPbhBnUYOFoW+t+UzfFQ28eJo+jQOoFtxcQu2hpLpipBaGjbl8owXSHEVkSWmb1
/8oW1uq+wBrTP0sghYxchr/7ByBeAMirvBuwkVIUrQr5S+XP6CAXnKNLfyxakMrE
4T5NAuAteSlZwUj6fvo2Ba67aQBdDO7FvA==
=C5As
-----END PGP MESSAGE-----
```

Для расшифровки сообщения в файле `message_to_sergey`:

```
[sergey@drwalbr sergey]$ gpg -d message_to_sergey.asc > message_to_sergey

You need a passphrase to unlock the secret key for
user: "Sergey Karlov <sergey@drwalbr.und>"
```

```
1024-bit ELG-E key, ID 69CADC7B, created 2003-03-19 (main
key ID 5BC241B3)
```

введите пароль:

```
Enter passphrase: $ecretnoe_$lovo_Sergeya
gpg: encrypted with 1024-bit ELG-E key, ID 69CADC7B,
created 2003-03-19
"Sergey Karlov <sergey@drwalbr.und>"
gpg: Signature made Срд 19 Мар 2003 16:05:22 MSK using DSA
key ID F3238EE5
gpg: Good signature from "Valentine Bruy
<valentine@drwalbr.und>"
gpg: checking the trustdb
gpg: checking at depth 0 signed=0
ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: next trustdb check due at 2004-03-18
gpg: WARNING: This key is not certified with a trusted
signature!
gpg: There is no indication that the signature
belongs to the owner.
Primary key fingerprint: BAD5 B986 F5AC 89E7 99A4 92CE
4678 9056 F323 8EE5
```

В результате в домашнем каталоге пользователя `sergey` появится файл `message_to_sergey`, содержащий исходное сообщение:

```
[sergey@drwalbr sergey]$ cat message_to_sergey
Привет, Сергей ! = Валентин
```

Глава 12

OpenSSL – программное обеспечение для безопасной передачи данных

В этой главе:

1. Ограничения и допущения
2. Пакеты
3. Инсталляция с помощью rpm-пакетов
4. Компиляция, оптимизация и инсталляция OpenSSL
5. Конфигурирование OpenSSL
6. Тестирование OpenSSL

Большинство сетевых протоколов, используемых в Интернете, например, IMAP, POP, SQL, SMTP, SMB, HTTP, FTP и LDAP, обеспечивают поддержку шифрования информации по протоколу SSL. Обычно шифрование используется для скрытия от злоумышленников передаваемых по сетям общего пользования логинов и паролей доступа к различным ресурсам, например, средствам администрирования через Web-интерфейс акаунтов для предоставления различных услуг (хостинг, электронная почта, управление мобильным телефоном и т. п.), почтовым ящикам, закрытым каталогам на FTP и Web-серверах для передачи различных конфиденциальных сообщений (например, ЦРУ имеет на своем сервере `http://www.cia.gov` форму, предназначенную для приема информации, которая при передаче будет зашифрована).

При передаче аутентификационной информации в виде обычного текста она может быть перехвачена третьими лицами с использованием программ-сниферов и использована для получения несанкционированного доступа к вашим ресурсам. Например, одна неверная супруга, ведущая переписку с любовником через почтовый ящик на `http://www.mail.com`, где логин и пароль передаются в виде обычного текста, была поймана с поличным (в полученном ей письме содержалась информация о месте и времени встречи). Аутентификационные параметры для доступа к почтовому ящику были получены мужем с помощью снифера, установленного на системе в локальной сети офиса, где работала беспечная дама.

В настоящее время протокол SSL практически незаметно для пользователя взаимодействует с остальными протоколами Интернет и обеспечивает передачу конфиденциальной информации по сетям общего пользования в зашифрованном виде.

Программное обеспечение OpenSSL поддерживает протоколы SSL v2/v3 (Secure Sockets Layer) и TLS v1 (Transport Layer Security). Большинство программ, описанных в этой книге, требует установки OpenSSL. Группа разработчиков предупреждает, что использование алгоритмов `RC5` и `IDEA`, также реализованных в OpenSSL, требует получения соответствующих лицензий, и рекомендует проконсультироваться на эту тему с вашим юристом. Для исключения из OpenSSL этих алгоритмов при установке на вашем компьютере исходные коды необходимо сконфигурировать с опциями `no-rc5` и `no-idea`.

В этой главе описаны процедуры установки, настройки и тестирования OpenSSL, включая операции по генерации и подписи ключей, применяемых для шифрования передаваемой по сетям общего пользования информации с использованием протоколов Интернет, поддерживающих OpenSSL.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

ЗАМЕЧАНИЕ В некоторых странах ввоз, распространение и использование программного обеспечения для криптографии запрещено.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта OpenSSL по состоянию на 22.03.2003. Регулярно посещайте домашнюю страницу проекта `http://www.openssl.org/` и отслеживайте обновления.

Исходные коды OpenSSL содержатся в архиве `openssl-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `openssl-0.9.7a.tar.gz`).

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет `openssl` с помощью следующей команды:

```
[root@dymatel /]# rpm -iq openssl
```

Шаг 2

Если пакет не установлен, перейдите в каталог, где находится пакет `openssl-0.9.6b-24asp.i686.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@dymatel /]# cd /home/distrib
```

и установите:

```
[root@dymatel distrib]# rpm –ihv openssl-0.9.6b-24asp.i686.rpm
```

или обновите пакет:

```
[root@dymatel distrib]# rpm –Uhv openssl-0.9.6b-24asp.i686.rpm
```

После установки пакета перейдите к настройке OpenSSL, описанной ниже.

Компиляция, оптимизация и инсталляция OpenSSL

Шаг 1

Проверьте целостность данных и подлинность архива, содержащего исходные коды OpenSSL.

Одним из способов проверки подлинности и целостности архива является определение его контрольной суммы MD5 и сравнение ее с суммой, опубликованной на сервере разработчика (контрольная сумма MD5 архива `openssl-0.9.7a.tar.gz` содержится в файле `ftp://ftp.openssl.org/source/openssl-0.9.7a.tar.gz.md5`).

Определите контрольную сумму MD5 пакета:

```
[root@dymatel /]# cd /var/tmp/
[root@drwalbr tmp]# md5sum openssl-0.9.7a.tar.gz
a0d3203ecf10989fdc61c784ae82e531 openssl-0.9.7a.tar.gz
```

Скачайте с сервера разработчика файл, содержащий контрольную сумму MD5 архива `openssl-0.9.7a.tar.gz`:

```
[root@drwalbr tmp]# wget ftp://ftp.openssl.org/source/openssl-
0.9.7a.tar.gz.md5
```

и сравните ее с контрольной суммой, полученной с помощью команды `md5sum`:

```
[root@drwalbr tmp]# cat openssl-0.9.7a.tar.gz.md5
a0d3203ecf10989fdc61c784ae82e531
```

Если полученные значения сумм совпадают, значит, в вашем распоряжении находится подлинный и сохранивший целостность при передаче по сетям общего пользования архив с исходными кодами OpenSSL.

Подлинность архива также может быть проверена с использованием утилит GnuPG. Для этого вам необходимо получить с сервера разработчика файлы, содержащие открытый ключ GPG (по непонятным для авторов причинам он находится не на сервере `http://www.openssl.org`, а на сервере одного из членов команды разработчиков `http://richard.levitte.org/pubkey2.asc`):

```
[root@drwalbr tmp]# wget http://richard.levitte.org/pubkey2.asc
```

и сигнатуру архива `openssl-0.9.7a.tar.gz`:

```
[root@drwalbr tmp]# wget ftp://ftp.openssl.org/source/openssl-
0.9.7a.tar.gz.asc
```

После получения необходимых файлов импортируйте открытый ключ `pubkey2.asc` в базу ваших GPG ключей:

```
[root@drwalbr tmp]# gpg --import pubkey2.asc
gpg: key E06D2CB1: public key "levitte@openssl.org" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

Подтвердите подлинность добавленного ключа:

```
[root@drwalbr tmp]# gpg --sign-key levitte@openssl.org

pub  2048R/E06D2CB1  created: 1998-09-18 expires: never      trust: -/-
(1). levitte@openssl.org
(2)  Richard Levitte <levitte@lp.se>
(3)  Richard Levitte <richard@levitte.org>
```

```
Really sign all user IDs? y

pub  2048R/E06D2CB1  created: 1998-09-18 expires: never      trust: -/-
 Primary key fingerprint: 35 3E 6C 9E 8C 97 85 24  BD 9F D1 9E 8F 75 23
6B

     levitte@openssl.org
     Richard Levitte <levitte@lp.se>
     Richard Levitte <richard@levitte.org>

How carefully have you verified the key you are about to sign actually
belongs
to the person named above?  If you don't know what to answer, enter "0".

   (0) I will not answer. (default)
   (1) I have not checked at all.
   (2) I have done casual checking.
   (3) I have done very careful checking.

Your selection? 3
Are you really sure that you want to sign this key
with your key: "root.drwalbr <root@drwalbr.und>"

I have checked this key very carefully.

Really sign? y

You need a passphrase to unlock the secret key for
user: "root.drwalbr <root@drwalbr.und>"
1024-bit DSA key, ID E3A03FAD, created 2003-05-10

Enter passphrase: $ecretnoe_Slovo_root.drwalbr
```

и проверьте подлинность архива:

```
[root@drwalbr tmp]# gpg --verify openssl-0.9.7a.tar.gz.asc openssl-
0.9.7a.tar.gz
```

Если вы получите вывод вида:

```
gpg: Signature made Wed Feb 19 16:07:58 2003 MSK using RSA key ID
E06D2CB1
gpg: Good signature from "levitte@openssl.org"
gpg:                 aka "Richard Levitte <levitte@lp.se>"
gpg:                 aka "Richard Levitte <richard@levitte.org>"
gpg: checking the trustdb
gpg: checking at depth 0 signed=1 ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: checking at depth 1 signed=0 ot(-/q/n/m/f/u)=1/0/0/0/0/0
```

то значит, в вашем распоряжении находится подлинный и сохранивший целостность при передаче по сетям общего пользования архив с исходными кодами OpenSSL.

Для демонстрации возможностей предлагаемых средств проверки подлинности архивов авторы вставили лишний байт, соответствующий символу «пробел» в архив `openssl-0.9.7a.tar.gz` и проверили его подлинность с помощью утилит `md5sum` и `gpg`:

```
[root@drwalbr tmp]# md5sum openssl-0.9.7a.tar.gz
c0312ab825c0c9465e411b1475ab5d47  openssl-0.9.7a.tar.gz
[root@drwalbr tmp]#
[root@drwalbr tmp]# gpg --verify openssl-0.9.7a.tar.gz.asc openssl-
0.9.7a.tar.gz
gpg: Signature made Wed Feb 19 16:07:58 2003 MSK using RSA key ID
E06D2CB1
gpg: BAD signature from "levitte@openssl.org"
```

Утилита `md5sum` выдала контрольную сумму:

```
c0312ab825c0c9465e411b1475ab5d47
```

не соответствующую контрольной сумме, указанной на сервере разработчиков программного продукта:

```
a0d3203ecf10989fdc61c784ae82e531
```

а утилита `gpg` сообщила о неправильной сигнатуре архивного файла:

```
gpg: BAD signature from "levitte@openssl.org"
```

ЗАМЕЧАНИЕ Проверка подлинности и целостности скачиваемых архивов очень важна, с точки зрения обеспечения безопасности вашей системы. Если пробел, который мы вставили выше, непреднамеренно или специально был бы вставлен в строку сценария, удаляющего после инсталляции OpenSSL ненужные временные файлы, т. е. строка вида:

```
rm –rf  /some_path/*
```

была бы заменена на:

```
rm –rf  /some_path /*
```

в результате выполнения сценария были бы удалены все файлы в вашей системе. Модифицированная команда сначала бы удалила каталог `/some_path`, а затем все в корневом каталоге системы – `/*`.

Шаг 2

Распакуйте архив с исходными кодами OpenSSL в каталоге `/var/tmp`:

```
[root@dymatel tmp]# tar xzpf openssl-0.9.7a.tar.gz
```

и перейдите во вновь созданный каталог, содержащий исходные коды OpenSSL:

```
[root@dymatel tmp]# cd openssl-0.9.7a/
```

Шаг 3

Для оптимизации откомпилированного кода OpenSSL применительно к процессору, используемому на вашей системе, в файле `/var/tmp/openssl-0.9.7a/Configure` замените сроку:

```
"linux-elf", "gcc:-DL_ENDIAN -DTERMIO -O3 –m486 -Wall::-D_REENTRANT::-
ldl:BN_LLONG ${x86_gcc_des} ${x86_gcc_opts}:${x86_elf_asm}:dlfcn:linux-
shared:-fPIC::.so.\$(SHLIB_MAJOR).\$(SHLIB_MINOR)",
```

на:

```
"linux-elf", "gcc:-DL_ENDIAN -DTERMIO -O3 -march=i686 -funroll-loops -
fomit-frame-pointer -Wall::-D_REENTRANT::-ldl:BN_LLONG ${x86_gcc_des}
${x86_gcc_opts}:${x86_elf_asm}:dlfcn:linux-shared:-
fPIC::.so.\$(SHLIB_MAJOR).\$(SHLIB_MINOR)",
```

Строку:

```
"debug-linux-elf", "gcc:-DBN_DEBUG -DREF_CHECK -DCONF_DEBUG -
DBN_CTX_DEBUG -DCRYPTO_MDEBUG -DL_ENDIAN -DTERMIO –g –m486 -Wall::-
D_REENTRANT::-lefence -ldl:BN_LLONG ${x86_gcc_des}
${x86_gcc_opts}:${x86_elf_asm}:dlfcn:linux-shared:-
fPIC::.so.\$(SHLIB_MAJOR).\$(SHLIB_MINOR)",
```

на:

```
"debug-linux-elf", "gcc:-DBN_DEBUG -DREF_CHECK -DCONF_DEBUG -
DBN_CTX_DEBUG -DCRYPTO_MDEBUG -DL_ENDIAN -DTERMIO -O3 -march=i686 -
funroll-loops -fomit-frame-pointer -Wall::-D_REENTRANT::-lefence -
ldl:BN_LLONG ${x86_gcc_des} ${x86_gcc_opts}:${x86_elf_asm}:dlfcn:linux-
shared:-fPIC::.so.\$(SHLIB_MAJOR).\$(SHLIB_MINOR)",
```

Строку:

```
"debug-linux-elf-noefence", "gcc:-DBN_DEBUG -DREF_CHECK -DCONF_DEBUG -
DBN_CTX_DEBUG -DCRYPTO_MDEBUG -DL_ENDIAN -DTERMIO -O3 –g –m486 -Wall::-
D_REENTRANT::-ldl:BN_LLONG ${x86_gcc_des}
${x86_gcc_opts}:${x86_elf_asm}:dlfcn",
```

на:

```
"debug-linux-elf-noefence", "gcc:-DBN_DEBUG -DREF_CHECK -DCONF_DEBUG -
DBN_CTX_DEBUG -DCRYPTO_MDEBUG -DL_ENDIAN -DTERMIO -O3 -march=i686 -
funroll-loops -fomit-frame-pointer -Wall::-D_REENTRANT::-ldl:BN_LLONG
${x86_gcc_des} ${x86_gcc_opts}:${x86_elf_asm}:dlfcn",
```

Шаг 4

В исходных кодах OpenSSL предполагается, что интерпретатор `perl` находится в каталоге `/usr/local/bin/`. Если вы точно следовали нашим рекомендациям по первичной установке системы, то интерпретатор должен находится в каталоге `/usr/bin/perl`. Для того, чтобы программа установки OpenSSL могла воспользоваться интерпретатором `perl`, выполните команду:

```
[root@dymatel openssl-0.9.7a]# perl util/perlpath.pl /usr/bin/perl
```

Шаг 5

Сконфигурируйте исходные коды OpenSSL:

```
[root@dymatel openssl-0.9.7a]#./configure linux-elf no-asm shared \
--prefix=/usr \
--openssldir=s/usr/share/ss1
```

Шаг 6

Откомпилируйте исходные коды, проверьте правильность компиляции и наличие соответствующих библиотек, проинсталлируйте файлы OpenSSL, создайте и сохраните список инсталлированных файлов:

```
[root@dymatel openssl-0.9.7a]# LD_LIBRARY_PATH=`pwd` make all build-
shared
[root@dymatel openssl-0.9.7a]# LD_LIBRARY_PATH=`pwd` make tests apps
tests
[root@dymatel openssl-0.9.7a]# find /* > /root/openssl1
[root@dymatel openssl-0.9.7a]# make install build-shared
[root@dymatel openssl-0.9.7a]# cd /usr/lib
[root@dymatel lib]# mv libcripto.so.0.9.7 ../../lib/
[root@dymatel lib]# mv libssl.so.0.9.7 ../../lib/
[root@dymatel lib]# ln –sf ../../lib/libcripto.so.0.9.7 libcripto.so
[root@dymatel lib]# ln –sf ../../lib/libcripto.so.0.9.7 libcripto.so.0
[root@dymatel lib]# ln –sf ../../lib/libssl.so.0.96 libssl.s0
[root@dymatel lib]# ln –sf ../../lib/libssl.so.0.96 libssl.s0.0
[root@dymatel lib]# mv /usr/share/ssl/man/manl/* /usr/share/man/man1/
[root@dymatel lib]# mv /usr/share/ssl/man/man3/* /usr/share/man/man3/
[root@dymatel lib]# mv /usr/share/ssl/man/man5/* /usr/share/man/man5/
[root@dymatel lib]# mv /usr/share/ssl/man/man7/* /usr/share/man/man7/
[root@dymatel lib]# rm -rf /usr/share/ssl/man/
[root@dymatel lib]# rm -rf /usr/share/ssl/lib/
[root@dymatel lib]# strip /usr/bin/openssl
[root@dymatel lib]# mkdir -p /usr/share/ssl/crl
[root@dymatel lib]# cd /var/tmp/openssl-0.9.7a/
[root@dymatel openssl-0.9.7a]# find /* > /root/openssl2
[root@dymatel openssl-0.9.7a]# diff /root/openssl1 /root/openssl2 >
/root/ openssl.installed
[root@dymatel openssl-0.9.7a]# mv /root/openssl.installed
/very_reliable_place/openssl.installed.YYYYMMDD
```

Шаг 7

Удалите архив и каталог с исходными кодами OpenSSL:

```
[root@dymatel /]# cd /var/tmp/
[root@dymatel tmp]# rm -rf openssl-0.9.7a /
[root@dymatel tmp]# rm -f opensal-0.9.7a.tar.gz
```

Конфигурирование OpenSSL

Конфигурирование OpenSSL осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/usr/shared/ssl/openssl.cnf`;
- скрипта для самостоятельной подписи (без привлечения сертификационного центра подписи сертификата) `/usr/shared/ssl/misc/sign`.

Шаг 1

Отредактируйте в соответствии с приведенными ниже рекомендациями и вашими потребностями файл`/usr/shared/ssl/openssl.cnf`:

ЗАМЕЧАНИЕ В файле `/usr/shared/ssl/openssl.cnf`, созданном при установке OpenSSL, необходимо изменить параметры только в разделах `[CA_default]`и `[req_distinguished_name]`.

```
OpenSSL example configuration file.
# This is mostly being used for generation of certificate requests.
#

# This definition stops the following lines choking if HOME isn't
# defined.
HOME                    = .
RANDFILE                = $ENV::HOME/.rnd

# Extra OBJECT IDENTIFIER info:
#oid_file               = $ENV::HOME/.oid
oid_section             = new_oids

# To use this configuration file with the "-extfile" option of the
# "openssl x509" utility, name here the section containing the
# X.509v3 extensions to use:
# extensions            =
# (Alternatively, use a configuration file that has only
# X.509v3 extensions in its main [= default] section.)

[ new_oids ]

# We can add new OIDs in here for use by 'ca' and 'req'.
# Add a simple OID like this:
# testoid1=1.2.3.4
# Or use config file substitution like this:
# testoid2=${testoid1}.5.6

####################################################################
[ ca ]
default_ca      = CA_default            # The default ca section

####################################################################
[ CA_default ]

dir             = /usr/share/ssl        # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/ca.db.index      # database index file.
new_certs_dir   = $dir/ca.db.certs      # default place for new certs.

certificate     = $dir/certs/ca.crt     # The CA certificate
serial          = $dir/ca.db.serial     # The current serial number
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/ca.key   # The private key
RANDFILE        = $dir/ca.db.rand       # private random number file

x509_extensions = usr_cert              # The extentions to add to the
cert

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2
CRLs
# so this is commented out by default to leave a V1 CRL.
# crl_extensions        = crl_ext

default_days    = 365                   # how long to certify for
default_crl_days= 30                    # how long before next CRL
default_md      = md5                   # which md to use.
preserve        = no                    # keep passed DN ordering

# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
```

```
policy          = policy_match

# For the CA policy
[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

# For the 'anything' policy
# At this point in time, you must list all acceptable 'object'
# types.
[ policy_anything ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

####################################################################
[ req ]
default_bits            = 1024
default_keyfile         = privkey.pem
distinguished_name      = req_distinguished_name
attributes              = req_attributes
x509_extensions = v3_ca # The extentions to add to the self signed cert

# Passwords for private keys if not present they will be prompted for
# input_password = secret
# output_password = secret

# This sets a mask for permitted string types. There are several options.
# default: PrintableString, T61String, BMPString.
# pkix   : PrintableString, BMPString.
# utf8only: only UTF8Strings.
# nombstr : PrintableString, T61String (no BMPStrings or UTF8Strings).
# MASK:XXXX a literal mask value.
# WARNING: current versions of Netscape crash on BMPStrings or
UTF8Strings
# so use this option with caution!
string_mask = nombstr

# req_extensions = v3_req # The extensions to add to a certificate re-
quest

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = RU
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Moscow region

localityName                    = Locality Name (eg, city)
localityName_default            = Ybileynyi

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = SIP RIA
```

```
# we can do this but it is not needed normally :-)
#1.organizationName            = Second Organization Name (eg, company)
#1.organizationName_default    = World Wide Web Pty Ltd

organizationalUnitName         = Organizational Unit Name (eg, section)

commonName                     = Common Name (eg, YOUR name)
commonName_default             = www.dymatel.und
commonName_max                 = 64

emailAddress                   = Email Address
emailAddress_default           = root@dymatel.und
emailAddress_max               = 40

# SET-ex3                      = SET extension number 3

[ req_attributes ]
challengePassword              = A challenge password
challengePassword_min          = 8
challengePassword_max          = 20

unstructuredName               = An optional company name

[ usr_cert ]

# These extensions are added when 'ca' signs a request.

# This goes against PKIX guidelines but some CAs do it and some software
# requires this to avoid interpreting an end user certificate as a CA.

basicConstraints=CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted
# the certificate can be used for anything *except* object signing.

# This is OK for an SSL server.
# nsCertType                   = server

# For an object signing certificate this would be used.
# nsCertType = objsign

# For normal client use this is typical
# nsCertType = client, email

# and for everything including object signing:
# nsCertType = client, email, objsign

# This is typical in keyUsage for a client certificate.
# keyUsage = nonRepudiation, digitalSignature, keyEncipherment

# This will be displayed in Netscape's comment listbox.
nsComment                      = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always

# This stuff is for subjectAltName and issuerAltname.
# Import the email address.
# subjectAltName=email:copy

# Copy subject details
# issuerAltName=issuer:copy
```

```
#nsCaRevocationUrl              = http://www.domain.dom/ca-crl.pem
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName

[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment

[ v3_ca ]


# Extensions for a typical CA


# PKIX recommendation.

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid:always,issuer:always

# This is what PKIX recommends but some broken software chokes on criti-
cal
# extensions.
#basicConstraints = critical,CA:true
# So we do this instead.
basicConstraints = CA:true

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
# keyUsage = cRLSign, keyCertSign

# Some might want this also
# nsCertType = sslCA, emailCA

# Include email address in subject alt name: another PKIX recommendation
# subjectAltName=email:copy
# Copy issuer details
# issuerAltName=issuer:copy

# DER hex encoding of an extension: beware experts only!
# obj=DER:02:03
# Where 'obj' is a standard or added object
# You can even override a supported extension:
# basicConstraints= critical, DER:30:03:01:01:FF

[ crl_ext ]

# CRL extensions.
# Only issuerAltName and authorityKeyIdentifier make any sense in a CRL.

# issuerAltName=issuer:copy
authorityKeyIdentifier=keyid:always,issuer:always
```

Шаг 2

Группа разработчиков OpenSSL предъявляет некоторые требования, затрудняющие использование файлов `CA.pl` или `CA.sh` для самостоятельной подписи ключей. Для подписи ключей авторы рекомендуют

самостоятельно воспользоваться скриптом, разработанным Ральфом С. Энгелчолом (Ralf S. Engelschall). Создайте файл `/usr/share/ssl/misc/sign` следующего содержания:

```
#!/bin/sh
##
##  sign.sh -- Sign a SSL Certificate Request (CSR)
##  Copyright (c) 1998-1999 Ralf S. Engelschall, All Rights Reserved.
##

#   argument line handling
CSR=$1
if [ $# -ne 1 ]; then
    echo "Usage: sign.sign <whatever>.csr"; exit 1
fi
if [ ! -f $CSR ]; then
    echo "CSR not found: $CSR"; exit 1
fi
case $CSR in
   *.csr ) CERT="`echo $CSR | sed -e 's/\.csr/.crt/'`" ;;
      * ) CERT="$CSR.crt" ;;
esac

#   make sure environment exists
if [ ! -d ca.db.certs ]; then
    mkdir ca.db.certs
fi
if [ ! -f ca.db.serial ]; then
    echo '01' >ca.db.serial
fi
if [ ! -f ca.db.index ]; then
    cp /dev/null ca.db.index
fi

#   create an own SSLeay config
cat >ca.config <<EOT
[ ca ]
default_ca = CA_own
[ CA_own ]
dir = /usr/share/ssl
certs = /usr/share/ssl/certs
new_certs_dir= /usr/share/ssl/ca.db.certs
database = /usr/share/ssl/ca.db.index
serial = /usr/share/ssl/ca.db.serial
RANDFILE = /usr/share/ssl/ca.db.rand
certificate = /usr/share/ssl/certs/ca.crt
private_key = /usr/share/ssl/private/ca.key
default_days = 365
default_crl_days = 30
default_md = md5
preserve = no
policy = policy_anything
[ policy_anything ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
EOT

#  sign the certificate
echo "CA signing: $CSR -> $CERT:"
openssl ca -config ca.config -out $CERT -infiles $CSR
echo "CA verifying: $CERT <-> CA cert"
```

```
openssl verify -CAfile /usr/share/ssl/certs/ca.crt $CERT

#  cleanup after SSLeay
rm -f ca.config
rm -f ca.db.serial.old
rm -f ca.db.index.old

#  die gracefully
exit 0
```

Шаг 3

Измените права доступа к файлу и назначьте владельцем файла суперпользователя `root`:

```
[root@dymatel /]# chmod 700 /usr/share/ssl/misc/sign
[root@dymatel /]# chown 0.0 /usr/share/ssl/misc/sign
```

Тестирование OpenSSL

Для проверки работоспособности OpenSSL создайте на вашей системе SSL-сертификат Web-сервера Apache. Для создания ключей RSA и запросов на подтверждение подлинности сертификатов (Certificate Signing Requests, CSR) используется утилита `/usr/bin/openssl`.

Шаг 1

Выберите пять любых больших файлов со случайным (уникальным) содержанием, скопируйте их в каталог `/usr/share/ssl` и переименуйте в `random1`, `random2`, `random3`, `random4`, `random5`.

Для выбора пяти случайных файлов и размещения их в `/usr/share/ssl` используйте команды:

```
[root@dymatel /]# cp /var/log/messages /usr/share/ssl/random1
[root@dymatel /]# cp /var/log/messages.1 /usr/share/ssl/random2
[root@dymatel /]# cp /var/log/messages.2 /usr/share/ssl/random3
[root@dymatel /]# cp /var/log/messages.3 /usr/share/ssl/random4
[root@dymatel /]# cp /var/log/messages.4 /usr/share/ssl/random5
```

Шаг 2

Создайте закрытый ключ RSA для Web-сервера, защищенный паролем:

```
[root@dymatel /]# cd /usr/share/ssl/
[root@dymatel ssl]# openssl genrsa -des3 -rand ran-
dom1:random2:random3:random4:random5 -out www.dymatel.und.key 1024
1540748 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
........++++++
.....................................................++++++
e is 65537 (0x10001)
```

Введите пароль для защиты вашего RSA-ключа:

```
Enter pass phrase for www.dymatel.und.key: $ecretn0e_Sl0vo
```

Подтвердите пароль:

```
Verifying - Enter pass phrase for www.dymatel.und.key: $ecretn0e_Sl0vo
```

ЗАМЕЧАНИЕ Обратите внимание, что в качестве имени системы нужно ввести `www.dymatel.und`, а не `dymatel.und`. В противном случае вы не сможете подписать сертификат.

Шаг 3

Сохраните ключ, содержащийся в файле `www.dymatel.und.key`, и защищающий его пароль в надежном месте, например, на дискете.

Шаг 4

Создайте запрос на подтверждение подлинности сертификата:

```
[root@dymatel ssl]# openssl req -new -key www.dymatel.und.key -out
www.dymatel.und.csr
```

Введите пароль, защищающий ключ `www.dymatel.und.key`:

```
Enter pass phrase for www.dymatel.und.key: $ecretn0e_Sl0vo
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

Подтвердите заданные ранее в файле `/usr/shared/ssl/openssl.cnf` название страны, области, города, организации, Web-сервера, почтового адреса администратора сервера:

```
Country Name (2 letter code) [RU]: <Enter>
State or Province Name (full name) [Moscow Region]: <Enter>
Locality Name (eg, sity) [Ybileynyi]: <Enter>
Organization Name (eg, company) [SIP RIA]: <Enter>
Organizational Unit Name (eg, section) []:<Enter>
Common Name (eg, YOUR name) [www.dymatel.und]: <Enter>
Email Address [root@dymatel.und]: <Enter>
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:<Enter>
An optional company name []:<Enter>
```

Файл `www.dymatel.und.csr`, содержащий запрос на подтверждение подлинности сертификата, отправьте в коммерческий сертификационный центр, оплатите его услуги, и через некоторое время вы получите файл `www.dymatel.und.crt`, который вы сможете использовать для подтверждения подлинности сертификата.

Если вы не желаете прибегать к услугам коммерческих сертификационных центров и желаете подписать его самостоятельно, то выполните операции, описанные в шагах 5, 6,7,8 и 9.

Шаг 5

Создайте закрытый RSA-ключ для своего собственного центра сертификации:

```
[root@dymatel ssl]# openssl genrsa -des3 -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
............++++++
..............++++++
e is 65537 (0x10001)
```

Введите пароль, защищающий ключ:

```
Enter pass phrase for ca.key: $ecretnoe_Slov0
```

Подтвердите пароль:

```
Verifying - Enter pass phrase for ca.key: $ecretnoe_Slov0
```

Шаг 6

Сохраните ключ и защищающий его пароль в надежном месте, например на дискете.

Шаг 7

Создайте и подпишите для ключа `ca.key` сертификат:

```
[root@dymatel ssl]# openssl req -new -x509 -days 365 -key ca.key -out
ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

Введите название страны, области, города, организации, Web-сервера, почтового адреса администратора сервера:

```
Country Name (2 letter code) [RU]:<Enter>
State or Province Name (full name) [Moscow Region]: <Enter>
```

```
Locality Name (eg, sity) [Ybileynyi]: <Enter>
Organization Name (eg, company) [SIP RIA]: <Enter>
Organizational Unit Name (eg, section) []: Sertification Department <En-
ter>
Common Name (eg, YOUR name) [www.dymatel.und]: <Enter>
Email Address [root@dymatel.und]: <Enter>
```

ЗАМЕЧАНИЕ В этом примере были подтверждены все параметры, определенные в файле `/usr/shared/ssl/openssl.cnf` и использованные при создании `www.dymatel.und.csr` (шаг 4), кроме названия подразделения (`Organizational Unit Name (eg, section)`). Для реализации возможности самостоятельной подписи сертификата исходные данные, вводимые для `www.dymatel.und.csr` и `ca.crt` должны различаться, в противном случае при подписании сертификата произойдет ошибка.

Шаг 8

Поместите все созданные файлы в соответствующие каталоги:

```
[root@dymatel ssl]# mv www.dymatel.und.key private/
[root@dymatel ssl]# mv ca.key private/
[root@dymatel ssl]# mv ca.crt certs/
```

Шаг 9

Подпишите созданный ранее запрос на подтверждение подлинности сертификата `www.dymatel.und.csr`:

```
[root@dymatel ssl]# /usr/share/ssl/misc/sign www.dymatel.und.csr
CA signing: www.dymatel.und.csr -> www.dymatel.und.crt:
Using configuration from ca.config
Enter PEM pass phrase:
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :PRINTABLE:'Moscow region'
localityName          :PRINTABLE:'Ybileyniy'
organizationName      :PRINTABLE:'SIP RIA'
organizationalUnitName:PRINTABLE:'Sertification Department'
commonName            :PRINTABLE:'www.dymatel.und'
emailAddress          :IA5STRING:'root@dymatel.und'
Certificate is to be certified until Mar 19 12:24:10 2004 GMT (365 days)
```

Подтвердите необходимость подписи сертификата:

```
Sign the certificate? [y/n]:y
```

Еще раз подтвердите необходимость подписи сертификата:

```
1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
CA verifying: www.dymatel.und.crt <-> CA cert
www.dymatel.und.crt: OK
```

Шаг 10

Поместите файл `www.dymatel.und.crt` в `/usr/share/ssl/cert`:

```
[root@dymatel ssl]# mv www.dymatel.und.crt certs/
```

и удалите `www.dymatel.und.csr`:

```
[root@dymatel ssl]# rm -f www.dymatel.und.csr
```

ЗАМЕЧАНИЕ Если во время подписывания сертификата выдается сообщение об ошибках, вероятно, это является следствием того, что при вводе полного доменного имени системы вы ввели `mydomain.ru` вместо `www.mydomain.ru` или информация, введенная при создании `ca.crt` (шаг 7) и `www.mydomain.ru.csr` (шаг 4) идентична.

Шаг 11

Для повышения безопасности измените права доступа к вновь созданным файлам:

```
[root@dymatel /]# chmod 750 /usr/share/ssl/private/
```

```
[root@dymatel /]# chmod 400 /usr/share/ssl/certs/ca.crt
[root@dymatel /]# chmod 400 /usr/share/ssl/certs/www.dymatel.und.crt
[root@dymatel /]# chmod 400 /usr/share/ssl/private/ca.key
[root@dymatel /]# chmod 400 /usr/share/ssl/private/www.dymatel.und.key
```

Шаг 12

Для того, чтобы созданный и подписанный вами сертификат мог использоваться Web-сервером Apache, в конфигурационный файл `httpd.conf` добавьте строки:

```
SSLCertificateFile /usr/share/ssl/certs/www.dymatel.und.crt
SSLCertificateFile /usr/share/ssl/private/www.dymatel.und.key
```

В этом случае при обращении к вашему серверу по протоколу HTTPS сведения о вашем сертификате (при использовании самостоятельной подписи и браузера MS Internet Explorer 5.x) будут иметь вид, представленный на рис. 12.1.

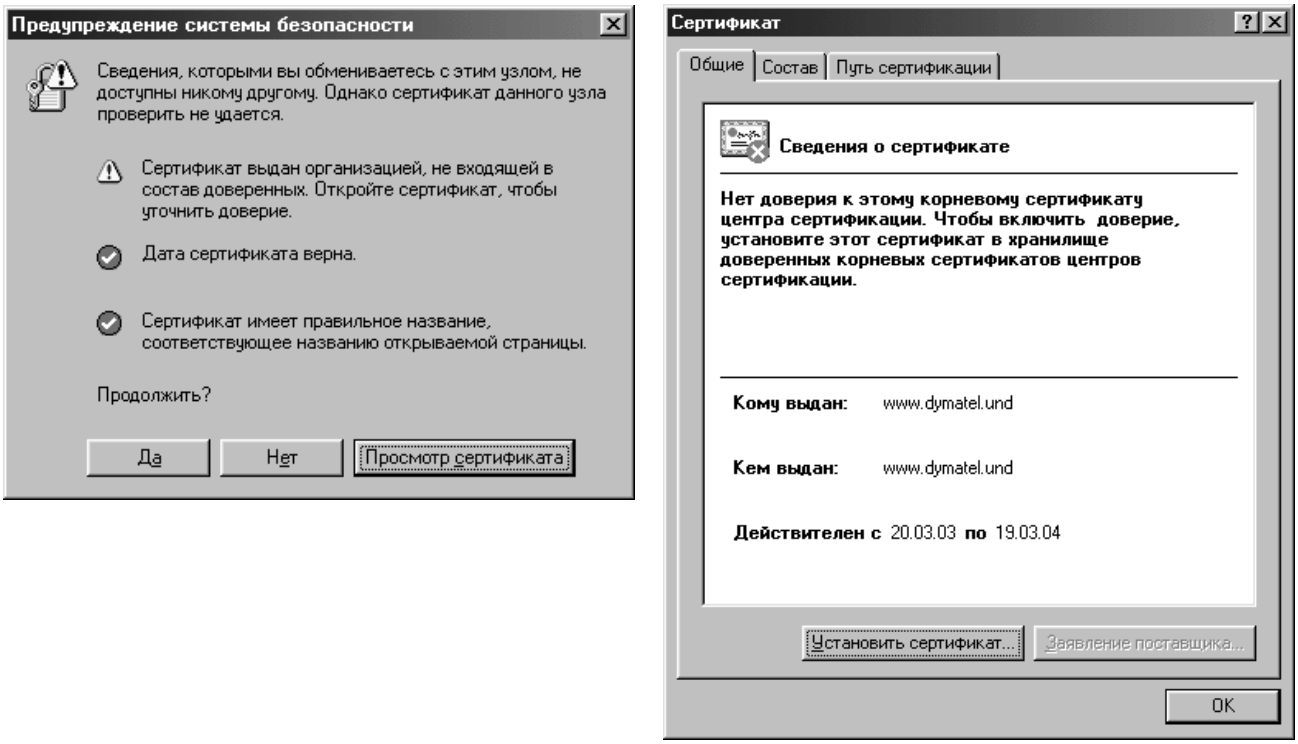


Рис. 12.1 Сведения о сертификате Web-сервера http://www.dymatel.und.

Глава 13

OpenSSH – программное обеспечение для безопасного администрирования удаленных систем

В этой главе:

1. Ограничения и допущения
2. Пакеты
3. Инсталляция с помощью rpm-пакетов
4. Компиляция, оптимизация и инсталляция OpenSSH
5. Конфигурирование OpenSSH
6. Тестирование OpenSSH
7. Использование OpenSSH
8. OpenSSH в окружении chroot-jail
9. Создание окружения chroot-jail
10. Компиляция, оптимизация, инсталляция, конфигурирование и тестирование OpenSSH в среде chroot-jail

Многие сетевые службы, предназначенные для администрирования удаленных систем (например, `telnet`, `rsh`, `rlogin` и др.) не обеспечивают должный уровень безопасности, т. к. передают аутентификационную информацию по сети в виде незашифрованного текста. Эта информация может быть перехвачена третьими лицами и использована для получения несанкционированного доступа к вашим системам. В настоящее время эти программы почти полностью вытеснены программой OpenSSH (Open Secure Shell), которая шифрует весь трафик, включая аутентификационную информацию, и позволяет:

- регистрироваться на удаленных системах;
- выполнять команды на удаленных системах;
- копировать файлы с одной системы на другую.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

ЗАМЕЧАНИЕ В некоторых странах ввоз, распространение и использование программного обеспечения для криптографии запрещено.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта OpenSSH по состоянию на 5.04.2003. Регулярно посещайте домашнюю страницу проекта `http://www.openssh.org/`и отслеживайте обновления.

Исходные коды OpenSSH содержатся в архиве `openssh-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `openssh-3.6.1p1.tar.gz`).

ЗАМЕЧАНИЕ Обратите внимание, что вам необходима именно «переносимая» (предназначенная для Linux и др. операционных систем) версия, название которой содержит индекс "p", например "`3.6.1p1`".

Для работы OpenSSH требуется наличие некоторых библиотек OpenSSL, поэтому перед установкой OpenSSH требуется установить OpenSSL в соответствии с рекомендациями главы 12 из исходных кодов или rpm-пакетов. Если вам необходим запуск OpenSSH в окружении chroot-jail, т. е. некоторым пользователям необходимо предоставить доступ к выполнению команд только в их домашних каталогах, без предоставления доступа к системе в целом, должны использоваться исходные коды OpenSSH, к которым применен соответствующий патч. Пропатченные исходные коды OpenSSH содержатся в архиве `openssh-version-chroot.tar.gz` (последняя доступная на момент написания главы стабильная версия `openssh-3.6.1p1.tar.gz`) и могут быть получены с `http://chrootssh.sourceforge.net`.

Инсталляция с помощью rpm-пакета

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить простые операции. Следует заметить, что в этом случае, к сожалению, вам не удастся в дальнейшем настроить работу программы в среде chroot-jail.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет `openssh` с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq openssh
```

Шаг 2

В случае его отсутствия перейдите в каталог, где находится пакет `openssh-3.1p1-6.1asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

и установите:

```
[root@drwalbr distrib]# rpm –ihv openssh-3.1p1-6.1asp.i386.rpm
```

или обновите пакет:

```
[root@drwalbr distrib]# rpm –Uhv openssh-3.1p1-6.1asp.i386.rpm
```

После установки пакета перейдите к настройке программы OpenSSH, процесс которой описан ниже.

Компиляция, оптимизация и инсталляция OpenSSH

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архив с исходными кодами в каталог `/var/tmp`:

```
[root@drwalbr tmp]# tar xzpf openssh-3.6.1p1.tar.gz
[root@drwalbr tmp]# cd openssh-3.6.1p1
```

Шаг 3

Создайте специального пользователя, от имени которого будет запускаться служба `sshd`:

```
[root@drwalbr openssh-3.6.1p1]# groupadd -g 39 sshd > /dev/null 2>&1 ||:
[root@drwalbr openssh-3.6.1p1]# useradd -u 39 -g 39 -s /bin/false -M -r -
d /var/empty sshd > / dev/null 2>&1 || :
```

Шаг 4

Добавьте имя несуществующего командного интерпретатора. Для этого в конец файла `/etc/shells` добавьте строку:

```
/bin/sh
/bin/bash
/bin/bash2
/bin/false/
```

Шаг 5

Сконфигурируйте исходные коды OpenSSH:

```
[root@drwalbr openssh-3.6.1p1]# CFLAGS="-O2 -march=i686 -funroll-loops";
export CFLAGS
./configure \
--prefix=/usr \
--sysconfdir=/etc/ssh \
--libexecdir=/usr/libexec/openssh \
--mandir=/usr/share/man \
--with-pam \
--with-ipaddr-display \
--with-ipv4-default \
--with-md5-passwords \
--with-zlib
```

При таких параметрах конфигурации осуществляется компиляция исходных кодов с оптимизацией применительно к архитектуре процессора i686, разрешается поддержка модулей аутентификации PAM и использование IP-адресов вместо имени системы, паролей MD5, инсталляция файлов осуществляется в соответствующие каталоги.

Шаг 6

Откомпилируйте исходные коды, проинсталлируйте файлы OpenSSH, создайте и сохраните список установленных файлов:

```
[root@drwalbr openssh-3.6.1p1]# make
[root@drwalbr openssh-3.6.1p1]# cd
[root@drwalbr openssh-3.6.1p1]# find /* > /root/openssh1
[root@drwalbr openssh-3.6.1p1]# make install
```

```
[root@drwalbr openssh-3.6.1p1]# mkdir /var/empty
[root@drwalbr openssh-3.6.1p1]# chown root.sys /var/empty
[root@drwalbr openssh-3.6.1p1]# find /* > /root/openssh2
[root@drwalbr openssh-3.6.1p1]# diff /root/openssh1 /root/openssh2 >
/root/openssh.installed
[root@drwalbr openssh-3.6.1p1]# mv /root/openssh.installed
/very_reliable_place/openssh.installed.YYYYMMDD
```

Шаг 7

Удалите архив и каталог с исходными кодами OpenSSH:

```
[root@drwalbr openssh-3.6.1p1]# cd /var/tmp/
[root@drwalbr tmp]# rm -rf openssh-3.6.1p1/
[root@drwalbr tmp]# rm -f openssh-3.6.1p1.tar.gz
```

Конфигурирование OpenSSH

Конфигурирование OpenSSH осуществляется с использованием следующих файлов:

- конфигурационный файл сервера `/etc/ssh/sshd_config`;
- конфигурационный файл клиента `/etc/ssh/ssh_config`;
- файл для поддержки модулей PAM `/etc/pam.d/sshd`;
- файл инициализации `/etc/init.d/sshd`.

Шаг 1

Для конфигурирования сервера создайте файл `/etc/ssh/sshd_config`, руководствуясь своими потребностями и нижеприведенными рекомендациями:

```
Port                            22
Protocol                        2,1
ListenAddress                   192.168.2.99
HostKey                         /etc/ssh/ssh_host_key
HostKey                         /etc/ssh/ssh_host_rsa_key
HostKey                         /etc/ssh/ssh_host_dsa_key
ServerKeyBits                   768
LoginGraceTime                  60
KeyRegenerationInterval         3600
PermitRootLogin                 no
IgnoreRhosts                    yes
IgnoreUserKnownHosts            yes
StrictModes                     yes
X11Forwarding                   no
X11DisplayOffset                10
PrintMotd                       yes
KeepAlive                       yes
SyslogFacility                  AUTHPRIV
LogLevel                        INFO
RhostsAuthentication            no
RhostsRSAAuthentication         no
RSAAuthentication               yes
PasswordAuthentication          no
PermitEmptyPasswords            no
AllowUsers                      drwalbr karlnext
UsePrivilegeSeparation          yes
Subsystem                       sftp /usr/libexec/openssh/sftp-server
```

Опция `Port 22` определяет номер порта, на котором сервер `sshd` ожидает запросов клиентов. В данном примере используется `22 порт`, установленный по умолчанию.

Опция `Protocol 2,1` определяет порядок версий протоколов, используемых при установке соединения. В рассматриваемом примере при установлении связи сначала будет предпринята попытка установки соединения по протоколу версии 2 и если она окажется неудачной, будет предпринята попытка установления соединения по протоколу версии 1.

Опция `ListenAddress 192.168.2.99` определяет IP-адрес сетевого интерфейса, на котором `sshd` ожидает запросы на подключение.

Опции `HostKey /etc/ssh/ssh_host_key`, `HostKey /etc/ssh/ssh_host_dsa_key` и `HostKey /etc/ssh/ssh_host_rsa__key` определяют местоположение файлов с ключами.

Опция `ServerKeyBits 768` определяет количество битов, отведенных под ключ сервера, и используется при генерировании ключей.

Опция `LoginGraceTime 60` определяет время в секундах, через которое сервер разрывает соединение в случае неудачной попытки регистрации удаленного пользователя. Эта настройка затрудняет реализацию DoS-атак (Denial of Service), основанных на установлении соединений пользователями, не имеющих доступа к аутентификационной информации.

Опция `KeyRegenerationinterval 3600` определяет продолжительность интервала времени в секундах, по окончании которого сервер автоматически генерирует новые ключи. Это настройка повышает безопасность системы за счет затруднения расшифровки третьими лицами трафика, генерируемого соединениями легитимных пользователей.

Опция `PermitRootLogin no` запрещает регистрацию пользователя `root`, используя `ssh`. В случае необходимости выполнения команд на удаленной системе от имени пользователя `root` безопаснее зарегистрироваться в системе в качестве обычного пользователя и затем повысить свои права доступа с помощью команд `su` или `sudo`.

Опции `IgnoreRhosts yes`, `IgnoreUserKnownHosts yes`, `StrictModes yes`, `RhostsAuthentication no` и `RhostsRSAAuthentication no` повышают безопасность системы за счет запрета использования файлов `rhosts` или `shosts` для аутентификации пользователей.

Опция `X11Forwarding no` запрещает поддержку X-сервера.

Опция `PrintMotd yes` разрешает вывод приветственного сообщения из файла `/etc/motd` после регистрации пользователя.

Опция `SyslogFacility AUTHPRIV` определяет вывод сообщений `sshd`.

Опция `LogLevel INFO` опрделяет степень подробности вывода информации `sshd`.

Опция `RSAAuthentication yes` разрешает использовать RSA аутентификацию. Она используется только протоколом SSH1. Протокол SSH2 использует DSA аутентификацию.

Опция `PasswordAuthentication no` повышает безопасность системы за счет запрещения использования паролей для аутентификации пользователей, предоставляя возможность для регистрации только тем удаленным пользователям, чьи открытые ключи, созданные с помощью утилиты `ssh-keygen`, размещены на сервере. Эти ключи так же защищены паролем. Такой предлагаемый вариант значения опции (`no`) запрещает регистрацию пользователей, которые узнали или подобрали пароль, но не имеют соответствующего ключа на своей системе.

Опция `PermitEmptyPasswords no` запрещает регистрацию на системе удаленных пользователей, для которых не определены значения паролей. В рассматриваемом примере значение этой опции не существенно, так как выше запрещено использование паролей для аутентификации пользователей. Тем не менее, из соображений безопасности, рекомендуется запретить использование пустых паролей.

Опция `AllowUsers drwalbr karlnext` определяет список удаленных пользователей, которым разрешена регистрация в системе.

Опция `UsePrivilegeSeparation yes` используется для повышения устойчивости системы к различного рода сбоям.

Шаг 2

Для конфигурирования клиента создайте и отредактируйте в соответствии с вашими потребностями файл `/etc/ssh/ssh_config`:

```
Host                        *
ForwardAgent                no
ForwardX11                  no
RhostsAuthentication        no
RhostsRSAAuthentication     no
RSAAuthentication           yes
PasswordAuthentication      no
FallBackToRsh               no
UseRsh                      no
BatchMode                   no
CheckHostIP                 yes
StrictHostKeyChecking       yes
IdentityFile                ~/.ssh/identity
IdentityFile                ~/.ssh/id_dsa
IdentityFile                ~/.ssh/id_rsa
Port                        22
Protocol                    2,1
```

```
Cipher                          blowfish
EscapeChar                      ~
```

Опция `Host *` предназначена для наложения ограничений на имена систем, с которыми разрешено соединение. В рассматриваемом примере образец "*" не устанавливает никаких ограничений. Опция `Host` в файле `/etc/ssh/ssh_config` может использоваться несколько раз, при этом задаваемый ей образец имен систем, с которыми разрешено соединение, действует до следующего упоминания опции `Host` или конца файла. Это позволяет реализовывать разные настройки клиента для соединения с различными системами.

Опции `ForwardAgent no` и `ForwardX11` no запрещают автоматическое распространение сеансов на вашу систему.

`RhostsAuthentication no` и `RhostsRSAAuthentication no` запрещают устаревшие и ставшими небезопасными механизмы аутентификации пользователей.

Опция `RSAAuthentication yes` разрешает использовать RSA аутентификацию. Этот тип аутентификации используется только протоколом SSH1. Протокол SSH2 использует DSA аутентификацию.

Опция `PasswordAuthentication no` повышает безопасность системы за счет запрещения использования паролей для аутентификации пользователей. Более подробно назначение этой опции рассматривалось выше при конфигурировании сервера.

Опция `FallBackToRsh no` запрещает в случае неудачной попытки соединения с помощью ssh-клиента автоматической попытки установки соединения с помощью rsh-клиента.

Опция UseRsh no запрещает использование небезопасных служб.

Опция `BatchMode no` требует безусловной проверки имени пользователя и пароля при установке соединения. Значение опции должно быть изменено, если вы разрабатываете скрипты, предназначенные для автоматической установки соединения, например, при резервном копировании данных.

Опция `checkHostIP yes` требует обязательной проверки соответствия IP-адреса и имени системы при установке соединения.

Опция `StrictHostKeyChecking yes` запрещает автоматическое добавление ключей удаленных систем в файл `known_hosts`. В начале, т. е. сразу после установки системы, можно изменить значение опции на "`no`", установить соединения со всеми системами, с которыми имеется необходимость установки ssh-соединений, при этом ключи автоматически добавятся в файл `known_hosts`. После чего необходимо установить значение опции "`yes`".

Опции `IdentityFile ~/.ssh/identity`, `IdentityFile ~/.ssh/id_dsa` и `IdentityFile ~/.ssh/id_rsa` позволяют определить местоположение файлов, используемых при аутентификации.

Опция `Protocol 2,1` определяет порядок версий протоколов, используемых при установке соединения. В рассматриваемом примере сначала будет предпринята попытка установки соединения по протоколу версии 2 и если она окажется неудачной, будет предпринята попытка установления соединения по протоколу версии 1.

Опция `Cipher blowfish` определяет алгоритм шифрования информации. Шифр `blowfish` предусматривает использование 64-битных блоков и ключей длиной до 448 битов.

Опция `EscapeChar ~` определяет возможность использования символа <ESC> для приостановки сеанса.

Шаг 3

Для повышения безопасности компиляция OpenSSH осуществлена с поддержкой аутентификации с использованием модулей PAM. Для настройки аутентификации создайте файл `/etc/pam.d/sshd`, содержащий следующие строки:

```
#%PAM-1.0
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_access.so
account    required     /lib/security/pam_time.so
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_limits.so
```

Установите права доступа к файлу, назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 640 /etc/pam.d/sshd
[root@drwalbr /]# chown 0.0 /etc/pam.d/sshd
```

Шаг 4

Создайте файл /etc/init.d/sshd, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping OpenSSH.
#
# chkconfig: 2345 55 25
# description: OpenSSH is a program thas allows to establish a secure re-
mote \
#              connection to a server.
#
# processname: sshd
# config: /etc/ssh/ssh_host_key
# config: /etc/ssh/ssh_host_key.pub
# config: /etc/ssh/ssh_random_seed
# config: /etc/ssh/sshd_config
# pidfile: /var/run/sshd.pid

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source OpenSSH configureation.
if [ -f /etc/sysconfig/sshd ] ; then
        . /etc/sysconfig/sshd
fi

RETVAL=0

# Some functions to make the below more readable.
KEYGEN=/usr/bin/ssh-keygen
RSA1_KEY=/etc/ssh/ssh_host_key
RSA_KEY=/etc/ssh/ssh_host_rsa_key
DSA_KEY=/etc/ssh/ssh_host_dsa_key
PID_FILE=/var/run/sshd.pid
my_success() {
  local msg
  if [ $# -gt 1 ]; then
    msg="$2"
  else
    msg="done"
  fi
  case "`type -type success`" in
    function)
      success "$1"
    ;;
    *)
      echo -n "${msg}"
    ;;
  esac
}
my_failure() {
  local msg
  if [ $# -gt 1 ]; then
    msg="$2"
  else
    msg="FAILED"
  fi
  case "`type -type failure`" in
    function)
      failure "$1"
    ;;
```

```
    *)
      echo -n "${msg}"
    ;;
  esac
}
do_rsa1_keygen() {
        if ! test -f $RSA1_KEY ; then
                echo -n "Generating SSH1 RSA host key: "
                if $KEYGEN -q -t rsa1 -f $RSA1_KEY -C '' -N ''
>&/dev/null; then
                        my_success "RSA1 key generation"
                        echo
                else
                        my_failure "RSA1 key generation"
                        echo
                        exit 1
                fi
        fi
}
do_rsa_keygen() {
        if ! test -f $RSA_KEY ; then
                echo -n "Generating SSH2 RSA host key: "
                if $KEYGEN -q -t rsa -f $RSA_KEY -C '' -N '' >&/dev/null;
then
                        my_success "RSA key generation"
                        echo
                else
                        my_failure "RSA key generation"
                        echo
                        exit 1
                fi
        fi
}
do_dsa_keygen() {
        if ! test -f $DSA_KEY ; then
                echo -n "Generating SSH2 DSA host key: "
                if $KEYGEN -q -t dsa -f $DSA_KEY -C '' -N '' >&/dev/null;
then
                        my_success "DSA key generation"
                        echo
                else
                        my_failure "DSA key generation"
                        echo
                        exit 1
                fi
        fi
}
do_restart_sanity_check() {
        sshd -t
        RETVAL=$?
        if [ ! "$RETVAL" = 0 ]; then
                my_failure "Configuration file or keys"
                echo
                exit $RETVAL
        fi
}


case "$1" in
        start)
                # Create keys if necessary
                do_rsa1_keygen;
                do_rsa_keygen;
                do_dsa_keygen;
```

```
                echo -n "Starting SSHD: "
                if [ ! -f $PID_FILE ] ; then
                        sshd $OPTIONS
                        RETVAL=$?
                        if [ "$RETVAL" = "0" ] ; then
                                my_success "sshd startup" "sshd"
                                touch /var/lock/subsys/sshd
                        else
                                my_failure "sshd startup" ""
                        fi
                fi
                echo
                ;;
        stop)
                echo -n "Shutting down SSHD: "
                if [ -f $PID_FILE ] ; then
                        killproc sshd
                        RETVAL=$?
                        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/sshd
                fi
                echo
                ;;
        restart)
                do_restart_sanity_check
                $0 stop
                $0 start
                RETVAL=$?
                ;;
        condrestart)
                if [ -f /var/lock/subsys/sshd ] ; then
                        do_restart_sanity_check
                        $0 stop
                        $0 start
                        RETVAL=$?
                fi
                ;;
        status)
                status sshd
                RETVAL=$?
                ;;
        *)
                echo "Usage: sshd
{start|stop|restart|status|condrestart}"
                exit 1
                ;;
esac
exit $RETVAL
```

Установите права доступа к файлу, назначьте его владельцем пользователя `root` и создайте соответствующие ссылки:

```
[root@drwalbr /]# chmod 700 /etc/init.d/sshd
[root@drwalbr /]# chown 0.0 /etc/init.d/sshd
[root@drwalbr /]# chkconfig --add sshd
[root@drwalbr /]# chkconfig --level 2345 sshd on
```

Тестирование OpenSSH

Для проверки работоспособности OpenSSH попытайтесь установить удаленное соединение между двумя системами. Ниже приведены подробные инструкции по установке соединения по протоколу SSH между двумя системами `drwalbr.und` (IP-адрес 192.168.1.105) и `karlnext.und` (IP-адрес 192.168.1.35).

Для реализации безопасного соединения на каждой из систем пользователь должен создать пару ключей (закрытый и открытый). Открытые ключи переносятся на другую систему (не ту на которой он был создан) и хранятся в домашнем каталоге пользователя в файле `/.ssh/authorized_keys`.

Шаг 1

Для создания пары ключей на системе `drwalbr.und` от имени пользователя `drwalbr` выполните:

```
[drwalbr@drwalbr drwalbr]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
```

Введите имя каталога, в котором будут сохранены ключи. Рекомендуется имя каталога, предлагаемое по умолчанию - `/home/drwalbr/.ssh/id_rsa`:

```
Enter file in which to save the key (/home/drwalbr/.ssh/id_rsa):
```

Введите пароль:

```
Enter passphrase (empty for no passphrase): $ecretnoe_Slovo_dr_Walbr
```

Подтвердите пароль:

```
Enter same passphrase again: $ecretnoe_Slovo_dr_Walbr
Your identification has been saved in /home/drwalbr/.ssh/id_rsa.
Your public key has been saved in /home/drwalbr/.ssh/id_rsa.pub.
The key fingerprint is:
f0:7f:09:90:5d:71:d4:59:1e:e5:9b:2b:b2:77:a1:ce drwalbr@drwalbr.und
```

На системе `karlnext.und` от имени пользователя `drwalbr`:

```
[drwalbr@drwalbr drwalbr]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
```

Введите имя каталога, в котором будут сохранены ключи. Рекомендуется имя каталога, предлагаемое по умолчанию - `/home/drwalbr/.ssh/id_rsa`:

```
Enter file in which to save the key (/home/drwalbr/.ssh/id_rsa):
```

Ведите пароль:

```
Enter passphrase (empty for no passphrase): $ecretnoe_Slovo_Karl_Next
```

Подтвердите пароль:

```
Enter same passphrase again: $ecretnoe_Slovo_Karl_Next
Your identification has been saved in /home/drwalbr/.ssh/id_rsa.
Your public key has been saved in /home/drwalbr/.ssh/id_rsa.pub.
The key fingerprint is:
f0:7f:09:90:5d:71:d4:59:1e:e5:9b:2b:b2:77:a1:ce drwalbr@karlnext.und
```

Закрытый ключ будет находиться в файле `id_rsa`, а открытый в файле `id_rsa.pub`.

ЗАМЕЧАНИЕ В приведенном выше примере описана генерация ключей для протокола SSH версии 2. Если вы по каким либо причинам собираетесь использовать ключи для протокола SSH версии 1, следует использовать команду:

```
[drwalbr@drwalbr drwalbr]$ ssh-keygen -t rsa1
```

В этом случае закрытый ключ будет находиться в файле `identity`, а открытый в - `identity.pub`.

Шаг 2

Скопируйте открытый ключ `id_rsa.pub`, находящийся на системе `drwalbr.und` в каталоге `/home/drwalbr/.ssh/`, в файл `/home/drwalbr/.ssh/authorized_keys` системы `karlnext.und`.

Шаг 3

Скопируйте открытый ключ `id_rsa.pub`, находящийся на системе `karlnext.und` в каталоге `/home/drwalbr/.ssh/`, в файл `/home/drwalbr/.ssh/authorized_keys` системы `drwalbr.und`. Копирование ключей может быть осуществлено с помощью электронной почты или в случае, если системы находятся поблизости, с помощью съемных носителей.

Шаг 4

На обеих системах зарегистрируйтесь в качестве суперпользователя root и запустите sshd:

```
[root@drwalbr /]# /etc/init.d/sshd start
Starting SSHD:       [OK]
[root@karlnext /]# /etc/init.d/sshd start
Starting SSHD:       [OK]
```

Шаг 5

Регистрация на удаленной системе осуществляется с помощью команды:

```
[drwalbr@drwalbr drwalbr]$ ssh name_of_user@name_of_remoute_system.domen
```

где:

name_of_user – имя пользователя;

name_of_remoute_system.domen – имя удаленной системы, на которой осуществляется регистрация.

Попробуйте зарегистрироваться в качестве пользователя drwalbr на удаленной системе karlnext.und с системы drwalbr.und. Для этого от имени пользователя drwalbr на системе drwalbr.und выполните:

```
[drwalbr@drwalbr drwalbr]$ ssh drwalbr@karlnext.und
```

Введите пароль, используемый для защиты закрытого ключа на системе drwalbr.und:

```
Enter passphrase for key '/home/drwalbr/.ssh/id_dsa': $ecret-
noe_Slovo_dr_Walbr
Last login: Tue Mar 25 11:52:56 2003 from drwalbr.und
[drwalbr@karlnext drwalbr]$
```

ЗАМЕЧАНИЕ Если вы работаете в локальной сети, в которой нет DNS-сервера, для нормальной работы SSH в файлы /etc/hosts на системе drwalbr.und следует добавить строку:

```
192.168.1.35 karlnext.und karlnext
```

а на системе karlnext.und - строку:

```
192.168.1.105 drwalbr.und drwalbr
```

Не рекомендуется использовать файлы /etc/hosts для преобразования имен систем в IP-адреса в сетях, содержащих больше 5…10 систем. В этом случае необходимо установить, настроить и запустить DNS-сервер.

Использование OpenSSH

Часто OpenSSH используется для копирования файлов с одной системы на другую. Для этого используется утилита scp (Secure Copy), синтаксис которой аналогичен синтаксису широко используемой для копирования файлов на локальной системе утилиты cp.

Для копирования файлов с локальной системы на удаленную наберите:

```
[drwalbr@drwalbr /]$ scp -p local_dir/local_file
name_of_user@name_of_remoute_system.domen:/dir/file
```

где:

-p – опция, предписывающая сохранять атрибуты копируемого файла;

local_dir – путь к каталогу, откуда копируется файл на локальной системе;

local_file –.имя копируемого файла на локальной системе;

name_of_user – имя пользователя удаленной системы;

name_of_remoute_system.domen – имя удаленной системы;

dir – путь к каталогу на удаленной системе, в который копируется файл;

file – имя файла на удаленной системе, в который осуществляется копирование.

Например, если вы хотите скопировать файлы test и test1, находящиеся на системе drwalbr.und в домашнем каталоге пользователя drwalbr, в домашний каталог пользователя drwalbr на системе karnext.und, то на системе drwalbr.und от имени пользователя drwalbr выполните команду:

```
[drwalbr@drwalbr drwalbr]$ scp -p test*
drwalbr@karlnext.und:/home/drwalbr/
```

Введите пароль, используемый для защиты закрытого ключа на системе drwalbr.und:

```
Enter passphrase for key '/home/drwalbr/.ssh/id_dsa':
20030325              100% |*********************|   229 KB    00:00
20030326              100% |*********************|   246 KB    00:00
```

Для копирования файлов с удаленной системы на локальную используйте:

```
[drwalbr@drwalbr /]$ scp -p
name_of_user@name_of_remoute_system.domen:/dir/file local_dir/local_file
```

Для копирования файлов с одной удаленной системы на другую удаленную систему выполните:

```
drwalbr@drwalbr /]$ scp -p
name_of_user@name_of_remoute_system.domen:/dir/file
name_of_user_1@name_of_remoute_system_1.domen_1:/dir_1/file_1
```

где:

`name_of_user_1`, `name_of_remoute_system_1`, `domen_1`, `dir_1`, `file_1` – соответственно, значения параметров `name_of_user`, `name_of_remoute_system`, `domen`, `dir`, `file` для удаленной системы, на которую копируется файл.

В некоторых случаях, например, если пользователь забыл пароль или он стал доступен третьим лицам, может потребоваться изменение пароля, используемого для защиты секретного ключа. Для изменения пароля пользователя `drwalbr` на системе `drwalbr` выполните:

```
[drwalbr@drwalbr drwalbr]$ ssh-keygen –p
```

Введите имя ключа, для которого должен быть изменен пароль, используемый для защиты:

```
Enter file in which the key is (/home/drwalbr/.ssh/id_rsa):<Enter>
```

Введите старый пароль:

```
Enter old passphrase: $ecretnoe_Slovo_dr_Walbr
```

Введите новый пароль:

```
Enter new passphrase again: New_$ecretnoe_Slovo
```

Подтвердите новый пароль:

```
Enter same passphrase again: New_$ecretnoe_Slovo
Your identification has been saved with the new passphrase
```

OpenSSH в окружении chroot-jail

Для того, что бы программа OpenSSH выполнялась в окружении chroot-jail – т. е. пользователь, зарегистрировавшийся с помощью клиента `ssh`, не имел бы доступа на чтение-запись и исполнение файлов за пределами своего пользовательского каталога – необходимо создать среду chroot-jail и установить версию OpenSSH, поддерживающую работу в этой среде. Этот вид установки полезен не только для компаний, предоставляющих услуги хостинга, но и для администраторов, желающих повысить безопасность своей системы. В этом случае, если злоумышленник получит доступ только к аутентификационной информации пользователя он вря ли сможет получить доступ к системе в целом.

Создание окружения chroot-jail

В конечном счете, вы должны создать подобие корневой файловой системы, содержащей все компоненты, необходимые для работы приложений (исполняемые файлы, файлы настроек, библиотеки и т. п.). Для повышения безопасности системы окружение chroot-jail лучше всего создавать на отдельном разделе диска, смонтированном в отдельный каталог, например `/chroot`. Если вы следовали рекомендациям главы 2, то такой раздел уже существует.

Шаг 1

Создайте нового пользователя:

```
[root@drwalbr /]# useradd -g users -d /chroot/urbanoff urbanoff
[root@drwalbr /]# passwd urbanoff
Changing password for user urbanoff
New UNIX password: Urbanoff's_$ecretnoe_$lovo
Retype new UNIX password: Urbanoff's_$ecretnoe_$lovo
passwd: all authentication tokens updated successfully
```

Шаг 2

Создайте необходимые каталоги в домашнем каталоге пользователя `urbanoff`:

```
[root@drwalbr /]# mkdir /chroot/urbanoff/bin
```

```
[root@drwalbr /]# mkdir /chroot/urbanoff/dev
[root@drwalbr /]# mkdir /chroot/urbanoff/etc
[root@drwalbr /]# mkdir /chroot/urbanoff/lib
[root@drwalbr /]# mkdir /chroot/urbanoff/usr
[root@drwalbr /]# mkdir /chroot/urbanoff/usr/bin
[root@drwalbr /]# mkdir /chroot/urbanoff/usr/lib
[root@drwalbr /]# mkdir /chroot/urbanoff/lib/i686
```

Шаг 3

Установите права доступа к каталогам:

```
[root@drwalbr /]# chmod -R 0111 /chroot/urbanoff/*
```

Шаг 4

Скопируйте минимальный набор программ, необходимый для работы пользователя, например, `cp`, `bash`, `ls`, `mkdir`, `grep`, `rm`, `vi`, `dircolors` в соответствующие каталоги:

```
[root@drwalbr urbanoff]# cp /bin/cp /chroot/urbanoff/bin
[root@drwalbr urbanoff]# cp /bin/bash /chroot/urbanoff/bin
[root@drwalbr urbanoff]# cp /bin/ls  /chroot/urbanoff/bin
[root@drwalbr urbanoff]# cp /bin/mkdir  /chroot/urbanoff/bin
[root@drwalbr urbanoff]# cp /bin/grep  /chroot/urbanoff/bin
[root@drwalbr urbanoff]# cp /bin/rm  /chroot/urbanoff/bin
[root@drwalbr urbanoff]# cp /bin/vi  /chroot/urbanoff/bin
[root@drwalbr urbanoff]# cp /usr/bin/dircolors  /chroot/urbanoff/usr/bin
```

Шаг 5

Установите права доступа к каталогам:

```
[root@drwalbr urbanoff]# chmod 0111 /chroot/urbanoff/bin/*
[root@drwalbr urbanoff]# chmod 0111 /chroot/urbanoff/usr/bin/*
```

Шаг 6

В файле `/etc/passwd` строку:

```
urbanoff:x:503:100::/chroot/urbanoff:/bin/bash
```

замените на:

```
urbanoff:x:503:100::/chroot/urbanoff/./:/bin/bash
```

Шаг 7

Исполняемые файлы в домашнем каталоге пользователя `urbanoff` используют динамические библиотеки, находящиеся в каталогах `/lib` и `/usr/lib`, недоступных пользователю, работающему в окружении chroot-jail. Поэтому необходимо создать локальные копии для всех библиотек, используемых исполняемыми файлами, расположенные в домашнем каталоге пользователя `urbanoff`. Для нахождения необходимых динамических библиотек используйте команду `ldd`:

```
[root@drwalbr urbanoff]# ldd bash cp ls mkdir grep rm vi
/usr/bin/dircolors
bash:
  libtermcap.so.2 => /lib/libtermcap.so.2 (0x4cc1e000)
  libdl.so.2 => /lib/libdl.so.2 (0x4cc23000)
  libc.so.6 => /lib/i686/libc.so.6 (0x4cc26000)
  /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x4cc07000)
cp:
  libc.so.6 => /lib/i686/libc.so.6 (0x4de49000)
  /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x4de32000)
ls:
  libtermcap.so.2 => /lib/libtermcap.so.2 (0x4db5c000)
  libc.so.6 => /lib/i686/libc.so.6 (0x4db61000)
  /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x4db45000)
mkdir:
  libc.so.6 => /lib/i686/libc.so.6 (0x40d9b000)
  /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40d84000)
grep:
  libc.so.6 => /lib/i686/libc.so.6 (0x44399000)
  /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x44382000)
rm:
  libc.so.6 => /lib/i686/libc.so.6 (0x439ef000)
```

```
    /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x439d8000)
  vi:
    libtermcap.so.2 => /lib/libtermcap.so.2 (0x4d667000)
    libdl.so.2 => /lib/libdl.so.2 (0x4d66c000)
    libc.so.6 => /lib/i686/libc.so.6 (0x4d66f000)
    /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x4d650000)
  /usr/bin/dircolors:
    libc.so.6 => /lib/i686/libc.so.6 (0x41203000)
    /lib/ld-linux.so.2 =>/lib/ld-linux.so.2 (0x411ec000)
```

Скопируйте библиотеки в соответствующие подкаталоги домашнего каталога пользователя `urbanoff` и удалите из них комментарии:

```
[root@drwalbr /]# cp /lib/libtermcap.so.2 /chroot/urbanoff/lib/
[root@drwalbr /]# cp /lib/libd1.so.2 /chroot/urbanoff/lib/
[root@drwalbr /]# cp /lib/libc.so.6 /chroot/urbanoff/lib/
[root@drwalbr /]# cp /lib/libgcc_s.so.1 /chroot/urbanoff/lib/
[root@drwalbr /]# cp /lib/ld-linux.so.2 /chroot/urbanoff/lib/
[root@drwalbr /]# cp /lib/i686/libc.so.6 /chroot/urbanoff/lib/i686/
[root@drwalbr /]# strip -R .comment /chroot/urbanoff/lib/*
```

Шаг 8

Скопируйте файлы настроек в соответствующие подкаталоги домашнего каталога пользователя `urbanoff`:

```
[root@drwalbr /]# cp /etc/dir_colors /chroot/urbanoff/etc/
[root@drwalbr /]# cp /etc/passwd /chroot/urbanoff/etc/
```

Шаг 9

Создайте в домашнем каталоге пользователя `urbanoff` файл устройства `/chroot/urbanoff/dev/null` и установите права доступа к нему:

```
[root@drwalbr /]# mknod /chroot/urbanoff/dev/null c 1 3
 [root@dr mknod walbr /]# chmod 666 /chroot/urbanoff/dev/null
```

ЗАМЕЧАНИЕ Если вы постоянно добавляете новых пользователей в окружение chroot-jail, для упрощения данной операции можно написать скрипт, реализующий шаги 1…9.

Компиляция, оптимизация, инсталляция, конфигурирование и тестирование OpenSSH в среде chroot-jail

Компиляция, оптимизация, инсталляция и конфигурирование OpenSSH в среде chroot-jail осуществляется так же, как и в случае инсталляции в обычной среде, с тем отличием, что используются исходные коды из архива `openssh-version-chroot.tar.gz` или исходные коды из архива `openssh-version.tar.gz`, модифицированные с помощью патча `osshChroot-version.diff`.

Если вы используете ядро, собранное из исходных кодов, к которым применен патч Grsecurity, убедитесь, что в настройках ядра опция `CONFIG_GRKERNSEC_CHROOT` не включена, т. е. при конфигурировании кодов ядра вы дали отрицательный ответ на вопрос:

```
Chroot jail restrictions (CONFIG_GRKERNSEC_CHROOT) [N/y/?] <n>
```

Тестирование OpenSSH в среде chroot-jail можно провести путем проверки возможности регистрации chroot-пользователя на удаленной системе с помощью ssh-клиента:

```
[dymatel@urbanoff urbanoff]$ ssh urbanoff@drwalbr.und
```

Введите пароль, используемый для защиты закрытого ключа пользователя `urbanoff` на системе `dymatel.und`:

```
Enter passphrase for key '/home/urbanoff/.ssh/id_dsa': Ur-
banoff's_$ecretnoe_$lovo
bash-2.05a$
```

Если регистрация прошла удачно, попробуйте «вырваться» из окружения chroot-jail, например, с помощью команды:

```
bash-2.05a$ cd /
```

Если вы окажетесь в корневом каталоге chroot-пользователя:

```
bash-2.05a$ ls
bin  dev  etc  lib  usr
```

то все настроено правильно.

Если вы окажетесь в корневом каталоге системы, т. е.:

```
bash-2.05a$ ls
bin   chroot  etc   initrd  lost+found  opt   root  tmp  var
boot  dev     home  lib     mnt         proc  sbin  usr
```

то среда chroot-jail не работает. Скорее всего, вы используете OpenSSH из rpm-пакета, входящего в состав дистрибутива ASPLinux 7.3 (Vostok).

Часть 4

Программное обеспечение для ограничения доступа к серверу и обнаружения попыток деструктивного воздействия

Глава 14

Sudo – программное обеспечение для делегирования пользователям сервера полномочий пользователя root в ограниченном объеме

В этой главе:

Sudo (superuser do) – программа, предназначенная для предоставления администратору системы возможности делегирования в ограниченном объеме привилегий пользователя `root` обычным пользователям системы.

Возможности Sudo аналогичны возможностям команды `su`. Однако Sudo предоставляет более широкие возможности для частичного делегирования полномочий обычным пользователям системы и протоколирования действий пользователя `root`. Sudo позволяет:

- ограничивать номенклатуру команд, выполняемых обычным пользователем с правами `root`;
- регистрировать все команды, выполняемые от имени пользователя `root`, при этом регистрация может осуществляться как на локальной, так и на удаленной системе, например, центральном сервере;
- конфигурационный файл имеет установку, позволяющую использовать утилиту на многих машинах.

Программа Sudo может оказаться просто незаменимой в ситуации, когда нужно разрешить доступ с правами пользователя `root` только к некоторым программам.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта Sudo по состоянию на 8.04.2003. Регулярно посещайте домашнюю страницу проекта `http://www.sudo.ws/` и отслеживайте обновления.

Исходные коды Sudo содержатся в архиве `sudo-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `sudo-1.6.7p3.tar.gz`).

Инсталляция с помощью rpm-пакета

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет `sudo` с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq sudo
```

Шаг 2

В случае его отсутствия перейдите в каталог, где находится пакет `sudo-1.6.5p2-2.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

и установите:

```
[root@drwalbr distrib]# rpm –ihv sudo-1.6.5p2-2.i386.rpm
```

или обновите пакет:

```
[root@drwalbr distrib]# rpm –Uhv sudo-1.6.5p2-2.i386.rpm
```

После установки пакета перейдите к конфигурированию программы Sudo, описанного ниже в соответствующем разделе.

Компиляция, оптимизация и инсталляция Sudo

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архив с исходными кодами в каталоге `/var/tmp`:

```
[root@drwalbr tmp]# tar xzpf sudo-1.6.7p3.tar.gz
```

Шаг 3

Сконфигурируйте исходные коды Sudo:

```
[root@drwalbr tmp]# cd sudo-1.6.7p3
[root@drwalbr sudo-1.6.7p3]# CFLAGS="-O2 -march=i686 -funroll-loops"; ex-
port CFLAGS
./configure \
--prefix=/usr \
--sbindir=/usr/sbin \
--with-logging=syslog \
--with-logfac=authpriv \
--with-pam \
--with-with-env-editor \
--with-ignore-dot \
--with-tty-tickets \
--disable-root-mailer \
--disable-root-sudo \
--disable-path-info \
--with-mail-if-noperms \
--with-mailsubject="*** Sudo SECURITY information for %h ***"
```

При таких параметрах конфигурации Sudo:

- регистрация сообщения Sudo будет осуществляться с использованием syslog;
- для аутентификации пользователей будут использоваться модули PAM;
- для редактирования конфигурационного файла будет использоваться программа visudo;
- символы "`.`" в путях к файлам будут игнорироваться;
- будут использоваться различные контрольные файлы для каждого пользователя и консоли;
- программа электронной почты не будет запускаться с правами пользователя `root`;
- пользователю `root` будет запрещено выполнять команду `sudo`;
- при попытке запуска обычным пользователем запрещенной команды от имени `root`, будет выводиться сообщение "`command not allowed`";
- в случае попытки запуска неразрешенных программ обычными пользователями администратору системы будет отправляться сообщение по электронной почте.

Шаг 4

Откомпилируйте исходные коды, проинсталлируйте файлы Sudo, создайте и сохраните список инсталлированных файлов:

```
[root@drwalbr sudo-1.6.7p3]# make
[root@drwalbr sudo-1.6.7p3]# find /* > /root/sudo1
[root@drwalbr sudo-1.6.7p3]# make install
[root@drwalbr sudo-1.6.7p3]# strip /usr/bin/sudo
[root@drwalbr sudo-1.6.7p3]# strip /usr/sbin/visudo
[root@drwalbr sudo-1.6.7p3]# mkdir -p -m0700 /var/run/sudo
[root@drwalbr sudo-1.6.7p3]# find /* > /root/sudo2
[root@drwalbr sudo-1.6.7p3]# diff /root/sdudo1 /root/sudo2 >
/root/sudo.installed
[root@drwalbr sudo-1.6.7p3]# mv /root/sudo.installed
/very_reliable_place/sudo.installed.YYYYMMDD
```

Шаг 5

Удалите архив и каталог с исходными кодами Sudo:

```
[root@drwalbr sudo-1.6.7p3]# cd /var/tmp/
```

```
[root@drwalbr tmp]# rm -rf sudo-1.6.7p3/
[root@drwalbr tmp]# rm -f sudo-1.6.7p3.tar.gz
```

Конфигурирование Sudo

Конфигурирование Sudo осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/sudoers`;
- файла для поддержки модулей PAM `/etc/pam.d/sudo`.

ЗАМЕЧАНИЕ Для редактирования файла `/etc/sudoers` используйте только `visudo`. Использование `vi` и других редакторов не допускается.

Шаг 1

Отредактируйте с помощью `visudo` файл `/etc/sudoers` в соответствии с приведенными рекомендациями:

```
# This file MUST be edited with the 'visudo' command as root.
# Defaults specification
Defaults rootpw
# User privilege specification
# Super-user root can run anything as any user.
root     ALL=(ALL) ALL

# Uncomment to allow people in group wheel to run all commands
%wheel   ALL=(ALL) ALL
```

В этой простейшей конфигурации (более сложные варианты рассмотрены ниже) всем пользователям из группы `wheel` разрешается получать права пользователя `root` в полном объеме.

Опция `Defaults rootpw`
указывает на необходимость при вызове `sudo` обычным пользователем запроса пароля пользователя `root`, а не своего пароля.

Опция `root ALL= (ALL) ALL`
позволяет пользователю `root` выполнять все операции на сервере.

Опция `%wheel ALL= (ALL) ALL`
предоставляет возможность любому пользователю из группы `wheel` выполнять все команды от имени пользователя `root`.

Шаг 2

Добавьте в группу `wheel` (для группы `wheel` GID=10) пользователей, которым вы хотите разрешить использовать `sudo` для получения прав пользователя `root`. Например, чтобы добавить пользователя `drwalbr` выполните команду:

```
[root@drwalbr /]# usermod -G10 drwalbr
```

Шаг 3

Создайте файл `/etc/pam.d/sudo`, содержащий следующие строки:

```
#%PAM-1.0
auth       required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Установите права доступа к файлу, назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 0640 /etc/pam.d/sudo
[root@drwalbr /]# chown 0.0 /etc/pam.d/sudo
```

Шаг 4

Для исключения возможности получения прав пользователя `root` обычными пользователями системы удалите SUID-бит программы `su`:

```
[root@drwalbr /]# chmod 0511 /bin/su
```

Тестирование Sudo

Шаг 1

Зарегистрируйтесь в системе в качестве пользователя из группы `wheel`. В рассматриваемом примере членом этой группы является пользователь `drwalbr`.

Шаг 2

Попытайтесь выполнить какую-нибудь команду от имени пользователя `root`, например, запустить сервер `sshd`:

```
[drwalbr@drwalbr /]$ sudo /etc/init.d/sshd start
```

Введите пароль пользователя `root`:

```
Password:Root's_$ecretnoe_Slovo
Starting SSHD:                                [OK]
```

Шаг 3

Зарегистрируйтесь в системе в качестве пользователя, не являющегося членом группы `wheel`, например `karlnext`.

Шаг 4

Попытайтесь выполнить какую-нибудь команду от имени пользователя `root`, например, остановить сервер `sshd`:

```
[karlnext@drwalbr /]$ sudo /etc/init.d/sshd stop
```

Пользователь получит предупреждение о возможности возникновения проблем с администратором системы, необходимости уважительного отношения к правам других пользователей на конфиденциальность и осмысленном использовании команд:

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these two things:

        #1) Respect the privacy of others.
        #2) Think before you type.
```

Даже если пользователь `karlnext` введет правильный пароль пользователя `root`:

```
Password: Root's_$ecretnoe_Slovo
```

команда не будет выполнена, а `karlnext` получит сообщение о том, что он не в праве использовать `sudo`. О попытке неправомерного использования им `sudo` будет сообщено администратору системы:

```
karlnext is not in the sudoers file.  This incident will be reported.
```

Более сложная конфигурация Sudo

Отредактируйте с помощью `visudo` файл `/etc/sudoers` в соответствии с приведенными рекомендациями:

```
# This file MUST be edited with the 'visudo' command as root.

# User alias specification
User_Alias      FULLTIME_USERS = drwalbr, karlnext
User_Alias      PARTTIME_USERS = hare, fish, cat

# Cmnd alias specification
Cmnd_Alias      HTTP = /etc/init.d/httpd, /bin/vi /etc/httpd/*

Cmnd_Alias      MYSQL  = /etc/init.d/mysqld, /usr/bin/mysql,
/usr/bin/mysqladmin

# Defaults specification
Defaults:FULLTIME_USERS         rootpw
Defaults:FULLTIME_USERS         !lecture

# User privilege specification
# Super-user root can run anything as any user.
root            ALL=(ALL) ALL
```

```
# Every users member of the group wheel will be allowed
# to run all commands as super-user root.
%wheel          ALL=(ALL) ALL

# Full time users may run anything but need a password.
FULLTIME_USERS  ALL = ALL

# Part time users may administrate httpd and mysqld servers.
PARTTIME_USERS  ALL = HTTP, MYSQL
```

В этом файле строки:

```
User_Alias      FULLTIME_USERS = drwalbr, karlnext
User_Alias      PARTTIME_USERS = hare, fish, cat
```

описывают две группы пользователей FULLTIME_USERS и PARTTIME_USERS. Пользователям из группы FULLTIME_USERS – drwalbr и karlnext – в дальнейшем будет разрешен доступ к серверу с правами root в полном объеме. Пользователям из группы PARTTIME_USERS – hare, fish и cat – в дальнейшем будет предоставлен доступ с правами пользователя root в объеме, достаточном для администрирования Web-сервера и сервера баз данных MySQL.

ЗАМЕЧАНИЕ Пользователи, описанные в разделе User alias specification, используя sudo, смогут получать доступ к системе с правами пользователя root даже, если они не являются членами группы wheel.

Строка:

```
root ALL= (ALL) ALL
```

позволяет пользователю root выполнять все операции на сервере.

Строка:

```
%wheel ALL= (ALL) ALL
```

предоставляет возможность любому пользователю из группы wheel выполнять все команды от имени пользователя root.

Строка:

```
FULLTIME_USERS  ALL = ALL
```

разрешает группе пользователей FULLTIME_USERS(drwalbr, karlnext) доступ к системе с правами пользователя root в полном объеме.

Строка:

```
Cmnd_Alias HTTP = /etc/init.d/httpd, /bin/vi /etc/httpd/*
```

описывает команды, которые в дальнейшем будет разрешено выполнять пользователям из группы PARTTIME_USERS для администрирования Web-сервера:

- /etc/init.d/httpd – запуск и остановка Web-сервера;
- /bin/vi /etc/httpd/* – редактора vi, необходимого для редактирования файлов конфигурации Web-сервера в каталоге /etc/httpd/*.

Строка:

```
Cmnd_Alias MySQL = /etc/init.d/mysqld, /usr/bin/mysql,
/usr/bin/mysqladmin
```

описывает команды, которые в дальнейшем будет разрешено выполнять пользователям из группы PARTTIME_USERS для администрирования сервера баз данных MySQL:

- /etc/init.d/mysqld – запуск и остановка сервера баз данных;
- /usr/bin/mysql – запуск клиентской программы mysql;
- /usr/bin/mysqladmin – запуск программы для администрирования сервера баз данных mysqladmin.

Строка:

```
Defaults:FULLTIME_USERS         rootpw
```

требует ввода пароля пользователя root при использовании sudo для пользователей из группы PARTTIME_USERS (по умолчанию sudo требует ввода пароля обычного пользователя).

Строка:

```
Defaults:FULLTIME_USERS         !lecture
```

отменяет вывод предостерегающих сообщений вида:

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these two things:
```

```
#1) Respect the privacy of others.
#2) Think before you type.
```

для пользователей из группы `FULLTIME_USERS`.

Строка:

```
PARTTIME_USERS  ALL = HTTP, MYSQL
```

разрешает доступ к системе с правами пользователя `root` пользователям из группы `PARTTIME_USERS` (`hare`, `fish` и `cat`) в объеме, достаточном для администрирования Web-сервера и сервера баз данных.

Глава15

sXid – программное обеспечение для поиска файлов, в правах доступа к которым установлены SUID и SGID-биты

В этой главе:

1. Ограничения и допущения
2. Пакеты
3. Инсталляция с помощью rpm-пакетов
4. Компиляция, оптимизации и инсталляция sXid
2. Конфигурирование sXid
3. Тестирование sXid

Многим системным программам (которые могут быть запущены любым, в том числе и непривилегированным пользователем) для правильного функционирования необходимы права пользователя `root`. Одной из таких программ является программа `passwd`, предназначенная для самостоятельного изменения пользователями системы своего пароля. Для нормального функционирования этой программе просто необходимо обеспечить доступ для чтения данных и внесения изменений в файл `/etc/shadow` с правами пользователя `root`. Поэтому программа, осуществляющая смену пароля пользователя, выполняется не от имени запустившего его пользователя, а от имени суперпользователя (который, естественно, имеет право на запись в файл `/etc/shadow`). Для этого у исполняемого файла программы установлен специальный SUID-бит, позволяющий изменять идентификатор пользователя у запущенного процесса. Эта, безусловно, нарушающая исходную модель разграничения доступа, особенность Linux используется большим числом приложений. Поэтому наличие SUID или SGID-битов у исполняемых файлов негативно влияет на безопасность системы.

Для поиска программ на файлы, у которых установлены SUID или SGID-биты используется программа sXid. После установки sXid регулярно запускается с помощью `cron` и сообщает администратору системы по электронной почте обо всех обнаруженных файлах, на которые установлены SUID или SGID-биты.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта sXid по состоянию на 22.04.2003. Регулярно посещайте домашнюю страницу проекта `http://www.phunnypharm.org/pub/` и отслеживайте обновления.

Исходные коды sXid содержатся в архиве `sxid_version.tar.gz` (последняя доступная на момент написания главы стабильная версия `sxid_4.0.2.tar.gz`).

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет sXid с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq sXid
```

Шаг 2

В случае его отсутствия перейдите в каталог, где находится пакет `sxid-4.0.1-1.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

и установите:

```
[root@drwalbr distrib]# rpm –ihv sxid-4.0.1-1.asp.i386.rpm
```

или обновите пакет:

```
[root@drwalbr distrib]# rpm –Uhv sxid-4.0.1-1.asp.i386.rpm
```

После установки пакета перейдите к конфигурированию программы sXid, подробно описанного ниже.

Компиляция, оптимизация и инсталляция sXid

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архив с исходными кодами `sxid_4.0.2.tar.gz` в каталоге `/var/tmp`, откомпилируйте и проинсталлируйте sXid, создайте список установленных файлов и сохраните его в надежном месте:

```
[root@drwalbr tmp]# tar xzpf sxid_4.0.2.tar.gz
[root@drwalbr tmp]# cd sxid-4.0.2
[root@drwalbr sxid-4.0.2]# CFLAGS="-O2 -march=i686 -funroll-loops"; ex-
port CFLAGS
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--mandir=/usr/share/man
[root@drwalbr sxid-4.0.2]# find /* > /root/sxid1
[root@drwalbr sxid-4.0.2]# make install
[root@drwalbr sxid-4.0.2]# find /* > /root/sxid2
[root@drwalbr sxid-4.0.2]# diff /root/sxid1 /root/sxid2 >
/root/sxid.installed
[root@drwalbr sxid-4.0.2]# diff sxid1 sxid2 > sxid.installed
[root@drwalbr sxid-4.0.2]# mv sxid.installed /very_reliable_place/
sxid.installed.YYYYMMDD
```

Шаг 3

Удалите каталоги с исходными кодами `sXid` и архив:

```
[root@drwalbr sxid-4.0.2]# cd /var/tmp/
[root@drwalbr tmp]# rm -rf sxid-4.0.2/
[root@drwalbr tmp]# rm -f sxid_4.0.2.tar.gz
```

Конфигурирование sXid

Конфигурирование sXid осуществляется с помощью двух конфигурационных файлов:

- конфигурационного файла sXid `/etc/sxid.conf`;
- файла `/etc/cron.daily/sxid` для автоматического запуска sXid с помощью `crond`.

Шаг 1

Создайте или отредактируйте файл `/etc/sxid.conf` в соответствии с приведенными ниже рекомендациями:

```
Configuration file for sXid
# Note that all directories must be absolute with no trailing /'s

# Where to begin our file search
SEARCH = "/"

# Which subdirectories to exclude from searching
EXCLUDE = "/proc /mnt /cdrom /floppy"

# Who to send reports to
EMAIL = "root"

# Always send reports, even when there are no changes?
ALWAYS_NOTIFY = "no"

# Where to keep interim logs. This will rotate 'x' number of
# times based on KEEP_LOGS below
LOG_FILE = "/var/log/sxid.log"

# How many logs to keep
KEEP_LOGS = "5"
```

```
# Rotate the logs even when there are no changes?
ALWAYS_ROTATE = "no"

# Directories where +s is forbidden (these are searched
# even if not explicitly in SEARCH), EXCLUDE rules apply
FORBIDDEN = "/home /tmp"

# Remove (-s) files found in forbidden directories?
ENFORCE = "yes"

# This implies ALWAYS_NOTIFY. It will send a full list of
# entries along with the changes
LISTALL = "no"

# Ignore entries for directories in these paths
# (this means that only files will be recorded, you
# can effectively ignore all directory entries by
# setting this to "/"). The default is /home since
# some systems have /home g+s.
IGNORE_DIRS = "/home"

# File that contains a list of (each on it's own line)
# other files that sxid should monitor. This is useful
# for files that aren't +s, but relate to system
# integrity (tcpd, inetd, apache...).
# EXTRA_LIST = "/etc/sxid.list"

# Mail program. This changes the default compiled in
# mailer for reports. You only need this if you have changed
# it's location and don't want to recompile sxid.
MAIL_PROG = "/bin/mail"
```

Шаг 2

Установите права доступа к файлу `/etc/sxid.conf`:

```
[root@drwalbr /]# chmod 400 /etc/sxid.conf
```

Шаг 3

Для ежедневного автоматического запуска sXid создайте файл `/etc/cron.daily/sxid`:

```
#!/bin/sh

SXID_OPTS=

if [ -x /usr/bin/sxid ]; then
        /usr/bin/sxid ${SXID_OPTS}
fi
```

Шаг 4

Сделайте файл `/etc/cron.daily/sxid` исполняемым:

```
[root@drwalbr /]# chmod 510 /etc/cron.daily/sxid
```

Тестирование sXid

Для проверки работоспособности убедитесь, что sXid обнаруживает в каталоге `/home` исполняемые файлы, имеющие SUID или SGID-биты, и удаляет SUID или SGID-биты. Для этого выполните следующие операции.

Шаг 1

Создайте в каталоге `/home` файл `worm` и сделайте его исполняемым:

```
[root@drwalbr root]# > cd /home
[root@drwalbr home]# > worm
[root@drwalbr home]# chmod +x worm
[root@drwalbr home]# ls -l worm
-rwxr-xr-x    1 root     root            0 Апр 23 19:02 worm
```

Шаг 2
Запустите sXid:

```
[root@drwalbr home]# sxid –k

sXid Vers  : 4.0.2
Check run  : Wed Apr 23 19:06:53 2003
This host  : drwalbr.und
Spotcheck  : /home
Excluding  : /proc /mnt /cdrom /floppy
Ignore Dirs: /home
Forbidden  : /home /tmp
  (enforcing removal of s[ug]id bits in forbidden paths)


No changes found
```

Проверка прошла успешно, файлы с SUID или SGID-битами не обнаружены.

Шаг 3
Установите SUID или SGID-биты в правах доступа к файлу `/home/worm`:

```
[root@drwalbr home]# chmod +s worm
[root@drwalbr home]# ls -l worm
-rwsr-sr-x    1 root     root            0 Апр 23 19:02 worm
```

Шаг 4
Снова запустите sXid:

```
[root@drwalbr home]# sxid –k

sXid Vers  : 4.0.2
Check run  : Wed Apr 23 19:09:44 2003
This host  : drwalbr.und
Spotcheck  : /home
Excluding  : /proc /mnt /cdrom /floppy
Ignore Dirs: /home
Forbidden  : /home /tmp
  (enforcing removal of s[ug]id bits in forbidden paths)


Checking for any additions or removals:
 + /home/worm                      *root.*root         6755


Checking for changed attributes or sums/inodes:


Checking for no user/group matches:


Checking for forbidden s[ug]id items:
home/worm                         *root.*root         755
```

sXid обнаружил файл `home/worm` с SUID или SGID-битами в правах доступа и удалил эти биты из прав доступа:

```
[root@drwalbr home]# ls -l worm
-rwxr-xr-x    1 root     root            0 Апр 23 19:02 worm
```

Глава 16

LogSentry – программное обеспечение для регистрации попыток несанкционированного доступа к системе

В этой главе:

Одной из важных задач в области обеспечения безопасности является регулярная проверка файлов регистрации. Частенько администраторы просто не успевают это сделать, что нередко приводит к довольно печальным последствиям.

Большинство хакеров не слишком отягощены каким-либо изыском или многообразием приемов, а зачастую просто используют перебор многочисленных попыток входа в систему. В этом случае программное обеспечение LogSentry может оказаться полезным для выявления таких попыток несанкционированного доступа к вашей системе, автоматизации аудита, обработки и регистрации информации обо всех неудачных попытках входа в систему, а также отправки соответствующих сообщений администратору системы. Этот пакет программ разработан для автоматического выполнения и проверки системных файлов регистрации на предмет обнаружения нарушений безопасности и необычного поведения системы. LogSentry запоминает последнюю просмотренную строку в файле регистрации и при следующем запуске начинает обрабатывать информацию со следующей за ней строки.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта LogSentry `http://www.psionic.com` в сентябре 2002 г. На момент написания этой главы – 24.04.2003 – с адреса `http://www.psionic.com` осуществляется переадресация на сервер компании Cisco System Inc.(`http://www.cisco.com`). По неофициальной и документально неподтвержденной информации, полученной авторами из различных списков рассылки, компания Psionic Software System приобретена Cisco System Inc. в конце 2002 г. Несмотря на это, разработчики проекта надеются в ближайшем будущем выложить исходные коды LogSentry для свободного использования в личных целях.

Исходные коды LogSentry содержатся в архиве `logsentry-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `logsentry-1.1.1.tar.gz`). Надеемся, что в ближайшее время вы сможете найти в Интернете исходные коды этой удобной и необходимой на каждой серверной системы программы. В противном случае никто не сможет запретить вам использовать исходные коды программы, распространяемые ранее компанией Psionic Software System. Вы также можете воспользоваться rpm-пакетом `logcheck-1.1.1-7.asp.i386.rpm`, входящим в комплект поставки дистрибутива ASPLinux 7.3 (Vostok).

Инсталляция с помощью rpm-пакета

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

> **ЗАМЕЧАНИЕ** Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет LogSentry с помощью следующей команды:

```
[root@www /]# rpm –iq logchec
```

Если вы следовали нашим рекомендациям, то пакет уже должен быть установлен.

Шаг 2

В случае его отсутствия перейдите в каталог, где находится пакет `logcheck-1.1.1-7.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@www /]# cd /home/distrib
```

и установите:

```
[root@www distrib]# rpm –ihv logcheck-1.1.1-7.asp.i386.rpm
```

или обновите пакет:

```
[root@www distrib]# rpm –Uhv logcheck-1.1.1-7.asp.i386.rpm
```

После установки пакета перейдите к настройке программы.

Компиляция, оптимизация и инсталляция LogSentry

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архив с исходными кодами в каталоге `/var/tmp`:

```
[root@www /]# cd /var/tmp/
[root@www tmp]# tar xzpf logsentry-1.1.1.tar.gz
```

Шаг 3

Измените заданное по умолчанию расположение конфигурационных файлов LogSentry. Для этого в файле `/var/tmp/logsentry/logcheck-1.1.1/system/linux/logcheck.sh` замените строку:

```
LOGTAIL=/usr/local/bin/logtail
```

на:

```
LOGTAIL=/usr/bin/logtail
```

Замените строку:

```
TMPDIR=/usr/local/etc/tmp
```

на:

```
TMPDIR=/var/logsentry
```

Замените строку:

```
HACKING_FILE=/usr/local/etc/logcheck.hacking
```

на:

```
HACKING_FILE=/etc/logsentry/hacking
```

Замените строку:

```
VIOLATIONS_FILE=/usr/local/etc/logcheck.violations
```

на:

```
VIOLATIONS_FILE=/etc/logsentry/violations
```

Замените строку:

```
VIOLATIONS_IGNORE_FILE=/usr/local/etc/logcheck.violations.ignore
```

на:

```
VIOLATIONS_IGNORE_FILE=/etc/logsentry/violations.ignore
```

Замените строку:

```
IGNORE_FILE=/usr/local/etc/logcheck.ignore
```

на:

```
IGNORE_FILE=/etc/logsentry/ignore
```

Шаг 4

Для установки флагов оптимизации и изменения заданного по умолчанию расположения исполняемых файлов LogSentry отредактируйте файл `/var/tmp/logsentry/logcheck-1.1.1/Makefile`.

Замените строку:

```
CFLAGS = -O
```

на:

```
-O2 -march=i686 -funroll-loops
```

Замените строку:

```
INSTALLDIR = /usr/local/etc
```

на:

```
INSTALLDIR = /etc/logsentry
```

Замените строку:
```
INSTALLDIR_BIN = /usr/local/bin
```
на:
```
INSTALLDIR_BIN = /usr/bin
```

Замените строку:
```
NSTALLDIR_SH = /usr/local/etc
```
на:
```
INSTALLDIR_SH = /usr/sbin
```

Замените строку:
```
TMPDIR = /usr/local/etc/tmp
```
на:
```
TMPDIR = /var/logsentry
```

Шаг 5

Откомпилируйте исходные коды, проинсталлируйте файлы LogSentry, создайте и сохраните список инсталлированных файлов:

```
[root@www tmp]# cd logcheck-1.1.1
[root@www logcheck-1.1.1]# find /* > /root/logsentry1
[root@www logcheck-1.1.1]# mkdir -m0700 /etc/logsentry
[root@www logcheck-1.1.1]# make linux
[root@www logcheck-1.1.1]# strip /usr/bin/logtail
[root@www logcheck-1.1.1]# cd /etc/logsentry
[root@www logsentry]# mv logcheck.hacking hacking
[root@www logsentry]# mv logcheck.violations violations
[root@www logsentry]# mv logcheck.violations.ignore violations.ignore
[root@www logsentry]# mv logcheck.ignore ignore
[root@www logsentry]# cd var/tmp/logcheck-1.1.1
[root@www logcheck-1.1.1]# find /* > /root/logsentry2
[root@www logcheck-1.1.1]# diff /root/logsentry1 /root/logtsentry2
>/root/logsentry.installed
[root@www logcheck-1.1.1]# mv /root/logsentry.installed
/very_reliable_place/logsentry.installed.YYYYMMDD
```

Шаг 6

Удалите архив и каталог с исходными кодами LogSentry:

```
[root@www logcheck-1.1.1]# cd /var/tmp/
[root@www tmp]# rm -rf logcheck-1.1.1/
[root@www tmp]# rm -f logsentry-1.1.1.tar.gz
```

Конфигурирование LogSentry

Конфигурирование LogSentry осуществляется с использованием следующих файлов:

- файла `/etc/logsentry/hacking`, содержащего перечень ключевых слов, соответствующих сообщениям о попытках неудачных регистраций в системе;
- файла `/etc/logsentry/violations`, содержащего перечень ключевых слов, соответствующих сообщениям о негативных событиях;
- файла `/etc/logsentry/ignore`, содержащего перечень ключевых слов, соответствующих сообщениям о негативных событиях, которые должны быть проигнорированы LogSentry.

ЗАМЕЧАНИЕ Более подробная информация о назначении каждого из конфигурационных файлов LogSentry содержится в файле `INSTALL`, находящимся в корневом каталоге исходных кодов LogSentry.

Большинство пользователей устраивают настройки по умолчанию, поэтому авторы не рекомендуют без необходимости изменять конфигурационные файлы LogSentry, находящиеся в каталоге `/etc/logsentry`. В приведенном примере конфигурирования LogSentry отсылает по электронной почте сообщения администратору системы только в случае, если произошли события, оставившие в файлах регистрации сообщения с ключевыми словами из перечня, указанного в конфигурационных файлах LogSentry.

Для ежедневного запуска LogSentry необходимо выполнить некоторые операции.

Шаг 1

Создайте в каталоге `/etc/cron.daily` файл `logsentry`, содержащий следующие строки:

```
cat <<EOF > /etc/cron.daily/logsentry
#!/bin/sh
/usr/bin/logcheck.sh
EOF
```

Шаг 2

Установите права доступа к файлу:

```
[root@www /]# chmod 510 /etc/cron.daily/logsentry
```

Тестирование LogSentry

Для тестирования работоспособности LogSentry выполните следующие операции.

Шаг 1

Внесите какие-нибудь уникальные ключевые слова (которые не могут появиться сами по себе в регистрационных файлах системы) в файл `/etc/logsentry/hacking` и `/etc/logsentry/violations`. Например, соответственно, WALBR и BAMBR.

Шаг 2

Добавьте в конец файла `/var/log/messagess` строки:

```
Apr 25 12:00:16 www -- root[1027]: ROOT LOGIN ON tty2 WALBR
Apr 25 12:00:30 www -- root[1027]: ROOT LOGIN ON tty2 BAMBR
```

Шаг 3

Проверьте через сутки почту администратора системы. Если в ней будет сообщение, сгенерированное `logcheck`, содержащее информацию о двух «страшных» событиях (записи о которых вы сами внесли в файл регистрации):

```
From root Fri Apr 25 12:08:04 2003
Date: Fri, 25 Apr 2003 12:08:04 +0400
From: root <root@www.dymatel.und>
To: root@www.dymatel.und
Subject: www.dymatel.und 04/25/03:12.08 system check


Security Violations
=-=-=-=-=-=-=-=-=-=-=
Apr 25 12:00:16 www -- root[1027]: ROOT LOGIN ON tty2 WALBR
Apr 25 12:00:30 www -- root[1027]: ROOT LOGIN ON tty2 BAMBR
Unusual System Events
=-=-=-=-=-=-=-=-=-=-=
Apr 25 12:00:16 www -- root[1027]: ROOT LOGIN ON tty2 WALBR
Apr 25 12:00:30 www -- root[1027]: ROOT LOGIN ON tty2 BAMBR
```

то LogSentry установлен, корректно настроен и надежно отслеживает нежелательные события в вашей системе.

Шаг 4

Подождите еще сутки и проверьте почту администратора системы. В ней не должно быть сообщения, сгенерированного `logcheck`, содержащего информацию о событиях, оставляющих в файлах регистрации строки, где есть ключевые слова WALBR и BAMBR (сами по себе записи, содержащие эти слова, вряд ли смогут появиться на вашей системе).

ЗАМЕЧАНИЕ Если вы не желаете проверять работоспособность и правильность настроек `logcheck` в течение двух дней, то запустите его вручную, используя команду:

```
[root@www /]# /usr/bin/logcheck.sh
```

Шаг 5

Удалите строки, содержащие ключевые слова WALBR и BAMBR, из файлов `/etc/logsentry/hacking` и `/etc/logsentry/violations`.

Глава 17

HostSentry – программное обеспечение для обнаружения необычной активности пользователей

В этой главе:

В системах, где пользователи имеют доступ к командному интерпретатору, важно отслеживать нестандартные попытки регистрации в системе (Login Anomaly Detection, LAD). Именно для этого предназначена программа HostSentry, которая позволяет администратору выявлять необычную активность пользователей, например, попытку одновременной регистрации пользователя `tetushka_luba`, допущенного к работе лишь на одной рабочей станции в локальной сети, на корпоративном сервере одновременно из Кореи и Польши в 3.00 первого января.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта `http://www.psionic.com` в сентябре 2002 г. На момент написания этой главы – 25.04.2003 – с адреса `http://www.psionic.com` осуществляется переадресация на сервер компании Cisco System Inc. (`http://www.cisco.com`). По неофициальной и документально неподтвержденной информации, полученной авторами из различных списков рассылки, компания Psionic Software System приобретена Cisco System Inc. в конце 2002 г. Несмотря на это, разработчики проекта надеются в ближайшем будущем выложить исходные коды HostSentry для свободного использования в личных целях.

Исходные коды HostSentry содержатся в архиве `hostsentry-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `hostsentry-0.02.tar.gz`). Надеемся, что ближайшее время вы сможете найти в Интернете исходные коды этой удобной и необходимой на каждой серверной системе программы. В противном случае никто не сможет запретить вам использовать исходные коды программы, свободно распространяемые ранее компанией Psionic Software System, для использования в личных целях. Вы также можете воспользоваться rpm-пакетом `hostsentry-0.02-4.noarch.rpm`.

ЗАМЕЧАНИЕ Авторы сожалеют, что лицензионное соглашение, по которому ранее распространялась программа HostSentry, не позволяет распространять ее без разрешения правообладателей.

Для нормальной инсталляции и работы программного обеспечения необходимо, чтобы в системе были установлены пакеты `db3-3.3.11-6.i386.rpm` и `python2-2.2-16.i386.rpm`, входящие в комплект поставки дистрибутива ASPLinux 7.3 (Vostok).

Компиляция, оптимизация и инсталляция HostSentry

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Установите rpm-пакеты `db3-3.3.11-6.i386.rpm` и `python2-2.2-16.i386.rpm`.

Если вы следовали нашим рекомендациям из главы 2, то первый пакет уже установлен. А для установки второго перейдите в каталог `/home/distrib` и выполните команду:

```
[root@www distrib]# rpm –ihv python2-2.2-16.i386.rpm
```

Шаг 3

Распакуйте архив с исходными кодами в каталоге `/var/tmp`:

```
[root@www /]# cd /var/tmp/
[root@www tmp]# tar xzpf hostsentry-0.02.tar.gz
```

Шаг 4

Измените заданное по умолчанию расположение файлов HostSentry.Для этого в файле `/var/tmp/hostsentry-0.02/Makefile` замените строку:

```
INSTALLDIR = /usr/local/abacus/hostsentry
```
на:
```
INSTALLDIR = /etc/hostsentry
LIBDIR = /usr/lib/hostsentry
```

Замените строки:
```
@echo "Installing hostsentryin:
$ (INSTALLDIR)"
install  -d-g 0-o root -m 0700 $(INSTALLDIR)
install  -d-g 0-o root -m 0700 $(INSTALLDIR)/modules
install  -g 0 -o root -m 0700 host* $(INSTALLDIR)
install  -g 0 -o root -m 0700 module* $(INSTALLDIR)/modules
```

на:
```
@echo "Installing HostSentry in:
$(INSTALLDIR)"
install -d -m 0700 $(INSTALLDIR)
install -d -m 0700 $(LIBDIR)/modules
install -m 0400 host* $(LIBDIR)
install -m 0400 module* $(LIBDIR)/modules
```

Шаг 5

В файле `/var/tmp/ hostsentry-0.02/hostSentryConfig.py` замените строку:
```
CONFIG= '/usr/local/abacus/hostsentry/hostsentry.conf'
```
на:
```
CONFIG= '/etc/hostsentry/hostsentry.conf'
```

Шаг 6

В файле `/var/tmp/ hostsentry-0.02/hostSentryStat.py` замените строку:
```
db = '/usr/iocal/abacus/hostsentry/hostsentry.db'
```
на:
```
db = '/var/host.sentry/hostsentry.db'
```

Шаг 7

В файле `/var/tmp/ hostsentry-0.02/moduleForeignDomain` замените строку:
```
ALLOW_FILE = '/moduleForeignDomain.allow'
```
на:
```
ALLOW_FILE = 'moduleForeignDomain.allow'
```

Замените строку:
```
allowPath = config.parseToken('MODULE_PATH')
```
на:
```
allowPath = ' /etc/hostsentry/ '
```

Шаг 8

В файле `/var/tmp/ hostsentry-0.02/MultipleLogins.py` замените строку:
```
ALLOW_FILE = '/moduleMultipleLogins.allow'
```
на:
```
ALLOW_FILE = 'moduleMultiplelogins.allow'
```

Строку:
```
allowPath = config.parseToken('MODULE_PATH')
```
на:
```
allowPath = '/etc/hostsentry/'
```

Шаг 9

В начало файла `hostsentry.py` добавьте строку:
```
#!/usr/bin/env python
```

Шаг 10

Откомпилируйте исходные коды, проинсталлируйте файлы HostSentry, создайте и сохраните список инсталлированных файлов:
```
[root@www tmp]# cd hostsentry-0.02/
```

```
[root@www hostsentry-0.02]# find /* > /root/hostsentry1
[root@www hostsentry-0.02]# make install
[root@www hostsentry-0.02]# mkdir -m0700 /var/hostsentry
[root@www hostsentry-0.02]# find /* > /root/hostsentry2
[root@www hostsentry-0.02]# diff /root/hostsentry1 /root/hostsentry2
>hostsentry.installed
[root@www hostsentry-0.02]# mv /root/hostsentry.installed
/very_reliable_place/hostsentry.installed.YYYYMMDD
```

Шаг 11

Удалите архив и исходные коды программы:

```
[root@www /]# cd /var/tmp/
[root@www tmp]# rm -rf hostsentry-0.02/
[root@www tmp]# rm -f hostsentry-0.02.tar.gz
```

Конфигурирование HostSentry

Конфигурирование HostSentry осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/hostsentry/hostsentry.conf`;
- файла `/etc/hostentry/hostsentry.ignore`, содержащего список игнорируемых пользователей;
- файла `/etc/hostentry/hostsentry.action`, неиспользуемого в версии 0.02;
- файла `/etc/hostentry/hostsentry.modules`, содержащего список модулей, выполняемых при входе и выходе пользователя из системы;
- файла `/etc/hostentry/moduleForeignDomain.allow`, содержащего список доменов, при удаленной регистрации с которых входы и выходы пользователей не регистрируются;
- файла `/etc/hostentry/moduleMultipleLogins.allow`, содержащего список хостов, при удаленной регистрации с которых пользователям разрешено одновременно несколько регистраций в системе;
- файла `/etc/init.d/hostsentry` для инициализации HostSentry.

Конфигурационный файл /etc/hostsentry/hostsentry.conf

Шаг 1

Создайте файл `/etc/hostsentry/hostsentry.conf`, содержащий следующие строки:

```
IGNORE_FILE = "/etc/hostsentry/hostsentry.ignore"
ACTION_FILE = "/etc/hostsentry/hostsentry.action"
MODULE_FILE = "/etc/hostsentry/hostsentry.modules"
MODULE_PATH = "/usr/iib/hostsentry/modules"
WTMP_FILE = "/var/log/wtmp"
DB_FILE = "/var/hostsentry/hostsentry.db"
DB_TTY_FILE = "/var/hostsentry/hostsentry.tty.db"
WTMP FORMAT = "384/8:32/44:32/76:256"
```

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www /]# chmod 600 /etc/hostsentry/hostsentry.conf
[root@www /]# chown 0.0 /etc/hostsentry/hostsentry.conf
```

Конфигурационный файл /etc/hostentry/hostsentry.ignore

Шаг 1

Создайте файл /`etc/hostentry/hostsentry.ignore`, содержащий список пользователей, вход и выход которых из системы не регистрируется HostSentry. Например, если программа установлена на FTP-сервере, в этот файл следует включить FTP-пользователей, которым разрешен анонимный доступ. Это позволит существенно снизить количество «ложных тревог». Имя каждого пользователя должно размещаться в отдельной строке. Для начала авторы рекомендуют в файл добавить только одну строку, содержащую комментарий, например:

```
# Place user-names in this file that you want to ignore (ftp, etc.)
```

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www /]# chmod 600 /etc/hostsentry/hostsentry.ignore
[root@www /]# chown 0.0 /etc/hostsentry/hostsentry.ignore
```

Конфигурационный файл /etc/hostentry/hostsentry.modules

Шаг 1

Создайте файл `/etc/hostentry/hostsentry.modules`, содержащий список модулей, выполняемых при входе и выходе пользователя из системы:

```
moduleLoginLogout
moduleFirstLogin
moduleForeignDomain
moduieMultipleLogins
moduleRhostsCheck
moduleHistoryTruncated
moduleOddDirnames
```

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www /]# chmod 600 /etc/hostsentry/hostsentry.modules
[root@www /]# chown 0.0 /etc/hostsentry/hostsentry.modules
```

Конфигурационный файл /etc/hostsentry/moduleForeignDomain.allow

Шаг 1

Создайте файл `/etc/hostsentry/moduleForeignDomain.allow`, содержащий список доменов, при удаленной регистрации с которых входы и выходы пользователей не регистрируются. Авторы рекомендуют добавить только свой собственный домен:

```
:0.)
```

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www /]# chmod 600 /etc/hostsentry/moduleForeignDomain.allow
[root@www /]# chown 0.0 /etc/ hostsentry/moduleForeignDomain.allow
```

Конфигурационный файл /etc/hostsentry/moduleMultipleLogins.allow

Создайте файл `/etc/hostsentry/moduleMultipleLogins.allow`, содержащий список хостов, при удаленной регистрации с которых пользователям разрешено одновременно несколько регистраций в системе, т. е. информация о возникновении таких событий игнорируется HostSentry. Авторы рекомендуют добавить в этот файл только `localhost`:

```
# Place hosts in here you want this module to disregard logins from.
localhost
```

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www /]# chmod 600 /etc/hostsentry/moduleMultipleLogins.allow
[root@www /]# chown 0.0 /etc/hostsentry/moduleMultipleLogins.allow
```

Файл инициализации /etc/init.d/hostsentry: hostsentry файл инициализации

Если вы хотите, что бы HostSentry автоматически запускался при загрузке системы, выполните следующие операции.

Шаг 1

Создайте файл `/etc/init.d/hostsentry`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping HostSentry.
#
# chkconfig: 345 98 85
```

```
# description: HostSentry is a host based intrusion detection tool that \
#              performs Login Anomaly Detection (LAD). This tool allows \
#              administrators to spot strange login behavior and quickly
\
#              respond to compromised accounts and unusual behavior.
#
# processname: hostsentry
# config: /etc/hostsentry/hostsentry.conf
# pidfile: /var/run/hostsentry.pid

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

RETVAL=0
prog="HostSentry"

start() {
        if [ -f /var/run/hostsentry.pid ] ; then
          pid=`cat /var/run/hostsentry.pid`
          if [ "$pid" != "" ] ; then
              echo $"HostSentry is already running"
              exit 0
          fi
        fi

        echo -n $"Starting $prog: "
        cd /usr/lib/hostsentry
        daemon python hostsentry.py
        RETVAL=$?
        echo
        echo `ps aux | grep "python hostsentry.py" | cut --delimiter=" "
-f 7` > /var/run/hostsentry.pid
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/hostsentry
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        cd /usr/lib/hostsentry
        killproc python hostsentry.py
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/hostsentry && rm -f
/var/run
/hostsentry.pid
        return $RETVAL
}

restart() {
        stop
        start
}

condrestart() {
        if [ -f /var/lock/subsys/hostsentry ]; then
          restart
        fi
}
```

```
# See how we were called.
case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        restart
        ;;
    condrestart)
        condrestart
        ;;
    *)
        echo $"Usage: $0 {start|stop|restart|condrestart}"
        exit 1
        ;;
esac
```

Шаг 2

Сделайте файл `/etc/init.d/hostsentry` исполняемым и определите его владельцем пользователя `root`:

```
[root@www /]# chmod 700 /etc/init.d/hostsentry
[root@www /]# chown 0.0 /etc/init.d/hostsentry
```

Шаг 3

Для создания необходимых символьных ссылок выполните команды:

```
[root@www /]# chkconfig --add hostsentry
[root@www /]# chkconfig --level 345 hostsentry on
```

Тестирование HostSentry

Шаг 1

Запустите HostSentry:

```
[root@www /]# /etc/init.d/hostsentry
```

Шаг 2

Зарегистрируйтесь в качестве обычного пользователя, имеющего учетную запись на данной системе. В рассматриваемом примере использовалась учетная запись `dymatel`.

В файле `/var/log/messages` должны появиться строки:

```
Apr 25 17:35:41 www hostSentry[4193]: securityalert: LOGIN User: dymatel
TTY: pts/1 Host: drwalbr.und
Apr 25 17:35:41 www hostSentry[4193]: securityalert: Foreign domain login
detected for user: dymatel from: drwalbr.und
Apr 25 17:35:41 www hostSentry[4193]: securityalert: Action being taken
for user: dymatel
Apr 25 17:35:41 www hostSentry[4193]: securityalert: Module requesting
action is: moduleForeignDomain
Apr 25 17:35:41 www hostSentry[4193]: securityalert: Action complete for
module: moduleForeignDomain
```

наличие которых указывает на нормальную работу HostSentry.

Шаг 3

Теперь попробуйте зарегистрироваться в системе в качестве несуществующего пользователя, например, `tetushka_luba`. В этом случае в файле `/var/log/messages` должны появиться строки:

```
Apr 28 09:43:15 www login(pam_unix)[1704]: check pass; user unknown
Apr 28 09:43:15 www login(pam_unix)[1704]: authentication failure; log-
name=LOGIN uid=0 euid=0 tty=tty2 ruser= rhost=
Apr 28 09:43:18 www login[1704]: FAILED LOGIN 1 FROM (null) FOR
tetushka_luba, Authentication failure
```

```
Apr 28 09:43:21 www hostSentry[1002]: securityalert: LOGOUT User: LOGIN
TTY: tty2 Host:
Apr 28 09:43:21 www hostSentry[1002]: adminalert: moduleRhostsCheck: log-
out: Cannot find user: LOGIN in passwd database: getpwnam(): name not
found
Apr 28 09:43:21 www hostSentry[1002]: adminalert: ERROR: Module file:
moduleRhostsCheck exec error: adminalert: moduleRhostsCheck: logout: Can-
not find user: LOGIN in passwd database: getpwnam(): name not found. Con-
tinuing with processing
Apr 28 09:43:21 www hostSentry[1002]: adminalert: moduleHistoryTruncated:
logout: Cannot find user: LOGIN in passwd database: getpwnam(): name not
found
Apr 28 09:43:21 www hostSentry[1002]: adminalert: ERROR: Module file:
moduleHistoryTruncated exec error: adminalert: moduleHistoryTruncated:
logout: Cannot find user: LOGIN in passwd database: getpwnam(): name not
found. Continuing with processing
Apr 28 09:43:21 www hostSentry[1002]: adminalert: moduleOddDirnames: log-
out: Cannot find user: LOGIN in passwd database: getpwnam(): name not
found
Apr 28 09:43:21 www hostSentry[1002]: adminalert: ERROR: Module file:
moduleOddDirnames exec error: adminalert: moduleOddDirnames: logout: Can-
not find user: LOGIN in passwd database: getpwnam(): name not found. Con-
tinuing with processing
Apr 28 09:43:22 www hostSentry[1002]: securityalert: Login TTY:  not
found in TTY state DB.
Apr 28 09:43:23 www hostSentry[1002]: securityalert: LOGIN User: LOGIN
TTY: tty2 Host:
Apr 28 09:43:23 www hostSentry[1002]: securityalert: Foreign domain login
detected for user: LOGIN from:
Apr 28 09:43:23 www hostSentry[1002]: securityalert: Action being taken
for user: LOGIN
Apr 28 09:43:23 www hostSentry[1002]: securityalert: Module requesting
action is: moduleForeignDomain
Apr 28 09:43:23 www hostSentry[1002]: securityalert: Action complete for
module: moduleForeignDomain
```

также указывающие на нормальную работу `HostSentry`.

Глава 18

PortSentry – программное обеспечение для автоматического ограничения доступа с систем, используемых для деструктивного воздействия

В этой главе:

Система сетевой защиты позволяет ограничить доступ от различного рода злоумышленников, оставляя открытыми только некоторые порты, необходимые для нормального функционирования используемых вами служб. Существуют программы, осуществляющие сканирование всех портов сервера и выявление открытых портов. Одной из таких программ является программа Network Mapper (Nmap), исходные коды которой, описания по инсталляции, настройке и использованию могут быть получены с домашней страницы проекта `http://www.insecure.org/nmap/`. Сканирование портов – если оно не осуществляется администратором системы для проверки правильности настроек – является признаком повышенного интереса к вашей системе. Программа PortSentry позволяет обнаруживать факт сканирования портов и реагировать на это событие в автоматическом режиме, делая соответствующие записи в файле регистрации и запуская различные приложения.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта `http://www.psionic.com` в сентябре 2002г. На момент написания этой главы – 25.04.2003 – с адреса `http://www.psionic.com` осуществляется переадресация на сервер компании Cisco System Inc. (`http://www.cisco.com`). По неофициальной и документально неподтвержденной информации, полученной авторами из различных списков рассылки, компания Psionic Software System приобретена Cisco System Inc. в конце 2002 г. Не смотря на это, разработчики проекта надеются в ближайшем будущем выложить исходные коды PortSentry для свободного использования в личных целях.

Исходные коды PortSentry содержатся в архиве `portsentry-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `portsentry-1.1.tar.gz`). Надеемся, что в ближайшее время вы сможете найти в Интернете исходные коды этой удобной и необходимой на каждой серверной системе программы. В противном случае, никто не сможет запретить вам использовать исходные коды программы, свободно распространяемые ранее компанией Psionic Software System, для использования в личных целях. Вы также можете воспользоваться rpm-пакетом `portsentry-1.1-2.asp.i386.rpm`, входящим в комплект поставки дистрибутива ASPLinux 7.3 (Vostok).

ЗАМЕЧАНИЕ Авторы сожалеют, что лицензионное соглашение, по которому ранее распространялась программа PortSentry, не позволяет распространять ее без разрешения правообладателей.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет PortSentry с помощью следующей команды:

```
[root@dymatel /]# rpm –iq portsentry
```

Шаг 2

В случае его отсутствия перейдите в каталог, где находится пакет `portsentry-1.1-2.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@www /]# cd /home/distrib
```

и установите:

```
[root@www distrib]# rpm –ihv portsentry-1.1-2.asp.i386.rpm
```

или обновите пакет:

```
[root@www distrib]# rpm –Uhv portsentry-1.1-2.asp.i386.rpm
```

После установки пакета перейдите к настройке программы.

Компиляция, оптимизация и инсталляция PortSentry

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архив с исходными кодами в каталоге `/var/tmp`:

```
[root@www /]# cd /var/tmp/
[root@www tmp]# tar xzpf portsentry-1.1.tar.gz
```

Шаг 3

Измените заданное по умолчанию расположение файлов PortSentry и подкорректируйте флаги компиляции применительно к вашей архитектуре процессора. Для этого в файле `/var/tmp/portsentry-1.1/Makefile` замените строку:

```
CFLAGS = -O -Wall
```

на

```
CFLAGS = -O2 -march=i686 -funroll-loops -Wall
```

Строки:

```
INSTALLDIR = /usr/local/psionic
CHILDDIR=/portsentry
```

на:

```
INSTALLDIR = /usr/sbin
CONFIGDIR=/etc/portsentry
```

Строку:

```
@if [ ! -d $(INSTALLDIR) ]; then /bin/mkdir $(INSTALLDIR); fi
```

на:

```
@if [ ! -d $(INSTALLDIR) ]; then /bin/mkdir -p $(INSTALLDIR); fi
```

Строки:

```
@if [ "$(INSTALLDIR)" = "/usr/local/psionic" ]; then /bin/chmod 700
$(INSTALLDIR) ; fi
@echo "Creating portsentry directory $(INSTALLDIR)$(CHILDDIR)"
@if [ ! -d $(INSTALLDIR)$(CHILDDIR) ]; then /bin/mkdir\
$(INSTALLDIR)$(CHILDDIR); fi
```

на:

```
@if [ "$(INSTALLDIR)" = "/usr/sbin" ]; then /bin/chmod 700 $(INSTALLDIR)
; fi
@echo "Creating portsentry directory $(CONFIGDIR)"
@if [ ! -d $(CONFIGDIR) ]; then /bin/mkdir -p \
$(CONFIGDIR); fi
```

Строку:

```
chmod 700 $(INSTALLDIR)$(CHILDDIR)
```

на:

```
chmod 700 $(CONFIGDIR)
```

Строки:

```
cp ./portsentry.conf $(INSTALLDIR)$(CHILDDIR)
cp ./portsentry.ignore $(INSTALLDIR)$(CHILDDIR)
cp ./portsentry $(INSTALLDIR)$(CHILDDIR)
```

на:

```
cp ./portsentry.conf $(CONFIGDIR)
cp ./portsentry.ignore $(CONFIGDIR)
cp ./portsentry $(INSTALLDIR)
```

Строки:

```
chmod 600 $(INSTALLDIR)$(CHILDDIR)/portsentry.ignore
chmod 600 $(INSTALLDIR)$(CHILDDIR)/portsentry.conf
chmod 700 $(INSTALLDIR)$(CHILDDIR)/portsentry
```

на:

```
chmod 600 $(CONFIGDIR)/portsentry.ignore
chmod 600 $(CONFIGDIR)/portsentry.conf
chmod 700 $(INSTALLDIR)/portsentry
```

Строку:

```
@echo "Edit $(INSTALLDIR)$(CHILDDIR)/portsentry.conf and change"
```

на:

```
@echo "Edit $(CONFIGDIR)/portsentry.conf
```

Строку:

```
@echo "and config files ($(INSTALLDIR)$(CHILDDIR))."
```

на:

```
@echo "and config files $(CONFIGDIR)."
```

Шаг 4

В файле `/var/tmp/portsentry-1.1/portsentry_config.h` замените следующую строку:

```
#define CONFIG_FILE "/usr/local/psionic/portsentry/portsentry.conf"
```

на:

```
#define CONFIG FILE "/etc/portsentry/portsentry.conf"
```

Шаг 5

Откомпилируйте исходные коды, проинсталлируйте файлы HostSentry, создайте и сохраните список инсталлированных файлов в надежном месте:

```
[root@www tmp]# cd portsentry-1.1
[root@www portsentry-1.1]# find /* > /root/portsentry1
[root@www portsentry-1.1]# make linux
[root@www portsentry-1.1]# make install
[root@www portsentry-1.1]# strip /usr/sbin/portsentry
[root@www portsentry-1.1]# mkdir -m0700 /var/portserntry
[root@www portsentry-1.1]# find /* > /root/portsentry2
[root@www portsentry-1.1]# diff /root/portsentry1 /root/portsentry2 >
/root/portsentry.installed
[root@www portsentry-1.1]# mv /root/ portsentry.installed
/very_reliable_place/portsentry.installed.YYYYMMDD
```

Шаг 6

Удалите архив и исходные коды программы:

```
[root@www portsentry-1.1]# cd /var/tmp
[root@www tmp]# rm -rf portsentry-1.1/
[root@www tmp]# rm -f portsentry-1.1.tar.gz
```

Конфигурирование PortSentry

Конфигурирование PortSentry осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/portsentry/portsentry.conf`;
- файла `/etc/portsentry/portsentry.ignore`, содержащего список систем, при сканировании портов с которых PortSentry не регистрирует факт сканирования и не предпринимает ответных мер;
- файла `/etc/portsentry/portsentry.modes`, предназначенного для выбора режима работы PortSentry;
- файла инициализации `/etc/init.d/portsentry`.

Конфигурационный файл /etc/portsentry/portsentry.conf

Шаг 1

Создайте (отредактируйте) файл `/etc/portsentry/portsentry.conf` в соответствии с приведенными ниже рекомендациями и вашими потребностями:

```
TCP_PORTS="1,11,81,82,83,1080,1720,1863,5190,8080"
UDP_PORTS="1,7,9,81,82,83,1080,1720,1863,5190,8080"
ADVANCED_PORTS_TCP="1024"
ADVANCED_PORTS_UDP="1024"
ADVANCED_EXCLUDE_TCP="113,139"
ADVANCED_EXCLUDE_UDP="520,138,137,67"
IGNORE_FILE="/etc/portsentry/portsentry.ignore"
HISTORY_FILE="/var/portsentry/portsentry.history"
BLOCKED_FILE="/var/portsentry/portsentry.blocked"
RESOLVE_HOST="0"
BLOCK_UDP="0"
BLOCK_TCP="1"
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
SCAN_TRIGGER="0"
PORT_BANNER="** UNAUTHORIZED ACCESS PROHIBITED **"
```

где строка:

```
TCP_PORTS="1,11,81,82,83,1080,1720,1863,5190,8080"
```

определяет TCP порты, которые должны прослушиваться PortSentry на предмет обнаружения сканирования вашей системы. Эта опция используется всеми режимами PortSentry, кроме режима Advanced Stealth Scan Detection, который полностью ее игнорирует, т. к. использует более гибкий и безопасный метод контроля портов. Именно этот режим используется в нашей конфигурации, поэтому не нужно определять эту опцию. Для других же режимов обнаружения сканирования определите в этой строке все TCP порты, которые, по вашему мнению, должны контролироваться PortSentry.

Строка:

```
UDP_PORTS="1,7,9,81,82,83,1080,1720,1863,5190,8080"
```

определяет UDP порты, которые должны прослушиваться PortSentry на предмет обнаружения сканирования вашей системы. Эта опция используется всеми режимами PortSentry, кроме режима Advanced Stealth Scan Detection, который полностью ее игнорирует, т. к. использует более гибкий и безопасный метод контроля портов. Именно этот режим используется в нашей конфигурации, поэтому не нужно определять эту опцию. Для других режимов обнаружения сканирования определите в этой строке все TCP порты, которые, по вашему мнению, должны контролироваться PortSentry.

Строка:

```
ADVANCED_PORTS_TCP="1024"
```

определяет максимальное значение номера TCP порта, до которого осуществляется контроль за сканированием. Все порты с меньшим значением номера контролируются на предмет сканирования. Предлагаемое значение по умолчанию – 1024 – соответствует диапазону зарезервированных портов.

Строка:

```
ADVANCED_PORTS_UDP = "1024"
```

определяет максимальное значение номера UDP порта, до которого осуществляется контроль за сканированием. Все порты с меньшим значением номера контролируются на предмет сканирования. Предлагаемое значение по умолчанию – 1024 – соответствует диапазону зарезервированных портов.

Строка:

```
ADVANCED_EXCLUDE_TCP="113,139"
```

определяет номера TCP портов из диапазона, определяемого опцией `ADVANCED_PORTS_TCP`, которые не должны контролироваться, например, порты, часто ошибочно используемые популярными удаленными клиентами.

Строка:

```
ADVANCED_EXCLUDE_UDP="520,138,137,67"
```

определяет номера UDP портов из диапазона, определяемого опцией `ADVANCED_PORTS_UDP`, которые не должны контролироваться, например, порты, часто ошибочно используемые популярными удаленными клиентами.

Строки:

```
IGNORE_FILE="/etc/portsentry/portsentry.ignore"
HISTORY_FILE="/var/portsentry/portsentry.history"
BLOCKED_FILE="/var/portsentry/portsentry.blocked"
```

определяют местоположение других конфигурационных файлов PortSentry.

Строка:

```
RESOLVE_HOST="0"
```

отключает использование DNS для повышения производительности. Если вы хотите получать информацию о системах, сканирующих ваши порты, не в виде IP-адресов, а в виде имен – измените значение опции `RESOLVE_HOST` с `"0"` на `"1"`. Однако это может негативно сказаться на производительности вашей системы.

Строка:

```
BLOCK_UDP="0"
```

отключает автоматические отклики системы на UDP-запросы, затрудняя реализацию атак типа отказа в обслуживании путем использования массовой отправки фальсифицированных пакетов. Регистрация запросов при этом не отключается.

Строка:

```
BLOCK_TCP="1"
```

разрешает автоматические отклики на TCP-запросы.

Строка:

```
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
```

предназначена для определения команды, ограничивающей доступ к вашей системе с IP-адреса, с которого осуществлялось сканирование портов. Для этого можно использовать IpTables или команду `route`. В рассматриваемом примере используется команда `route`, запрещающая доступ к системе с IP-адреса, передаваемого PortSentry в переменной `$TARGET$`.

ЗАМЕЧАНИЕ Авторы не рекомендуют использовать эту опцию для запуска (перед блокировкой доступа) программ, осуществляющих негативное воздействие на систему, с которой осуществляется сканирование, т. к. это противоречит известной пословице: «Не рой яму другому – сам в нее попадешь» и возможно ст. 272, 273 и 274 Уголовного кодекса РФ.

Строка:

```
SCAN_TRIGGER="0"
```

определяет максимальное количество попыток сканирования портов некоторого IP-адреса, после которого PortSentry начинает реагировать, т. е. выполнять команду, указанную в опции `KILL_ROUTE`.

Строка:

```
PORT_BANNER="** UNAUTHORIZED ACCESS PROHIBITED **"
```

определяет текстовое сообщение, которое будет появляться на удаленной системе при попытке соединения с системой, на которой запущен PortSentry.

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www tmp]# chmod 600 /etc/portsentry/portsentry.conf
[root@www tmp]# chown 0.0 /etc/portsentry/portsentry.conf
```

Конфигурационный файл /etc/portsentry/portsentry.ignore

В файл `/etc/portsentry/portsentry.ignore` следует добавить все системы, которые никогда не должны блокироваться PortSentry. К числу таких адресов, по крайней мере, относятся 127.0.0.1 и адреса сетевых интерфейсов вашего сервера.

Шаг 1

Например, для сервера `www.dymatel.und`, имеющего два сетевых интерфейса:

- `eth0` (172.16.181.100, 172.16.181.101) в сети 172.16.181.0/24;
- `eth1` (192.168.14.85) в сети 192.168.0.0/16

создайте файл `/etc/portsentry/portsentry.ignore`, содержащий следующие строки:

```
# Put hosts in here you never want blocked. This includes the IP ad-
dresses
# of all local interfaces on the protected host (i.e virtual host, mult-
home)
# Keep 127.0.0.1 and 0.0.0.0 to keep people from playing games.
#
# PortSentry can support full netmasks for networks as well. Format is:
#
# <IP Address>/<Netmask>
#
# Example:
#
# 192.168.2.0/24
```

```
# 192.168.0.0/16
# 192.168.2.1/32
# Etc.
#
# If you don't supply a netmask it is assumed to be 32 bits.
#
#

127.0.0.0/8
0.0.0.0
172.16.181.100
172.16.181.101
192.168.14.85
```

ЗАМЕЧАНИЕ В данном конфигурационном файле строка `0.0.0.0` запрещает PortSentry блокировать – в случае сканирования портов с фальсифицируемого IP-адреса `0.0.0.0` – доступ к вашей системе со всех возможных адресов.

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www tmp]# chmod 600 /etc/portsentry/portsentry.ignore
[root@www tmp]# chown 0.0 /etc/portsentry/portsentry.ignore
```

Конфигурационный файл /etc/portsentry/portsentry.modes

Файл служит для определения режима работы PortSentry. В версии `portsentry-1.1` доступны следующие шесть опций, предназначенных для задания режимов работы:

- `tcp` – основной режим обнаружения сканирования для протокола TCP;
- `udp` – основной режим обнаружения сканирования для протокола UDP;
- `stcp` – «незаметный» режим обнаружения сканирования для протокола TCP;
- `sudp` – «незаметный» режим обнаружения сканирования для протокола UDP;
- `atcp` – расширенный «незаметный» режим обнаружения сканирования для протокола TCP;
- `audp` – расширенный «незаметный» режим обнаружения сканирования для протокола UDP.

Одновременно для каждого протокола (TCP или UDP) может быть запущен только один режим. Например, совместно не смогут работать два режима для TCP протокола – `tcp` и `atcp`. Для полного использования своих возможностей программу PortSentry лучше запускать в режимах `atcp` и `audp`. Более подробную информацию о режимах обнаружения сканирования можно найти в файлах `readme.install` и `readme.stealth` в корневом каталоге исходных кодов PortSentry.

Для задания режима работы PortSentry выполните простые операции.

Шаг 1

Создайте файл `/etc/portsentry/portsentry.modes`, содержащий следующие строки:

```
# These are the available startup modes for PortSentry. Uncomment the
# modes you want PortSentry to run in. For information about each
# available mode, please see the PortSentry documentation.
#
# Normal TCP/UDP scanning:
#tcp
#udp
#
# Steal TCP/UDP scanning:
#stcp
#sudp
#
# Advanced Stealth TCP/UDP scanning:
atcp
audp
```

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@www tmp]# chmod 600 /etc/portsentry/portsentry.modes
[root@www tmp]# chown 0.0 /etc/portsentry/portsentry.modes
```

Файл инициализации /etc/init.d/portsentry

Для автоматического запуска PortSentry при загрузке системы выполните следующие операции.

Шаг 1

Создайте файл `/etc/init.d/portsentry`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping the Port Scan De-
tector.
#
# chkconfig: 345 98 05
# description: PortSentry Port Scan Detector is part of the Abacus Proj-
ect \
#              suite of tools. The Abacus Project is an initiative to re-
lease \
#              low-maintenance, generic, and reliable host based intru-
sion \
#              detection software to the Internet community.
#
# processname: portsentry
# config: /etc/portsentry/portsentry.conf
# pidfile: /var/run/portsentry.pid

# Source function library.
. /etc/rc.d/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

RETVAL=0
prog="PortSentry"

start() {
        SENTRYDIR=/etc/portsentry
        if [ -s $SENTRYDIR/portsentry.modes ] ; then
        modes=`cut -d "#" -f 1 $SENTRYDIR/portsentry.modes`
        else
        modes="tcp udp"
        fi

        for i in $modes ; do
        action "Starting $prog -$i: " /usr/sbin/portsentry -$i
        RETVAL=$?
        done

        echo
        [ $RETVAL = 0 ] && touch /var/lock/subsys/portsentry
        return $RETVAL
}

stop() {
        echo -n "Shutting down $prog: "
        killproc portsentry
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && rm -f /var/lock/subsys/portsentry
        return $RETVAL
}

# See how we were called.
case "$1" in
```

```
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart|reload)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        [ -f /var/lock/subsys/portsentry ] && restart || :
        ;;
  status)
        status portsentry
        ;;
  *)
    echo "Usage: portsentry
{start|stop|restart|reload|condrestart|status}"
    exit 1
esac
```

Шаг 2

Сделайте файл исполняемым и определите его владельцем пользователя `root`:

```
[root@www /]# chmod 700 /etc/irit.d/portsentry
[root@www /]# chown 0.0 /etc/irit.d/portsentry
```

Шаг 3

Создайте необходимые символьные ссылки:

```
[root@www /]# chkconfig --add portsentry
[root@www /]# chkconfig --level 345 portsentry on
```

Тестирование PortSentry

Для тестирования правильности установки настройки PortSentry необходимо выполнить следующие операции.

Шаг 1

Запустите PortSentry:

```
[root@www /]# /etc/init.d/portsentry start
Starting PortSentry                    [OK]
```

Шаг 2

Просканируйте порты системы, на которой установлен PortSentry, с помощью программы-сканера, например, Nmap:

```
[root@drwalbr /]# nmap -O www.dymatel.und

Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (0), OS
detection may be less accurate
Interesting ports on www.dymatel.und (172.16.181.100):
(The 1553 ports scanned but not shown below are in state:
closed)
Port       State       Service
22/tcp     open        ssh
80/tcp     open        http
443/tcp    open        https
Remote operating system guess: Linux Kernel 2.4.0 - 2.4.18
(X86)

Nmap run completed -- 1 IP address (1 host up) scanned in
8 seconds
```

В нашем случае сканируется сервер `www.dymatel.und` с рабочей станции `drwalbr.und`. При этом также определяется тип операционной системы (опция `-O`). Для большей наглядности сервер был запущен со стандартным ядром версии 2.4.18, входящий в комплект поставки дистрибутива ASPLinux 7.3. Система сетевой защиты была выключена.

Шаг 3

Просканируйте порты системы, на которой установлен PortSentry, повторно:

```
[root@drwalbr /]# nmap -O www.dymatel.und

Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking
our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in
30 seconds
```

Nmap сообщает, что сканируемый компьютер, скорее всего, неработоспособен и для надежности рекомендует просканировать его скрытно, т. е. с использованием опции `-P0`. При этом сервер доступен с других систем, просто PortSentry обнаружил сканирование портов `drwalbr.und` и выполнил команду, определенную в конфигурационном файле `/etc/portsentry/portsentry.conf` в строке:

```
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
```

Шаг 4

Просканируйте порты системы, на которой установлен PortSentry в третий раз с использованием опции `-P0`:

```
[root@drwalbr /]# nmap -O -P0 www.dymatel.und

Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Warning:  OS detection will be MUCH less reliable because
we did not find at least 1 open and 1 closed TCP port
All 1556 scanned ports on www.dymatel.und (172.16.181.100)
are: filtered
Too many fingerprints match this host for me to give an
accurate OS guess

Nmap run completed -- 1 IP address (1 host up) scanned in
1946 seconds
```

Nmap выдает сообщение о том, что все порты на сканируемом сервере закрыты. Тем не менее, с других систем сервер `www.dymatel.und` доступен.

Шаг 5

Для определения компьютеров, доступ с которых к серверу с установленной программой PortSentry закрыт, с консоли сервера выполните команду:

```
[root@www /]# /sbin/route
…
drwalbr.und  -            255.255.255.255 !H 0 - 0 -
172.16.181.0 *            255.255.255.0    U 0 0 0 eth0
192.168.0.0  *            255.255.0.0      U 0 0 0 eth1
127.0.0.0    *            255.0.0.0        U 0 0 0 lo
default      172.16.181.1 0.0.0.0         UG 0 0 0 eth0
```

Шаг 6

Для снятия блокировки доступа с `drwalbr.und` выполните команду:

```
[root@www /]# route del -host drwalbr.und reject
```

и удалите строки, содержащие сведения о блокировке доступа с `drwalbr.und`.

Из файла `/var/portsentry/portsentry.history` – строку:

```
1051283728 - 04/25/2003 19:15:28 Host: 172.16.181.103/172.16.181.103
Port: 410 TCP Blocked
```

и строку:

```
1051283729 - 04/25/2003 19:15:29 Host: 172.16.181.103/172.16.181.103
Port: 1 UDP Blocked
```

Из файла `/var/portsentry/portsentry.blocked.atcp` – строку:

```
1051283728 - 04/25/2003 19:15:28 Host: 172.16.181.103/172.16.181.103
Port: 410 TCP Blocked
```

Из файла `/var/portsentry/portsentry.blocked.audp` – строку:

```
1051283729 - 04/25/2003 19:15:29 Host: 172.16.181.103/172.16.181.103
Port: 1 UDP Blocked
```

Удаление этих строк необходимо для возможности осуществления повторной блокировки доступа с `drwalbr.und`, т. к. перед выполнением блокировки PortSentry осуществляет проверку наличия блокировки, руководствуясь содержимым файлов `portsentry.history`, `portsentry.blocked.atcp` и `portsentry.blocked.audp`.

Для проверки восстановления доступа с `drwalbr.und` повторно выполните команду:

```
[root@www /]# /sbin/route
…
172.16.181.0 *            255.255.255.0    U 0 0 0 eth0
192.168.0.0  *            255.255.0.0      U 0 0 0 eth1
127.0.0.0    *            255.0.0.0        U 0 0 0 lo
default      172.16.181.1 0.0.0.0         UG 0 0 0 eth0
```

В выводе команды должна отсутствовать строка, содержащая запись для блокировки доступа с системы `drwalbr.und`, т. е.:

```
drwalbr.und  -            255.255.255.255 !H 0 - 0 -
```

Глава 19

Snort – программное обеспечение для обнаружения попыток вторжения

В этой главе:

1. Ограничения и допущения
2. Пакеты
3. Компиляция, оптимизация и инсталляция Snort
4. Конфигурирование Snort
5. Тестирование Snort
6. Выполнение Snort в среде chroot-jail

Как бы хорошо ни была защищена система, всегда существует возможность ее взлома. И для системного администратора было бы лучше узнавать о попытках взлома еще до того, как одна из них увенчается успехом. Поэтому особенно важны средства, позволяющие не только обнаружить факт проникновения в систему, но и предупредить о предстоящем вторжении.

Snort – это сетевая система обнаружения вторжений (Intrusion Detection Systems, IDS), способная выполнять в режиме реального времени анализ сетевого трафика с целью обнаружения попыток взлома или поиска уязвимостей вашей системы (например, таких, как переполнения буфера, CGI-атак, сканирования портов, определения типа операционной системы, идентификации версий используемых сетевых сервисов и т. п.).

Авторы настоятельно рекомендуют установить Snort и использовать его в качестве оружия в борьбе против спамеров, различных взломщиков программной защиты и других покушений на вашу безопасность.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью root.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта Snort по состоянию на 20.04.2003. Регулярно посещайте домашнюю страницу проекта `http://www.snort.org/` и отслеживайте обновления. Исходные коды Snort содержатся в архиве `snort-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `snort-1.9.1.tar.gz`).

Для нормальной работы Snort необходимо программное обеспечение, разрабатываемое в рамках проекта tcpdump/libcap. Регулярно посещайте домашнюю страницу проекта `http://www.tcpdump.org/` и отслеживайте обновления.

Snort использует функции библиотеки LIBCAP. Исходные коды библиотеки содержатся в архиве `libpcap-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `libpcap-0.7.2.tar.gz`);

Для реализации некоторых дополнительных настроек Snort необходима программа TCPDUMP, позволяющая переводить сетевую плату в режим promiscuous. В этом режиме фиксируется каждый пакет, проходящий по кабелю, к которому подключен сетевой интерфейс. В обычном режиме сетевые платы регистрируют только пакеты, адресованные на поддерживаемый ею адрес и широковещательные адреса. Исходные коды программы содержатся в архиве `tcpdump-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `tcpdump-3.7.2.tar.gz`).

Компиляция, оптимизация и инсталляция Snort

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 раздела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архив с исходными кодами `libpcap-0.7.2.tar.gz` в каталоге `/var/tmp`, откомпилируйте и проинсталлируйте библиотеку:

```
[root@drwalbr tmp]# tar xzpf libpcap-0.7.2.tar.gz
[root@drwalbr tmp]# cd libpcap-0.7.2
[root@drwalbr libpcap-0.7.2]# ./configure
[root@drwalbr libpcap-0.7.2]# make
[root@drwalbr libpcap-0.7.2]# find /* > /root/libcap1
[root@drwalbr libpcap-0.7.2]# make install
[root@drwalbr libpcap-0.7.2]# find /* > /root/libcap2
[root@drwalbr libpcap-0.7.2]# diff /root/libcap1 /root/libcap2 >
/root/libcap.installed
[root@drwalbr libpcap-0.7.2]# mv /root/libcap.installed
/very_reliable_place/libcap.installed.YYYYMMDD
```

ЗАМЕЧАНИЕ Вы можете установить библиотеку из rpm-пакета `libcap-1.10-8.i386.rpm`, для этого перейдите в каталог, в котором находятся пакеты, входящие в состав дистрибутива ASPLinux 7.3, и выполните команду:

```
[root@drwalbr distrib]# rpm –ihv libcap-1.10-8.i386.rpm
```

Шаг 3

Распакуйте архив с исходными кодами **tcpdump-3.7.2.tar.gz** в каталоге `/var/tmp`, откомпилируйте и проинсталлируйте программу:

```
[root@drwalbr tmp]# tar xzpf tcpdump-3.7.2.tar.gz
[root@drwalbr tmp]# cd tcpdump-3.7.2
[root@drwalbr tcpdump-3.7.2]# ./configure
[root@drwalbr tcpdump-3.7.2]# make
[root@drwalbr tcpdump-3.7.2]# find /* > /root/tcpdump1
[root@drwalbr tcpdump-3.7.2]# make install
[root@drwalbr tcpdump-3.7.2]# find /* > /root/tcpdump1
[root@drwalbr tcpdump-3.7.2]# diff /root/tcpdump1 /root/ tcpdump2 >
/root/tcpdump.installed
[root@drwalbr tcpdump-3.7.2]# mv /root/libcap.installed
/very_reliable_place/libcap.installed.YYYYMMDD
```

ЗАМЕЧАНИЕ Вы можете установить программу из rpm-пакета `tcpdump-3.6.2-12.asp.i386.rpm`, для этого перейдите в каталог в котором находятся пакеты, входящие в состав дистрибутива ASPLinux 7.3, и выполните команду:

```
[root@drwalbr distrib]# rpm –ihv tcpdump-3.6.2-12.asp.i386.rpm
```

Шаг 4

Распакуйте архивы с исходными кодами Snort в каталоге `/var/tmp`:

```
[root@drwalbr tmp]# tar xzpf snort-1.9.1.tar.gz
[root@drwalbr tmp]# cd snort-1.9.1
```

Шаг 5

Создайте специального пользователя, от имени которого будет запускаться Snort:

```
[root@drwalbr snort-1.9.1]# groupadd -g 69 snort > /dev/null 2>&l || :
[root@drwalbr snort-1.9.1]# useradd -u 69 -g 69 -s /bin/false -M -r -d
/var/log/snort snort > /dev/null 2>&l || :
```

Шаг 6

Проверьте наличие, а при необходимости добавьте в конец файла `/etc/shells` строку:

```
/bin/false/
```

Шаг 7

Отконфигурируйте исходные коды Snort:

```
[root@drwalbr snort-1.9.1]# CFLAGS="-O2 -march=i686 -funroll-loops"; ex-
port CFLAGS
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--localstatedir=/var \
--mandir=/usr/share/man \
--with-openssl
```

Шаг 8

Откомпилируйте и проинсталлируйте Snort, создайте список проинсталлированных файлов и сохраните его в надежном месте:

```
[root@drwalbr snort-1.9.1]# make
[root@drwalbr snort-1.9.1]# find /* > /root/snort1
[root@drwalbr snort-1.9.1]# make install
[root@drwalbr snort-1.9.1]# mkdir -p /var/log/snort
[root@drwalbr snort-1.9.1]# mkdir -p /etc/snort
[root@drwalbr snort-1.9.1]# chown -R snort.snort /var/log/snort/
[root@drwalbr snort-1.9.1]# cd etc/
[root@drwalbr etc]# install classification.config /etc/snort/
[root@drwalbr etc]# cd ../rules
```

```
[root@drwalbr rules]# install snort.conf *.rules /etc/snort/
[root@drwalbr rules]# chmod 0644 /etc/snort/*
[root@drwalbr rules]# strip /usr/bin/snort
[root@drwalbr rules]# cd /var/tmp/snort-1.9.1
[root@drwalbr rules]# find /* > /root/snort2
[root@drwalbr rules]# diff /root/snort1 /root/snort2 >
/root/snort.installed
[root@drwalbr rules]# mv /root/snort.installed
/very_reliable_place/snort.installed.YYYYMMDD
```

Шаг 9

Удалите архивы и каталоги с исходными кодами программ:

```
[root@drwalbr snort-1.9.1]# cd /var/tmp
[root@drwalbr tmp]# rm –r snort-1.9.1.tar.gz tcpdump-3.7.2.tar.gz
libpcap-0.7.2.tar.gz
[root@drwalbr tmp]# rm –rf snort-1.9.1 tcpdump libpcap-0.7.2
```

Конфигурирование Snort

Конфигурирование Snort осуществляется с использованием следующих файлов:

- основного конфигурационного файла `/etc/snort/snort.conf`;
- файла инициализации `/etc/init.d/snort`.

Шаг 1

Отредактируйте в соответствии с приведенными ниже рекомендациями и вашими потребностями файл `/etc/snort/snort.conf`:

```
var HOME_NET $eth0_ADDRESS
var EXTERNAL_NET any
var SMTP $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET
var DNS_SERVERS $HOME_NET
var RULE_PATH ./
preprocessor frag2
preprocessor stream4: detect_scans,detect_state_problems
preprocessor stream4_reassemble: both,ports all
preprocessor http_decode: 80
preprocessor rpc_decode: 111 32771
preprocessor bo
preprocessor telnet_decode
preprocessor portscan: $HOME_NET 4 3 portscan.log
preprocessor portscan-ignorehosts: 212.45.28.122 212.45.28.123
output alert_syslog: LOG_AUTH LOG_ALERT
include classification.config
```

где строка:

```
var HOME_NET $eth0_ADDRESS
```

определяет прослушиваемый сетевой интерфейс.

Строка:

```
var EXTERNAL_NET any
```

определяет отслеживаемые IP-адреса. В рассматриваемом примере отслеживаются все адреса.

Строка:

```
var SMTP  $HOME_NET
```

предписывает отслеживать атаки на службы SMTP на системах вашей сети.

Строка:

```
var HTTP_SERVERS $HOME_NET
```

предписывает отслеживать атаки на службы HTTP на системах вашей сети.

Строка:

```
var SQL_SERVERS $HOME_NET
```

предписывает отслеживать атаки на службы SQL на системах вашей сети.

Строка:

```
var DNS_SERVERS $HOME_NET
```

предписывает отслеживать атаки на службы DNS на системах вашей сети.

Строка:

```
var RULE_PATH ./
```

определяет путь к файлам, содержащим правила Snort.

Строка:

```
preprocessor frag2
```

предписывает обнаруживать дефрагментацию IP-пакетов и основанных на ней атаках.

Строка:

```
preprocessor stream4: detect_scans,detect_state_problems
```

предписывает осуществлять детальный анализ TCP и регистрировать на его основе попытки сканирования портов, определения типа операционной системы и др. Для конфигурирования используются следующие опции:

- `detect_scans` – используется для обнаружения незаметных сканирований портов и выдачи предупреждений;
- `detect_state_problems` – используется для обнаружения сбоев в работе TCP;
- `keepstats` – используется для сохранения статистики сеанса;
- `noinspect` – используется только для выключения режима детального анализа трафика TCP;
- `timeout` – используется для установки или изменения заданного по умолчанию счетчика времени блокировки сеанса;
- `memcap` – используется для ограничения объема памяти;
- `log_flushed_streams` – используется для записи всей информации, накопленной в буфере, на диск.

В рассматриваемом примере используются только опции `detect_scans` и `detect_state_problems`, позволяющие регистрировать сканирование портов и сбои TCP.

Строка:

```
preprocessor stream4_reassemble: both, ports all
```

предписывает использовать дополнительные возможности детального анализа трафика TCP. Для конфигурирования дополнительных возможностей используются следующие опции:

- `clientonly` – используется для детального анализа трафика только со стороны клиента;
- `serveronly` – используется для детального анализа трафика только со стороны сервера;
- `both` – используется для детального анализа трафика, как со стороны клиента, так и сервера;
- `noalerts` м используется для выключения всех предупреждений во время анализа трафика;
- `ports` – используется для задания отслеживаемых номеров портов.

В рассматриваемом примере используются только опции `detect_scans` и `detect_state_problems`, позволяющие осуществлять детальный анализ трафика как со стороны клиента, так и сервера для всех номеров портов.

Строка:

```
preprocessor http_decode: 80
```

предписывает отслеживать деструктивные воздействия на вашу систему по протоколу HTTP.

Строка:

```
preprocessor rpc_decode: 111 32771
```

предписывает отслеживать деструктивные воздействия на вашу систему по протоколу RPC. В рассматриваемом примере в качестве опций используются номера портов, задаваемые по умолчанию.

Строка:

```
preprocessor bo
```

предписывает отслеживать трафик Back Orifice.

Строка:

```
preprocessor telnet_decode
```

предписывает отслеживать деструктивные воздействия на вашу систему по протоколу TELNET и FTP.

Строка:

```
preprocessor portscan: $HOME_NET 4 3 portscan.log
```

предписывает обнаруживать и регистрировать сканирование портов с использованием UDP или TCP-пакетов с SYN-битом. В рассматриваемом примере регистрируются пакеты, обращающиеся к четырем различным портам за время меньшее, чем три секунды.

Строка:

```
preprocessor portscan-ignorehosts: 212.45.28.122 212.45.28.123
```

предписывает не анализировать и не регистрировать трафик с IP-адресов 212.45.28.122 и 212.45.28.123.

Строка:

```
output alert_syslog: LOG_AUTH LOG_ALERT
```

предписывает регистрировать все обращения Snort с помощью `syslogd`.

Строка:

```
include classification.config
```

предписывает подключить файл `classification.config`.

Шаг 2

Для запуска и остановки Snort создайте файл `/etc/init.d/snort`, содержащий следующие строки:

```
#!/bin/bash
# This shell script takes care of starting and stopping the snort IDS
daemon.
#
# chkconfig: 2345 40 60
# description:  Snort is a lightweight network intrusion detection tool
that \
#               currently detects more than 1100 host and network \
#               vulnerabilities, portscans, backdoors, and more.

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# Specify your network interface here
INTERFACE=eth0

RETVAL=0
prog="Snort"

start() {
        echo -n $"Starting $prog: "
        daemon /usr/bin/snort -A fast -u snort -g snort -b -s -z -d -D \
                -i $INTERFACE -c /etc/snort/snort.conf
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && touch /var/lock/subsys/snort
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc snort
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && rm -f /var/lock/subsys/snort
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status snort
        ;;
  restart)
        stop
        start
        ;;
```

```
  condrestart)
        [ -f /var/lock/subsys/snort ] && restart
        ;;
  *)
        echo $"Usage: $prog {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 3

Установите права доступа к файлу, назначьте его владельцем пользователя `root` и создайте соответствующие ссылки:

```
[root@drwalbr /]# chmod 700 /etc/init.d/snort
[root@drwalbr /]# chown 0.0 /etc/init.d/snort
```

Если вы хотите, чтобы Snort автоматически запускался при загрузке системы, создайте соответствующие ссылки:

```
[root@drwalbr /]# chkconfig --add sshd
[root@drwalbr /]# chkconfig --level 2345 sshd on
```

Тестирование Snort

Шаг 1

Запустите Snort:

```
[root@drwalbr snort]# /etc/init.d/snort start
Запускается Snort: eth0: Promiscuous mode enabled.
                                                    [OK]
```

Шаг 2

Просканируйте какую-нибудь систему в локальной сети с помощью сканера портов, например, Nmap (`http://www.insecure.org/`) в режиме определения типа операционной системы:

```
[root@drwalbr snort]# nmap -O 192.168.10.5
eth0: Promiscuous mode enabled.
…
eth0: Promiscuous mode enabled.
Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on  (192.168.10.5):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     filtered    ssh
25/tcp     filtered    smtp
80/tcp     open        http
110/tcp    filtered    pop-3
3000/tcp   open        ppp
3306/tcp   filtered    mysql
6667/tcp   open        irc
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=2.54BETA34%P=i386-asplinux-linux-
gnu%D=4/10%Time=3E953AC4%O=21%C=1)
T1(Resp=Y%DF=N%W=E000%ACK=S++%Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
```

```
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=0%ULEN=134%DAT=
E)

Nmap run completed -- 1 IP address (1 host up) scanned in 52 seconds
```

ЗАМЕЧАНИЕ Нужно осуществлять сканирование систем, не указанных в строке: `preprocessor portscan-ignorehosts: 212.45.28.122 212.45.28.123` файла `/etc/snort/snort.conf`.

Шаг 3

В файле `/var/log/snort/portscan.log`:

```
Apr 10 13:32:33 192.168.2.99:39192 -> 192.168.10.5:21 SYN ******S*
Apr 10 13:32:35 192.168.2.99:39197 -> 192.168.10.5:21 SYN ******S*
Apr 10 13:34:28 192.168.2.99:37780 -> 192.168.10.5:2035 SYN ******S*
Apr 10 13:34:28 192.168.2.99:38239 -> 192.168.10.5:657 SYN ******S*
Apr 10 13:34:28 192.168.2.99:51081 -> 192.168.10.5:329 SYN ******S*
Apr 10 13:34:28 192.168.2.99:52548 -> 192.168.10.5:1516 SYN ******S*
Apr 10 13:34:28 192.168.2.99:59773 -> 192.168.10.5:1472 SYN ******S*
Apr 10 13:34:28 192.168.2.99:40720 -> 192.168.10.5:314 SYN ******S*
Apr 10 13:34:28 192.168.2.99:38440 -> 192.168.10.5:388 SYN ******S*
Apr 10 13:34:28 192.168.2.99:54059 -> 192.168.10.5:586 SYN ******S*
Apr 10 13:34:28 192.168.2.99:54856 -> 192.168.10.5:613 SYN ******S*
…
Apr 10 13:34:38 192.168.2.99:35300 -> 192.168.10.5:21 SYN *2****S*
Apr 10 13:34:40 192.168.2.99:35301 -> 192.168.10.5:21 NULL ********
Apr 10 13:34:38 192.168.2.99:35302 -> 192.168.10.5:21 NMAPID **U*P*SF
Apr 10 13:34:38 192.168.2.99:35304 -> 192.168.10.5:1 SYN ******S*
Apr 10 13:34:38 192.168.2.99:35306 -> 192.168.10.5:1 XMAS **U*P**F
Apr 10 13:34:40 192.168.2.99:35302 -> 192.168.10.5:21 NMAPID **U*P*SF
Apr 10 13:34:44 192.168.2.99:35299 -> 192.168.10.5:21 SYN ******S*
Apr 10 13:34:46 192.168.2.99:35300 -> 192.168.10.5:21 SYN *2****S*
Apr 10 13:34:48 192.168.2.99:35301 -> 192.168.10.5:21 NULL ********
Apr 10 13:34:46 192.168.2.99:35302 -> 192.168.10.5:21 NMAPID **U*P*SF
Apr 10 13:34:46 192.168.2.99:35304 -> 192.168.10.5:1 SYN ******S*
Apr 10 13:34:46 192.168.2.99:35306 -> 192.168.10.5:1 XMAS **U*P**F
Apr 10 13:34:48 192.168.2.99:35302 -> 192.168.10.5:21 NMAPID **U*P*SF
Apr 10 13:34:52 192.168.2.99:35297 -> 192.168.10.5:21 SYN ******S*
Apr 10 13:34:55 192.168.2.99:35300 -> 192.168.10.5:21 SYN ******S*
Apr 10 13:34:56 192.168.2.99:35301 -> 192.168.10.5:21 NULL ********
Apr 10 13:34:55 192.168.2.99:35302 -> 192.168.10.5:21 NMAPID **U*P*SF
Apr 10 13:34:55 192.168.2.99:35304 -> 192.168.10.5:1 SYN ******S*
Apr 10 13:34:55 192.168.2.99:35306 -> 192.168.10.5:1 XMAS **U*P**F
Apr 10 13:34:56 192.168.2.99:35302 -> 192.168.10.5:21 NMAPID **U*P*SF
Apr 10 13:35:00 192.168.2.99:35298 -> 192.168.10.5:21 SYN ******S*
```

вы увидите информацию о пакетах, с помощью которых Nmap пытался обнаружить открытые порты и тип операционной системы на сервере `192.168.10.5`.

Выполнение Snort в среде chroot-jail

Потенциальные уязвимости Snort, как и любого другого программного обеспечения, могут использоваться для реализации атак на вашу систему. Поэтому для повышения безопасности системы рекомендуется выполнять Snort в окружении chroot-jail. Для этого необходимо выполнить следующие операции.

Шаг 1

Создайте каталоги для размещения Snort в окружении chroot-jail, назначьте владельцем второго из них пользователя `snort`:

```
[root@drwalbr /]# mkdir -p /chroot/snort/etc/snort
[root@drwalbr /]# mkdir -p /chroot/snort/var/log/snort
[root@drwalbr /]# chown -R snort.snort /chroot/snort/var/log/snort
```

ЗАМЕЧАНИЕ Для повышения безопасности вашей системы каталог `/chroot/snort/` рекомендуется размещать на отдельном разделе диска.

Шаг 2

Переместите конфигурационные файлы Snort в соответствующие подкаталоги окружения chroot-jail:

```
[root@drwalbr /]# mv /etc/snort/* /chroot/snort/etc/snort
[root@drwalbr /]# chmod 0644 /chroot/snort/etc/snort/*
```

Шаг 3

Для запуска и остановки Snort в окружении chroot-jail создайте файл `/etc/init.d/snort`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping the snort IDS
daemon.
#
# chkconfig: 2345 40 60
# description:  Snort is a lightweight network intrusion detection tool
that \
#               currently detects more than 1100 host and network \
#               vulnerabilities, portscans, backdoors, and more.

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# Specify your network interface here
INTERFACE=eth0

RETVAL=0
prog="Snort"

start() {
        echo -n $"Starting $prog: "
        daemon /usr/bin/snort -A fast -u snort -g snort -b -s -z -d -D \
                -i $INTERFACE -c /etc/snort/snort.conf -t /chroot/snort/
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && touch /var/lock/subsys/snort
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc snort
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && rm -f /var/lock/subsys/snort
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
```

```
        ;;
  status)
        status snort
        ;;
  restart)
        stop
        start
        ;;
  condrestart)
        [ -f /var/lock/subsys/snort ] && restart
        ;;
  *)
        echo $"Usage: $prog {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

и установите права доступа к файлу:

```
[root@drwalbr /]# chmod 700 /etc/init.d/snort
```

Шаг 4

Запустите Snort:

```
[root@drwalbr /]# /etc/init.d/snort start
Запускается Snort: eth0: Promiscuous mode enabled.
                                                    [OK]
```

Шаг 5

Проверьте, запущен ли Snort, и определите соответствующий номер процесса:

```
[root@drwalbr /]# ps -ax | grep snort
6171 ?    R    0:02 /usr/bin/snort -A fast -u snort -g snort -b -s -z -d
```

Шаг 6

Проверьте, запущен ли Snort в окружении chroot-jail:

```
[root@drwalbr /]# ls -la /proc/6171/root/
```

Если вы получите вывод вида (отображающий ссылку на корневой каталог среды chroot-jail):

```
lrwxrwxrwx    1 root     root            0 Апр 23 21:01 /proc/6171/root -
> /chroot/snort
```

то Snort корректно работает в окружении chroot-jail.

Если вы получите вывод вида (отображающий корневой каталог системы, на которой он установлен):

```
итого 124
drwxr-xr-x   19 root     root         1024 Апр 23 20:01 .
drwxr-xr-x   19 root     root         1024 Апр 23 20:01 ..
-rw-r--r--    1 root     root            0 Апр 23 20:01 .autofsck
drwxr-xr-x    2 root     root         2048 Апр 22 12:13 bin
drwxr-xr-x    5 root     root         1024 Апр  5 17:31 boot
drwxr-xr-x    5 root     root         1024 Апр 15 18:57 chroot
drwxr-xr-x   19 root     root        82944 Апр 23 20:01 dev
drwxr-xr-x   28 root     root         3072 Апр 23 20:01 etc
drwxr-xr-x   37 root     root         4096 Апр 23 19:02 home
drwxr-xr-x    2 root     root         1024 Июн 21  2001 initrd
drwxr-xr-x    7 root     root         3072 Апр  5 14:16 lib
drwx------    2 root     root        12288 Апр  5 03:10 lost+found
drwxr-xr-x    5 root     root         1024 Апр  4 23:20 mnt
drwxr-xr-x    2 root     root         1024 Авг 23  1999 opt
dr-xr-xr-x   45 root     root            0 Апр 24  2003 proc
drwxr-x---    5 root     root         1024 Апр 22 12:05 root
drwxr-xr-x    2 root     root         3072 Апр  4 23:23 sbin
drwxrwxrwt    4 root     root         2048 Апр 23 20:01 tmp
drwxr-xr-x   15 root     root         4096 Апр  7 21:30 usr
drwxr-xr-x   16 root     root         1024 Апр 16 20:29 var
```

то Snort работает в обычной среде и, в принципе, может быть использован для реализации атаки на систему вцелом.

Глава 20

ucspi-tcp – программное обеспечение для запуска обычных программ в режиме сервера

В этой главе:

Программное обеспечение ucspi-tcp (UNIX Client-Server Program Interface), разработанное Д. Бернштейном (D.R. Bernstein), содержит пакет программ. Эти программы используются при создании различных клиент-серверных приложений и позволяют запускать в режиме сервера различные программы, которые не могут быть запущены в режиме службы. Программы tcpserver и tcpclient, наиболее часто используемые из данного пакета, являются более быстродействующей и безопасной альтернативой для таких широко известных программ, как inet и xinetd.

При этом программа tcpserver позволяет ограничивать максимальное количество одновременных соединений, ограничивать доступ к запущенной службе в соответствии с заданными правилами, выполнять проверку легитимности IP-адреса через DNS и регистрировать соединения в файле регистрации.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта ucspi-tcp по состоянию на 11.05.2003. Регулярно посещайте домашнюю страницу проекта `http://cr.yp.to/ucspi-tcp/install.html` и отслеживайте обновления.

Исходные коды ucspi содержатся в архиве `ucspi-tcp-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `ucspi-tcp-0.88.tar.gz`).

Компиляция, оптимизация и инсталляция ucspi-tcp

Для установки ucspi-tcp необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архив с исходными кодами ucspi-tcp в каталоге `/var/tmp`:

```
[root@drwalbr /]# cd /var/tmp/
[root@drwalbr tmp]# tar xzpf
```

и перейдите во вновь созданный каталог, содержащий исходные коды ucspi-tcp:

```
[root@drwalbr tmp]# cd ucspi-tcp-0.88/
```

Шаг 3

В файле `/var/tmp/ucspi-tcp-0.88/conf-home` замените строку:

```
/usr/local
```

на:

```
/usr
```

Шаг 4

В файле `/var/tmp/ucspi-tcp-0.88/conf-cc` замените строку:

```
gcc -O2
```

на:

```
gcc -O2 -march=i686 -funroll-loops
```

Шаг 5

Откомпилируйте исходные коды, проинсталлируйте файлы ucspi-tcp, создайте и сохраните список инсталлированных файлов:

```
[root@drwalbr ucspi-tcp-0.88]# make
[root@drwalbr ucspi-tcp-0.88]# find /* > /root/ucspi1
[root@drwalbr ucspi-tcp-0.88]# make setup check
[root@drwalbr ucspi-tcp-0.88]# chmod 0510 /usr/bin/tcpserver
```

```
[root@drwalbr ucspi-tcp-0.88]# chmod 0510 /usr/bin/tcpclient
[root@drwalbr ucspi-tcp-0.88]# find /* > /root/ucspi2
[root@drwalbr ucspi-tcp-0.88]# diff /root/ucspi1 /root/ucspi2 >
/root/ucspi.installed
[root@drwalbr ucspi-tcp-0.88]# mv /root/ucspi.installed
/very_reliable_place/ucspi.installed.YYYYMMDD
```

Шаг 6

Удалите архив и каталог с исходными кодами ucspi-tcp:

```
[root@drwalbr /]# cd /var/tmp/
[root@drwalbr tmp]# rm -rf ucspi-tcp-0.88/
[root@drwalbr tmp]# rm -f ucspi-tcp-0.88.tar.gz
```

Использование ucspi-tcp

Как уже отмечалось, программы из пакета ucspi-tcp могут быть использованы для запуска ряда служб. Подробные инструкции по их использованию приведены в документации на соответствующее программное обеспечение. В этой главе рассматриваются простейшие варианты использования программы tcpserver, носящие иллюстративно-ознакомительный характер.

Запуск службы с помощью программы tcpserver осуществляется с использованием команды:

```
[root@drwalbr /]# tcpserver opts host port /path/prog
```

где:

`opts` – набор опций;

`host` – имя системы, на которой требуется запустить службу;

`port` – номер порта, на котором будет выполняться служба;

`prog` – полный путь и имя исполняемого файла службы.

Опция `-c` используется для определения максимального количества одновременных соединений, обрабатываемых tcpserver. Значение по умолчанию – `40` . Т. е. не более 40 одновременных подключений могут обрабатываться tcpserver. Очевидно, что для высокопроизводительного и сильно загруженного сервера необходимо увеличить это значение.

Опции `-u` и `-g` используется для определения пользователя и соответствующей ему группы пользователей, от имени которого должна быть запущена соответствующая служба.

Опции `–D`, `-H`, `-R` и `-I` используются для повышения производительности системы.

Для запуска vsFTPd FTP-сервера используется команда:

```
[root@drwalbr /]# tcpserver -c 4096 –DRHl localhost 0 21 /usr/sbin/vsftpd
```

В результате выполнения команды будет запущен FTP-сервер, ожидающий соединений на 21 порту всех сетевых интерфейсов локальной системы. При этом максимально возможное число устанавливаемых одновременно соединений не должно превышать 4096.

Для запуска ipop3d POP3-сервера используется команда:

```
[root@drwalbr /]# tcpserver -c 1024 –DRH1 localhost 195.2.72.152 110
/usr/sbin/ipop3d
```

В результате выполнения команды будет запущен POP3-сервер, ожидающий подключений на 110 порту сетевого интерфейса с IP-адресом 195.2.72.152. При этом максимально возможное число одновременно устанавливаемых соединений не должно превышать 1024.

Глава 21

xinetd – программное обеспечение для запуска обычных программ в режиме сервера

В этой главе:

Программа xinetd, так же как и программа tcpserver из пакета ucspi-tcp, предназначена для запуска приложений, которые не могут выполняться в режиме демона.

Данная программа обладает следующими возможностями:

- обеспечивает механизмы управления доступом;
- предотвращает атаки отказа в обслуживании;
- обеспечивает возможность регистрации большого количества пользователей;
- обеспечивает повременной доступ службам;
- ограничивает число запускаемых серверов.

К сожалению, xinetd недостаточно корректно работает с рядом служб, например, `ftp` и `ssh`. Поэтому авторы рекомендуют использовать для запуска служб, которые не могут выполняться в режиме сервера, программы из пакета ucspi-tcp, обладающие большим быстродействием, надежностью и приемлемыми показателями безопасности.

Желающие протестировать xinetd могут воспользоваться рекомендациями настоящей главы.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта xinetd по состоянию на 02.05.2003. Регулярно посещайте домашнюю страницу проекта `http://www.xinetd.org/` и отслеживайте обновления.

Исходные коды xinetd содержатся в архиве `xinetd-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `xinetd-2.3.11.tar.gz`).

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет программы xinetd с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq xinetd
```

Шаг 2

В случае его отсутствия перейдите в каталог, где находится пакет `xinetd-2.3.5-1.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

и установите:

```
[root@drwalbr distrib]# rpm –ihv xinetd-2.3.5-1.asp.i386.rpm
```

или обновите пакет:

```
[root@drwalbr distrib]# rpm –Uhv xinetd-2.3.5-1.asp.i386.rpm
```

После установки пакета перейдите к настройке программы.

Компиляция, оптимизация и инсталляция xinetd

Для установки xinetd из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Проверьте подлинность и целостность полученных архивов с исходными кодами (для получения более подробной информации о порядке действий см. соответствующий раздел главы 12).

Шаг 2

Распакуйте архивы с исходными кодами xinetd в каталоге `/var/tmp`:

```
[root@drwalbr /]# cd /var/tmp/
[root@drwalbr tmp]# tar xzpf xinetd-2.3.11.tar.gz
```

Шаг 3

Сконфигурируйте исходные коды xinetd:

```
[root@drwalbr tmp]# cd xinetd-2.3.11/
[root@drwalbr xinetd-2.3.11]# CFLAGS="-O2 -march=i686 -funroll-loops";
export CFLAGS
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--with-loadavg \
--mandir=/usr/share/man
```

Шаг 4

Откомпилируйте, проинсталлируйте xinetd, создайте и сохраните список установленных файлов:

```
[root@drwalbr xinetd-2.3.11]# make
[root@drwalbr xinetd-2.3.11]# find /* > /root/xinet1
[root@drwalbr xinetd-2.3.11]# make install
[root@drwalbr xinetd-2.3.11]# rm -f /usr/sbin/itox
[root@drwalbr xinetd-2.3.11]# rm -f /uar/sbin/xconv.pl
[root@drwalbr xinetd-2.3.11]# rm -f /usr/ahare/lnan/man8/itox.8
[root@drwalbr xinetd-2.3.11]# chmod 0510 /usr/sbin/xinetd
[root@drwalbr xinetd-2.3.11]# strip /usr/sbin/xinetd
[root@drwalbr xinetd-2.3.11]# find /* > /root/xinetd2
[root@drwalbr xinetd-2.3.11]# diff /root/xinet1 /root/xinet1 >
/root/xinetd.installed
[root@drwalbr xinetd-2.3.11]# mv /root/xinet.installed
/very_reliable_place/ xinet.installed.YYYYMMDD
```

Шаг 5

Удалите архивы и каталоги с исходными кодами xinetd:

```
[root@drwalbr /]# cd /var/tmp/
[root@drwalbr tmp]# rm -rf xinetd-2.3.11/
[root@drwalbr tmp]# rm-f xinetd-2.3.11.tar.gz
```

Шаг 6

Если в вашей системе имеются файлы `/etc/hosts.allow` и `/etc/hosts.deny`, то удалите их:

```
[root@drwalbr /]# rm-f /etc/hosts.allow
[root@drwalbr /]# rm-f /etc/hosts.deny
```

Конфигурирование xinetd

Конфигурирование xinetd осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/xinetd.conf`;
- файлов из каталога `/etc/xinetd.d`;
- файла инициализации `/etc/init.d/xinetd`.

Конфигурационный файл /etc/xinetd.conf

Шаг 1

Создайте файл `/etc/xinetd.conf` в соответствии с приведенными рекомендациями и вашими потребностями:

```
defaults
{
```

```
    instance=60
    log_type=SYSLOG authpriv
    log_on_success= HOST PID
    log_on_failure= HOST
    only_from=
    per_source=5
}
includedir/etc/xinet.d
```

где строка:

```
instance = 60
```

определяет максимальное количество одновременно создаваемых соединений для любой службы, выполняемой через xinetd. Если для данной службы не определено собственное значение параметра `instance` (как это сделать – показано ниже), то при ее запуске будет использоваться значение, определенное в рассматриваемой строке. Эта опция используется для защиты служб, запущенных с использованием `xinetd` от DoS-атак.

Строка:

```
log_type = SYSLOG authpriv
```

определяет способ регистрации. В данной редакции для регистрации используется служба `syslogd`.

При использовании параметра `FILE`, т. е. строки вида:

```
log_type = FILE /var/log/servicelog
```

регистрация осуществляется в файл `/var/log/servicelog`.

Строка

```
log_on_success = HOST PID
```

определяет, что будет регистрироваться при успешном обращении к службе, запущенной с использованием xinetd. В рассматриваемом примере регистрируется IP-адрес компьютера, с которого осуществляется обращение к вашему серверу и номер процесса. Опция `log_on_success`, кроме того, может использоваться со следующими параметрами:

- `USERID` – регистрация идентификатора пользователя;
- `EXIT` – регистрация кода завершения процесса;
- `DURATION` – регистрация продолжительности сеанса.

Строка:

```
log_on_failure = HOST
```

определяет, что будет регистрироваться при неудачной попытке обращения к службе, запущенной с использованием xinetd. В рассматриваемом примере регистрируется IP-адрес компьютера, с которого осуществляется обращение к вашему серверу.

Опция `log_on_failure`, кроме того, может использоваться со следующими параметрами:

- `USERID` – регистрация идентификатора пользователя;
- `ATTEMPT` – подтверждение факта неудачного запуска сервера;
- `RECORD` – регистрация максимально полной информации об удаленной системе, с которой осуществляется обращение к вашему серверу.

Строка:

```
only_from =
```

запрещает доступ к службам, запускаемым с использованием xinetd, с любых IP-адресов. Далее, создавая файлы в каталоге `/etc/xinetd.d`, можно разрешить доступ к соответствующим службам только с определенных удаленных систем.

Строка:

```
per_source = 5
```

ограничивает максимальное количество соединений – в рассматриваемом примере 5 – которое может быть установлено между определенным удаленным IP-адресом и сервером. Значение может быть выражено целым числом или параметром `unlimited`, снимающим ограничения на количество устанавливаемых соединений. Этот параметр может быть использован для защиты от DoS-атак.

Строка:

```
includedir /etc/xinetd.d
```

определяет каталог, в котором находятся конфигурационные файлы, используемые xinetd для запуска соответствующих серверов. В рассматриваемом примере используется каталог `/etc/xinetd.d`

Шаг 2

Установите права доступа к файлу и определите его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 600 /etc/xinetd.conf
[root@drwalbr /]# chown 0.0 /etc/xinetd.conf
```

Каталог /etc/xinetd.d

В каталоге `/etc/xinetd.d` необходимо создать файлы, ответственные за запуск соответствующих служб. Ниже приведены примеры конфигурационных файлов для запуска с использованием xinetd следующих служб:

- защищенного протокола получения электронной почты – `pop3s`;
- `time`;
- `chargen`;
- `echo`;
- `daytime`;
- `imaps`.

Конфигурационный файл /etc/xinetd.d/pop3s

Для запуска службы защищенного протокола получения электронной почты `pop3s` с использованием xinetd создайте файл `/etc/xinetd.d/pop3s`, руководствуясь вашими потребностями и ниже приведенными рекомендациями:

```
service pop3s
{
socket type             = stream
wait                    = no
user                    = root
server                  = /usr/sbin/ipop3d
only_from               = 0.0.0.0/0
no_access               = 207.35.78.10
instances               = 30
log_on_success          += DURATION HOST
log on failure          += HOST
nice                    = -2
disable                 = no
}
```

где строка:

```
service pop3s
```

определяет название конфигурируемой службы.

ЗАМЕЧАНИЕ Имя службы, заданное в этой строке, программа будет использовать для поиска служебной информации в файле `/etc/services`. Если вы не знаете правильное и точное название необходимой службы, то определите его, просмотрев файл `/etc/services`.

Строка:

```
socket_type = stream
```

определяет тип сокета, используемого с соответствующей службой. Опция может использоваться с параметрами `stream`, `dgram`, `raw`, `rdm` или `seqpacket`.

В строке:

```
wait = no
```

если значение параметра установлено "yes", служба запускается в режиме single-threaded, т. е. запускается служба и xinetd перестает обрабатывать запросы клиентов к ней. Если используется устанавливаемое по умолчанию значение "no", то xinetd запускает службу в режиме multi-threaded, т. е. запускает службу и продолжает обрабатывать запросы к ней.

Строка:

```
user = root
```

определяет имя пользователя, запускающего службу. В рассматриваемом примере это пользователь `root`. В некоторых случаях могут быть и другие пользователи, поэтому желательно проверить для всех служб, возможен ли их запуск пользователями с меньшими привилегиями.

Строка:

```
server = /usr/sbin/ipop3d
```

определяет путь к исполняемому файлу запускаемой службы.

Строка:

```
only_from = 0.0.0.0/0
```

определяет IP-адреса систем, с которых разрешен доступ к службе `pop3s` на вашем сервере.

ЗАМЕЧАНИЕ Вспомните, что в файле `/etc/xinetd.conf` вы запретили доступ ко всем службам, запущенным с использованием xinetd со всех IP-адресов. Строка:

```
only_from = 0.0.0.0/0
```

переопределяет это правило только для службы pop3s, разрешая доступ к нему с любого IP-адреса. Вы так же можете использовать другие (более жесткие) параметры, ограничивающие диапазон IP-адресов, с которых возможно обращение клиентов к службе доставки электронной почты.

Строка:

```
no_access = 212.24.38.75
```

определяет IP-адреса удаленных систем, доступ с которых к службе запрещен. В данном случае определен один компьютер с IP-адресом 212.24.38.75.

Строка:

```
instance = 30
```

определяет число запросов, которое может обработать служба. Значение параметра "30", установленное в рассматриваемом примере, переопределяет значение "40", установленное в файле `/etc/initd.conf` для всех служб. Т. е. служба `pop3s` сможет обслуживать до 30 клиентских соединений одновременно.

Строка:

```
log_on_success += DURATION HOST
```

определяет дополнительные (в дополнение к тем, что были установлены в строке `log_on_success` в файле `/etc/initd.conf`) параметры, регистрируемые при успешном обращении к службе, запущенной с использованием `xinetd`. Это достигается использованием символов "+=".

Строка:

```
log on_failure += HOST
```

определяет дополнительные параметры, регистрируемые при неудачном обращении к службе.

Строка:

```
nice = -2
```

определяет приоритет выполнения процесса. Минимальное значение параметра составляет "-20" (самый высокий приоритет), максимальное задается числом "19" (самый низкий приоритет). Более подробная информация об использовании этой опции может быть получена из руководства по команде `nice`:

```
[root@drwalbr /]# man 1 nice
```

Строка:

```
disable = no
```

определяет, разрешен запуск службы или нет. В рассматриваемом примере значение "no" снимает блокировку и разрешает запуск службы.

Конфигурационный файл /etc/xinet.d.d/time

Для запуска службы `time` создайте файл `/etc/xinetd.d/time`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
service time
{
socket type             = stream
wait                    = no
user                    = root
type                    = INTERNAL
id                      = time-stream
protocol                = tcp
only_from               = 192.168.1.0/24
disable                 = no
}
service time-udp
{
socket type             = dgram
wait                    = yes
user                    = root
type                    = INTERNAL
id                      = time-dgram
protocol                = udp
only_from               = 192.168.1.0/24
port                    = 37
disable                 = no
}
```

где строки:

`socket type = stream` и `socket type = dgram`

определяют, соответственно, тип сокета для соединений по протоколу TCP и UDP.

Строки:

`wait = no` и `wait = yes`

определяют режим запуска службы. Если значение параметра установлено "yes", служба запускается в режиме single-threaded. Если используется устанавливаемое по умолчанию значение "no", то xinetd запускает службу в режиме multi-threaded.

Строка:

`type = INTERNAL`

определяет тип службы. Опция `type` может использоваться со следующими параметрами:

- `RPC` – служба RPC (Remote Procedure Call);
- `INTERNAL` – служба, поддерживаемая xinetd;
- `UNLISTED` – служба, не перечисленная в файлах `/etc/rpc` и `/etc/services`.

Строки:

`id = time-stream` и `id = time-dgram`

используются для переопределения названия служб. В рассматриваемом примере используются различные названия для одной и той же службы, работающей с различными протоколами, соответственно, TCP и UDP.

Строки:

`protocol = tcp` и `protocol = udp`

определяют тип протокола, используемый службой. В рассматриваемом примере используются протоколы TCP и UDP.

Строка:

`port = 37`

определяет номер порта, который прослушивается сервером.

Конфигурационный файл /etc/xinetd.d/chargen

Для запуска службы `chargen` создайте файл `/etc/xinetd.d/chargen`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
service chargen
{
socket_type             = stream
wait                    = no
user                    = root
type                    = INTERNAL
id                      = chargen-stream
protocol                = tcp
only from               = 192.168.1.0/24
noaccess                = 212.24.38.75
disable                 = yes
}
service chargen-udp
{
socket_type             = dgram
wait                    = yes
user                    = root
type                    = INTERNAL
id                      = chargen-dgram
protocol                = udp
only from               = 192.168.1.0/24
no access               = 212.24.38.75
port                    = 19
disable                 = yes
}
```

Назначение всех строк, используемых в этом примере конфигурационного файла, аналогично приведенным выше.

Конфигурационный файл /etc/xinetd.d/echo

Для запуска службы `echo` создайте файл `/etc/xinetd.d/echo`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
service echo
{
socket_type             = stream
wait                    = no
user                    = root
type                    = INTERNAL
id                      = echo-stream
protocol                = tcp
only from               = 192.168.1.0/24
noaccess                = 212.24.38.75
disable                 = yes
}
service echo-udp
{
socket_type             = dgram
wait                    = yes
user                    = root
type                    = INTERNAL
id                      = echo-dgram
protocol                = udp
only from               = 192.168.1.0/24
no access               = 212.24.38.75
port                    = 7
disable                 = yes
}
```

Назначение всех строк, используемых в этом примере конфигурационного файла, аналогично приведенным выше.

Конфигурационный файл /etc/xinetd.d/daytime

Для запуска службы `daytime` создайте файл `/etc/xinetd.d/daytime`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
service daytime
{
socket_type             = stream
wait                    = no
user                    = root
type                    = INTERNAL
id                      = daytime-stream
protocol                = tcp
only from               = 192.168.1.0/24
noaccess                = 212.24.38.75
disable                 = yes
}
service daytime-udp
{
socket_type             = dgram
wait                    = yes
user                    = root
type                    = INTERNAL
id                      = echo-dgram
protocol                = udp
only from               = 192.168.1.0/24
no access               = 212.24.38.75
port                    = 13
disable                 = yes
}
```

Назначение всех строк, используемых в этом примере конфигурационного файла, аналогично приведенным выше.

Конфигурационный файл /etc/xinetd.d/imaps

Для запуска службы `imaps` создайте файл `/etc/xinetd.d/imaps`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
service imaps
{
socket_type             = stream
wait                    = no
user                    = root
server                  = /usr/sbin/imapd
only_from               = 0.0.0.0/0
no_access               = 212.24.38.75
instances               = 30
log_on_success          += DURATION HOST
log on failure          += HOST
nice                    = -2
redirect                = 172.16.181.105 993
bind                    = 212.45.28.122
disable                 = yes
}
```

где строка:

```
redirect = 172.16.181.105 993
```

переадресовывает запросы к службе, якобы работающей на 993 порту сетевого интерфейса 212.24.38.75, на 993 порт сетевого интерфейса другой системы с IP-адресом 172.16.181.105.

Строка:

```
bind = 212.45.28.122
```

определяет IP-адрес сетевого интерфейса, прослушиваемого службой `imaps`. Назначение остальных строк, используемых в этом примере конфигурационного файла, рассмотрено выше.

Файл инициализации /etc/init.d/xinetd

Если вы хотите, что бы xinetd запускался автоматически при загрузке системы, необходимо выполнить следующие операции.

Шаг 1

Создайте файл `/etc/init.d/xinetd`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping Xinetd.
#
# chkconfig: 345 56 50
# description: Xinetd is a powerful replacement for inetd. It has access
\
#              control machanisms, extensive logging capabilities, the \
#              ability to make services available based on time, and can
\
#              place limits on the number of servers that can be
started, \
#              among other things.
#
# processname: /usr/sbin/xinetd
# config: /etc/sysconfig/network
# config: /etc/xinetd.conf
# pidfile: /var/run/xinetd.pid

prog="Xinetd"
PATH=/sbin:/bin:/usr/bin:/usr/sbin

# Source function library.
```

```
. /etc/init.d/functions

# Get config.
test -f /etc/sysconfig/network && . /etc/sysconfig/network
test -f /etc/sysconfig/xinetd && . /etc/sysconfig/xinetd

# Check that networking is up.
[ ${NETWORKING} = "yes" ] || exit 0

[ -f /usr/sbin/xinetd ] || exit 1
[ -f /etc/xinetd.conf ] || exit 1

RETVAL=0

start() {
        echo -n $"Starting $prog: "
        LANG=en_US
        LC_TIME=en_US
        LC_ALL=en_US
        LC_MESSAGES=en_US
        LC_NUMERIC=en_US
        LC_MONETARY=en_US
        LC_COLLATE=en_US
        export LANG LC_TIME LC_ALL LC_MESSAGES LC_NUMERIC LC_MONETARY
LC_COLLATE
        unset HOME MAIL USER USERNAME

        daemon xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
"$EXTRAOPTIONS"
        RETVAL=$?
        echo
        touch /var/lock/subsys/xinetd
        return $RETVAL
}

stop() {
        echo -n $"Stopping $prog: "
        killproc xinetd
        RETVAL=$?
        echo
        rm -f /var/lock/subsys/xinetd
        return $RETVAL

}

reload() {
        echo -n $"Reloading configuration: "
        killproc xinetd -USR2
        RETVAL=$?
        echo
        return $RETVAL
}

restart() {
        stop
        start
}

condrestart() {
        [ -e /var/lock/subsys/xinetd ] && restart
        return 0
}
```

```
# See how we were called.
case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        restart
        ;;
    reload)
        reload
        ;;
    condrestart)
        condrestart
        ;;
    *)
        echo $"Usage: $0 {start|stop|restart|condrestart|reload}"
        RETVAL=1
esac
exit $RETVAL
```

Шаг 2

Сделайте файл исполняемой программой и определите его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 700 /etc/init.d/xinetd
[root@drwalbr /]# chown 0.0 /etc/init.d/xinetd
```

Шаг 3

Если вы хотите, чтобы программа xinetd автоматически запускалась при загрузке системы, создайте соответствующие ссылки:

```
[root@drwalbr /]# chkconfig --add xinetd
[root@drwalbr /]# chkconfig --level 345 xinetd on
```

Шаг 4

Для запуска xinetd используйте команду:

```
[root@drwalbr /]# /etc/init.d/xinetd start
Starting Xinetd:              [OK]
```

Глава 22

NTP – программное обеспечение для синхронизации времени

В этой главе:

Синхронизация системного времени на всех серверах и рабочих станциях вашей сети является важной мерой по обеспечению безопасности. Как правило, поиск уязвимостей и негативные воздействия со стороны злоумышленников осуществляются не на одну, а на несколько систем одновременно. Для упрощения анализа информации о поиске уязвимости и попытках деструктивного воздействия на вашу сеть в многочисленных файлах регистрации и сообщениях электронной почты системное время должно совпадать, по крайней мере, с точностью до 1 секунды. Синхронизация системного времени также необходима для нормальной работы многих служб, например службы DNS, обмен информацией в которой между первичным и вторичным DNS-серверами предъявляет достаточно жесткие требования по синхронизации времени. Кроме того, наличие точного времени на рабочих станциях сети вашего предприятия просто удобно для решения различных задач прикладного характера (синхронизация прибытия сотрудников на служебные совещания, чаепития, товарищеские ужины, обеды, завтраки и т. п., поддержание исполнительской дисциплины).

Протокол Network Time Protocol (NTP), описанный в RFC-1305 и RFC-2030, предусматривает иерархическую структуру, используемую для согласования системного времени. В соответствии с протоколом NTP серверы первого уровня (stratum 1) синхронизуют свое время по часам-эталонам (например, атомным часам). Серверы второго уровня (stratum 2) получают информацию о точном времени от серверов первого уровня, используя поправки на удаленность. Обычным пользователям рекомендуется использовать сервера второго уровня для синхронизации времени на одном из серверов своей сети, который также используется в качестве сервера первого уровня для всех систем в вашей сети.

Схема, реализующая синхронизацию времени в сети масштаба предприятия с использованием внешних эталонов, представлена на рис. 22.1.

Важным фактором для настройки синхронизации времени в вашей сети является правильный выбор серверов, используемых для получения точного времени главным сервером вашей сети. Выбранные сервера должны удовлетворять следующим условиям:

- временная задержка должна быть минимальной;
- владельцы сервера не должны возражать против его использования вами.

Старайтесь не использовать сервера первого уровня во избежание их перегрузки. Если вы не решаете задачи, связанные с управлением космическими полетами, использованием высокоточного оружия и т. п. точности серверов второго уровня вполне достаточно.

Для реализации протокола Network Time Protocol авторы предлагают использовать программное обеспечение NTP, разрабатываемое под руководством доктора Дэвида Миллса (David L. Mills, University of Delaware).

Если по каким-либо причинам вы предъявляете достаточно высокие требования к точности синхронизации времени в ваших сетях, одним из вариантов реализации этих требований является создание собственного эталонного сервера времени, получающего информацию от глобальной навигационной системы GPS (Global Positioning System). На домашней странице проекта NTP вы можете найти список совместимых с NTP – Linux и платформой Intel – приемников. Некоторые из них на момент написания этой главы продавались в Москве и Днепропетровске (`http://www.gpshome.ru`) и стоили порядка нескольких сотен долларов США.

В данной главе рассматривается простейший вариант инсталляции настройки сервера времени, используемого в вашей сети для синхронизации системного времени на других серверах и рабочих станциях с операционной системой Linux. В более сложных случаях авторы рекомендуют пользоваться документацией с домашней страницы проекта NTP и других специализированных источников.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта NTP по состоянию на 08.05.2003. Регулярно посещайте домашнюю страницу проекта `http://www.ntp.org/` и отслеживайте обновления. Исходные коды NTP содержатся в архиве `ntp-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `ntp-4.1.1.tar.gz`).

Для нормальной работы NTP необходима библиотека LIBCAP. Исходные коды библиотеки содержатся в архиве `libpcap-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `libpcap-0.7.2.tar.gz`).

Рис. 22.1. Схема реализации синхронизации времени в сети масштаба предприятия с использованием внешних эталонов.

Для запуска NTP от имени обычного пользователя и возможности запуска NTP в окружении chroot-jail необходим патч `ntp-chroot.patch` разработки Open Network Architecture Inc., который может быть получен с FTP-сервера компании `ftp://openna.com`.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет программы NTP с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq ntp
```

Шаг 2

В случае его отсутствия перейдите в каталог, где находится пакет `ntp-4.1.1-1.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

и установите:

```
[root@drwalbr distrib]# rpm –ihv libcap-1.10-8.i386.rpm
[root@drwalbr distrib]# rpm –ihv ntp-4.1.1-1.i386.rpm
```

или обновите пакет:

```
[root@drwalbr distrib]# rpm –Uhv ntp-4.1.1-1.i386.rpm
```

После установки пакета перейдите к настройке программы.

Компиляция, оптимизация и инсталляция NTP

Для инсталляции NTP необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Если вы не установили ранее библиотеку LIBCAP, установите её в соответствии с рекомендациями главы 19.

Шаг 3

Распакуйте архивы с исходными кодами NTP в каталоге `/var/tmp`:

```
[root@drwalbr tmp]# tar xzpf ntp-4.1.1.tar.gz
[root@drwalbr tmp]# cd ntp-4.1.1/
```

Шаг 4

Скопируйте патч `ntp-chroot.patch` в каталог `/var/tmp` и модифицируйте исходные коды NTP:

```
[root@drwalbr ntp-4.1.1]# patch –p1 < ../ntp-chroot.patch
patching file ntpd/Makefile.in
Hunk #1 succeeded at 197 (offset -2 lines).
patching file ntpd/cmd_args.c
patching file ntpd/ntpd.c
patching file ntpdate/Makefile.in
patching file ntpdate/ntpdate.c
```

ЗАМЕЧАНИЕ Эту операцию необходимо выполнить, если вы собираетесь запускать NTP от имени пользователя, отличного от root, или в окружении chroot-jail. Именно этот вариант настоятельно рекомендуется авторами.

Шаг 5

Создайте специального пользователя `ntp`, от имени которого будет запускаться NTP:

```
[root@drwalbr ntp-4.1.1]# groupadd -g 38 ntp > /dev/null 2>&l || :
[root@drwalbr ntp-4.1.1]# useradd -u 38 -g 38 -s /bin/false -M -r -d
/etc/ntp ntp > /dev/null 2>&l || :
```

ЗАМЕЧАНИЕ Эту операцию необходимо выполнить если вы собираетесь запускать NTP от имени пользователя отличного от root. Именно этот вариант настоятельно рекомендуется авторами.

Шаг 6

Для добавления несуществующего командного интерпретатора добавьте в файл `/etc/shells` строку:

```
/bin/false/
```

Шаг 7

Откonфигурируйте исходные коды NTP:

```
[root@drwalbr ntp-4.1.1]# CFLAGS="-O2 -march=i686 -funroll-loops"; export
CFLAGS
./configure \
--prefix=/usr \
--bindir=/usr/sbin \
--sbindir=/usr/sbin \
--sysconfdir=/etc \
--localstatedir=/var \
--mandir=/usr/share/man \
--disable-debugging \
--enable-all-clocks \
--enable-parse-clocks
```

Шаг 8

Откомпилируйте, проинсталлируйте NTP, создайте и сохраните в надежном месте список установленных файлов:

```
[root@drwalbr ntp-4.1.1]# make
[root@drwalbr ntp-4.1.1]# find /* > /root/ntp1
[root@drwalbr ntp-4.1.1]# make install
[root@drwalbr ntp-4.1.1]# strip /usr/sbin/ntp*
strip: /usr/sbin/ntp-wait: File format not recognized
[root@drwalbr ntp-4.1.1]# find /* > /root/ntp2
[root@drwalbr ntp-4.1.1]# diff /root/ntp1 /root/ntp2 >
/root/ntp.installed
[root@drwalbr ntp-4.1.1]# mv /root/ntp.installed
/very_reliable_place/ntp.installed.YYYYMMDD
```

Шаг 9

Удалите архивы и каталоги с исходными кодами программ:

```
[root@drwalbr ntp-4.1.1]# cd /var/tmp
[root@drwalbr tmp]# rm –r ntp-4.1.1.tar.gz libpcap-0.7.2.tar.gz
[root@drwalbr tmp]# rm –rf ntp-4.1.1/ libpcap-0.7.2/
```

Конфигурирование NTP

Конфигурирование NTP осуществляется с использованием следующих файлов:

- основного конфигурационного файла `/etc/ntp.conf`;
- файла `/etc/ntp.drift`, содержащего поправку (drift) на различную скорость хода системных часов вашей системы и эталона;
- файла `/etc/sysconfig/ntpd`, используемого для запуска NTP от имени пользователя, отличного от `root`, и в окружении chroot jail;
- файла инициализации `/etc/init.d/ntpd`.

Конфигурационный файл /etc/ntp.conf для сервера

Ниже рассматривается конфигурация NTP для сервера времени вашей сети. При этом предполагается, что сервер синхронизует время по находящимся в Интернет серверам и используется клиентами (серверами и рабочими станциями в локальной сети).

Для конфигурирования NTP в качестве сервера необходимо выполнить следующие операции.

Шаг 1

Создайте файл `/etc/ntp.conf`, содержащий следующие строки:

```
restrict default notrust nomodify ignore
restrict 127.0.0.1
restrict 172.16.181.0 mask 255.255.255.0 notrust nomodify notrap
restrict 195.83.132.135 mask 255.255.255.255 nomodify notrap noquery
restrict 216.27.190.202 mask 255.255.255.255 nomodify notrap noquery
restrict 199.212.17.34 mask 255.255.255.255 nomodify notrap noquery
server 195.83.132.135 prefer
server 216.27.190.202
server 199.212.17.34
server 127.127.1.0
fudge 127.127.1.0 stratum 10
driftfile /etc/ntp.drift
broadcastdelay 0.008
```

Строки, начинающиеся с ключевого слова `restrict`, являются директивами управления доступом к NTP-серверу. Для создания директив используется следующий синтаксис:

```
restrict numeric-address [ mask numeric-mask ] [flag1] [flag2]…[flagN]
```

где:

`numeric-address [ mask numeric-mask ]`

определяет диапазон IP-адресов, к которому относится данная директива, ключевое слово `default` означает все допустимые IP-адреса;

`[flag1] [flag2]…[flagN]`

определяют параметры доступа. Отсутствие флагов предоставляет неограниченный доступ. При обращении к NTP-серверу осуществляется последовательный просмотр директив управления доступом до первой директивы, разрешающей доступ. Если хотя бы одна директива, разрешающая доступ к серверу, отсутствует – доступ к серверу запрещается.

Наиболее часто используются следующие флаги:

- `notrust` –м не рассматривать системы из определенного выше диапазона адресов как источник синхронизации;
- `nomodify` – игнорировать пакеты, предназначенные для модификации состояния вашего сервера;
- `ignore` – игнорировать все остальные пакеты;
- `noquery` – запрет на запросы о состоянии вашего сервера;

Строка:

```
restrict default notrust nomodify ignore
```

запрещает доступ к службе `ntp` со всего возможного диапазона IP-адресов.

Строка:

```
restrict 127.0.0.1
```

разрешает полный доступ к службе `ntp` через интерфейс возвратной петли.

Строка:

```
restrict 172.16.181.0 mask 255.255.255.0 notrust nomodify notrap
```

разрешает использовать клиентам из локальной сети 172.16.181.0/255.255.255.0 ваш сервер в качестве NTP-сервера.

Строки:

```
restrict 195.83.132.135 mask 255.255.255.255 nomodify notrap noquery
restrict 216.27.190.202 mask 255.255.255.255 nomodify notrap noquery
restrict 199.212.17.34 mask 255.255.255.255 nomodify notrap noquery
server 195.83.132.135 prefer
server 216.27.190.202
server 199.212.17.34
```

разрешают использовать сервера 195.83.132.135, 216.27.190.202 и 199.212.17.34 для синхронизации времени на вашем сервере, при этом предпочтительным является использование сервера с IP-адресом 195.83.132.135.

Строки:

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
```

разрешают использовать при отсутствии связи системные часы вашего сервера.

Строка:

```
driftfile /etc/ntp.drift
```

определяет файл, в который записывается отклонение частоты системных часов вашего сервера относительно эталонных серверов.

Строка:

```
broadcastdelay 0.004
```

определяет величину временной задержки при широковещательной рассылке. Здесь устанавливается предполагаемое значение, в дальнейшем оно автоматически вычисляется сервером и корректируется.

Шаг 2

Установите права доступа к файлу `/etc/ntp.conf` и определите его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 644 /etc/ntp.conf
[root@drwalbr /]# chown 0.0 /etc/ntp.conf
```

Конфигурационный файл /etc/ntp.conf для клиента

Вполне возможно, что использование термина «клиент» в данном случае является не совсем удачным, т. к. ниже рассматривается пример конфигурации NTP-сервера, опрашивающего другие сервера для получения текущего времени с NTP-сервера сети или внешних NTP-серверов. В отличие от предыдущей конфигурации в рассматриваемом ниже примере NTP-сервер не позволяет использовать себя другим системам в качестве эталона для синхронизации времени.

Для конфигурирования NTP в качестве клиента необходимо выполнить следующие операции.

Шаг 1

Создайте файл `/etc/ntp.conf`, содержащий следующие строки:

```
restrict default notrust nomodify ignore
restrict 127.0.0.1
restrict 172.16.181.0 mask 255.255.255.0 notrust nomodify notrap
server 172.16.181.111
server 127.127.1.0
fudge 127.127.1.0 stratum 10
driftfile /etc/ntp.drift
broadcastdelay 0.004
```

В рассматриваемой конфигурации в качестве эталона используется сервер времени локальной сети, запущенный на системе с IP-адресом 172.16.181.111.

Шаг 2

Установите права доступа к файлу `/etc/ntp.conf` и определите его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 644 /etc/ntp.conf
[root@drwalbr /]# chown 0.0 /etc/ntp.conf
```

Конфигурационный файл /etc/ntp.drift

В файл `/etc/ntp.drift` записывается вычисляемое ежечасно отклонение частоты системных часов вашего сервера относительно системных часов эталонных серверов.

Шаг 1

Создайте файл `/etc/ntp.drift` и запишите в него строку, соответствующую нулевому отклонению частот:

```
[root@drwalbr /]# echo '0.0' > /etc/ntp.drift
```

ЗАМЕЧАНИЕ Введенное значение никак не отразится на точности вашего сервера, т. к. через час NTP рассчитает отклонение частоты и запишет найденное значение в файл `/etc/ntp.drift`

Шаг 2

Установите права доступа к файлу `/etc/ntp.conf` и определите его владельцем пользователя `ntp`:

```
[root@drwalbr /]# chmod 600 /etc/ntp.drift
[root@drwalbr /]# chown ntp.ntp /etc/ntp.drift
```

Конфигурационный файл /etc/sysconfig/ntpd

Шаг 1

Для запуска NTP от имени пользователя `ntp` создайте файл `/etc/sysconfig/ntpd`, содержащий следующую строку:

```
OPTIONS="-U ntp"
```

ЗАМЕЧАНИЕ Применение опции `-U ntp` допустимо только, если вы модифицировали исходные коды NTP патчем `ntp-chroot.patch`.

Шаг 2

Установите права доступа к файлу `/etc/sysconfig/ntpd` и определите его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 644 /etc/sysconfig/ntpd
[root@drwalbr /]# chown 0.0 /etc/sysconfig/ntpd
```

Файл инициализации /etc/init.d/ntpd

Шаг 1

Для запуска и остановки NTP создайте файл `/etc/init.d/ntpd`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping ntpd.
#
# chkconfig: 345 58 74
# description: NTPD is used to provide time server.

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/ntpd ];then
        . /etc/sysconfig/ntpd
fi

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If NTPD is not available stop now.
[ -f /usr/sbin/ntpd ] || exit 0
[ -f /chroot/ntpd/etc/ntp.conf ] || exit 0

# Path to the NTPD binary.
ntpd=/usr/sbin/ntpd

RETVAL=0
prog="NTPD"

start() {
        echo -n $"Starting $prog: "
        daemon $ntpd $ROOTDIR $OPTIONS
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/ntpd
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $ntpd
        RETVAL=$?
```

```
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/ntpd
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $ntpd
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/ntpd ]; then
            stop
            start
            RETVAL=$?
        fi
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 2

Установите права доступа к файлу, назначьте его владельцем пользователя `root` и создайте соответствующие ссылки:

```
[root@drwalbr /]# chmod 700 /etc/init.d/ntpd
[root@drwalbr /]# chown 0.0 /etc/init.d/ntpd
```

Шаг 3

Если вы хотите, чтобы NTP запускался автоматически при загрузке системы, создайте соответствующие ссылки:

```
[root@drwalbr /]# chkconfig --add ntpd
[root@drwalbr /]# chkconfig --level 345 ntpd on
```

Тестирование NTP

Шаг 1

Проверьте правильность установки даты и времени на NTP-сервере сети по календарю и обычным часам.

Шаг 2

Выполните предварительную синхронизацию системных часов вашего сервера сети и эталонного сервера:

```
[root@drwalbr /]# ntpdate -b 195.83.132.135
grsec: time set by (ntpdate:2447) UID(0) EUID(0), parent (bash:8680)
UID(0) EUID(0)
30 Apr 20:02:45 ntpdate[2447]: step time server 195.83.132.135 offset
0.020454 sec
```

Шаг 3

Запустите NTP на NTP-сервере сети:

```
[root@drwalbr /]# /etc/init.d/ntpd start
Запускается NTPD:                                  [OK]
```

Шаг 4

Просканируйте UDP порты системы с помощью сканера портов, например, Nmap:

```
[root@drwalbr /]# nmap 192.168.2.99 -sU

Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Interesting ports on drwalbr.und (192.168.2.99):
(The 1458 ports scanned but not shown below are in state: closed)
Port       State       Service
123/udp    open        ntp

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
```

Проверьте состояние `ntpd` с помощью утилиты `ntpq`:

```
[root@drwalbr /]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
ntp1.laas.fr    chronos.cru.fr  2  u 15 64 377 73.955  21.977   1.995
+io.berkeley.net usno.pa-x.dec.c 2  u 1  64 367 220.845 19.380   0.929
+dns1.cmc.ec.gc. goes-bkp.cmc.ec 2  u 4  64 377 234.186 51.588  11.285
 LOCAL(0)        LOCAL(0)        10 l 11 64 377 0.000   0.000   0.015
```

Если вы увидите сообщения, подобные приведенным выше, то NTP-сервер работает.

Шаг 5

Через несколько часов проверьте правильность установки даты и времени, выполните предварительную синхронизацию системных часов по NTP-серверу вашей сети и запустите NTP-сервера на всех Linux-системах вашей сети. Проверьте работоспособность NTP-серверов на всех Linux-системах вашей сети в соответствии с рекомендациями шага 4.

ЗАМЕЧАНИЕ Если вы не предъявляете жестких требований по синхронизации времени в пределах вашей сети, то вместо запуска NTP на Linux-системах вашей сети можно использовать команду синхронизации времени `ntpdate`, используемую нами для предварительной синхронизации системного времени на втором шаге тестирования NTP, регулярно запускаемую с помощью `crond`.

Для синхронизации времени на системах с операционной системой MS Windows 98 авторы используют свободно распространяемую программу Dimension 4 Version 4.3, разработанную Робертом Чамберсом (Robert Chambers) и доступную с `http://www.thinkman.com/~thinkman/`. Программа имеет удобный интерфейс, внешний вид которого представлен на рис. 22.2, и удачно выбранные значения параметров по умолчанию, поэтому для синхронизации времени вам необходимо установить лишь IP-адрес NTP-сервера вашей сети.

По информации, полученной с `http://support.microsoft.com`, более поздние версии операционной системы Windows имеют собственную службу синхронизации времени, которая может быть использована для синхронизации времени как по NTP-серверу сети, так и внешним NTP-серверам. Однако из-за отсутствия в распоряжении авторов систем с последними версиями операционной системы Windows тестирование их совместимости с NTP-сервером не проводилось.

Выбор оптимальных внешних NTP-серверов осуществляется с использованием утилиты `ntptrace`:

```
[root@drwalbr /]# ntptrace 195.83.132.135
ntp1.laas.fr: stratum 2, offset -0.031820, synch distance 0.07150
horlogegps.reseau.jussieu.fr: stratum 1, offset -0.036271, synch distance 0.00000, refid 'GPS'
```

В выводе утилиты отображаются временная погрешность и удаленность до тестируемого NTP-сервера. Вам следует выбрать два-три сервера с минимальными значениями этих параметров.

ЗАМЕЧАНИЕ Авторы не дают практических рекомендаций по использованию открытых NTP-серверов по следующим причинам:

- выбор сервера зависит от маршрута прохождения сигнала (месторасположения вашей сети, организации доступа в Интернет и т. п.);
- авторы не имеют опыта использования для синхронизации времени в своих сетях открытых NTP-серверов, т. к. используют NTP-сервера (в приобретении оборудования для которых, инсталляции и настройке принимали непосредственное участие) с аутентификацией, принадлежащие дружественным организациям.

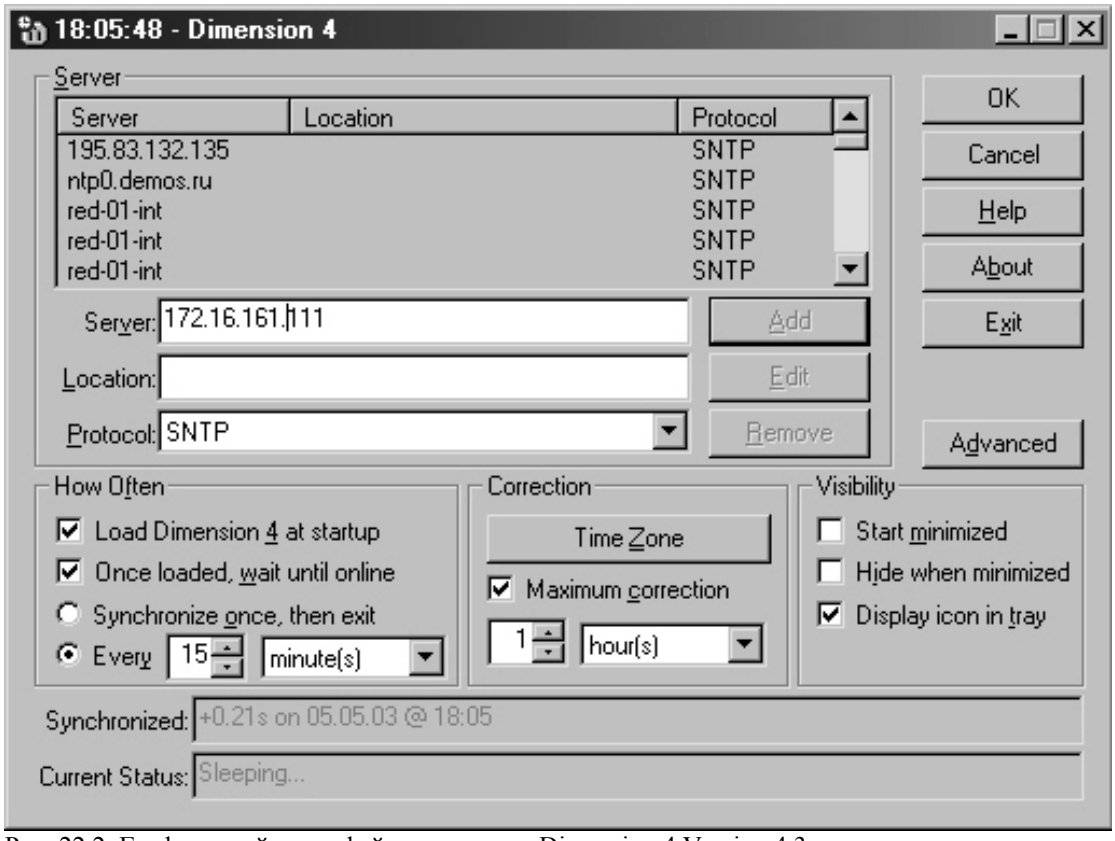


Рис. 22.2. Графический интерфейс программы Dimension 4 Version 4.3.

Для отображения состояния NTP-сервера используется утилита `ntpdc`, для запуска которой в интерактивном режиме используется команда:

```
[root@drwalbr /]# ntpdc
ntpdc> help
Commands available:
addpeer      addrefclock  addserver    addtrap      authinfo
broadcast    clkbug       clockstat    clrtrap      controlkey
ctlstats     debug        delay        delrestrict  disable
dmpeers      enable       exit         fudge        help
host         hostnames    iostats      kerninfo     keyid
keytype      listpeers    loopinfo     memstats     monlist
passwd       peers        preset       pstats       quit
readkeys     requestkey   reset        reslist      restrict
showpeer     sysinfo      sysstats     timeout      timerstats
traps        trustedkey   unconfig     unrestrict   untrustedkey
version
ntpdc> quit
```

Выполнение NTP в среде chroot-jail

Потенциальные уязвимости NTP, как и любого другого программного обеспечения, могут использоваться для реализации атак на вашу систему. Поэтому для повышения безопасности вашей системы рекомендуется выполнять NTP в окружении chroot-jail. Для этого необходимо выполнить следующие операции.

Шаг 1

Создайте каталоги для размещения исполняемых файлов и файлов настройки NTP:

```
[root@drwalbr /]# mkdir -p /chroot/ntpd/etc
[root@drwalbr /]# chown ntp.ntp /chroot/ntpd/etc
```

Шаг 2

Переместите конфигурационные файлы NTP в соответствующие подкаталоги окружения chroot-jail:

```
[root@drwalbr /]# mv /etc/ntp.conf /chroot/ntpd/etc/
[root@drwalbr /]# mv /etc/ntp.drift /chroot/ntpd/etc/
[root@drwalbr /]# chown ntp.ntp /chroot/ntpd/etc/ntp.drift
```

Шаг 3

Скопируйте системные файлы, необходимые для работы NTP, в соответствующие подкаталоги окружения chroot-jail:

```
[root@drwalbr /]# cp /etc/resolv.conf /chroot/ntpd/etc/
[root@drwalbr /]# cp /etc/localtime /chroot/ntpd/etc/
[root@drwalbr /]# chown ntp.ntp /chroot/ntpd/etc/localtime
```

Шаг 4

В файл `/etc/sysconfig/ntpd` добавьте строку:

```
ROOTDIR="-T /chroot/ntpd"
OPTIONS="-U ntp"
```

Шаг 5

Создайте файл инициализации `/etc/init.d/ntpd`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping ntpd.
#
# chkconfig: 345 58 74
# description: NTPD is used to provide time server.

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/ntpd ];then
        . /etc/sysconfig/ntpd
fi

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If NTPD is not available stop now.
[ -f /usr/sbin/ntpd ] || exit 0
[ -f /chroot/ntpd/etc/ntp.conf ] || exit 0

# Path to the NTPD binary.
ntpd=/usr/sbin/ntpd

RETVAL=0
prog="NTPD"

start() {
        echo -n $"Starting $prog: "
        daemon $ntpd $ROOTDIR $OPTIONS
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/ntpd
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $ntpd
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/ntpd
        return $RETVAL
}
```

```
# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $ntpd
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/ntpd ]; then
            stop
            start
            RETVAL=$?
        fi
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 6

Для дополнительной безопасности сделайте файл неизменяемым:

```
[root@drwalbr /] # cd /chroot/ntpd/etc/
[root@drwalbr etc]# chattr +i ntp.conf
```

ЗАМЕЧАНИЕ Не забудьте удалить атрибут immutable перед внесением изменений и установить его вновь после их завершения.

Шаг 7

Для тестирования NTP в окружении chroot jail запустите `ntpd`, просканируйте UDP порты вашей системы и проверьте работоспособность NTP с использованием утилиты `ntpq`, в соответствии с рекомендациями по тестированию NTP в обычной среде, изложенными выше.

Шаг 8

Проверьте, запущен ли `ntpd` и определите соответствующий номер процесса:

```
[root@drwalbr /]# ps -axf | grep ntpd
21889 ?        SL     0:00 /usr/sbin/ntpd -T /chroot/ntpd -U ntp
```

Проверьте, действительно ли NTP работает в окружении chroot-jail:

```
[root@drwalbr /]# ls -la  /proc/21889/root
```

Если вы получите вывод вида (отображающий ссылку на корневой каталог среды chroot-jail):

```
lrwxrwxrwx    1 root     root            0 Апр 30 20:54 /proc/21889/root
-> /chroot/ntpd
```

то NTP корректно работает в окружении chroot-jail.

Если вы получите вывод, отображающий корневой каталог системы, на которой он установлен, то NTP работает в обычном режиме, а не в безопасной среде.

Часть 5

Служба DNS

Глава 23

ISC BIND – программное обеспечение для организации службы DNS

В этой главе:

Каждый компьютер или другое устройство, подключенное к сети Интернет, имеют уникальный IP-адрес. Именно по IP-адресу происходит поиск и взаимодействие устройств в сети. IP-адрес представляет собой последовательность из четырех чисел, разделенных точками. Поначалу для облегчения взаимодействия с удаленными информационными ресурсами в Интернет стали использовать таблицы соответствия IP-адресов именам систем и псевдонимам. Пример такого соответствия вы можете посмотреть в файле `/etc/hosts`.

Эти таблицы использовались для преобразования IP-адресов в имена и обратно. Авторство их создания, по-видимому, принадлежит Д. Постелю (John Postel), который первым стал поддерживать (собирать информацию об IP-адресах и соответствующих им именах систем) файл `hosts`. Доступ к файлу предоставлялся всем желающим по протоколу FTP. С развитием Интернет хранение и использование файла на каждом компьютере, подключенном к Интернет, стала невозможной. Поэтому вместо единого для всех файла была создана доменная система имен (Domain Name System, DNS), представляющая собой распределенную базу данных, позволяющая устанавливать соответствие между IP-адресами и символьными именами.

Однако файл `/etc/hosts` не ушел безвозвратно в прошлое и используется в небольших сетях для установления соответствия между IP-адресами и именами систем.

Впервые DNS была описана Паулем Моккапетрисом (Paul Mockapetris) в 1984 году в RFC-882 и RFC-883. Позже эти документы были заменены на RFC-1034 и RFC-1035. Система доменных имен строится по иерархическому принципу. Точнее, по принципу вложенных друг в друга множеств. Корень системы, согласно RFC-1034, имеет пустое имя. Иногда ошибочно полагают, что обозначение корневого домена – символ `"."`, но это не так. Точка – это всего лишь разделитель компонентов доменного имени, а т. к. у корневого домена нет обозначения, то эту точку и ошибочно принимают за обозначение корневого домена.

Корень – это все множество хостов Интернет. Данное множество подразделяется на домены первого или верхнего уровня (top-level domen или TLD). Домен `ru`, например, соответствует множеству хостов российской части Интернет. Домены верхнего уровня дробятся на более мелкие домены, например, корпоративные.

В 80-е годы были определены первые домены первого уровня (top-level): `gov`, `mil`, `edu`, `com`, `net`. Позднее, когда сеть перешагнула национальные границы США, появились национальные домены: `uk`, `jp`, `au`, `ch`, и т. п. Для СССР также был выделен домен `su`. После 1991 года, когда республики Союза стали суверенными, многие из них получили свои собственные домены: `ua`, `ru`, `la`, `li` и т. п.

Слово «хост» не является в полном смысле синонимом имени компьютера, как это часто упрощенно представляется, т. к. у компьютера может быть множество IP-адресов, каждому из которых можно поставить в соответствие одно или несколько доменных имен. Кроме того, одному доменному имени можно поставить в соответствие несколько разных IP-адресов, которые, в свою очередь могут быть закреплены за разными компьютерами. Символьное имя хоста включает в себя доменное имя и имя системы и состоит из нескольких полей, разделенных точками. Крайнее правое поле является именем домена верхнего уровня, далее, справа налево, следуют имена доменов более низкого уровня. Крайнее левое поле, является именем системы.

В RFC-1034 и RFC-1035 определяется несколько типов DNS-серверов. Одним из способов классификации серверов является тип отклика на запрос:

- авторитетный (authoritative response) ответ серверами, ответственными за зону (фрагмент DNS, управляемый этим сервером);
- неавторитетный (non authoritative response) ответ выдается по запросам клиентов серверами, которые не отвечают за зону, а просто по каким-либо причинам обладают (содержат в кэше) необходимую для ответа на запрос информацию.

Например, если ваш сервер доменных имен поддерживает зону `sipria.msk.ru`, и клиент запрашивает у него IP-адрес почтового сервера `mail.sipria.msk.ru`, то ответ вашего сервера считается авторитетным, т. к. именно ваш сервер несет ответственность за ответы на запросы, касающиеся хостов в зоне `sipria.msk.ru`.

Если клиент обратится к вашему DNS-серверу, поддерживающего, зону `sipria.msk.ru` с запросом об IP-адресе сервера `www.yandex.ru`, то он, вероятно, выдаст информацию из кэша (кто-то из пользователей мог уже обращаться с таким запросом). В этом случае ответ, скорее всего, является правильным, но не авторитетным. В рассматриваемом примере авторитетный ответ на запрос могут дать либо первичный сервер, отвечающий за зону `yandex.ru`, или дублирующие его функции вторичные сервера.

Администратор первичного сервера доменных имен вручную создает описание файлов зон, за которые отвечает сервер. Все остальные серверы только копируют информацию с первичного сервера. Для зоны можно определить только один первичный сервер, являющийся первоисточником для всех вторичных серверов.

Вторичный сервер также предоставляет клиентам авторитетные ответы на запросы, касающиеся обслуживаемых им зон, подстраховывая работу первичного сервера доменных имен и отвечая на часть запросов, адресуемых первичному серверу. В больших зонах может быть несколько вторичных серверов, так, например, из 13 серверов, обслуживающих корневую зону, 12 являются вторичными серверами.

Администратор вторичного сервера не создает файлов описания зон, он только обеспечивает настройку своего сервера таким образом, чтобы он копировал описание зон с первичного сервера, поддерживая описание зон в актуализированном состоянии.

Существует оговоренная практика резервирования серверов, которая описана в рекомендациях по ведению зон. Она заключается в том, что для домена второго уровня необходимо иметь, как минимум, два сервера, ответственных за зону, т. е. дающих авторитетные отклики на запросы. При этом эти серверы должны иметь независимые подключения к Интернет для обеспечения бесперебойного обслуживания запросов в случае потери связи или выхода из строя одного из серверов.

Наиболее популярным приложением, реализующим систему доменных имен, является Berkeley Internet Name Domain (BIND) от Internet Software Consortium (ISC). По оценкам, более 90 % компьютеров в Интернет используют программу ISC BIND, которая содержит сервер, библиотеку клиента и несколько утилит. В этой главе мы рассмотрим инсталляцию и настройку ISC BIND на примере организации поддержания собственной зоны небольшой компании. Принципиальная схема организации службы DNS представлена на рис. 23.1.

В рассматриваемом примере служба DNS реализуется с помощью:

- первичного DNS-сервера;
- вторичного DNS-сервера, имеющего независимое подключение к Интернет (например, установленного на одной из систем дружественной заокеанской фирмы);
- кэширующих DNS-серверов на шлюзе, других серверах и Linux-системах в локальной сети.

ЗАМЕЧАНИЕ Если вы используете DNS-сервера провайдера, то необходимость в инсталляции и настройке первичного и вторичного DNS-серверов отпадает. При этом файлы описания вашей зоны должны создаваться и актуализироваться провайдером. На шлюзе в Интернет необходимо установить кэширующий DNS-сервер, а на остальных Linux системах в вашей сети желательно установить «облегченный» вариант DNS-сервера - .

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта ISC BIND по состоянию на 13.05.2003. Регулярно посещайте домашнюю страницу проекта `http://www.isc.org/`и отслеживайте обновления.

Исходные коды ISC BIND содержатся в архиве `bind-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `bind-9.2.2.tar.gz`).

Для нормальной работы ISC BIND с поддержкой протокола SSL необходима установка программного обеспечения OpenSSL, описанная в главе 12.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет программы `bind` с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq bind
```

Шаг 2

Перейдите в каталог, где находится пакет `bind-9.2.1-1.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

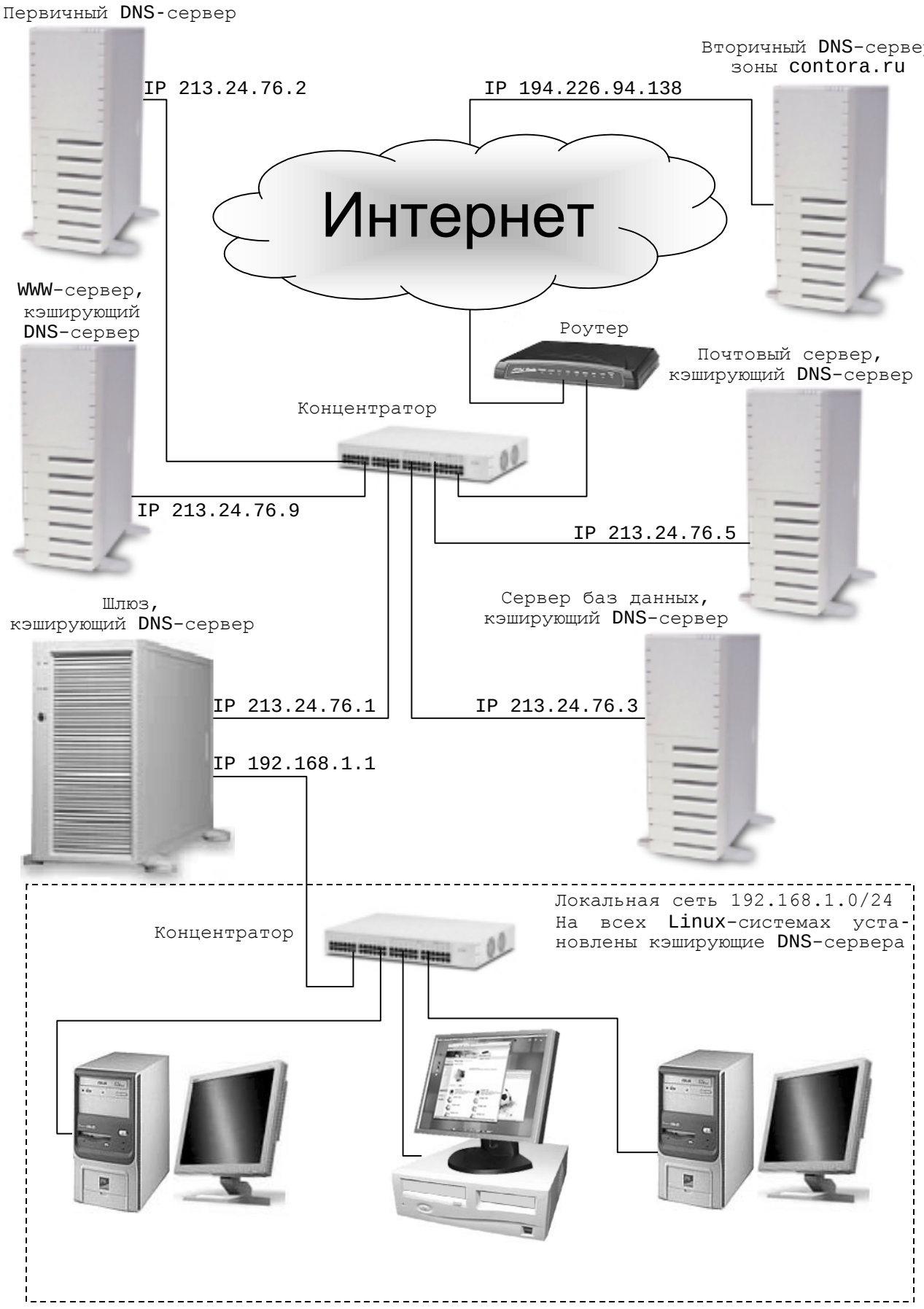


Рис. 23.1 Принципиальная схема организации службы DNS.

и установите:

```
 [root@drwalbr distrib]# rpm -ihv bind-utils-9.2.1-1.asp.i386.rpm
[root@drwalbr distrib]# rpm –ihv bind-9.2.1-1.asp.i386.rpm
```

или обновите пакет:

```
[root@drwalbr distrib]# rpm –Uhv bind-9.2.1-1.asp.i386.rpm
```

После установки пакета перейдите к настройке программы.

Компиляция, оптимизация и инсталляция ISC BIND

Для инсталляции ISC BIND из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Если вы собираетесь использовать ISC BIND с поддержкой протокола SSL, и на вашей системе не установлено программное обеспечение OpenSSL, установите его в соответствии с рекомендациями главы 12.

Шаг 3

Распакуйте архивы с исходными кодами ISC BIND в каталоге `/var/tmp`:

```
[root@drwalbr tmp]# tar xzpf bind-9.2.2.tar.gz
[root@drwalbr tmp]# cd bind-9.2.2
```

Шаг 4

Создайте специального пользователя `named`, от имени которого будет запускаться ISC BIND:

```
[root@drwalbr bind-9.2.2]# groupadd -g 25 named > /dev/null || :
[root@drwalbr bind-9.2.2]# useradd -u 25 -g 25  -s /bin/false -M -r -d
/var/named named > /dev/null 2>&1 || :
```

Шаг 5

Для добавления несуществующего командного интерпретатора добавьте в файл `/etc/shells` строку:

```
/bin/false/
```

Шаг 6

Для изменения используемых для хранения файлов `named.pid` и `lwresd.pid` в файле `/var/tmp/bind-9.2.2/bin/named/include/named/giobals.h` замените строку:

```
          "/run/named .pid");
```

на:

```
          "/run/named/named.pid");
```

Строку:

```
          "/run/lwresd.pid");
```

на:

```
          "/run/named/lwresd.pid");
```

Шаг 7

Отконфигурируйте исходные коды ISC BIND:

```
[root@drwalbr bind-9.2.2]# CFLAGS="-O2 -march=i686 -funroll-loops"; ex-
port CFLAGS
./configure \
--prefix=/usr \
--atedir=/var \
--mandir=/usr/share/man \
--with-openssl \
--with-libtool \
--disable-ipv6
```

Шаг 8

Откомпилируйте, проинсталлируйте ISC BIND, создайте и сохраните в надежном месте список установленных файлов:

```
[root@drwalbr bind-9.2.2]# make
[root@drwalbr bind-9.2.2]# find /* > /root/dns1
[root@drwalbr bind-9.2.2]# make install
[root@drwalbr bind-9.2.2]# strip /usr/sbin/named
[root@drwalbr bind-9.2.2]# mkdir -p /var/named
[root@drwalbr bind-9.2.2]# mkdir -p /var/run/named
[root@drwalbr bind-9.2.2]# install -c -m0600  bin/rndc/rndc.conf /etc/
[root@drwalbr bind-9.2.2]# chown named.named  /etc/rndc.conf
[root@drwalbr bind-9.2.2]# chown named.named  /var/named/
[root@drwalbr bind-9.2.2]# chown named.named  /var/run/named
[root@drwalbr bind-9.2.2]# /sbin/ldconfig
[root@drwalbr bind-9.2.2]# find /* > /root/dns2
[root@drwalbr bind-9.2.2]# diff /root/dns1  /root/dns2 >
/root/dns.installed
[root@drwalbr bind-9.2.2]# mv /root/dns.installed
/very_reliable_place/dns.installed.YYYYMMDD
```

Шаг 9

Удалите архивы и каталоги с исходными кодами программ:

```
[root@drwalbr /]# cd /var/tmp/
[root@drwalbr tmp]# rm -rf bind-9.2.2/
[root@drwalbr tmp]# rm -f bind-9.2.2.tar.gz
```

Конфигурирование ISC BIND

Конфигурирование ISC BIND осуществляется с использованием следующих файлов:

- основного конфигурационного файла `/etc/named.conf`;
- файла`/var/named/db.cache`, содержащего IP-адреса DNS-серверов, обслуживающих корневую зону;
- файлов зон `/var/named/db.*`;
- файлов обратных зон `/var/named/*.*.*.in-addr.arp`;
- системного конфигурационного файла `/etc/sysconfig/named`, необходимого для запуска ISC BIND в окружении chroot-jail.
- файла инициализации `/etc/init.d/named`, необходимого для запуска ISC BIND.

Конфигурирование ISC BIND в режиме кэширующего DNS-сервера

Кэширующий DNS-сервер не отвечает ни за какие зоны, кроме локальной, и предназначен для хранения и выдачи по запросам клиентов из локальной сети информации о соответствии имен IP-адресам и наоборот. При невозможности ответа на запрос клиента из-за отсутствия соответствующей информации в кэше, кэширующий DNS-сервер переадресовывает запрос соответствующим DNS-серверам, получает на него ответ и сохраняет полученную информацию в кэше. В последующем эта информация может быть использована при ответе на другие запросы.

Конфигурационный файл /etc/named.conf

Шаг 1

Создайте файл `/etc/named.conf`, руководствуясь своими потребностями и ниже приведенными рекомендациями:

```
// Authorized source addresses.
acl "trusted" {
        localhost;
};

// Known fake source addresses shouldn't be replied to.
acl "bogon" {
        0.0.0.0/8;
        1.0.0.0/8;
```

```
        2.0.0.0/8;
        192.0.2.0/24;
        224.0.0.0/3;
        169.254.0.0/16;
        // Enterprise networks may or may not be bogus.
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
};

options {
        directory "/var/named";
        allow-transfer { none; };
        allow-query { trusted; };
        allow-recursion { trusted; };
        blackhole { bogon; };
        tcp-clients 32;
        forwarders { 213.24.76.2; 194.226.94.138; };
        version "Hangry Bambr DNS v. 0.01";
};

logging {
        category lame-servers { null; };
};

// Root server hints
zone "." { type hint; file "db.cache"; };

// Provide a reverse mapping for the loopback address 127.0.0.1/24
zone "localhost" {
        type master;
        file "db.localhost";
        notify no;
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa";
        notify no;
};
```

где строки:

```
acl "trusted" {
          localhost;
};
```

определяют список контроля доступа с именем `trusted`, содержащий список хостов, которым в дальнейшем будет разрешено обращаться с запросами к DNS-серверу, обрабатывающему все разрешенные IP-адреса или имена хостов в нашей конфигурации. Для кэширующего DNS-сервера необходимо включить в список только `localhost`.

Строки:

```
acl "bogon" {
        0.0.0.0/8;
        1.0.0.0/8;
        2.0.0.0/8;
        192.0.2.0/24;
        224.0.0.0/3;
        169.254.0.0/16;
…
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
};
```

определяют список контроля доступа с именем `bogon`, содержащий список хостов, которым в дальнейшем будет запрещено обращаться с запросами к DNS-серверу. Вы можете дополнить этот список любыми адресами, с которых не желателен доступ к вашему серверу.

Директивы строки `options {}` определяют основные настройки сервера.

Строка:

```
directory "/var/named";
```

определяет путь к рабочему каталогу сервера.

Строка:

```
allow-transfer { none; };
```

определяет хосты, с которых разрешен перенос файлов зоны с конфигурируемого сервера. Значение ISC BIND, используемое по умолчанию, разрешает перенос файлов зон с любых хостов. Эта опция используется при конфигурировании вторичных DNS-серверов и в случае кэширующего DNS-сервера должна быть отключена.

Строка:

```
allow-query { trusted; };
```

разрешает обрабатывать запросы только от хостов, включенных в список контроля доступа с именем `trusted`.

Строка:

```
allow-recursion { trusted; };
```

разрешает обрабатывать рекурсивные запросы от хостов, включенных в список контроля доступа с именем `trusted`. Если вы используете настройку по умолчанию, которая разрешает обрабатывать рекурсивные запросы от всех хостов, ваш сервер, может быть подвергнут атаке типа «отравление кэша» (cache poisoning), при которой в кэш вашего сервера могут быть добавлены некорректные данные о соответствии имен IP-адресам.

Строка:

```
blackhole { bogon; };
```

запрещает обработку запросов от хостов, включенных в список контроля доступа с именем `bogon`.

Строка:

```
tcp-clients 32;
```

определяет максимальное число соединений, которое может быть одновременно установлено с конфигурируемым сервером.

Строка:

```
forwarders { 213.24.76.2; 194.226.94.138; };
```

определяет IP-адреса первичного и вторичного DNS-серверов, к которым обращается кэширующий DNS-сервер при отсутствии в его кэше необходимой клиенту информации.

Строка:

```
version "Hangry Bambr DNS v. 0.01";
```

позволяет переопределить описание версии используемого вами DNS-сервера.

Строки:

```
logging {
        category lame-servers { null; };
};
```

запрещают вносить в файлы регистрации сообщения вида:

```
lame server on 'domen.ru' (in 'dome.ru'?) x.x.x.x
```

обычно генерируемые при обращении к DNS-серверу, сконфигурированному как авторитетный для некоторой зоны, но таковым не являющимся.

Строка:

```
zone "." { type hint; file "db.cache"; };
```

определяет имя файла `db.cache`, содержащего IP-адреса серверов, обслуживающих корневую зону.

Строки:

```
zone "localhost" {
        type master;
        file "db.localhost";
        notify no;
};
```

и

```
zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa";
        notify no;
}; localhost
```

определяют файл зоны `db.localhost`, с помощью которого IP-адрес 127.0.0.1 преобразуется в имя `localhost`, и файл обратной зоны `0.0.127.in-addr.arpa`, с помощью которого имя `localhost` пре-

образуется в IP-адрес 127.0.0.1. При этом запрещается (`notify no`) перемещение файлов зоны и обратной зоны на другие (вторичные) DNS-сервера.

Шаг 2

Установите права доступа к файлу `/etc/named.conf` и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# chmod 600 /etc/named.conf
[root@drwalbr /]# chown named.named /etc/named.conf
```

Конфигурационный файл /var/named/db.cache

Шаг 1

Для получения последней версии файла выполните на системе, где уже установлена служба DNS, команду:

```
[root@drwalbr /]# dig @a.root-servers.net.ns > db.cache
```

Скопируйте этот файл в каталог `/var/named` с помощью утилиты `scp`, использование которой описано в конце главы. Если в вашем распоряжении нет системы с установленной службой DNS, воспользуйтесь приведенным ниже примером:

```
; <<>> DiG 9.2.2 <<>> @a.root-servers.net.ns
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61928
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.              IN  NS

;; ANSWER SECTION:
.       518400  IN  NS  D.ROOT-SERVERS.NET.
.       518400  IN  NS  A.ROOT-SERVERS.NET.
.       518400  IN  NS  H.ROOT-SERVERS.NET.
.       518400  IN  NS  C.ROOT-SERVERS.NET.
.       518400  IN  NS  G.ROOT-SERVERS.NET.
.       518400  IN  NS  F.ROOT-SERVERS.NET.
.       518400  IN  NS  B.ROOT-SERVERS.NET.
.       518400  IN  NS  J.ROOT-SERVERS.NET.
.       518400  IN  NS  K.ROOT-SERVERS.NET.
.       518400  IN  NS  L.ROOT-SERVERS.NET.
.       518400  IN  NS  M.ROOT-SERVERS.NET.
.       518400  IN  NS  I.ROOT-SERVERS.NET.
.       518400  IN  NS  E.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
D.ROOT-SERVERS.NET.  3600000  IN  A  128.8.10.90
A.ROOT-SERVERS.NET.  3600000  IN  A  198.41.0.4
H.ROOT-SERVERS.NET.  3600000  IN  A  128.63.2.53
C.ROOT-SERVERS.NET.  3600000  IN  A  192.33.4.12
G.ROOT-SERVERS.NET.  3600000  IN  A  192.112.36.4
F.ROOT-SERVERS.NET.  3600000  IN  A  192.5.5.241
B.ROOT-SERVERS.NET.  3600000  IN  A  128.9.0.107
J.ROOT-SERVERS.NET.  3600000  IN  A  192.58.128.30
K.ROOT-SERVERS.NET.  3600000  IN  A  193.0.14.129
L.ROOT-SERVERS.NET.  3600000  IN  A  198.32.64.12
M.ROOT-SERVERS.NET.  3600000  IN  A  202.12.27.33
I.ROOT-SERVERS.NET.  3600000  IN  A  192.36.148.17
E.ROOT-SERVERS.NET.  3600000  IN  A  192.203.230.10

;; Query time: 143 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net)
;; WHEN: Fri May  9 08:22:18 2003
;; MSG SIZE  rcvd: 436
```

ЗАМЕЧАНИЕ Если вы воспользовались нашим примером конфигурационного файла, не забудьте обновить его сразу же после запуска DNS-сервера.

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# chmod 600 /etc/db.cache
[root@drwalbr /]# chown named.named /etc/db.cache
```

ЗАМЕЧАНИЕ В последующем, примерно два раза в год, обновляйте файл `/etc/db.cache` на всех DNS-серверах.

Конфигурационный файл зоны localhost /var/named/db.localhost

Шаг 1

Создайте файл `db.localhost`, содержащий следующие строки:

```
$TTL 86400
@               IN      SOA     localhost. root.localhost. (
                                00      ; Serial
                                10800   ; Refresh after 3 hours
                                3600    ; Retry after 1 hour
                                604800  ; Expire after 1 week
                                86400 ) ; Minimum

                IN      NS      localhost.

localhost       IN      A       127.0.0.1
```

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# chmod 644 /var/named/db.localhost
[root@drwalbr /]# chown named.named /var/named/db.localhost
```

Конфигурационный файл обратной зоны /var/named/0.0.127.in-addr.arpa

Шаг 1

Создайте файл `0.0.127.in-addr.arpa`, содержащий следующие строки:

```
$TTL 86400
@       IN      SOA     localhost. root.localhost. (
                                00      ; Serial
                                10800   ; Refresh after 3 hours
                                3600    ; Retry after 1 hour
                                604800  ; Expire after 1 week
                                86400 ) ; Minimum

        IN      NS      localhost.
1   IN  PTR  localhost.
```

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# chmod 644 /var/named/0.0.127.in-addr.arpa
[root@drwalbr /]# chown named.named /var/named/0.0.127.in-addr.arpa
```

Системный конфигурационный файл /etc/sysconfig/named

Шаг 1

Если вы собираетесь запускать ISC BIND в окружении chroot-jail, создайте файл `/etc/sysconfig/named`, содержащий следующие строки:

```
#This option will run named in a chroot environment.
#ROOTDIR="/chroot/named/"
# These additional options will be passed to named at startup.
# Don't add -t here, use ROOTDIR instead.
#OPTIONS=""
```

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя named из группы named:

```
[root@drwalbr /]# chmod /etc/sysconfig/named
[root@drwalbr /]# chown named.named /etc/sysconfig/named
```

Файл инициализации /etc/init.d/named

Шаг 1

Создайте инициализационный файл /etc/init.d/named, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping named.
#
# chkconfig: 2345 55 45
# description: Named (BIND) is a Domain Name Server (DNS) that is used \
#              to resolve host names to IP addresses.
#
# processname: named

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/named ] ; then
        . /etc/sysconfig/named
fi

# Check that networking is up.
[ "${NETWORKING}" = "no" ] && exit 0

# If Named is not available stop now.
[ -f /usr/sbin/named ] || exit 0
[ -f "${ROOTDIR}"/etc/named.conf ] || exit 0

# Path to the Named binary.
named=/usr/sbin/named

RETVAL=0
prog="Named"

start() {
        echo -n $"Starting $prog: "
        if [ -n "${ROOTDIR}" -a "x${ROOTDIR}" != "x/" ]; then
                OPTIONS="${OPTIONS} -t ${ROOTDIR}"
        fi
        daemon $named -u named ${OPTIONS}
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/named
        return $RETVAL
}

stop() {
```

```
        echo -n $"Shutting down $prog: "
        killproc $named
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/named
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $named
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/named ]; then
                stop
                start
                RETVAL=$?
        fi
        ;;
  reload)
        /usr/sbin/rndc reload >/dev/null 2>&1 || /usr/bin/killall -HUP
$named
        return $RETVAL
        ;;
  probe)
        /usr/sbin/rndc reload >/dev/null 2>&1 || echo start
        return $RETVAL
        ;;
  *)
        echo $"Usage: $0
{start|stop|status|restart|condrestart|reload|probe}"
        exit 1
esac
exit $RETVAL
```

Шаг 2

Сделайте файл исполняемым и определите его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 700 /etc/init.d/named
[root@drwalbr /]# chown 0.0 /etc/init.d/named
```

Для автоматического запуска ISC BIND при загрузке системы создайте необходимые ссылки:

```
[root@drwalbr /]# chkconfig --add named
[root@drwalbr /]# chkconfig --level 2345 named on
```

Конфигурирование ISC BIND в режиме первичного DNS-сервера

Для каждой зоны существует один и только один первичный DNS-сервер, на котором администратор зоны создает файл описания зоны, являющийся первоисточником для всех вторичных серверов. Все остальные серверы только копируют информацию с первичного сервера. Настройку первичного DNS-сервера рассмотрим на примере первичного DNS-сервера, отвечающего за зону `contora.ru`.

Конфигурационные файлы /var/named/db.cache, /var/named/db.localhost, /var/named/0.0.127.in-addr.arpa, /etc/sysconfig/named и /etc/init.d/named

Конфигурация файлов `/var/named/db.cache`, `/var/named/db.localhost`, `/var/named/0.0.127.in-addr.arpa`, `/etc/sysconfig/named` и `/etc/init.d/named` идентична описанной выше конфигурации файлов для кэширующего DNS-сервера.

Конфигурационный файл /etc/named.conf

Шаг 1

Создайте файл `/etc/named.conf`, руководствуясь своими потребностями и ниже приведенными рекомендациями:

```
// Authorized source addresses.
acl "trusted" {
        localhost;
        192.168.1.0/24;
        213.24.76.0/24;
};

// Known fake source addresses shouldn't be replied to.
acl "bogon" {
        0.0.0.0/8;
        1.0.0.0/8;
        2.0.0.0/8;
        192.0.2.0/24;
        224.0.0.0/3;
        169.254.0.0/16;
        // Enterprise networks may or may not be bogus.
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
};

options {
        directory "/var/named";
        allow-transfer { 194.226.76.138 ; };
        allow-query { trusted; };
        allow-recursion { trusted; };
        blackhole { bogon; };
        tcp-clients 1024;
        forwarders { none; };
        version "Hangry Bambr DNS v. 0.01";
};

logging {
        category lame-servers { null; };
};

// Root server hints
zone "." { type hint; file "db.cache"; };

// Provide a reverse mapping for the loopback address 127.0.0.1/24
zone "localhost" {
        type master;
        file "db.localhost";
        notify no;
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa";
        notify no;
};
```

```
// We are the master server for contora.ru
zone "contora.ru" {
        type master;
        file "db.contora";
        allow-query { any; };
};

// Provide a reverse mapping for domains network 213.24.76.0/24
zone "76.24.213.in-addr.arpa" {
        type master;
        file "76.24.213.in-addr.arpa";
        allow-query { any; };
};
```

где строки:

```
acl "trusted" {
        localhost;
        192.168.1.0/24;
        213.24.76.0/24;
};
```

определяют (расширяют по отношению к приведенному выше примеру, используемого для кэширующего DNS-сервера) список контроля доступа с именем `trusted`, содержащий список хостов, которым в дальнейшем будет разрешено обращаться с запросами к DNS-серверу, который обрабатывает все разрешенные IP-адреса или имена хостов в нашей конфигурации. Для первичного DNS-сервера необходимо включить в список только `localhost`, локальную сеть организации и находящиеся в Интернет системы организации.

Строка:

```
allow-transfer { 194.226.76.138 ; };
```

определяет IP-адреса систем, которым разрешено копировать файлы зон первичного сервера. Здесь необходимо указать только IP-адреса вторичных DNS-серверов. По умолчанию ISC BIND разрешает копировать файлы зон на любые системы с любыми IP-адресами. В рассматриваемом примере, где организация имеет единственный вторичный DNS-сервер с IP-адресом 194.226.76.138, перенос файлов зон разрешен только на этот сервер.

ЗАМЕЧАНИЕ Это очень важная настройка, т. к. затрудняет получение информации об IP-адресах и именах систем организации как в Интернет, так и локальной сети организации, необходимой для спамеров и злоумышленников, использующих для своих целей пакеты с фальсифицированными IP-адресами.

Строка:

```
tcp-clients 1024;
```

определяет максимально возможное число клиентских TCP-соединений, которое может быть одновременно установлено с DNS-сервером.

Строка:

```
forwarders { none; };
```

запрещает перенаправление запросов, касающихся зоны `contora.ru` на другие сервера. Конфигурируемый сервер является наиболее авторитетным источником информации о зоне `contora.ru` и нет никакой необходимости в переадресации запросов об этой зоне к другим серверам.

Строки:

```
zone "contora.ru" {
        type master;
        file "db.contora";
        allow-query { any; };
};
```

конфигурируют сервер в качестве первичного DNS-сервера для зоны `contora.ru`.

В рассматриваемом примере строка:

```
zone "contora.ru" {
```

определяет зону, в которой сервер является авторитетным.

Строка:

```
type master;
```

определяет сервер в качестве первичного.

Строка:

```
file "db.contora";
```

указывает, что файл зоны, содержащей таблицу соответствия, используемую для преобразования имен систем в IP-адреса, находится в файле `db.contora`.

ЗАМЕЧАНИЕ Файл зоны, в принципе, может иметь любое имя, однако для удобства желательно, чтобы его название имело смысловую связь с названием зоны.

Строка:
```
allow-query { any; };
```
разрешает отвечать на запросы клиентов о соответствии IP-адресов именам систем в зоне `contora.ru` для клиентов с любых IP-адресов.

Строки:
```
zone "76.24.213.in-addr.arpa" {
        type master;
        file "76.24.213.in-addr.arpa";
        allow-query { any; };
};
```
определяют конфигурируемый сервер в качестве первичного для обратной зоны.

В рассматриваемом примере строка:
```
zone "76.24.213.in-addr.arpa" {
```
определяет обратную зону, в которой сервер является авторитетным.

Строка:
```
type master;
```
определяет сервер в качестве первичного.

Строка:
```
file "76.24.213.in-addr.arpa";
```
указывает, что файл обратной зоны, содержащей таблицу соответствия, используемую для преобразования имен систем в IP-адреса, находится в файле `76.24.213.in-addr.arpa`;

Строка:
```
allow-query { any; };
```
разрешает отвечать на запросы клиентов о соответствии имен систем IP-адресам в зоне `contora.ru` для клиентов с любых IP-адресов.

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя `named` из группы `named`:
```
[root@drwalbr /]# chmod 600 /etc/named.conf
[root@drwalbr /]# chown named.named /etc/named.conf
```

Конфигурационный файл зоны /var/named/db.contora

Шаг 1

Создайте файл зоны `/var/named/db.contora`, руководствуясь приведенным ниже рекомендациями и вашими потребностями:
```
;Configuration for primary nameserver
;$ORIGIN      contora.ru
$TTL 172800
@  IN  SOA  ns1.contora.ru. admin.contora.ru.  (
                                    2003051801 ; Serial
                                    10800      ; Refresh after 3 hours
                                    3600       ; Retry after 1 hour
                                    604800     ; Expire after 1 week
                                    172800 )   ; Minimum TTL of 2 days

; Name Servers (NS) records.
;
        IN      NS      ns1.contora.ru.
        IN      NS      ns2.contora.ru.

; Mail Exchange (MX) records.
;
        MX      0       mail1.contora.ru.



; Addresses for the canonical names (A) records.
```

```
;
localhost       IN      A       127.0.0.1
gateway         IN      A       213.24.76.1
www             IN      A       213.24.76.9
beta            IN      CNAME   www
db              IN      A       213.24.76.3
mail1           IN      A       213.24.76.5
```

Все записи в файле имеют формат вида:

```
[domain] [opt_ttl] [opt_class] [type] [data]
```

где:

`[domain]` – имена домена или системы, текущий домен обозначается символом "`@`", если имя не указано, то оно берется из предыдущей строки;

`[opt_ttl]` – время жизни записи в секундах;

`[opt_class]` – тип адреса, в настоящее время используется только один тип – `IN`;

`[type]` – тип записи;

`[data]` – данные соответствующего типа.

Файл зоны должен начинаться с описания зоны ответственности – записи типа SOA (Start Of Authorizing), в рассматриваемом примере:

```
@  IN  SOA  ns1.contora.ru. admin.contora.ru.  (
                                    2003051801 ; Serial
                                    10800      ; Refresh after 3 hours
                                    3600       ; Retry after 1 hour
                                    604800     ; Expire after 1 week
                                    172800 )   ; Minimum TTL of 2 days
```

В этой записи для текущего домена `@` – т. е. `contora.ru` – определяются:

- `ns1.contora.ru.` – имя первичного DNS-сервера. Символ точка на конце является обязательным и означает, что к описанию домена не следует добавлять ничего, например, имя текущего домена;
- `admin.contora.ru.` – адрес электронной почты администратора DNS-сервера, в котором символ "`@`" заменен на "`.`";
- `2003051801 ; Serial` – серийный номер, с помощью которого вторичные DNS-сервера получают информацию об изменении файла зоны;
- `10800 ; Refresh after 3 hours` – длительность интервала времени, измеряемого в секундах, по истечении которого вторичный сервер должен обновлять файл зоны;
- `3600 ; Retry after 1 hour` – длительность интервала времени, измеряемого в секундах, по истечении которого в случае неудачной попытки обновления файла зоны осуществляется его повторное обновление;
- `604800 ; Expire after 1 week` – длительность интервала времени отсутствия связи с первичным сервером, измеряемого в секундах, по истечении которого вторичный сервер уничтожает файл зоны;
- `172800 ) ; Minimum TTL of 2 days` – минимальное время жизни записей в файле зоны, измеряемого в секундах.

ЗАМЕЧАНИЕ В каждой последующей редакции файла серийный номер должен быть больше предыдущего.

Строки:

```
IN      NS      ns1.contora.ru.
IN      NS      ns2.contora.ru.
```

определяют имена первичного и вторичного DNS-серверов;

Строка:

```
MX      0       mail.contora.ru.
```

определяет сервер, на который пересылается почта, адресованная на почтовые адреса данного домена. Значение 0 определяет приоритет сервера. В принципе, для получения почты домена может использоваться несколько серверов. В этом случае при выходе из строя основного сервера, имеющего более высокий приоритет, почта будет пересылаться на резервный сервер и при первой возможности – на основной. Подобная конфигурация может быть реализована с помощью записей вида:

```
MX     10       mail1.contora.ru.
MX     50       smtp.drygayacontora.ru.
```

Значение приоритета варьируется в диапазоне от 0 до 32767, причем значение 0 соответствует самому высокому приоритету. Поэтому в рассматриваемом примере сначала будет осуществляется попытка доставки почты на `mail.contora.ru`, а в случае невозможности – на `smtp.drygayacontora.gov`.

В строках:

```
localhost       IN      A       127.0.0.1
gateway         IN      A       213.24.76.1
www             IN      A       213.24.76.9
beta            IN      CNAME   www
db              IN      A       213.24.76.3
mail1           IN      A       213.24.76.5
```

записи типа A устанавливают соответствия между именами систем и IP-адресами в зоне `contora.ru`. Так, например, строка:

```
www             IN      A       213.24.76.9
```

ставит в соответствие имени `www.contora.ru` IP-адрес 213.24.76.9.

Записи типа CNAME предназначены для присвоения дополнительных имен (алиасов). Например, строка:

```
dymatel         IN     CNAME    www
```

ставит в соответствие имени `dymatel.contora.ru` IP-адрес 213.24.76.9, соответствующий также имени `www.contora.ru`.

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# chmod 644 /var/named/db.contora
[root@drwalbr /]# chown named.named /var/named/db.contora
```

Конфигурационный файл обратной зоны /var/named/76.24.213.in-addr.arpa

Шаг 1

Создайте файл зоны `/var/named/76.24.213.in-addr.arpa`, руководствуясь приведенным ниже рекомендациями и вашими потребностями:

```
;Configuration for primary nameserver
;$ORIGIN 76.24.213.in-addr.arpa.
$TTL 172800
@  IN  SOA  ns1.contora.ru. admin.contora.ru.  (
                                  2003051801 ; Serial
                                  10800      ; Refresh after 3 hours
                                  3600       ; Retry after 1 hour
                                  604800     ; Expire after 1 week
                                  172800 )   ; Minimum TTL of 2 days


; Name Servers (NS) records.
;
                  IN      NS      ns1.contora.ru.
                  IN      NS      ns2.contora.ru.

; Addresses Point to Canonical Names (PTR) for Reverse lookups
;
1                 IN      PTR     gateway.contora.ru.
9                 IN      PTR     www.contora.ru.
3                 IN      PTR     db.contora.ru.
5                 IN      PTR     mail1.contora.ru.
```

Записи типа PTR устанавливают соответствие между IP-адресами и именами систем. При этом в начале записи находится последнее число в IP-адресе, например, для IP-адреса 213.24.76.9, соответствующего имени `www.contora.ru`, в начале записи указывается "9".

ЗАМЕЧАНИЕ Важно чтобы данные, содержащиеся в файле зоны и соответствующему ему файле обратной зоны, не противоречили друг другу. В противном случае результаты могут оказаться непредсказуемыми.

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# chmod 644 /var/named/76.24.213.in-addr.arpa
[root@drwalbr /]# chown named.named /var/named/76.24.213.in-addr.arpa
```

Конфигурирование ISC BIND в режиме вторичного DNS-сервера

Вторичный DNS-сервер используется для повышения надежности службы DNS и снижения загрузки первичного DNS-сервера. Вторичный DNS-сервер периодически загружает файлы зон и обратных зон с первичного или других вторичных DNS-серверов. Этот процесс называют переносом. Настройку вторичного DNS-сервера рассмотрим на примере вторичного DNS сервера отвечающего за зону `contora.ru`.

Шаг 1

Создайте файл `/etc/named.conf`, руководствуясь своими потребностями и ниже приведенными рекомендациями:

```
// Authorized source addresses.
acl "trusted" {
        localhost;
        192.168.1.0/24;
        213.24.76.0/24;

// Known fake source addresses shouldn't be replied to.
acl "bogon" {
        0.0.0.0/8;
        1.0.0.0/8;
        2.0.0.0/8;
        192.0.2.0/24;
        224.0.0.0/3;
        169.254.0.0/16;
        // Enterprise networks may or may not be bogus.
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
};

options {
        directory "/var/named";
        allow-transfer { none; };
        allow-query { trusted; };
        allow-recursion { trusted; };
        blackhole { bogon; };
        tcp-clients 1024;
        forwarders { none; };
        version "Hangry Bambr DNS v. 0.01";
};

logging {
        category lame-servers { null; };
};

// Root server hints
zone "." { type hint; file "db.cache"; };

// Provide a reverse mapping for the loopback address 127.0.0.1/24
zone "localhost" {
        type master;
        file "db.localhost";
        notify no;
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa";
```

```
        notify no;
};

// We are the slave server for contora.ru
zone "contora.ru" {
        type slave;
        file "db.contora";
        masters { 213.24.76.2; };
        allow-query { any; };
};

// Provide a reverse mapping for domains network 213.24.76.0/24
zone "76.24.213.in-addr.arpa" {
        type slave;
        file "76.24.213.in-addr.arpa";
        masters { 213.24.76.2; };
        allow-query { any; };
};
```

Предлагаемый пример конфигурационного файла аналогичен файлу, используемому при конфигурировании первичного DNS-сервера. Отличием является определение в строках:

```
type slave;
```

конфигурируемого сервера в качестве вторичного для зоны и обратной зоны;

и в строках:

```
masters { 213.24.76.2; };
```

указывающих на IP-адрес первичного DNS-сервера.

Шаг 2

Установите права доступа к файлу и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# chmod 600 /etc/named.conf
[root@drwalbr /]# chown named.named /etc/named.conf
```

Конфигурационные файлы /var/named/db.cache, /var/named/db.localhost, /var/named/0.0.127.in-addr.arpa, /etc/sysconfig/named и /etc/init.d/named

Конфигурация файлов `/var/named/db.cache`, `/var/named/db.localhost`, `/var/named/0.0.127.in-addr.arpa`, `/etc/sysconfig/named` и `/etc/init.d/named` идентична описанной выше конфигурации файлов для кэширующего и первичного DNS-серверов.

Обеспечение безопасности транзакций для ISC BIND с использованием TSIG

Механизм подписи транзакций (Transaction Signature, TSIG), используемый в ISC BIND версии 9, позволяет проверять подлинность транзакций. Например, установить, что запрос на перенос зоны поступает действительно от вторичного сервера, а не злоумышленника, пытающегося путем переноса файла зоны DNS-сервера получить информацию, необходимую для подготовки атаки на вашу сеть. Если вы хотите повысить безопасность службы DNS с использованием механизма TSIG, установите на первичном и вторичном DNS-серверах поддержку механизма подписи транзакций.

Для включения поддержки TSIG необходимо выполнить следующие операции.

Шаг 1

На одном из серверов сгенерируйте ключ для первичного и вторичного DNS-серверов:

```
[root@drwalbr /]# dnssec-keygen -a hmac-md5 -b 128 -n HOST ns1-ns2
Kns1-ns2.+157+40221
```

В результате выполнения следующей команды будет сгенерирован и сохранен в файле `Kns1-ns2.+157+40221.private` 128-битный HMAC-MD5 ключ:

```
[root@drwalbr /]# cat Kns1-ns2.+157+40221.private
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: 2rhwwM2En/n5KScRtssAbA==
```

Ключ, в рассматриваемом примере выделенный жирным шрифтом, впоследствии используется в конфигурационных файлах `/etc/named.conf` на первичном и вторичном DNS-серверах. На паре взаимодействующих серверов используется один и тот же ключ.

Шаг 2

Внесите изменения в файл `/etc/named.conf` в соответствии с вашими потребностями и приводимыми ниже рекомендациями.

Для первичного DNS-сервера:

```
// Authorized source addresses.
acl "trusted" {
        localhost;
        192.168.1.0/24;
        213.24.76.0/24;
};

// Known fake source addresses shouldn't be replied to.
acl "bogon" {
        0.0.0.0/8;
        1.0.0.0/8;
        2.0.0.0/8;
        192.0.2.0/24;
        224.0.0.0/3;
        169.254.0.0/16;
        // Enterprise networks may or may not be bogus.
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
};

key "ns1-ns2" {
        algorithm hmac-md5;
        secret "2rhwwM2En/n5KScRtssAbA==";
};

server 194.226.76.0 {
        keys {"ns1-ns2";}
};

options {
        directory "/var/named";
        allow-transfer { key ns1-ns2; };
        allow-query { trusted; };
        allow-recursion { trusted; };
        blackhole { bogon; };
        tcp-clients 1024;
        forwarders { none; };
        version "Hangry Bambr DNS v. 0.01";
};

logging {
        category lame-servers { null; };
};

// Root server hints
zone "." { type hint; file "db.cache"; };

// Provide a reverse mapping for the loopback address 127.0.0.1/24
zone "localhost" {
        type master;
        file "db.localhost";
        notify no;
};

zone "0.0.127.in-addr.arpa" {
```

```
        type master;
        file "0.0.127.in-addr.arpa";
        notify no;
};

// We are the master server for contora.ru
zone "contora.ru" {
        type master;
        file "db.contora";
        allow-query { any; };
};

// Provide a reverse mapping for domains network 213.24.76.0/24
zone "76.24.213.in-addr.arpa" {
        type master;
        file "76.24.213.in-addr.arpa";
        allow-query { any; };
};
```

Для вторичного DNS-сервера:

```
// Authorized source addresses.
acl "trusted" {
        localhost;
        192.168.1.0/24;
        213.24.76.0/24;

// Known fake source addresses shouldn't be replied to.
acl "bogon" {
        0.0.0.0/8;
        1.0.0.0/8;
        2.0.0.0/8;
        192.0.2.0/24;
        224.0.0.0/3;
        169.254.0.0/16;
        // Enterprise networks may or may not be bogus.
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
};

key "ns1-ns2" {
        algorithm hmac-md5;
        secret "2rhwwM2En/n5KScRtssAbA==";
};

server 213.24.76.2 {
        keys {"ns1-ns2";}
};


options {
        directory "/var/named";
        allow-transfer { none; };
        allow-query { trusted; };
        allow-recursion { trusted; };
        blackhole { bogon; };
        tcp-clients 1024;
        forwarders { none; };
        version "Hangry Bambr DNS v. 0.01";
};

logging {
        category lame-servers { null; };
};
```

```
// Root server hints
zone "." { type hint; file "db.cache"; };

// Provide a reverse mapping for the loopback address 127.0.0.1/24
zone "localhost" {
        type master;
        file "db.localhost";
        notify no;
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa";
        notify no;
};

// We are the slave server for contora.ru
zone "contora.ru" {
        type slave;
        file "db.contora";
        masters { 213.24.76.2; };
        allow-query { any; };
};

// Provide a reverse mapping for domains network 213.24.76.0/24
zone "76.24.213.in-addr.arpa" {
        type slave;
        file "76.24.213.in-addr.arpa";
        masters { 213.24.76.2; };
        allow-query { any; };
};
```

Шаг 3

Удалите файлы `Kns1-ns2.+157+40221.key` и `Kns1-ns2.+157+40221.private`, созданные при генерации ключа:

```
[root@drwalbr /]# rm -f Kns1-ns2.+157+40221.key
[root@drwalbr /]# rm -f Kns1-ns2.+157+40221.private.private
```

Использование TSIG для безопасного администрирования ISC BIND с использованием утилиты rndc

Утилита `rndc` предназначена для управления сервером ISC BIND. Если вы хотите использовать эту утилиту для администрирования DNS-сервера с поддержкой TSIG, вам необходимо внести соответствующие изменения в конфигурационный файл утилиты `rndc` – `/etc/rndc.conf` и главный конфигурационный файл DNS-сервера – `/etc/named.conf`. Для этого необходимо выполнить следующие операции.

Шаг 1

Сгенерируйте ключ:

```
[root@drwalbr /]# dnssec-keygen -a hmac-md5 -b 128 -n user rndc
Krndc.+157+45611
```

В результате выполнения следующей команды будет сгенерирован и сохранен в файле `Krndc.+157+45611.private` 128-битный HMAC-MD5 ключ:

```
[root@drwalbr /]# cat Krndc.+157+45611.private
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: erNkIU6wLgAfd7XZdfKiO==
```

Ключ, в рассматриваемом примере выделенный жирным шрифтом, используется утилитой `rndc` и должен быть добавлен в конфигурационные файлы `/etc/rndc.conf` и `/etc/named.conf`.

Шаг 2

Вставьте в файл /etc/rndc.conf ключ, сгенерированный на предыдущем шаге:

```
options {
        default-server  localhost;
        default-key     "key";
};

server localhost {
        key     "key";
};

key "key" {
        algorithm       hmac-md5;
        secret "erNkIU6wLgAfd7XZdfKiO==";
};
```

Шаг 3

Отредактируйте файл /etc/named.conf в соответствии с вашими требованиями и ниже приведенными рекомендациями (в рассматриваемом примере в качестве исходного используется файл для первичного DNS-сервера):

```
// Authorized source addresses.
acl "trusted" {
        localhost;
        192.168.1.0/24;
        213.24.76.0/24;
};

// Known fake source addresses shouldn't be replied to.
acl "bogon" {
        0.0.0.0/8;
        1.0.0.0/8;
        2.0.0.0/8;
        192.0.2.0/24;
        224.0.0.0/3;
        169.254.0.0/16;
        // Enterprise networks may or may not be bogus.
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
};
key "key" {
algorithm hmac-md5;
secret "erNkIU6wLgAfd7XZdfKiO==";
};
controls {
inet 127.0.0.1 allow { localhost; } keys { "key"; };
};

key "ns1-ns2" {
        algorithm hmac-md5;
        secret "2rhwwM2En/n5KScRtssAbA==";
};

server 194.226.76.0 {
        keys {"ns1-ns2";}
};

options {
        directory "/var/named";
        allow-transfer { key ns1-ns2; };
        allow-query { trusted; };
        allow-recursion { trusted; };
        blackhole { bogon; };
        tcp-clients 1024;
        forwarders { none; };
```

```
        version "Hangry Bambr DNS v. 0.01";
};

logging {
        category lame-servers { null; };
};

// Root server hints
zone "." { type hint; file "db.cache"; };

// Provide a reverse mapping for the loopback address 127.0.0.1/24
zone "localhost" {
        type master;
        file "db.localhost";
        notify no;
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa";
        notify no;
};

// We are the master server for contora.ru
zone "contora.ru" {
        type master;
        file "db.contora";
        allow-query { any; };
};

// Provide a reverse mapping for domains network 213.24.76.0/24
zone "76.24.213.in-addr.arpa" {
        type master;
        file "76.24.213.in-addr.arpa";
        allow-query { any; };
};
```

Шаг 4

Удалите файлы `Krndc.+157+45611.key` и `Krndc.+157+45611.private`, созданные при генерации ключа:

```
[root@drwalbr /]# rm -f Krndc.+157+45611.key
[root@drwalbr /]# rm -f Krndc.+157+45611.private
```

Тестирование и администрирование ISC BIND

Шаг 1

Запустите ISC BIND:

```
[root@drwalbr /]# /etc/init.d/named start
Запускается Named:                         [OK]
```

Шаг 2

Проверьте работоспособность вашего DNS-сервера с использованием утилиты `dig`:

```
[root@drwalbr /]# dig @nsl.contora.ru
; <<>> DiG 9.2.2 <<>> @ns1.contora.ru
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19554
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.            IN   NS

;; ANSWER SECTION:
```

```
.          341774   IN   NS   G.ROOT-SERVERS.NET.
.          341774   IN   NS   H.ROOT-SERVERS.NET.
.          341774   IN   NS   I.ROOT-SERVERS.NET.
.          341774   IN   NS   J.ROOT-SERVERS.NET.
.          341774   IN   NS   K.ROOT-SERVERS.NET.
.          341774   IN   NS   L.ROOT-SERVERS.NET.
.          341774   IN   NS   M.ROOT-SERVERS.NET.
.          341774   IN   NS   A.ROOT-SERVERS.NET.
.          341774   IN   NS   B.ROOT-SERVERS.NET.
.          341774   IN   NS   C.ROOT-SERVERS.NET.
.          341774   IN   NS   D.ROOT-SERVERS.NET.
.          341774   IN   NS   E.ROOT-SERVERS.NET.
.          341774   IN   NS   F.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
G.ROOT-SERVERS.NET.   428174   IN   A   192.112.36.4
H.ROOT-SERVERS.NET.   428174   IN   A   128.63.2.53
I.ROOT-SERVERS.NET.   428174   IN   A   192.36.148.17
J.ROOT-SERVERS.NET.   428174   IN   A   192.58.128.30
K.ROOT-SERVERS.NET.   428174   IN   A   193.0.14.129
L.ROOT-SERVERS.NET.   428174   IN   A   198.32.64.12
M.ROOT-SERVERS.NET.   428174   IN   A   202.12.27.33
A.ROOT-SERVERS.NET.   428174   IN   A   198.41.0.4
B.ROOT-SERVERS.NET.   428174   IN   A   128.9.0.107
C.ROOT-SERVERS.NET.   428174   IN   A   192.33.4.12
D.ROOT-SERVERS.NET.   428174   IN   A   128.8.10.90
E.ROOT-SERVERS.NET.   428174   IN   A   192.203.230.10
F.ROOT-SERVERS.NET.   428174   IN   A   192.5.5.241

;; Query time: 15 msec
;; SERVER: 213.24.76.2#53(ns1.contora.ru)
;; WHEN: Thu May 22 15:04:36 2003
;; MSG SIZE  rcvd: 436
```

Шаг 3

Проверьте наличие возможности администрирования DNS-сервера с использованием утилиты `rndc`. Для получения информации о возможностях утилиты используйте команду:

```
[root@drwalbr /]# rndc
command is one of the following:

  reload        Reload configuration file and zones.
  reload zone [class [view]]
                Reload a single zone.
  refresh zone [class [view]]
                Schedule immediate maintenance for a zone.
  reconfig      Reload configuration file and new zones only.
  stats         Write server statistics to the statistics file.
  querylog      Toggle query logging.
  dumpdb        Dump cache(s) to the dump file (named_dump.db).
  stop          Save pending updates to master files and stop the server.
  halt          Stop the server without saving pending updates.
  trace         Increment debugging level by one.
  trace level   Change the debugging level.
  notrace       Set debugging level to 0.
  flush         Flushes all of the server's caches.
  flush [view]  Flushes the server's cache for a view.
  status        Display status of the server.
  *restart      Restart the server.

* == not yet implemented
Version: 9.2.2
```

Шаг 4

Попробуйте узнать IP-адреса хостов, находящиеся в зоне ответственности вашего DNS-сервера:

```
[root@drwalbr /]# nslookup -sil www.contora.ru
Server:         213.24.76.2
Address:        213.24.76.2#53

www.contora.ru
Name:   www.contora.ru
Address: 212.111.78.9
```

и за её пределами:

```
[root@drwalbr /]# nslookup -sil www.bruy.info
Server:         213.24.76.2
Address:        213.24.76.2#53

Non-authoritative answer:
Name:   www.bruy.info
Address: 212.24.38.75
```

Шаг 5

Попробуйте получить информацию о записях, соответствующих почтовым серверам в файлах зоны вашего DNS-сервера с использованием утилиты `host`:

```
[host@drwalbr /]# host -t MX contora.ru
contora.ru mail is handled by 1 mail1.contora.ru.
```

Для получения информации о возможностях утилиты используйте команду:

```
[root@drwalbr /]# host
Usage: host [-aCdlrTwv] [-c class] [-n] [-N ndots] [-t type] [-W time]
            [-R number] hostname [server]
       -a is equivalent to -v -t *
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -l lists all hosts in a domain, using AXFR
       -n Use the nibble form of IPv6 reverse lookup
       -N changes the number of dots allowed before root lookup is done
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -t specifies the query type
       -T enables TCP/IP mode
       -v enables verbose output
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
```

Выполнение ISC BIND в среде chroot-jail

Потенциальные уязвимости ISC BIND, как и любого другого программного обеспечения, могут использоваться для реализации атак на вашу систему. Поэтому для повышения безопасности системы рекомендуется выполнять ISC BIND в окружении chroot-jail. Для этого необходимо выполнить следующие операции.

Шаг 1

Создайте каталоги, необходимые для размещения файлов ISC BIND в окружении chroot-jail:

```
[root@drwalbr /]# mkdir -p /chroot/named/etc
[root@drwalbr /]# mkdir -p /chroot/named/dev
[root@drwalbr /]# mkdir -p /chroot/named/var/run/named
[root@drwalbr /]# mkdir -p /chroot/named/var/named
[root@drwalbr /]# chown -R named.named /chroot/named/etc
[root@drwalbr /]# chown -R named.named /chroot/named/dev
[root@drwalbr /]# chown -R named.named /chroot/named/var/run/named
[root@drwalbr /]# chown -R named.named /chroot/named/var/named
```

ЗАМЕЧАНИЕ Для повышения безопасности вашей системы каталог `/chroot/named/` рекомендуется размещать на отдельном разделе диска.

Шаг 2

Переместите конфигурационные файлы ISC BIND в соответствующие подкаталоги окружения chroot-jail, создайте файл устройства `random`, установите права доступа к файлам и назначьте владельцем файла пользователя `named` из группы `named`:

```
[root@drwalbr /]# mv /etc/named.conf /chroot/named/etc
[root@drwalbr /]# mv /var/named/* /chroot/named/var/named
[root@drwalbr /]# mknod /chroot/named/dev/random c 1 8
[root@drwalbr /]# chmod 644 /chroot/named/dev/random
[root@drwalbr /]# chown named.named /chroot/named/etc/named.conf
[root@drwalbr /]# chown -R named.named /chroot/named/var/named/*
```

Шаг 3

В качестве дополнительной меры безопасности сделайте файл `/chroot/named/etc/named.conf` защищенным от изменений:

```
[root@drwalbr /]# chattr +i /chroot/named/etc/named.conf
```

ЗАМЕЧАНИЕ Если потребуется внести изменения в файл `/chroot/named/etc/named.conf` не забудьте удалить атрибут `immutable` для этого файла, используя команду:

```
[root@drwalbr /]# chattr -i /chroot/named/etc/named.conf
```

Шаг 4

Удалите ненужные каталоги `/var/named` и `/var/run/named`, ранее используемые ISC BIND при инсталляции в обычном окружении:

```
[root@drwalbr /]# rm -rf /var/named/
[root@drwalbr /]# rm -rf /var/run/named/
```

Шаг 5

В файле `/etc/sysconfig/named` раскомментируйте или добавьте строку:

```
ROOTDIR="/chroot/named/"
```

Шаг 6

Запустите ISC BIND в окружении chroot-jail:

```
[root@drwalbr /]# /etc/init.d/named start
Запускается Named:                         [OK]
```

Шаг 7

Проверьте, запущен ли ISC BIND, и определите соответствующий номер процесса:

```
[root@drwalbr /]# ps ax | grep named
17450 ?        S      0:00 /usr/sbin/named -u named -t /chroot/named/
```

Шаг 8

Проверьте, запущен ли ISC BIND в окружении chroot-jail:

```
[root@drwalbr /]# ls -la /proc/17450/root/
```

Если вы получите вывод вида, отображающий содержимое корневого каталога среды chroot-jail:

```
итого 5
drwxr-xr-x    5 root     root         1024 Май 18 21:01 .
drwxr-xr-x    9 root     root         1024 Май 18 21:01 ..
drwxr-xr-x    2 named    named        1024 Май 18 21:10 dev
drwxr-xr-x    2 named    named        1024 Май 18 21:09 etc
drwxr-xr-x    4 root     root         1024 Май 18 21:05 var
```

то ISC BIND корректно работает в окружении chroot-jail.

Демон lwresd

В состав версии 9 ISC BIND входит демон `lwresd`, установка которого рекомендуется на всех Linux-системах вашей сети, за исключением DNS-серверов и шлюза. `lwresd` является «облегченной» версией демона `named` и позволяет реализовывать функции кэширующего DNS-сервера с меньшими затратами ресурсов системы. Для установки `lwresd` в окружении chroot-jail необходимо выполнить следующие операции.

Шаг 1

Добавьте в файл `/etc/resolv.conf` строку с указанием на IP-адрес вашего внешнего интерфейса:

```
lwserver 192.168.1.112
```

Шаг 2
Скопируйте файл `resolv.conf` в соответствующий каталог окружения chroot-jail:

```
[root@drwalbr /]# cp /etc/resolv.conf /chroot/named/etc/
```

Шаг 3
Создайте файл инициализации `lwresd`:

```
#!/bin/bash

# This shell script takes care of starting and stopping lwresd.
#
# chkconfig: - 55 45
# description: Lwresd is essentially a Caching-Only Name Server that \
#              answers requests using the lightweight resolver protocol \
#              rather than the DNS protocol.
#
# processname: lwresd

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/named ] ; then
        . /etc/sysconfig/named
fi

# Check that networking is up.
[ "${NETWORKING}" = "no" ] && exit 0

# If Lwresd is not available stop now.
[ -f /usr/sbin/lwresd ] || exit 0
[ -f "${ROOTDIR}"/etc/lwresd.conf ] || exit 0
[ -f "${ROOTDIR}"/etc/resolv.conf ] || exit 0

# Path to the Lwresd binary.
lwresd=/usr/sbin/lwresd

RETVAL=0
prog="Lwresd"

start() {
        echo -n $"Starting $prog: "
        if [ -n "${ROOTDIR}" -a "x${ROOTDIR}" != "x/" ]; then
                OPTIONS="${OPTIONS} -t ${ROOTDIR}"
        fi
        daemon $lwresd -P 53 -u named ${OPTIONS}
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/lwresd
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $lwresd
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/lwresd
        return $RETVAL
}
```

```
# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $lwresd
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/lwresd ]; then
                stop
                start
                RETVAL=$?
        fi
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 4

Сделайте файл исполняемым и определите его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 700 /etc/init.d/lwresd
[root@drwalbr /]# chown 0.0 /etc/init.d/lwread
```

Шаг 5

Для автоматического запуска `lwresd` создайте необходимые символьные ссылки:

```
[root@drwalbr /]# chkconfig --add lwresd
[root@drwalbr /]# chkconfig --level 2345 lwresd on
```

и удалите инициализационный файл и ссылки, используемые ранее для автоматического запуска демона `named`:

```
[root@drwalbr /]# chkconfig --del named
[root@drwalbr /]# chkconfig --level 2345 named off
[root@drwalbr /]# rm -f /etc/init.d/named
```

Шаг 6

Формат файла идентичен формату файла `named.conf`. Поэтому переименуйте файл `/chroot/named/etc/named.conf` в `lwresd.conf`:

```
[root@drwalbr /]# cd /chroot/named/etc/
[root@drwalbr etc]# mv named.conf lwresd.conf
```

Шаг 7

Для запуска демона `lwresd` выполните команду:

```
[root@drwalbr /]# /etc/init.d/lwresd start
Запускается Lwresd:          [OK]
```

Шаг 8

Протестируйте `lwresd` в соответствии с рекомендациями по тестированию `named`, приведенными выше.

Часть 6

Программное обеспечение для организации шлюза

Глава 24

Кэширующий прокси-сервер Squid

В этой главе:

Кэширующий прокси-сервер Squid разработан на основе результатов научно-исследовательского проекта Harvest, финансируемого управлением перспективных исследований и разработок (ARPA). Исследования проводились в национальной Лаборатории прикладных сетевых исследований (National Laboratory for Applied Network Research) и финансировались национальным научным Фондом (National Science Foundation). Squid сохраняет в оперативной памяти и на диске документы и другие объекты данных, получаемые с Web-ресурсов, ускоряя при этом доступ к ним и сокращая затраты на трафик. Обычно Squid используется для организации шлюза из локальных сетей в Интернет. Использование Squid в качестве кэширующего прокси-сервера на корпоративном шлюзе в сочетании с IPTables и GIPTables Firewall позволяет установить ограничения на доступ пользователей к Web-ресурсам (аутентификация пользователей, ограничения по IP-адресам, времени и пропускной способности канала). Кроме того, Squid может использоваться для увеличения производительности сильно загруженных Web-серверов путем предоставления клиентам часто запрашиваемых объектов из кэша прокси-сервера без обращения к Web-серверу.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Все команды выполняются от имени суперпользователя `root`.

Перекомпиляции ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта Squid Web Proxy Cache от 01.03.2003. Регулярно проверяйте обновления на `http://www.squid-cache.orq`. Мы используем установку требуемых компонентов с исходного архива, так как это открывает широкие возможности для настроек инсталляции.

Исходные коды содержатся в пакете `squid-version.tar.gz` (последняя доступная на момент написания главы версия `squid-2.5.STABLE1.tar.gz`).

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

> **ЗАМЕЧАНИЕ** Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет программы Squid с помощью следующей команды:

```
[root@bastion /]# rpm –iq squid
```

Если вы следовали нашим рекомендациям, то пакет не установлен.

Шаг 2

Перейдите в каталог, где находится пакет `squid-2.4.STABLE6-1.7.2.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@bastion /]# cd /home/distrib
```

и установите:

```
[root@bastion distrib]# rpm –ihv openssl-0.9.6b-24asp.i686.rpm\
cyrus-sasl-1.5.24-25.i386.rpm\
openldap-2.0.23-4.i386.rpm\
squid-2.4.STABLE6-1.7.2.asp.i386.rpm
```

или обновите пакет:

```
[root@bastion distrib]# rpm –Uhv squid-2.4.STABLE6-1.7.2.asp.i386.rpm
```

ЗАМЕЧАНИЕ Процедура настройки Squid версии 2.4.STABLE6 существенно отличаются от процедуры настройки Squid версии 2.5.STABLE1, подробно описанной ниже. Особенно это касается аутентификации пользователей. Если вы устанавливаете Squid версии 2.4.STABLE6 ознакомьтесь с документацией, которая может быть получена с домашней страницы проекта `http://www.squid-cache.org/`.

Компиляция, оптимизация и инсталляция Squid

Для инсталляции Squid из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Распакуйте архив с пакетом `squid-2.5.STABLE1.tar.gz` в каталоге `/var/tmp`:

```
[root@bastion tmp]# tar -xzpf squid-2.5.STABLE1.tar.gz
```

Перейдите в каталог `/var/tmp/squid-2.5.STABLE1`:

```
[root@bastion tmp]#cd /var/tmp/squid-2.5.STABLE1
```

Шаг 2

Создайте учетную запись пользователя `squid` без пароля и доступа к командному интерпретатору:

```
[root@bastion squid-2.5.STABLE1]# useradd -c "Squid user" –u 23 -s
/bin/false –r -d /var/spool/squid squid 2>/dev/null || :
```

Шаг 3

Для изменения заданных по умолчанию каталогов размещения файлов `cache.log`, `access.log` и `store.log` на `/var/log/squid`, файла `squid.pid` – на каталог `/var/run` и местоположения каталога кэша – на `/var/spool/squid`, в файле `/var/tmp/squid-2.5.STABLE1/src/Makefile.in` измените строку:

```
DEFAULT_LOG_PREFIX = $(localstatedir)/logs
```

на:

```
DEFAULT_LOG_PREFIX = $(localstatedir)/log/squid
```

Строку:

```
DEFAULT_PID_FILE = $(DEFAULT_LOG_PREFIX)/squid.pid
```

на:

```
DEFAULT_PID_FILE = /var/run/squid.pid
```

Строку:

```
DEFAULT_SWAP_DIR = $(localstatedir)/cache
```

на:

```
DEFAULT_SWAP_DIR = $(localstatedir)/var/spool/squid
```

ЗАМЕЧАНИЕ Размещение кэша в каталоге `/var/spool/`, находящегося на отдельном разделе, позволит оптимизировать производительность кэширующего прокси-сервера, например, используя `ulimit`.

Шаг 4

Сконфигурируйте исходные коды Squid:

```
[root@bastion squid-2.5.STABLE1]# CFLAGS="-O2 -march=i686 -funroll-loops"
\
./configure \
--prefix='' \
--sysconfdir=/etc/squid \
--libexecdir=/usr/lib/squid \
--localstatedir=/var \
--bindir=/usr/sbin \
--exec_prefix=/usr \
--datadir=/usr/lib/squid \
--mandir=/usr/share/man \
--enable-gnuregex \
--with-pthreads \
--enable-storeio=diskd,ufs \
--enable-removal-policies="heap" \
--enable-delay-pools \
```

```
--enable-cache-digests \
--enable-kill-parent-hack \
--enable-poll \
--enable-default-err-language="Russian-1251" \
--enable-err-language="Russian-1251" \
--enable-linux-netfilter \
--disable-ident-lookups \
--enable-truncate \
--enable-auth="basic" \
--enable-basic-auth-helpers="PAM" \
--enable-ssl
```

Предложенные опции конфигурации указывают на то, что исходные коды должны быть откомпилированы с поддержкой библиотек, повышающих производительность прокси-сервера, и с использованием базовой схемы аутентификации пользователей на основе стандартных модулей PAM. Сообщения об ошибках должны выдаваться на русском языке в кодировке Windows-1251.

Шаг 5
Откомпилируйте основную часть кода:
```
[root@bastion squid-2.5.STABLE1]# make all
```

Шаг 6
Проинсталлируйте основные файлы Squid:
```
[root@bastion squid-2.5.STABLE1]# find /* > /root/instfiles/squid1
[root@bastion squid-2.5.STABLE1]# make install
```

Шаг 7
Проинсталлируйте модуль аутентификации `auth_pam`:
```
[root@bastion squid-2.5.STABLE1]# cd helpers/basic/auth_pam
[root@bastion auth_pam]# install –m 4511 pam_auth /usr/lib/squid
```

Шаг 8
Создайте каталоги, необходимые для нормальной работы Squid, назначьте права доступа к ним:
```
[root@bastion auth_pam]# mkdir –p /var/spool/squid
[root@bastion auth_pam]# mkdir –p /var/spool/squid
[root@bastion auth_pam]# chown –R squid.squid /var/spool/squid
[root@bastion auth_pam]# mkdir –R squid.squid /var/spool/squid
```

Шаг 9
Удалите ненужные файлы, содержащие стандартные сценарии для запуска Squid:
```
[root@bastion auth_pam]# rm –f /usr/sbin/RunCashe
[root@bastion auth_pam]# rm –f /usr/sbin/RunAccel
```

Шаг 10
Создайте ссылки на соответствующие библиотеки:
```
[root@bastion auth_pam]# /sbin/ldconfig
```

Шаг 11
Создайте и сохраните в надежном месте список установленных файлов:
```
[root@bastion auth_pam]# find /* /root/instfiles/squid2
[root@bastion auth_pam]# diff /root/squid1 /root/squid2 >
/root/squid.installed
[root@bastion auth_pam]# mv /root/squid.installed /very reli-
able_place/squid.installed.YYYYMMDD
```

Шаг 12
Удалите каталоги с исходными кодами Squid и архив:
```
[root@bastion auth_pam]# rm –rf /var/tmp/squid-2.5.STABLE1
[root@bastion auth_pam]# rm –f /var/tmp/squid-2.5.STABLE1.tar.gz
```

Шаг 13
Создайте файл `/etc/rc.d/init.d/squid`, содержащий следующие строки:
```
#!/bin/bash
```

```
# This shell script takes care of starting and stopping Squid (Proxy
server).
#
# chkconfig: 345 90 25
# description: Squid - Internet Object Cache. Internet object caching is
\
#       a way to store requested Internet objects (i.e., data available \
#       via the HTTP, FTP, and gopher protocols) on a system closer to
the \
#       requesting site than to the source. Web browsers can then use the
\
#       local Squid cache as a proxy HTTP server, reducing access time as
\
#       well as bandwidth consumption.
#
# processname: squid

# pidfile: /var/run/squid.pid
# config: /etc/squid/squid.conf

PATH=/usr/bin:/sbin:/bin:/usr/sbin
export PATH

# Source function library.
. /etc/rc.d/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# Check if the squid.conf file is present.
[ -f /etc/squid/squid.conf ] || exit 0

# Source Squid configureation.
if [ -f /etc/sysconfig/squid ]; then
        . /etc/sysconfig/squid
else
  SQUID_OPTS="-D"
  SQUID_SHUTDOWN_TIMEOUT=100
fi

# Determine the name of the squid binary.
[ -f /usr/sbin/squid ] && SQUID=squid
[ -z "$SQUID" ] && exit 0

prog="$SQUID"

# Determine which one is the cache_swap directory
CACHE_SWAP=`sed -e 's/#.*//g' /etc/squid/squid.conf | \
        grep cache_dir |  awk '{ print $3 }'`
[ -z "$CACHE_SWAP" ] && CACHE_SWAP=/var/spool/squid

RETVAL=0

start() {
    for adir in $CACHE_SWAP; do
        if [ ! -d $adir/00 ]; then
             echo -n "init_cache_dir $adir... "
             $SQUID -z -F 2>/dev/null
        fi
    done
```

```
    echo -n $"Starting $prog: "
    $SQUID $SQUID_OPTS 2> /dev/null &
    # Trap and prevent certain signals from being sent to the Squid proc-
ess.
    trap '' 1 2 3 18
    RETVAL=$?
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/$SQUID
    [ $RETVAL -eq 0 ] && echo_success
    [ $RETVAL -ne 0 ] && echo_failure
    echo
    return $RETVAL
}

stop() {
    echo -n  $"Stopping $prog: "
    $SQUID -k check >/dev/null 2>&1
    RETVAL=$?
    if [ $RETVAL -eq 0 ] ; then
        $SQUID -k shutdown &
        rm -f /var/lock/subsys/$SQUID
        timeout=0
        while : ; do
                [ -f /var/run/squid.pid ] || break
                if [ $timeout -ge $SQUID_SHUTDOWN_TIMEOUT ]; then
                    echo
                    return 1
                fi
                sleep 2 && echo -n "."
                timeout=$((timeout+2))
        done
        echo_success
        echo
    else
        echo_failure
        echo
    fi
    return $RETVAL
}
reload() {
        $SQUID $SQUID_OPTS -k reconfigure
}

restart() {
        stop
        start
}

condrestart() {
        [ -e /var/lock/subsys/squid ] && restart || :
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  reload)
        reload
        ;;
  restart)
        restart
```

```
        ;;
  condrestart)
        condrestart
        ;;
        *)
        echo $"Usage: $0 {start|stop|reload|restart|condrestart}"
        exit 1
esac
exit $?
```

Шаг 14

Сделайте файл `/etc/rc.d/init.d/squid` исполняемым и назначьте его владельцем пользователя `root`:

```
[root@bastion /]# chmod 700 /etc/init.d/squid
[root@bastion /]# chown 0.0 /etc/init.d/squid
```

Если вы хотите, чтобы Squid запускался при загрузке системы, создайте символьные ссылки в каталоге `/etc/rc.d`:

```
[root@bastion /]# chkconfig --add squid
[root@bastion /]# chkconfig --level 345 squid on
```

Шаг 15

Создайте файл `/etc/pam.d/squid`, содержащий следующие строки:

```
#%PAM-1.0
auth       required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_stack.so service=system-auth
```

Конфигурирование Squid

Основной конфигурационный файл Squid - `/etc/squid/squid.conf`. На момент написания этой главы документация для версии 2.5.STABLE1 находилась в стадии разработки. Ниже приведенные рекомендации получены в результате анализа достаточно подробных комментариев, содержащихся в файле `/etc/squid/squid.conf.default`.

Пример конфигурации Squid для шлюза

Типовой вариант сопряжения прокси-сервера с локальной сетью и Интернет представлен на рис. 24.1.

Настройка Squid осуществляется следующим образом.

Шаг 1

Создайте или отредактируйте в соответствии с приведенными ниже рекомендациями и вашими требованиями файл `/etc/squid/squid.conf` (жирным шрифтом выделены комментарии, которые поясняют значения основных параметров, и фрагменты, которые обязательно нужно изменить в соответствии с реальной конфигурацией шлюза):

```
#Установите номер порта на котором Squid ожидает запросы HTTP-клиентов.
#Значение по умолчанию 3128
http_port 3128
#Обеспечьте корректную работу Squid с браузерами, некорректно
#поддерживающими SSL
ssl_unclean_shutdown on
#Установите номер порта, на котором Squid принимает и получает запросы
#с других прокси-серверов. Установив значение порта, равное 0, вы повыси-
те #производительность вашей системы
icp_port 0
#Установите запрет кэширования некоторого типа объектов.
#В данном случае – файлов, находящихся в каталоге cgi-bin.
acl QUERY urlpath_regex cgi-bin \?
```

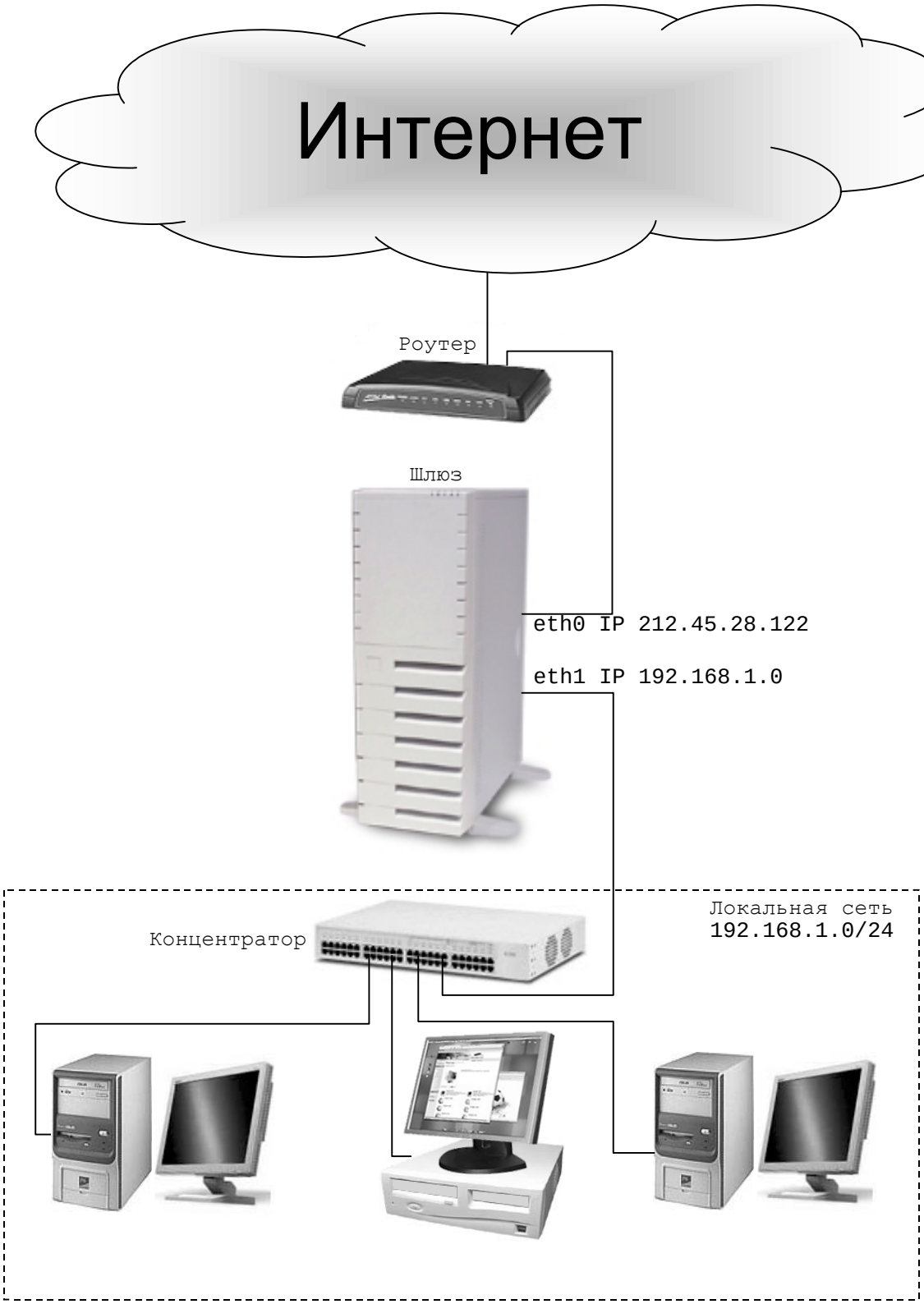


Рис. 24.1. Типовой вариант сопряжения прокси-сервера с локальной сетью и Интернет

```
no_cache deny QUERY
#Определите объем памяти, выделяемый под кэширование In-Transit objects,
#Hot Objects,Negative-Cached objects (примерно 1/3 от общего объема #опе-
ративной памяти). Оптимальное значение для системы с памятью
#512 МБайт –170.
cache_mem 170 MB
#Определите политику очистки кэша
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
#Определите формат представления данных в кэше (DISKD), каталог,
#в котором он размещается (/var/spool/squid), объем дискового пространст-
ва
#(1250 МБайт), количество подкаталогов первого и второго уровня в
#каталоге /var/spool/squid.
cache_dir diskd /var/spool/squid 1250 16 256
#Запретите создание файла, в котором регистрируется удаление и помещение
#объектов в кэш. Авторам не известны утилиты, предназначенные для обра-
ботки
#информации, содержащейся в этих файлах.
cache_store_log none
#Разрешите запись в файлы регистрации доменных имен вместо IP-адресов.
#Использование этой возможности облегчает анализ файлов регистрации,
#но снижает производительность шлюза.
log_fqdn on
#Разрешите создание файлов регистрации SQUID в формате Apache.
#Анализ этих файлов возможен с помощью стандартных утилит, предназначен-
ных
#для анализа файлов регистрации Apache, например Webalizer.
emulate_httpd_log on
#Определите элементы списков контроля доступа (ACL elements)
#Определите имя элемента ACL и параметры для локальной сети.
acl localnet src 192.168.1.0/255.255.255.0
#Определите имя элемента ACL и параметры локального хоста.
acl localhost src 127.0.0.1/255.255.255.255
#Определите имена элементов ACL и номера SSL и безопасных портов.
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535 280 488 591 777
#Определите имя элемента ACL для метода CONNECT.
acl CONNECT method CONNECT
#Определите имя элемента ACL для метода PURGE(очистка кэша).
acl all src 0.0.0.0/0.0.0.0
#Создайте Access List(правила доступа для всех элементов ACL).
#Squid воспринимает правила в том порядке, в котором они встречаются в
#/etc/squid/squid.conf.
#Разрешите доступ пользователей из локальной сети и с локальной системы
http_access allow localnet
http_access allow localhost
#Разрешите очистку кэша с локальной системы
http_access allow PURGE localhost
#Запретите обращение к небезопасным портам
http_access deny !Safe_ports
#Запретите обращение к портам, неиспользуемым SSL, с помощью метода
#CONNECT
http_access deny CONNECT !SSL_ports
#Запретите метод CONNECT
http_access deny CONNECT
#Запретите очистку кэша со всех систем
http_access deny PURGE
#Запретите доступ для всех хостов
http_access deny all
#Укажите e-mail администратора
cache_mgr admin@domain.ru
#Эти опции повышают безопасность системы за счет запуска
#Squid от имени пользователя squid группы squid
```

```
cache_effective_user squid
cache_effective_group squid
logfile_rotate 0
#Запретите обмен с другими прокси-серверами
log_icp_queries off
#Задайте пароль, используемый утилитой администрирования прокси-сервера
#cachemgr через Web-интерфейс (если вы собираетесь ее использовать).
#cachemgr_passwd $ecretnoe_Sl0vo all
#Включите поддержку ускорения записи файлов регистрации
buffered_logs on
```

При поступлении запроса на доступ в Интернет последовательно проверяются правила, указанные в ACL. Если условие, указанное в правиле вида "`http_access allow …`" выполняется, доступ разрешается и дальнейший просмотр правил прекращается. Если условие не выполняется, осуществляется переход к проверке условий, определяемых следующим правилом. Если условие, указанное в правиле вида "`http_access deny …`" выполняется, доступ запрещается, и дальнейший просмотр правил прекращается. Если условие не выполняется, осуществляется переход к проверке следующего правила.

В рассматриваемом примере при получении запроса от клиента в локальной сети на установление соединения с Web-сервером в Интернет в соответствии с первым правилом, указанным в ACL – `http_access allow localnet` – доступ разрешается. При получении запроса от клиента с консоли шлюза на установление соединения с Web-сервером в Интернет в соответствии с первым правилом в ACL доступ не разрешается и осуществляется переход к проверке выполнения условий второго правила. В соответствии с ним доступ в Интернет разрешается.

Работа различных клиентов в локальной сети может инициировать обращение к «безопасным» портам шлюза. При возникновении таких обращений в соответствии с первым и вторым правилом доступ не разрешается и осуществляется переход к проверке выполнения условий сначала третьего, а затем четвертого правила. В соответствии с одним из этих правил, доступ разрешается, причем к портам 443 и 563 даже с помощью метода CONNECT. При получении запроса на очистку кэша со шлюза (использования метода PURGE) в соответствии с правилами 1…4 доступ будет запрещен, и осуществляется переход к проверке выполнения условий пятого правила `http_access allow PURGE localhost`, в соответствии с которым доступ будет разрешен.

Шестое, седьмое и восьмое правило служат для реализации запрета всех остальных возможных соединений. Например, при попытке установления соединения с 22 портом, будут просмотрены первое, второе, третье и четвертое правила. При этом первое, второе и третье правила не дадут разрешения на установку соединения, а при проверке выполнения условий пятого правила соединение будет запрещено, а проверка выполнения условий правил прекращена.

ЗАМЕЧАНИЕ При написании правил в ACL важно учитывать не только их содержание, но и последовательность.

Если вы хотите, чтобы пользователи перед получением доступа в Интернет проходили аутентификацию, файл `/etc/squid/squid.conf` необходимо отредактировать в соответствии со следующими рекомендациями:

```
#Установите номер порта, на котором Squid ожидает запросы HTTP-клиентов.
#Значение по умолчанию 3128
http_port 3128
#Обеспечьте корректную работу Squid с браузерами, некорректно
#поддерживающими SSL
ssl_unclean_shutdown on
#Установите номер порта, на котором Squid принимает и получает запросы
#с других прокси-серверов. Установив значение порта, равное 0, вы повысите #производительность вашей системы
icp_port 0
#Установите запрет кэширования некоторого типа объектов.
#В данном случае – файлов, находящихся в каталоге cgi-bin.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
#Определите объем памяти, выделяемый под кэширование In-Transit objects,
#Hot Objects,Negative-Cached objects (примерно 1/3 от общего объема #оперативной памяти). Оптимальное значение для системы с памятью
#512 МБайт -170.
cache_mem 170 MB
#Определите политику очистки кэша
```

```
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
#Определите формат представления данных в кэше (DISKD), каталог,
#в котором он размещается (/var/spool/squid), объем дискового пространст-
ва
#(1250 МБайт), количество подкаталогов первого и второго уровня в
#каталоге /var/spool/squid.
cache_dir diskd /var/spool/squid 1250 16 256
#Запретите создание файла, в котором регистрируется удаление и помещение
#объектов в кэш. Авторам неизвестны утилиты, предназначенные для обработ-
ки
#информации, содержащейся в этих файлах.
cache_store_log none
#Разрешите запись в файлы регистрации доменных имен вместо IP-адресов.
#Использование этой возможности облегчает анализ файлов регистрации,
#но снижает производительность шлюза.
log_fqdn on
#Разрешите создание файлов регистрации SQUID в формате Apache.
#Анализ этих файлов возможен с помощью стандартных утилит, предназначен-
ных
#для анализа файлов регистрации Apache, например Webalizer.
emulate_httpd_log on
#Определите параметры аутентификации пользователей.
#Пример - базовая схема с использованием стандартных модулей PAM.
auth_param basic program /usr/lib/squid/pam_auth
auth_param basic children 5
auth_param basic realm Squid Proxy-Caching Web Server
auth_param basic credentialsttl 2 hours
#Определите элементы списков контроля доступа (ACL elements).
#Определите имя элемента ACL, определяющего список пользователей,
#которые должны проходить аутентификацию при обращении к SQUID.
#REQUIRED - любое допустимое имя пользователя.
acl usera proxy_auth REQUIRED
#Определите имя элемента ACL и параметры для локальной сети.
acl localnet src 192.168.1.0/255.255.255.0
#Определите имя элемента ACL и параметры локального хоста.
acl localhost src 127.0.0.1/255.255.255.255
#Определите имена элементов ACL и номера SSL и безопасных портов.
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535 280 488 591 777
#Определите имя элемента ACL для метода CONNECT.
acl CONNECT method CONNECT
#Определите имя элемента ACL и IP-адрес, к которому разрешен
#доступ без аутентификации пользователей.
#Определите имя элемента ACL для метода PURGE.
acl PURGE method PURGE
#Определите имя элемента ACL для Интернет.
acl all src 0.0.0.0/0.0.0.0
#Создайте Access List(правила доступа для всех элементов ACL).
#Squid воспринимает правила в том порядке, в котором они встречаются в
#/etc/squid/squid.conf.
#Разрешите доступ пользователей только с аутентификацией.
http_access allow usera
Разрешите доступ пользователей из локальной сети и с локальной системы
http_access allow localnet
http_access allow localhost
#Разрешите очистку кэша с локальной системы
http_access allow PURGE localhost
#Запретите обращение к небезопасным портам
http_access deny !Safe_ports
#Запретите обращение к портам, неиспользуемым SSL с помощью
#метода CONNECT
http_access deny CONNECT !SSL_ports
#Запретите метод CONNECT
```

```
http_access deny CONNECT
#Запретите очистку кэша со всех систем
http_access deny PURGE
#Запретите доступ для всех хостов
http_access deny all
#Укажите e-mail администратора
cache_mgr admin@domain.ru
#Эти опции повышают безопасность системы за счет запуска
#Squid от имени пользователя squid группы squid
cache_effective_user squid
cache_effective_group squid
logfile_rotate 0
#Запретите обмен с другими прокси-серверами
log_icp_queries off
#Задайте пароль, используемый утилитой администрирования прокси-сервера
#cachemgr через Web-интерфейс (если вы собираетесь ее использовать).
#cachemgr_passwd $ecretnoe_Sl0vo all
#Включите поддержку ускорения записи файлов регистрации
buffered_logs on
```

В некоторых случаях бывает необходимо ограничить перечень Web-ресурсов, доступ к которым могут иметь пользователи локальной сети. Аутентификация пользователей при этом не требуется. Ниже приведен пример конфигурационного файла `/etc/squid/squid.conf`, разрешающий всем пользователям локальной сети доступ только к серверам `http://www.rian.ru`, `http://www.interfax.ru` и `http://www.finmarket.ru` без аутентификации пользователей:

```
#Установите номер порта, на котором Squid ожидает запросы HTTP-клиентов.
#Значение по умолчанию 3128
http_port 3128
#Обеспечьте корректную работу Squid с браузерами, некорректно
#поддерживающими SSL
ssl_unclean_shutdown on
#Установите номер порта, на котором Squid принимает и получает запросы
#с других прокси-серверов. Установив значение порта, равное 0, вы повысите #производительность вашей системы.
icp_port 0
#Установите запрет кэширования некоторого типа объектов.
#В данном случае – файлов, находящихся в каталоге cgi-bin.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
#Определите объем памяти, выделяемый под кэширование In-Transit objects,
#Hot Objects,Negative-Cached objects (примерно 1/3 от общего объема #оперативной памяти). Оптимальное значение для системы с памятью
#512 МБайт –170.
cache_mem 170 MB
#Определите политику очистки кэша.
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
#Определите формат представления данных в кэше (DISKD), каталог,
#в котором он размещается (/var/spool/squid), объем дискового пространства
#(1250 МБайт), количество подкаталогов первого и второго уровня в
#каталоге /var/spool/squid.
cache_dir diskd /var/spool/squid 1250 16 256
#Запретите создание файла, в котором регистрируется удаление и помещение
#объектов в кэш. Авторам не известны утилиты, предназначенные для обработки
#информации, содержащейся в этих файлах.
cache_store_log none
#Разрешите запись в файлы регистрации доменных имен вместо IP-адресов.
#Использование этой возможности облегчает анализ файлов регистрации,
#но снижает производительность шлюза.
log_fqdn on
#Разрешите создание файлов регистрации SQUID в формате Apache.
```

```
#Анализ этих файлов возможен с помощью стандартных утилит, предназначен-
ных
#для анализа файлов регистрации Apache, например Webalizer.
emulate_httpd_log on
#Определите элементы списков контроля доступа (ACL elements).
#Определите имя элемента ACL и параметры для локальной сети.
acl localnet src 192.168.1.0/255.255.255.0
#Определите имя элемента ACL и параметры локального хоста.
acl localhost src 127.0.0.1/255.255.255.255
#Определите имена элементов ACL и номера SSL и безопасных портов.
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535 280 488 591 777
#Определите имя элемента ACL для метода CONNECT.
acl CONNECT method CONNECT
#Определите имя элемента ACL для метода PURGE(очистка кэша).
acl PURGE method PURGE
#Определите имя элемента ACL для Интернет.
acl all src 0.0.0.0/0.0.0.0
#Определите имя элемента ACL остальных Web-ресурсов.
acl WWW dst 0.0.0.0/0.0.0.0
#Определите имя элементов ACL для серверов, к которым разрешен доступ
acl www_rian_ru 195.230.73.54
acl www_interfax_ru 212.69.102.3
acl www_finmarket_ru 195.151.92.50
#Создайте Access List(правила доступа для всех элементов ACL).
#Squid воспринимает правила в том порядке в котором они встречаются
#/etc/squid/squid.conf.
#Разрешите доступ пользователей с локальной системы
http_access allow localhost
#Разрешите доступ к трем серверам.
http_access allow www_rian_ru
http_access allow www_interfax_ru
http_access allow www_finmarket_ru
#Разрешите очистку кэша с локальной системы.
http_access allow PURGE localhost
#Запретите обращение к небезопасным портам.
http_access deny !Safe_ports
#Запретите обращение к портам, неиспользуемым SSL.
http_access deny CONNECT !SSL_ports
#Запретите метод CONNECT.
http_access deny CONNECT
#Запретите очистку кэша со всех систем.
http_access deny PURGE
#Запретите обращение к остальным Web-ресурсам.
http_access deny WWW
#Запретите доступ для всех хостов.
http_access deny all
#Укажите e-mail администратора.
cache_mgr admin@domain.ru
#Эти опции повышают безопасность системы за счет запуска
#Squid от имени пользователя squid группы squid.
cache_effective_user squid
cache_effective_group squid
logfile_rotate 0
#Запретите обмен с другими прокси-серверами.
log_icp_queries off
#Задайте пароль, используемый утилитой администрирования прокси-сервера.
#cachemgr через Web-интерфейс (если вы собираетесь ее использовать).
#cachemgr_passwd $ecretnoe_Sl0vo all
#Включите поддержку ускорения записи файлов регистрации
buffered_logs on
```

Возможность ограничения доступа в Интернет по времени иллюстрируется следующим примером конфигурационного файла `/etc/squid/squid.conf`:

```
#Установите номер порта, на котором Squid ожидает запросы HTTP-клиентов.
#Значение по умолчанию 3128
http_port 3128
#Обеспечьте корректную работу Squid с браузерами, некорректно
#поддерживающими SSL.
ssl_unclean_shutdown on
#Установите номер порта, на котором Squid принимает и получает запросы
#с других прокси-серверов. Установив значение порта, равное 0, вы повыси-
те #производительность вашей системы.
icp_port 0
#Установите запрет кэширования некоторого типа объектов.
#В данном случае – файлов, находящихся в каталоге cgi-bin.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
#Определите объем памяти, выделяемый под кэширование In-Transit objects,
#Hot Objects,Negative-Cached objects (примерно 1/3 от общего объема #опе-
ративной памяти). Оптимальное значение для системы с памятью
#512 МБайт –170.
cache_mem 170 MB
#Определите политику очистки кэша.
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
#Определите формат представления данных в кэше (DISKD), каталог,
#в котором он размещается (/var/spool/squid), объем дискового пространст-
ва
#(1250 МБайт), количество подкаталогов первого и второго уровня в
#каталоге /var/spool/squid.
cache_dir diskd /var/spool/squid 1250 16 256
#Запретите создание файла, в котором регистрируется удаление и помещение
#объектов в кэш. Авторам не известны утилиты, предназначенные для обра-
ботки
#информации, содержащейся в этих файлах.
cache_store_log none
#Разрешите запись в файлы регистрации доменных имен вместо IP-адресов.
#Использование этой возможности облегчает анализ файлов регистрации,
#но снижает производительность шлюза.
log_fqdn on
#Разрешите создание файлов регистрации SQUID в формате Apache.
#Анализ этих файлов возможен с помощью стандартных утилит, предназначен-
ных
#для анализа файлов регистрации Apache, например Webalizer.
emulate_httpd_log on
#Определите элементы списков контроля доступа (ACL elements).
#Определите имя элемента ACL и параметры для локальной сети.
acl localnet src 192.168.1.0/255.255.255.0
#Определите имя элемента ACL и интервал времени, в течение
#которого разрешен доступ в Интернет.
acl WorkDay MTWHF 09:00-18:20
#Определите имя элемента ACL и параметры локального хоста.
acl localhost src 127.0.0.1/255.255.255.255
#Определите имена элементов ACL и номера SSL и безопасных портов.
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535 280 488 591 777
#Определите имя элемента ACL для метода CONNECT.
acl CONNECT method CONNECT
#Определите имя элемента ACL для метода PURGE(очистка кэша).
acl PURGE method PURGE
#Определите имя элемента ACL для Интернет.
acl all src 0.0.0.0/0.0.0.0
#Создайте Access List(правила доступа для всех элементов ACL).
#Squid воспринимает правила в том порядке, в котором они встречаются
#в /etc/squid/squid.conf.
#Разрешите доступ пользователей с локальной системы.
http_access allow localhost
```

```
#Разрешите доступ в Интернет в рабочее время.
http_access allow all WorkDay
#Разрешите очистку кэша с локальной системы.
http_access allow PURGE localhost
#Запретите обращение к небезопасным портам.
http_access deny !Safe_ports
#Запретите обращение к портам, неиспользуемым SSL.
http_access deny CONNECT !SSL_ports
#Запретите метод CONNECT.
http_access deny CONNECT
#Запретите очистку кэша со всех систем.
http_access deny PURGE
#Запретите доступ в Интернет в нерабочее время.
http_access deny localnet
#Запретите доступ для всех хостов.
http_access deny all
#Укажите e-mail администратора.
cache_mgr admin@domain.ru
#Эти опции повышают безопасность системы за счет запуска
#Squid от имени пользователя squid группы squid.
cache_effective_user squid
cache_effective_group squid
logfile_rotate 0
#Запретите обмен с другими прокси-серверами.
log_icp_queries off
#Задайте пароль, используемый утилитой администрирования прокси-сервера
#cachemgr через Web-интерфейс (если вы собираетесь ее использовать).
#cachemgr_passwd $ecretnoe_Sl0vo all
#Включите поддержку ускорения записи файлов регистрации
buffered_logs on
```

Шаг 2

Создайте файл `/etc/sysconfig/squid`, содержащий следующие строки:

```
#Если на момент запуска Squid отсутствует подключение к Интернет,
#используйте опцию -D для отмены начальных обращений к DNS.
#SQUID_OPTS="-D"
#Определите интервал времени, в течении которого Squid будет продолжать
#работать при получении сигнала на остановку.
SQUID_SHUTDOWN_TIMEOUT=100
```

Шаг 3

В приведенных выше примерах файла `/etc/squid/squid.conf` установлено значение опции `logfile_rotate`, равное `0`. Это означает, что для осуществления циклической замены файлов регистрации используется не значения параметров по умолчанию, а параметры, определяемые файлом `/etc/logrotate.d/squid`. Для еженедельной циклической перестановки файлов регистрации создайте файл `/etc/logrotate.d/squid`, содержащий следующие строки:

```
/var/log/squid/access.log {
    weekly
    rotate 5
    copytruncate
    compress
    notifempty
    missingok
}
/var/log/squid/cache.log {
    weekly
    rotate 5
    copytruncate
    compress
    notifempty
    missingok
}
```

```
/var/log/squid/store.log {
    weekly
    rotate 5
    copytruncate
    compress
    notifempty
    missingok
postrotate
      /usr/sbin/squid -k rotate
    endscript
}
```

Шаг 4

Если вы будете использовать аутентификацию пользователей, создайте для них соответствующие учетные записи (без доступа к командному интерпретатору и пользовательского каталога):

```
[root@bastion /]# useradd -s /bin/false drwalbr
[root@bastion /]# passwd drwalbr
Changing password for user drwalbr
New UNIX password:SeCreTnoe_SlOvO
Retype new UNIX password:SeCreTnoe_SlOvO
passwd: all authentication tokens updated successfully
```

Шаг 5

Если каталог `/var/spool/squid` смонтирован на отдельном разделе, то повышение безопасности системы может быть обеспечено за счет исключения возможности выполнения файлов, содержащихся в кэше. Для этого замените в файле `/etc/fstab` строку:

```
/dev/hda10   /var/spool  ext3  defaults    0     1
```

на:

```
/dev/hda10   /var/spool  ext3  defaults,noexec,nodev,nosuid  0     1
```

и перемонтируйте раздел:

```
[root@bastion /]# mount /var/spool -oremount
```

Проверьте правильность вновь установленных опций монтирования раздела:

```
[root@bastion /]# cat /proc/mounts | grep hda10
/dev/hda10 /var/spool    ext3  rw,noexec,nodev,nosuid 0 0
```

Шаг 6

Для устранения случайного или преднамеренного изменения главного конфигурационного файла `/etc/squid/squid.conf`, выполните:

```
[root@bastion /]# chattr+i /etc/squid/squid.conf
```

Тестирование Squid

Проверка работоспособности и правильности настройки Squid осуществляется следующим образом.

Шаг 1

Запустите Squid:

```
[root@bastion /]# /etc/init.d/squid start
Запускается squid:              [OK]
```

Перезапустите Squid:

```
[root@bastion /]# /etc/init.d/squid restart
Останавливается squid:          [OK]
Запускается squid:              [OK]
```

Если в процессе выполнения этих операций появились сообщения об ошибках, то необходимо проверить правильность конфигурационных файлов.

Шаг 2

Попробуйте с помощью браузера на системе в локальной сети, в которой не настроен доступ в Интернет через прокси-сервер, обратиться к какому-нибудь ресурсу. Если появился доступ, то проверьте настройки системы сетевой защиты.

ЗАМЕЧАНИЕ Доступ в Интернет, минуя прокси-сервер, должен быть закрыт для того, чтобы пользователи локальной сети, отключив использование прокси-сервера в браузере, не могли преодолеть установленные вами ограничения.

Шаг 3

В браузере на системе в локальной сети настройте доступ через прокси-сервер и попробуйте обратиться к какому-нибудь ресурсу. Если соединение устанавливается, протестируйте работоспособность всех правил, установленных в файле `/etc/squid/squid.conf`.

Администрирование Squid

После выполнения команды:

```
[root@bastion /]# /etc/init.d/squid start
```

Squid не останавливается немедленно, а дожидается завершения всех установленных соединений. Для немедленной остановки Squid используйте команду:

```
[root@bastion /]# /usr/sbin/squid –k kill
```

Иногда возникает необходимость удаления из кэша некоторых объектов. Никогда не пытайтесь добиться этого путем удаления файлов и каталогов в `/var/spool/squid`. Для решения этой задачи используйте утилиту `squidclient`, которая является мощным средством для тестирования и администрирования Squid. По умолчанию очистка кэша (использование метода PURGE) в Squid запрещена. Для разрешения очистки кэша во всех переведенных выше примерах файла `/etc/squid/squid.conf` добавлены строки, разрешающие очистку кэша с локальной системы, т. е. консоли шлюза:

```
…
#Определите имя элемента ACL для метода PURGE.
acl PURGE method PURGE
…
#Разрешите очистку кэша с локальной системы.
http_access allow PURGE localhost
…
#Запретите очистку кэша со всех систем.
http_access deny PURGE
…
```

Для получения краткой справочной информации о возможностях утилиты, наберите:

```
[root@bastion /]# /usr/sbin/squidclient
```

Удаление некоторого объекта из кэша осуществляется следующим образом.

При использовании Squid без аутентификации пользователей:

```
[root@bastion /]# /usr/sbin/squidclient –m PURGE
```

При использовании аутентификации:

```
[root@bastion /]# /usr/sbin/squidclient –m PURGE –u drwalbr –w SeCreT-
noe_SlOvO
```

В случае успешного удаления объекта вы получите сообщение вида:

```
HTTP/1.0 200 OK
Server: squid/2.5.STABLE1
Mime-Version: 1.0
Date: Mon, 03 Mar 2003 19:01:40 GMT
Content-Length: 0
X-Cache: MISS from bastion.und
X-Cache-Lookup: NONE from bastion.und:3128
Proxy-Connection: close
```

В случае отсутствия объекта в кэше – сообщение вида:

```
HTTP/1.0 404 Not Found
Server: squid/2.5.STABLE1
Mime-Version: 1.0
Date: Mon, 03 Mar 2003 19:02:50 GMT
Content-Length: 0
X-Cache: MISS from bastion.und
```

```
X-Cache-Lookup: NONE from bastion.und:3128
Proxy-Connection: close
```

Утилита `cachemgr.cgi` предназначена для администрирования Squid и получения информации о его настройках и статистике через Web-интерфейс. На наш взгляд утилита содержит ошибки, в некоторых случаях приводящих к совершенно непредсказуемым и загадочным результатам. Даже при правильной конфигурации не всегда можно подключиться к ее Web-интерфейсу. Протестировать `cachemgr.cgi` можно следующим образом.

Шаг 1

Удалите комментарий и введите пароль в строку файла `/etc/squid/squid.conf`:

```
#cachemgr_passwd $ecretnoe_Sl0vo all
```

Перезапустите Squid:

```
[root@bastion /]# /etc/init.d/squid restart
Останавливается squid:          [OK]
Запускается squid:              [OK]
```

Шаг 2

Переместите файл `cachemgr.cgi` из каталога `/usr/lib/squid` в каталог `cgi-bin` вашего Web-сервера `/var/www/cgi-bin/`:

```
[root@bastion /]# mv /usr/lib/squid/cachemgr.cgi /var/www/cgi-bin/
```

Шаг 3

Назначьте владельцем файла пользователя `root` и установите права доступа к файлу:

```
[root@bastion/]# cd/var/www/cgi-bin/
[root@bastion cgi-bin]# chmod 0511 cachemgr.cgi
[root@bastion cgi-bin]# chown 0.0 cachemgr.cgi
```

Шаг 4

Обратитесь с консоли шлюза к Web-интерфейсу утилиты, в нашем примере:

```
[root@bastion cgi-bin] # lynx www.bastion.und/cgi-bin/cachemgr.cgi
```

Шаг 5

Если вы используете конфигурацию с аутентификацией пользователя, то в отобразившейся на экране форме введите параметры – имя шлюза, порт на котором он работает, имя пользователя и пароль. В рассматриваемом примере – это, соответственно, `bastion.und`, `3128`, `drwalbr` и `$ecretnoe_Sl0vo` (установлен с помощью опции `cachemgr_passwd` в файле `/etc/squid/squid.conf`).

ЗАМЕЧАНИЕ В рассматриваемой конфигурации установка соединения возможна только с системы, на которой установлен шлюз.

Пример конфигурации Squid в качестве Web-ускорителя

Squid может использоваться для увеличения производительности сильно загруженных Web-серверов путем предоставления клиентам часто запрашиваемых объектов из кэша прокси-сервера без непосредственного обращения к Web-серверу. Типовой вариант сопряжения Squid, используемого в качестве Web-ускорителя, с Web-сервером представлена на рис. 24.2.

Пример конфигурационного файла `/etc/squid/squid.conf` прокси-сервера, запущенного на отдельной системе с IP-адресом 212.45.28.123, используемого в качестве Web-ускорителя для Web-сервера с IP-адресом 212.45.28.122, приведен ниже:

```
#Установите номер порта, на котором Squid ожидает запросы HTTP-клиентов.
http_port 80
#Обеспечьте корректную работу Squid с браузерами, некорректно
#поддерживающими SSL
ssl_unclean_shutdown on
#Установите номер порта, на котором Squid принимает и получает запросы
#с других прокси-серверов. Установка значения порта на 0 может повысить
производительность вашей системы.
icp_port 0
```

Рис. 24.2. Вариант сопряжения Squid, используемого в качестве Web-ускорителя, с Web-сервером

```
#Установите запрет кэширования некоторого типа объектов.
#В данном случае – файлов, находящихся в каталоге cgi-bin.
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
#Определите объем памяти, выделяемый под кэширование In-Transit objects,
#Hot Objects,Negative-Cached objects (примерно 1/3 от общего объема #опе-
ративной памяти). Оптимальное значение для системы с памятью
#512 МБайт –170.
cache_mem 170 MB
#Запретите изменять заголовки в перенаправляемых запросах. redi-
rect_rewrites_host_header off
#Определите политику очистки кэша.
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
#Определите формат представления данных в кэше (DISKD), каталог,
#в котором он размещается (/var/spool/squid), объем дискового пространст-
ва
#(1250 МБайт), количество подкаталогов первого и второго уровня в
#каталоге /var/spool/squid.
cache_dir diskd /var/spool/squid 1000 16 256
#Запретите создание файла, в котором регистрируется удаление и помещение
#объектов в кэш. Авторам не известны утилиты, предназначенные для обра-
ботки
#информации, содержащейся в этих файлах.
cache_store_log none
#Разрешите запись в файлы регистрации доменных имен вместо IP-адресов
#Использование этой возможности облегчает анализ файлов регистрации,
#но снижает производительность шлюза.
log_fqdn on
#Разрешите создание файлов регистрации SQUID в формате Apache.
#Анализ этих файлов возможен с помощью стандартных утилит, предназначен-
ных
#для анализа файлов регистрации Apache, например Webalizer.
emulate_httpd_log on
acl all src 0.0.0.0/0.0.0.0
#Разрешите доступ со всех хостов.
http_access allow all
#Укажите почтовый ящик администратора.
cache_mgr administrator@domen.ru
#Эти опции повышают безопасность системы за счет запуска
#Squid от имени пользователя squid группы squid
cache_effective_user squid
cache_effective_group squid
#Укажите IP-адрес ускоряемого Web-сервера.
httpd_accel_host 212.45.28.122
#Укажите номер порта Web-сервера.
httpd_accel_port 80
#Отключите заданный по умолчанию алгоритм logfile_rotate.
#Мы используем свой сценарий.
logfile_rotate 0
#Запретите взаимодействие с другими прокси-серверами.
log_icp_queries off
#Задайте пароль, используемый утилитой администрирования прокси-сервера
#cachemgr через Web-интерфейс (если вы собираетесь ее использовать).
#cachemgr_passwd $ecretnoe_Slovo all
#Включите поддержку ускорения записи файлов регистрации
buffered_logs on
```

В рассматриваемом примере Squid запущен на системе 212.45.28.123 и ожидает запросов клиентов на используемом по умолчанию Web-сервером 80 порту (`http_port 80`). При наличии в кэше прокси-сервера необходимого объекта он выдается запрашивающему его клиенту без обращения к Web-серверу, установленного на системе с IP-адресом 212.45.28.123. При отсутствии запрашиваемого объекта в кэше, он за-

прашивается путем обращения к 80 порту Web-сервера (`httpd_accel_port` **`80`**), установленного на системе с IP-адресом 212.45.28.122 (`httpd_accel_host 212.45.28.122`) и передается клиенту. Если полученный с Web-сервера объект относится к типу кешируемых объектов (в нашем примере – это любой объект, кроме файлов, размещенных в каталоге `cgi-bin`) он одновременно будет помещен в кэш, и при следующем обращении клиента будет выдан из кэша без обращения к Web-серверу.

Совместная работа Web-ускорителя и Web-сервера на одной системе может быть обеспечена путем изменения номера порта, на котором Web-сервер ожидает запросы клиентов по умолчанию, и внесения соответствующих изменений в файл `/etc/squid/squid.conf`:

```
#Установите номер порта, на котором Squid ожидает запросы HTTP-клиентов.
http_port 80
…
#Укажите IP-адрес ускоряемого Web-сервера.
httpd_accel_host 212.45.28.122
#Укажите номер порта Web-сервера.
httpd_accel_port 8080
…
```

Тестирование, запуск и администрирование Squid осуществляется также, как и в случае использования его в качестве кэширующего прокси-сервера на шлюзе.

Глава 25

SquidGuard – программное обеспечение для настройки Squid

В этой главе:

Настройка Squid с использованием списков контроля доступа (Access Control Lists) сложна и ограничивает возможности управления доступом пользователей локальной сети в Интернет. Для расширения возможностей управления доступом и упрощения настроек в Squid предусмотрено использование внешних программ, обеспечивающих расширенные возможности ограничения доступа в Интернет. Одной из таких программ является SquidGuard. Эта утилита позволяет закрывать доступ к нежелательным ресурсам, перенаправлять запросы к ним на другие ресурсы, например, содержащие информацию воспитательного характера, запрещать доступ в определенное время, дни недели, даты и т. п. Оптимизированный код SquidGuard позволяет обрабатывать большие списки (порядка миллиона записей) нежелательных Web-ресурсов без потери производительности шлюза. Ниже рассмотрен процесс установки, настройки и оптимизации этой полезной утилиты.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Все команды выполняются от имени суперпользователя `root`.

Установлен `squid-2.5.STABLE1`.

Перекомпиляции ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других дистрибутивов Linux, однако авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта SquidGuard от 07.03.2003. Регулярно проверяйте обновления на `http://www.squidguard.org`. Мы используем установку требуемых компонентов с исходного архива, так как это открывает широкие возможности для настроек инсталляции.

Исходный коды содержатся в пакете `squidGuard-version.tar.gz` (последняя доступная на момент написания главы версия - `squidGuard-1.2.0.tar.gz`).

Компиляция, оптимизация и инсталляция SquidGuard

Шаг 1

Распакуйте архив с пакетом `squidGuard-1.2.0.tar.gz` в каталоге `/var/tmp`:

```
[root@bastion tmp]# tar -xzpf squidGuard-1.2.0.tar.gz
```

Перейдите в каталог `/var/tmp/squidGuard-1.2.0`:

```
[root@bastion tmp]#cd /var/tmp/squidGuard-1.2.0
```

Шаг 2

Сконфигурируйте исходные коды SquidGuard:

```
[root@bastion squidGuard-1.2.0]# CFLAGS="-O2 -march=i686 -funroll-loops"
\
./configure --prefix=/usr \
--sysconfdir=/etc \
--localstatedir=/var \
--with-sg-config=/etc/squid/squidGuard.conf \
--with-sg-logdir=/var/log/squid/squidGuard \
--with-sg-dbhome=/var/spool/squid/squidGuard \
--with-db-inc=/usr/include \
--with-db-lib=/usr/lib
```

Предложенные опции конфигурации определяют каталоги, в которых будут размещены конфигурационные файлы, файлы регистрации и библиотеки.

Шаг 3

Откомпилируйте исходный код:

```
[root@bastion squidGuard-1.2.0]# make
```

ЗАМЕЧАНИЕ Во время компиляции с сервера `http://www.squidguard.org` получаются обновления файлов документации. Поэтому если у вас установлен Squid с поддержкой аутентификации пользователей и вы не хотите, чтобы вместо обновленных файлов документации у вас были сообщения Squid о невозможности доставки URL, отключите аутентификацию пользователей на время установки SquidGuard.

Шаг 4

Проинсталлируйте основные файлы SquidGuard:

```
[root@bastion squidGuard-1.2.0]# find /* > /root/squidGuard1
[root@bastion squidGuard-1.2.0]# make install
```

Шаг 5

Проинсталлируйте скрипт `squidGuard.cgi`, предназначенный для вывода сообщений о причине отказа в доступе пользователю:

```
[root@bastion squidGuard-1.2.0]# cd samples/
[root@bastion samples]# install –m 511 squidGuard1.cgi
```

Шаг 6

Измените владельца и установите права доступа к каталогу с файлами регистрации SquidGuard:

```
[root@bastion samples]# chown –R squid.squid /var/log/squid/squidGuard
[root@bastion samples]# chmod 0750 /var/log/squid/squidGuard
```

Шаг 7

Распакуйте архив, содержащий фильтры (IP-адреса, к которым запрещено обращение и регулярные выражения, соответствующие URL), создайте каталоги для размещения фильтров и проинсталлируйте файлы фильтров:

```
[root@bastion samples]# cd dest/
[root@bastion dest]# mkdir –p /var/spool/squid/squidGuard
[root@bastion dest]# cp blaklists.tar.gz /var/spool/squid/squidGuard
[root@bastion dest]# cd /var/spool/squid/squidGuard
[root@bastion squidGuard]# tar xzpf blaklists.tar.gz
[root@bastion squidGuard]# mkdir ads
[root@bastion squidGuard]# mkdir aggressive
[root@bastion squidGuard]# mkdir audio-video
[root@bastion squidGuard]# mkdir drugs
[root@bastion squidGuard]# mkdir gambling
[root@bastion squidGuard]# mkdir hacking
[root@bastion squidGuard]# mkdir mail
[root@bastion squidGuard]# mkdir porn
[root@bastion squidGuard]# mkdir proxy
[root@bastion squidGuard]# mkdir violence
[root@bastion squidGuard]# mkdir warez
[root@bastion squidGuard]# cd blaklists
[root@bastion blaklists]# install –m 644 ads/domains ../ads/
[root@bastion blaklists]# install –m 644 ads/urls ../ads/
[root@bastion blaklists]# install –m 644 aggressive/domains
../aggressive/
[root@bastion blaklists]# install –m 644 aggressive/urls ../aggressive/
[root@bastion blaklists]# install –m 644 audio-video/domains ../audio-
video/
[root@bastion blaklists]# install –m 644 audio-video/urls ../audio-video/
[root@bastion blaklists]# install –m 644 drugs/domains ../drugs/
[root@bastion blaklists]# install –m 644 drugs/urls ../drugs/
[root@bastion blaklists]# install –m 644 gambling/domains ../gambling/
[root@bastion blaklists]# install –m 644 gambling/urls ../gambling/
[root@bastion blaklists]# install –m 644 hacking/domains ../ hacking/
[root@bastion blaklists]# install –m 644 hacking/urls ../hacking/
[root@bastion blaklists]# install –m 644 mail/domains ../mail/
[root@bastion blaklists]# install –m 644 porn/domains ../porn/
[root@bastion blaklists]# install –m 644 porn/urls ../porn/
[root@bastion blaklists]# install –m 644 porn/expressions../porn/
[root@bastion blaklists]# install –m 644 proxy/domains ../proxy/
[root@bastion blaklists]# install –m 644 proxy/urls ../proxy/
[root@bastion blaklists]# install –m 644 violence/domains ../violence/
[root@bastion blaklists]# install –m 644 violence/urls ../violence/
[root@bastion blaklists]# install –m 644 warez/domains ../warez/
[root@bastion blaklists]# install –m 644 warez/urls ../warez/
[root@bastion blaklists]# chown –R squid.squid
/var/spool/squid/squidGuard/
```

```
[root@bastion blaklists]# chmod 0750 /var/spool/squid/squidGuard/
[root@bastion blaklists]# cd ..
[root@bastion squidGuard]# rm –rf blaklists.tar.gz blaklists
```

ЗАМЕЧАНИЕ Выше приведен перечень команд, с помощью которых устанавливаются все фильтры, входящие в дистрибутив SquidGuard-1.2.0. Авторы рекомендуют установить их все и отключать ненужные на этапе конфигурации. Тем не менее, вы имеете возможность не устанавливать некоторые из них. Так, например, если вы не желаете запретить доступ к ресурсам из списков, содержащихся в каталоге `warez`, не выполняйте следующие команды:

```
[root@bastion squidGuard]# mkdir warez
[root@bastion blaklists]# install –m 644 warez/domains ../warez/
[root@bastion blaklists]# install –m 644 warez/urls ../warez/
```

Шаг 8

Настройте привязку динамических ссылок:

```
[root@bastion squidGuard]# /sbin/ldconfig
```

Шаг 9

Для повышения производительности удалите лишние фрагменты из исполняемого файла `squidGuard`:

```
[root@bastion squidGuard]# strip /usr/bin/squidGuard
```

Шаг 10

Создайте и сохраните в надежном месте список установленных файлов:

```
[root@bastion squidGuard]# find /* > /root/instfiles/squidGuard2
[root@bastion squidGuard]# diff /root/instfiles/squidGuard1
/root/squidGuard2 > /root/squidGuard2.installed
[root@bastion squidGuard]# mv /root/squidGuard2.installed /very reli-
able_place/squidGuard2.installed.YYYYMMDD
```

Шаг 11

Удалите каталоги с исходными кодами SquidGuard и архив:

```
[root@bastion squidGuard]# rm –rf /var/tmp/squidGuard-1.2.0/
[root@bastion squidGuard]# rm –f /var/tmp/squidGuard-1.2.0.tar.gz
```

Конфигурирование SquidGuard

Шаг 1

Создайте или отредактируйте в соответствии с приведенными ниже рекомендациями и вашими потребностями файл `/etc/squid/squidGuard.conf`:

```
#Path declarations
#Укажите путь к корневому каталогу с фильтрами
dbhome /var/spool/squid/squidGuard
#Укажите путь к корневому каталогу с файлами регистрации
logdir /var/log/squid/squidGuard
#Time space declarations
#В данном примере доступ разрешен по рабочим дням с 09:00 до 18:15
time workhours {
    weekly mtwhf 09:00 - 19:15
}
#Source group declarations
# Описание локальной сети
src internal {
    ip     192.168.1.1/24
}
#Destination group declarations
#Описание ресурсов, доступ к которым запрещен
dest ads {
    domainlist     ads/domains
    urllist        ads/urls
}
dest aggressive {
    domainlist     aggressive/domains
```

```
    urllist        aggressive/urls
}
dest audio-video {
    domainlist     audio-video/domains
    urllist        audio-video/urls
}
dest drugs {
    domainlist     drugs/domains
    urllist        drugs/urls
}
dest gambling {
    domainlist     gambling/domains
    urllist        gambling/urls
}
dest hacking {
    domainlist     hacking/domains
    urllist        hacking/urls
}
dest mail {
    domainlist     mail/domains
}
dest porn {
    domainlist     porn/domains
    urllist        porn/urls
    expressionlist porn/expressions
}
dest proxy {
    domainlist     proxy/domains
    urllist        proxy/urls
}
dest violence {
    domainlist     violence/domains
    urllist        violence/urls
}
dest varez {
    domainlist     warez/domains
    urllist        warez/urls
}
#Rewrite rule group declarations
#Авторы не рекомендуют использовать этот раздел.

#Access Control Lists

#Списки контроля доступа (ACCESS CONTROL LISTS)
#
#Разрешите доступ со всех машин в локальной сети
#в рабочие дни и рабочее время
#ко всем ресурсам, кроме перечисленных в фильтре.
acl {
     internal within workhours {
     pass !ads !aggressive !audio-video !drugs !gambling
     !hacking !mail !porn !proxy !violence !warez
     all
    }
#Запрет и переадресация всех остальных запросов
    default {
       pass     none
       redirect http://bastion.und/cgi-
bin/squidGuard.cgi?clientaddr=%a&clientname=%n&clientuser=%i&clientgroup=
%s&targetgroup=%t&url=%u
    }
}
```

В файле `squidGuard.conf` могут использоваться следующие зарезервированные слова:

```
– acl                  – rewrite
– anonymous            – sat
– date                 – saturday
– dbhome               – saturdays
– dest                 – source
– destination          – src
– domain               – sun
– domainlist           – sunday
– else                 – sundays
– expressionlist       – thu
– fri                  – thursday
– friday               – thursdays
– fridays              – time
– ip                   – tue
– log                  – tuesday
– logdir               – tuesdays
– logfile              – urllist
– mon                  – user
– monday               – userlist
– mondays              – wed
– outside              – wednesday
– pass                 – wednesdays
– redirect             – weekly
vrew                   – within
```

Поэтому использование этих слов в качестве имен объектов не допускается.

В разделе `Path declarations` вы можете задать пути к корневому каталогу файла с фильтрами и каталогу с файлами регистрации.

Раздел `Time space declarations` используется для задания различных интервалов времени в следующем формате:

```
time name {
specification
specification
...
specification

}
```

где:

- `time` – зарезервированное слово, используемое в качестве признака начала описания временных интервалов;
- `name` – имя описания временных интервалов;
- `specification –` описание интервала.

Дни недели и имеющие к ним отношения интервалы времени могут быть записаны в виде:

```
weekly {smtwhfa} [HH:MM-HH:MM]
```

где:

- `s -` воскресенье;
- `m -` понедельник;
- `t -` вторник;
- `w -`среда;
- `h -` четверг;
- `f -`пятница;
- `a-`воскресенье.

В рассматриваемом примере конфигурационного файла `/etc/squid/squidGuard.conf` запись:

```
time workhours {
    weekly mtwhf 09:00 - 19:15
}
```

определяет интервалы времени с именем `workhours`, включающие рабочее время, т. е. с 9.00 по 19.15 с понедельника по пятницу.

Запись:

```
Time notworktime
{
```

```
  weekly   * 00:00-09:00 # Нерабочее время после полуночи
  weekly   * 19:15-24:00 # Нерабочее время до полуночи
  weekly   {sa}# B
  date   *.01.01 # Новый год
  date   *.02.01 # Новый год
  date   *.07.01 # Рождество
  date   *.14.02 # День святого Валентина
  date   *.23.02 # День защитника Отечества
   ...
  date   *.31.12 # Новый год
}
```

определяет интервалы времени с именем `notworktime`, включающие нерабочее время, т. е. нерабочее время ежедневно и круглосуточно в праздники.

В разделе `Source group declarations` описываются группы источников, обращающихся к Web-ресурсам, например локальная сеть:

```
src|source name within|outside time_space_name {
specification
specification
...
specification

} else {
specification
specification
...
specification

}
```

где:

`src или source` – зарезервированное слово, используемое в качестве признака начала описания группы источников, обращающихся к Web-ресурсам (используйте только одно слово – `src` или `source` – на ваше усмотрение);

`name` – имя описания группы источников;

`within или outside` – используется для задания отношения группы источников к временным интервалам, соответственно, в течение интервала, или вне его;

`time_space_name` – имя описания временных интервалов;

`specification` – описание источников.

В рассматриваемом примере конфигурационного файла `/etc/squid/squidGuard.conf` запись:

```
src internal {
    ip     192.168.1.1/24
```

определяет локальную сеть с возможным диапазоном IP-адресов 192.168.1.1- 192.168.1.254.

IP-адреса группы источников могут задаваться в различных форматах:

- список IP-адресов:

```
ip 192.168.1.1 192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.100
```

- сеть с указанием маски:

```
192.168.1.1/24
192.168.1.0/255.255.255.0
```

- диапазон IP-адресов:

```
192.168.1.1-192.168.1.54
```

Для описания группы источников можно использовать зарезервированные слова:

- `domain` – для описания доменов или группы доменов, например:

```
domain und
```

- `user` – для описания групп пользователей, например:

```
user root drwalbr karlnext
```

Списки IP-адресов и пользователей могут размещаться в отдельных файлах, для описания этих файлов используются строки вида:

- `iplist filename`;
- `userlist filename`;

где:

`iplist` и `userlist` – зарезервированные слова, предназначенные для описания содержания файла список IP-адресов или пользователей соответственно;

`filename` – имя файла.

IP-адреса и имена пользователей должны размещаться по одному в каждой строке файла.

В разделе `Destination group declarations` описываются IP-дреса и имена доменов, доступ к которым должен блокироваться:

```
dest|destination name within|outside time_space_name {
specification
specification
...
specification

} else {
specification
specification
...
specification

}
```

где:

- `dest` или `destination` – зарезервированное слово, используемое в качестве признака начала описания группы ресурсов, доступ к которым должен быть запрещен (используйте только одно слово – `dest` или `destination` – на ваше усмотрение);
- `name` – имя ресурсов, доступ к которым должен быть запрещен;
- `within` или `outside` – используется для задания отношения группы ресурсов к временным интервалам, соответственно, в течение интервала, или вне его;
- `time_space_name` – имя описания временных интервалов,
- `specification` – описание ресурсов.

В рассматриваемом примере конфигурационного файла `/etc/squid/squidGuard.conf` запись:

```
dest ads {
    domainlist     ads/domains
    urllist        ads/urls
}
dest aggressive {
    domainlist     aggressive/domains
    urllist        aggressive/urls
}
dest audio-video {
    domainlist     audio-video/domains
    urllist        audio-video/urls
}
dest drugs {
    domainlist     drugs/domains
    urllist        drugs/urls
}
dest gambling {
    domainlist     gambling/domains
    urllist        gambling/urls
}
dest hacking {
    domainlist     hacking/domains
    urllist        hacking/urls
}
dest mail {
    domainlist     mail/domains
}
dest porn {
    domainlist     porn/domains
    urllist        porn/urls
    expressionlist porn/expressions
}
```

```
dest proxy {
    domainlist     proxy/domains
    urllist        proxy/urls
}
dest violence {
    domainlist     violence/domains
    urllist        violence/urls
}
dest varez {
    domainlist     warez/domains
    urllist        warez/urls
}
```

определяет список, содержащий 11 типов ресурсов.

Так, например, тип ресурсов с именем `porn`, описанный с помощью:

```
dest porn {
    domainlist     porn/domains
    urllist        porn/urls
    expressionlist porn/expressions
}
```

указывает на то, что:

- перечень блокируемых доменов содержится в файле `/var/spool/squid/squidGuard/porn/domains`;
- список блокируемых URL – в файле `/var/spool/squid/squidGuard/porn/urls/`;
- список регулярных выражений, описывающих список блокируемых URL – в файле `/var/spool/squid/squidGuard/porn/expressions`.

Вы имеете возможность, редактируя файлы `domains`, `urls` и `expressions`, определять новые блокируемые домены и URL. Используя конструкции вида:

```
 dest my_block_list {
    domainlist     my_block_list/domains
    urllist        my_block_list/urls
    expressionlist my_block_list/expressions
}
```

и собственные файлы `my_block_list/domains`, `my_block_list/urls` и `my_block_list/expressions`, вы имеете возможность настройки блокировки любых нежелательных Web-ресурсов.

ЗАМЕЧАНИЕ Список регулярных выражений, описывающих блокируемые URL, содержащихся в файле `/var/spool/squid/squidGuard/porn/expressions`, иногда мешает просмотру совершенно легитимных Web-ресурсов. Поэтому авторы рекомендуют подвергнуть этот файл детальной ревизии с учетом замечаний, поступающих от пользователей вашей сети. В крайнем случае этот файл можно удалить вместе с соответствующей строкой `/etc/squid/squidGuard.conf`.

Если вы не желаете запрещать доступ к ресурсам из некоторых списков, например, содержащихся в каталоге `warez`, удалите или закомментируйте в файле `/etc/squid/squidGuard.conf` следующие строки:

```
dest warez {
    domainlist     warez/domains
    urllist        warez/urls
}
```

В разделе `Rewrite rule group declarations` описываются настройки переадресации запросов к локальным копиям часто запрашиваемых Web-ресурсов.

Авторы не рекомендуют использовать настройки этого раздела, так как это может привести к ошибкам и существенному снижению производительности шлюза.

В разделе `Access Control Lists` осуществляется объединение всех сделанных ранее описаний:

```
acl {
sourcegroupname [within|outside timespacename] {
pass [!]destgroupname [...]
[redirect [301:|302:]new_url]
```

```
}

sourcegroupname within|outside timespacename {
pass [!]destgroupname [...]
[redirect [301:|302:]new_url]
} else {
pass [!]destgroupname [...]
[redirect [301:|302:]new_url]
}

...

default [within|outside timespacename] {
pass [!]destgroupname [...]
redirect [301:|302:]new_url
}[ else {
pass [!]destgroupname [...]
redirect [301:|302:]new_url
]
}
```

где:

`acl` – зарезервированное слово, обозначающее начало списка контроля доступа (свода правил блокирования и переадресации запросов к Web-ресурсам);

`sourcegroupname` - имя группы источников запросов;

`timespacename` – имя группы временных интервалов;

`pass` – подраздел, в котором определяются правила пропуска и блокировки запросов;

`destgroupname` – имя группы блокируемых ресурсов;

`redirect` – подраздел, в котором определяется параметры переадресации заблокированного запроса;

`new_url` – URL, на который осуществляется переадресация;

`default` – подраздел, в котором определяются правила для всех запросов, не определенных в предыдущих подразделах.

В рассматриваемом примере файла `/etc/squid/squidGuard.conf`:

```
acl {
     internal within workhours {
     pass !ads !aggressive !audio-video !drugs !gambling
     !hacking !mail !porn !proxy !violence !warez
     all
    }
#Запрет и переадресация всех остальных запросов
    default {
       pass     none
       redirect redirect http://bastion.und/cgi-
bin/squidGuard.cgi?clientaddr=%a&clientname=%n&clientuser=%i&clientgroup=
%s&targetgroup=%t&url=%u
    }
}
```

разрешен доступ из локальной сети в рабочее время ко всем ресурсам Интернет, кроме ресурсов, определенных в файлах фильтров.

Запросы к ресурсам, определенным в файлах фильтров переадресуются на `http://bastion.und/cgi-bin/squidGuard.cgi?clientaddr=%a&clientname=%n&clientuser=%i&clientgroup=%s&targetgroup=%t&url=%u`.

> **ЗАМЕЧАНИЕ** В файле нельзя определять или использовать более одного блока `acl SquidGuard.conf`.

Примеры конфигурационного файла `/etc/squid/squidGuard.conf` для более сложных случаев рассмотрены в документации `http://www.squidguard.org/config/`.

Шаг 2

В используемый вами файл /etc/squid/squid.conf добавьте строки, выделенные жирным шрифтом:

```
#Установите номер порта, на котором Squid ожидает запросы HTTP-клиентов.
#Значение по умолчанию 3128
http_port 3128
#Обеспечьте корректную работу Squid с браузерами, некорректно
#поддерживающими SSL
ssl_unclean_shutdown on
#Установите номер порта, на котором Squid принимает и получает запросы
#с других прокси-серверов. Установив значение порта, равное 0, вы #повы-
сите производительность вашей системы
icp_port 0
#Установите запрет кэширования некоторого типа объектов.
#В данном случае – файлов, находящихся в каталоге cgi-bin.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
#Определите объем памяти, выделяемый под кэширование In-Transit objects,
#Hot Objects,Negative-Cached objects (примерно 1/3 от общего объема #опе-
ративной памяти). Оптимальное значение для системы с памятью
#512 МБайт –170.
cache_mem 170 MB
#Определите политику очистки кэша.
cache_replacement_policy heap GDSF
memory_replacement_policy heap GDSF
#Определите формат представления данных в кэше (DISKD), каталог,
#в котором он размещается (/var/spool/squid), объем дискового #простран-
ства,
#(1250 МБайт), количество подкаталогов первого и второго уровня в
#каталоге /var/spool/squid.
cache_dir diskd /var/spool/squid 1250 16 256
#Запретите создание файла, в котором регистрируется удаление и помещение
#объектов кэш. Авторам неизвестны утилиты, предназначенные для обработки
#информации, содержащейся в этих файлах.
cache_store_log none
#Разрешите запись в файлы регистрации доменных имен вместо IP-адресов.
#Использование этой возможности облегчает анализ файлов регистрации,
#но снижает производительность шлюза.
log_fqdn on
#Разрешите использование squidGuard
redirect_program /usr/bin/squidGuard
redirect_children 5
#Разрешите создание файлов регистрации SQUID в формате Apache.
#Анализ этих файлов возможен с помощью стандартных утилит, #предназначен-
ных
#для анализа файлов регистрации Apache, например Webalizer.
emulate_httpd_log on
#Определите элементы списков контроля доступа (ACL elements).
#Определите имя элемента ACL и параметры для локальной сети.
acl localnet src 192.168.1.0/255.255.255.0
#Определите имя элемента ACL и параметры локального хоста.
acl localhost src 127.0.0.1/255.255.255.255
#Определите имена элементов ACL и номера SSL и безопасных портов.
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535 280 488 591 777
#Определите имя элемента ACL для метода CONNECT.
acl CONNECT method CONNECT
#Определите имя элемента ACL для метода PURGE(очистка кэша).
acl all src 0.0.0.0/0.0.0.0
#Создайте Access List (правила доступа для всех элементов ACL).
#Squid воспринимает правила в том порядке, в котором они встречаются в
#/etc/squid/squid.conf.
#Разрешите доступ пользователей из локальной сети и с локальной системы.
http_access allow localnet
http_access allow localhost
```

```
#Разрешите очистку кэша с локальной системы.
http_access allow PURGE localhost
#Запретите обращение к небезопасным портам.
http_access deny !Safe_ports
#Запретите обращение к портам, не используемым SSL, с помощью метода
#CONNECT
http_access deny CONNECT !SSL_ports
#Запретите метод CONNECT.
http_access deny CONNECT
#Запретите очистку кэша со всех систем.
http_access deny PURGE
#Запретите доступ для всех хостов.
http_access deny all
#Укажите e-mail администратора.
cache_mgr administrator@domen.ru
#Эти опции повышают безопасность системы за счет запуска
#Squid от имени пользователя squid группы squid
cache_effective_user squid
cache_effective_group squid
logfile_rotate 0
#Запретите обмен с другими прокси-серверами.
log_icp_queries off
#Задайте пароль, используемый утилитой администрирования прокси-сервера
#cachemgr через Web-интерфейс (если вы собираетесь ее использовать).
#cachemgr_passwd $ecretnoe_Sl0vo all
#Включите поддержку ускорения записи файлов регистрации
buffered_logs on
```

Те же строки должны быть вставлены и в случае использования конфигурационного файла `/etc/squid/squid.conf` с поддержкой аутентификации пользователей.

Шаг 3

В файле `/var/www/cgi-bin/squidGuard.cgi` укажите имя системы, на которой установлены Squid и SquidGuard. Для этого строку:

```
$proxy       = "proxy.your-domain";
```

замените на:

```
$proxy       = "bastion.und";
```

а строку:

```
$proxymaster = "operator\@your-domain";
```

замените на:

```
$proxymaster = "administrator\@domain.ru";
```

ЗАМЕЧАНИЕ Использование скрипта `squidGuard.cgi` имеет смысл только на этапе отладки вновь установленного шлюза. Выдаваемые им сообщения о причинах отказа в доступе к Web- ресурсам могут быть использованы для корректировки фильтров. После отладки, с целью сокращения загрузки Web-сервера, переадресацию лучше осуществлять на статическую html-страницу информационно-воспитательного содержания.

Запуск и тестирование SquidGuard

Шаг 1

Перезапустите Squid:

```
[root@bastion /]# /etc/init.d/squid restart
Останавливается squid:          [OK]
Запускается squid:              [OK]
```

Шаг 2

Проверьте доступность URL, на который осуществляется переадресация.

Шаг 3

Проверьте доступность Web-ресурсов, обычно используемых пользователями вашей локальной сети.

Шаг 4

Проверьте недоступность блокируемых Web-ресурсов, наиболее популярных среди пользователей вашей сети.

Шаг 5

В случае необходимости проведите соответствующую корректировку фильтров, после чего перейдите к шагу 1.

Оптимизация SquidGuard

Каждый раз при обработке запроса к внешним Web-ресурсам из локальной сети SquidGuard должен просматривать достаточно большое количество текстовых файлов. Если процесс настройки фильтров на вашей системе завершен, то имеет смысл преобразовать текстовые файлы в файлы баз данных, что позволит повысить производительность шлюза.

Шаг 1

Преобразуйте текстовые файлы в файлы баз данных:

```
[root@bastion /]# cd /var/spool/squid/squidGuard
[root@bastion squidGuard]# /usr/bin/squidGuard -C ads/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C ads/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C aggressive/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C aggressive/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C audio-video/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C audio-video/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C drugs/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C drugs/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C gambling/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C gambling/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C hacking/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C hacking/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C mail/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C porn/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C porn/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C proxy/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C proxy/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C violence/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C violence/urls
[root@bastion squidGuard]# /usr/bin/squidGuard -C warez/domains
[root@bastion squidGuard]# /usr/bin/squidGuard -C warez/urls
```

ЗАМЕЧАНИЕ Файл `/var/spool/squid/squidGuard/expressions` не может быть преобразован в файл баз данных.

Шаг 2

Отредактируйте файл `/etc/squid/squidGuard`:

```
#Path declarations
#Укажите путь к корневому каталогу с фильтрами.
dbhome /var/spool/squid/squidGuard
#Укажите путь к корневому каталогу с файлами регистрации.
logdir /var/log/squid/squidGuard
#Time space declarations
#В данном примере доступ разрешен по рабочим дням с 09:00 до 18:15
time workhours {
    weekly mtwhf 09:00 - 19:15
}
#Source group declarations
# Описание локальной сети.
src internal {
    ip     192.168.1.1/24
}
#Destination group declarations
#Описание ресурсов доступ, к которым запрещен.
dest ads {
    domainlist     ads/domains.db
```

```
    urllist        ads/urls.db
}
dest aggressive {
    domainlist     aggressive/domains.db
    urllist        aggressive/urls.db
}
dest audio-video {
    domainlist     audio-video/domains.db
    urllist        audio-video/urls.db
}
dest drugs {
    domainlist     drugs/domains.db
    urllist        drugs/urls.db
}
dest gambling {
    domainlist     gambling/domains.db
    urllist        gambling/urls.db
}
dest hacking {
    domainlist     hacking/domains.db
    urllist        hacking/urls.db
}
dest mail {
    domainlist     mail/domains.db
}
dest porn {
    domainlist     porn/domains.db
    urllist        porn/urls.db
    expressionlist porn/expressions
}
dest proxy {
    domainlist     proxy/domains.db
    urllist        proxy/urls.db
}
dest violence {
    domainlist     violence/domains.db
    urllist        violence/urls.db
}
dest varez {
    domainlist     warez/domains.db
    urllist        warez/urls.db
}
#Rewrite rule group declarations
#Авторы не рекомендуют использовать этот раздел.

#Access Control Lists

#Списки контроля доступа (ACCESS CONTROL LISTS)
#
#Разрешите доступ со всех машин в локальной сети
#в рабочие дни и рабочее время
#ко всем ресурсам, кроме перечисленных в фильтре.
acl {
     internal within workhours {
     pass !ads !aggressive !audio-video !drugs !gambling
     !hacking !mail !porn !proxy !violence !warez
     all
    }
#Запрет и переадресация всех остальных запросов.
    default {
       pass     none
       redirect redirect http://bastion.und/cgi-
bin/squidGuard.cgi?clientaddr=%a&clientname=%n&clientuser=%i&clientgroup=
%s&targetgroup=%t&url=%u
```

```
        }
}
```

Шаг 3
Протестируйте работоспособность SquidGuard в соответствии с вышеприведенными рекомендациями.

Глава 26

Виртуальные частные сети, VPN

В этой главе:

Виртуальные частные сети (Virtual Private Network) – по своей сути довольно широкий термин, не определяющий определенного типа сетей или протоколов, но вцелом, предполагающий использование «туннельной» пересылки конфиденциальных данных по сетям общего пользования. В настоящей главе рассмотрены два метода формирования туннелей:

- по протоколу IPSec (Internet Protocol Security);
- и достаточно уязвимый и устаревший протокол PPTP (Point-To-Point Tunneling Protocol), по непонятным для авторов причинам широко используемый провайдерами для предоставления доступа в Интернет через так называемые широкополосные сети.

Протокол IPSec, реализованный в рамках проекта FreeS/WAN, обычно используют для объединения фрагментов корпоративных сетей с помощью сетей общего пользования. При этом данные, передаваемые из одной сети в другую, инкапсулируются в пакеты другого типа, шифруются исходящим шлюзом при передаче через сети общего пользования и преобразуются в исходный вид принимающим шлюзом. В настоящее время нет достоверной информации о безопасности этого протокола.

Уязвимость протокола PPTP в реализации Microsoft, используемого провайдерами для передачи по сетям общего пользования информации от шлюза в Интернет к своим клиентам, описана в работах Брюса Шнейера (Bruce Shneier) и Петера Муджа (Peter Mudge), опубликованных на `http://www phrack.com`. Учитывая типичность ситуации, когда в качестве шлюза в Интернет используется VPN-сервер на базе MS Windows NT, и единственной возможностью подключить Linux-систему является использование PPTP, в этой главе также рассматривается установка и конфигурирование пакетов Microsoft Point-To-Point Encryption и PPTP Client, реализующих такое соединение.

ЗАМЕЧАНИЕ В случае, если ваши учетные данные при подключении по протоколу PPTP к MS Windows NT VPN-серверу провайдера будут использованы злоумышленниками, а счет за услуги будет выставлен вам, всегда можно грамотно предъявить претензии своему провайдеру, сославшись на широко известную уязвимость этого протокола в реализации Microsoft.

VPN-сервер FreeS/WAN

FreeS/WAN – очень специфичный программный продукт, исходные коды которого состоят из двух частей – патча для исходных кодов ядра и файлов, устанавливаемых на системе обычным образом. Обновления кода ядра выходят гораздо чаще, чем обновления кодов FreeS/WAN, поэтому не все версии ядер и FreeS/WAN совместимы. Сведения о совместимости различных версий ядра и FreeS/WAN могут быть получены с `http://www.freeswan.ca/download.php#contact`, кроме того, авторы протестировали работоспособность FreeS/WAN версии 1.99 с версиями ядер 2.4.18 и 2.4.19, исходные коды которых были модифицированы патчем Grsecurity.

FreeS/WAN использует три протокола:

- протокол аутентификации (Authentication Header, AH);
- протокол шифрования (Encapsulation Security Payload, ESP);
- протокол обмена ключами (Internet Key Exchange, IKE).

Функции по поддержанию защищенного канала распределяются между этими протоколами следующим образом:

- протокол AH используется для контроля целостности и проверки подлинности данных;
- протокол ESP предназначен для шифрования данных, но он может также контролировать аутентификацию и целостность данных;
- протокол IKE предназначен для автоматического предоставления конечным точкам канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

Ядро IPSec – KLIPS (Kernel IPSec) реализует протоколы AH и ESP и взаимодействие пакетов с ядром. Демон `pluto` реализует через протокол IKE взаимодействие с другими системами.

Схема типового варианта построения виртуальной частной сети, объединяющей локальные сети двух офисов с использованием сетей общего пользования, представлена на рис.26.1.

Ограничения и допущения

Исходные коды находятся в каталоге `/usr/src`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Используется ядро версии 2.4.18 или 2.4.19, собранное из исходных кодов в соответствии с рекомендациями главы 6. К исходным кодам ядер возможно применение патча Grsecurity.

Требуется перекомпиляция ядра.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

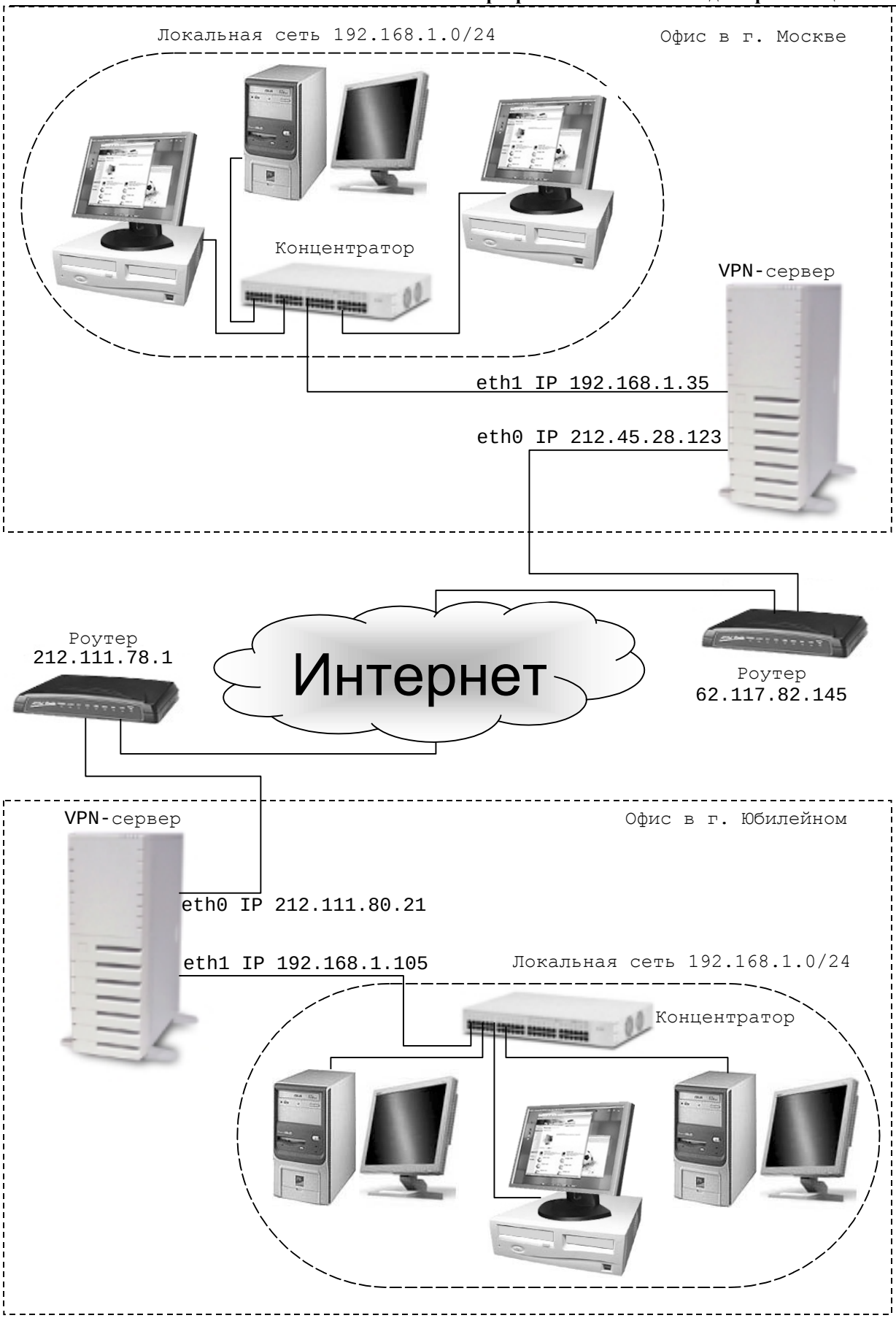


Рис. 26.1. Схема типового варианта построения виртуальной частной сети.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта FreeS/WAN по состоянию на 15.03.2003. Регулярно посещайте домашнюю страницу проекта `http://www.giptables.org` и отслеживайте обновления.

Исходные коды FreeS/WAN содержатся в архиве `freeswan-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `freeswan-1.99.tar.gz`).

Для нормальной инсталляции и работы программного обеспечения необходимо, чтобы в системе были дополнительно установлены пакеты `gmp-4.0.1-3.i386.rpm` и `gmp-devel-4.0.1-3.i386.rpm`, входящие в дистрибутив ASPLinux 7.3 (Vostok). Если вы следовали рекомендациям главы 2, то они уже должны быть установлены.

Компиляция, оптимизация и инсталляция FreeS/WAN

Для компиляции, оптимизации и инсталляции FreeS/WAN на каждом из шлюзов выполните следующие операции.

Шаг 1

Распакуйте архив с пакетом `freeswan-1.99.tar.gz` в каталоге `/usr/src`:

```
[root@yubileyny src]# tar -xzpf freeswan-1.99.tar.gz
```

Шаг 2

Для размещения файлов FreeS/WAN в соответствующих каталогах и повышения производительности VPN в файле `/usr/src/freeswan-1.99/Makefile.inc` измените строку:

```
INC_USRLOCAL=/usr/local
```

на:

```
INC_USRLOCAL=/usr/
```

Строку:

```
INC_MANDIR=man
```

на:

```
INC_MANDIR=share/man
```

Строку:

```
USERCOMPILE=-g -O3
```

на:

```
USERCOMPILE=-g –O2
```

Строку:

```
KLIPSCOMPILE=-O3
```

на:

```
KLIPSCOMPILE=-O2
```

Шаг 3

Сконфигурируйте исходные коды ядра с поддержкой FreeS/WAN:

```
[root@yubileyny src]# cd freeswan-1.99
[root@yubileyny freeswan-1.99]# make ogo
```

После запуска программы вам будет предложено ответить на вопросы связанные с конфигурацией ядра.

Для включения поддержки FreeS/WAN в коды ядра необходимо ответить на приведенные ниже вопросы следующим образом:

```
Kernel/User netlink socket (CONFIG_NETLINK) [Y/n/?] <y>
Netlink device emulation (CONFIG_NETLINK_DEV) [Y/n/?] (NEW) <y>
...
IP Security Protocol (FreeS/WAN IPSEC) (CONFIG_IPSEC) [Y/n/?] <Enter>
*
IPSEC options (FreeS/WAN)
*
IPSEC: IP-in-IP encapsulation (tunnel mode) (CONFIG_IPSEC_IPIP)
[Y/n/?]<Enter>
```

```
IPSEC: Authentication Header (CONFIG_IPSEC_AH) [Y/n/?]<Enter>
HMAC-MD5 authentication algorithm (CONFIG_IPSEC_AUTH_HMAC_MD5) [Y/n/?]
<Enter>
HMAC-SHA1 authentication algorithm (CONFIG_IPSEC_AUTH_HMAC_SHA1) [Y/n/?]
<Enter>
IPSEC: Encapsulating Security Payload (CONFIG_IPSEC_ESP) [Y/n/?] <Enter>
3DES encryption algorithm (CONFIG_IPSEC_ENC_3DES) [Y/n/?] <Enter>
IPSEC: IP Compression (CONFIG_IPSEC_IPCOMP) [Y/n/?] <Enter>
IPSEC Debugging Option (CONFIG IPSEC_DEBUG) [Y/n/?] <Enter>
```

ЗАМЕЧАНИЕ Все настройки, сделанные для ядра при его первичной настройке, сохраняются и будут предложены вам в качестве значений опций, предлагаемых по умолчанию.

Шаг 4

Проинсталлируйте FreeS/WAN, создайте и сохраните список проинсталлированных файлов:

```
[root@yubileyny freeswan-1.99]# find /* > /root/freeswan1
[root@yubileyny freeswan-1.99]# make install
[root@yubileyny freeswan-1.99]# find /* > /root/freeswan2
[root@yubileyny freeswan-1.99]# diff /root/freeswan1 /root/freeswan2 >
/root/freeswan.installed
[root@yubileyny freeswan-1.99]# mv /root/ freeswan.installed
/very_reliable_place/freeswan.installed.YYYYMMDD
```

Шаг 5

Проинсталлируйте в соответствии с рекомендациями главы 6 новое ядро, конфигурация которого была осуществлена на 2 шаге.

Шаг 6

Удалите архив с исходными кодами и каталог `freeswan-1.99`:

```
[root@yubileyny freeswan-1.99]# cd ..
[root@yubileyny src]# rm -rf freeswan-1.99/
[root@yubileyny src]# rm -f freeswan-1.99.tar.gz
```

Конфигурирование FreeS/WAN

Основными конфигурационными файлами FreeS/WAN являются файлы:

- `/etc/ipsec.conf`;
- `/etc/ ipsec.secrets`.

Для конфигурирования шлюзов виртуальной частной сети, организуемой с помощью FreeS/WAN, на обоих шлюзах необходимо выполнить следующие настройки.

Шаг 1

Отредактируйте в соответствии с вашими потребностями и ниже приведенными рекомендациями файл `/etc/ipsec.conf`. В рассматриваемом примере:

```
# /etc/ipsec.conf – конфигурационный файл FreeS/WAN
# Примеры конфигурационных файлов находятся в каталоге
# doc/examples исходных кодов.
config setup
# Сетевой интерфейс, используемый IPSec
interfaces="IPSEC0=eth0"
# Запрет на выдачу отладочных сообщений
# all – включение выдачи отладочных сообщений
klipsdebug=none
plutodebug=none
# Автоматическая установка соединений и аутентификация
# при запуске IPSec
plutoload=%search
plutostart=%search
# Параметры соединения между локальными сетями
# Название соединения (произвольная строка)
conn Moscow-Yubileyny
# Исходные данные для шлюза в Москве
# IP адрес
```

```
left=212.45.28.123
# Описание локальной сети
leftsubnet=192.168.1.0/24
# IP ближайшего к шлюзу в Москве роутера
# (может быть определен с помощью traceroute)
leftnexthop=62.117.82.145
# Исходные данные для шлюза в Юбилейном
# IP адрес
right=212.111.80.21
# Описание локальной сети
rightsubnet=192.168.1.0/24
# IP ближайшего к шлюзу в Юбилейном роутера
rightnexthop=212.111.78.1
# Количество попыток проверки ключей
# 0 – до достижения положительного результата
keyingtries=0
# Тип аутентификации(AH или ESP)
auth=ah
# Устанавливать соединение при запуске IPSec
auto=start
```

ЗАМЕЧАНИЕ Файлы на обоих шлюзах должны быть идентичны с точностью до значения параметра `interfaces`, которое должно соответствовать имени внешнего интерфейса каждого из шлюзов.

В рассматриваемом примере файл `/etc/ipsec.conf` состоит из двух разделов.

Первый раздел – `config setup` – содержит общие опции конфигурации, используемые всеми соединениями.

Опция `interfaces="IPSEC0=eth0"`
определяет сетевое устройство для интерфейса IPSec. В данном случае это первая сетевая карта. При использовании значения по умолчанию, т. е. `interfaces=%defaultroute`, в качестве сетевого интерфейса будет выбрано устройство, используемое для соединения с Интернет или локальной сетью.

Опция `plutoload=%search`
определяет соединения, автоматически загружаемые в память при старте демона `pluto`. Значение опции по умолчанию `none` запрещает загрузку всех соединений, `%search` – загружает все соединения с установленным значением опции `auto=start` или `auto=add`. В качестве значения опции может использоваться имя соединения, например, `plutoload="Moscow-Yubileyny"` или список имен соединений, разделенных пробелами.

Опция `plutostart=%search`
определяет соединения, автоматически устанавливаемые при старте демона `pluto`. Значение опции по умолчанию `none` запрещает установку всех соединений, `%search` – устанавливает все соединения с установленным значением опции `auto=start`. В качестве значения опции может использоваться имя соединения, например, `plutoload="Moscow-Yubileyny"` или список имен соединений, разделенных пробелами.

Во втором разделе – `conn Moscow-Yubileyny` – устанавливаются опции, имеющие отношение только к определенному соединению, в нашем примере, соединению с именем `Moscow-Yubileyny`.

Опции `left=212.45.28.123` и `right=212.111.80.21`
определяют, соответственно, IP-адрес шлюза в г. Москве и г. Юбилейном.

Опция `leftsubnet=192.168.1.0/24`
определяет параметры локальных сетей в г. Москве и г. Юбилейном.

Опции `leftnexthop=62.117.82.145` и `rightnexthop=212.111.78.1`
соответственно, определяют IP-адреса ближайших к шлюзам в г. Москве и в г. Юбилейном роутеров.

Опция `keyingtries=0`
определяет максимальное количество попыток обмена ключами при установке соединения. Значение опции равное `0`, устанавливаемое по умолчанию, предполагает неограниченное (до получения положительного результата) количество попыток.

Опция `auth=ah`
определяет протокол аутентификации данных (AH или ESP).

Опция `auto=start` определяет операции, которые должны быть выполнены при запуске IPSec. При установке значения `start` – соединение должно быть установлено автоматически, `add` – параметры соединения должны быть загружены в память.

Шаг 2

FreeS/WAN поддерживает два формата ключей, используемых демоном `pluto` для проверки подлинности соединений длиной до 256 бит. Каждый из этих форматов требует определенных операций по созданию ключей и изменению конфигурационных файлов FreeS/WAN.

В случае использования открытых зашифрованных ключей, для создания нового ключа на одном из шлюзов выполните команду:

```
[root@yubileyny /]# ipsec ranbits 256 > /root/key
```

Файл `/root/key.txt` содержит новый ключ:

```
[root@yubileyny /]# cat /root/key
0xaf4a2a4c_f58a942f_5a36d31e_23885ac4_490a58e2_b6ea25a3_0ee661d4_daf15661
```

Этим ключом необходимо заменить ключи, имеющиеся в файлах `/etc/ipsec.secrets`. Для этого в файлах `/etc/ipsec.secrets` на обоих шлюзах замените строку вида (у вас она может выглядеть по-другому):

```
10.0.0.1 11.0.0.1
"0x9748cc31_2e99194f_d230589b_cd846b57_dc070b01_74b66f34_19c40ala_804906e
d"
```

на:

```
212.45.28.123 212.111.80.21
"0xaf4a2a4c_f58a942f_5a36d31e_23885ac4_490a58e2_b6ea25a3_0ee661d4_daf1566
1"
```

Проверьте и установите права доступа для файлов `/etc/ipsec.conf` и `/etc/ipsec.secrets` на обоих шлюзах:

```
[root@yubileyny /]# chmod 600 /etc/ipsec.secrets
[root@yubileyny /]# chmod 644 /etc/ipsec.conf
```

В случае использования RSA-ключей, необходимо выполнить следующие операции для файлов `ipsec.conf` и `ipsec.secrets`, как описано ниже:

Создайте ключи RSA для каждого шлюза.

На шлюзе 212.45.28.123 (в г. Москве):

```
[root@moskow root]# cd /
[root@moskow /]# ipsec rsasigkey --verbose 1024 > /root/moscow-key
getting 64 random bytes from /dev/random...
looking for a prime starting there (can take a while)...
found it after 1233 tries.
getting 64 random bytes from /dev/random...
looking for a prime starting there (can take a while)...
found it after 9 tries...
computing modulus...
computing lcm(p-1, q-1)...
computing d...
computing exp1, exp1, coeff...
output...
```

На шлюзе 212.111.80.21 (в г. Юбилейном):

```
[root@yubileyny root]# cd /
[root@yubileyny /]# ipsec rsasigkey --verbose 1024 > /root/yubileyny-key
getting 64 random bytes from /dev/random...
looking for a prime starting there (can take a while)...
found it after 13 tries.
getting 64 random bytes from /dev/random...
looking for a prime starting there (can take a while)...
found it after 233 tries...
computing modulus...
computing lcm(p-1, q-1)...
computing d...
computing exp1, exp1, coeff...
output...
```

Измените файлы `/etc/ipsec.conf` на обоих шлюзах для обеспечения возможности использования RSA-ключей. На каждом из шлюзов в раздел файла `/etc/ipsec.conf` добавьте строки, выделенные более жирным шрифтом:

```
# /etc/ipsec.conf - конфигурационный файл FreeS/WAN
```

```
# Примеры конфигурационных файлов находятся в каталоге
# doc/examples исходных кодов.
config setup
# Сетевой интерфейс, используемый IPSec
interfaces="IPSEC0=eth0"
# Запрет на выдачу отладочных сообщений
# all – включение выдачи отладочных сообщений
klipsdebug=none
plutodebug=none
# Автоматическая установка соединений и аутентификация
# при запуске IPSec
plutoload=%search
plutostart=%search
# Параметры соединения между локальными сетями
# Название соединения (произвольная строка)
conn Moscow-Yubileyny
# Исходные данные для шлюза в Москве
# IP адрес
left=212.45.28.123
# Описание локальной сети
leftsubnet=192.168.1.0/24
# IP ближайшего к шлюзу в Москве роутера
# (может быть определен с помощью traceroute)
leftnexthop=62.117.82.145
# Исходные данные для шлюза в Юбилейном
# IP адрес
right=212.111.80.21
# Описание локальной сети
rightsubnet=192.168.1.0/24
# IP ближайшего к шлюзу в Юбилейном роутера
rightnexthop=212.111.78.1
# Количество попыток проверки ключей
# 0 – до достижения положительного результата
keyingtries=0
# Тип аутентификации(AH или ESP)
auth=ah
#Опции устанавливаемые для использования RSA-ключей
authby=rsasig
leftrsasigkey=<Public key of 212.45.28.123>
rightrsasigkey=<Public key of 212.111.80.21>
# Устанавливать соединение при запуске IPSec
auto=start
```

Опция `authby=rsasig` используется для включения поддержки проверки подлинности соединения с использованием RSA-ключей.

Опции `leftrsasigkey=<Public key of moscow>` и `rightrsasigkey=<Public key of yubileyny >` используются для ввода открытых ключей для 212.45.28.123 и 212.111.80.21, соответственно. Открытые ключи содержатся в файле `/root/moscow-key`:

```
# RSA 1024 bits   drwalbr.und   Mon Mar 10 17:41:55 2003
# for signatures only, UNSAFE FOR ENCRYPTION
#pubkey=0sAQN/KebjvkF/xc7IdhwJA/46FhuHvn1bU7UGbCwohsCttWoidHbO8pPDTmR8fwR
NKqcHTSkp5hiGr6CFXHVZ/5bmuqYb9Xv58/dUCqf6sHUbyTSseRjTv4+RcI4YYaxcrf51ZG5D
aZJa8RKDxsIfLF2jcG9IUzDOPSfYXpUo0gsQJQ==
#IN KEY 0x4200 4 1
AQN/KebjvkF/xc7IdhwJA/46FhuHvn1bU7UGbCwohsCttWoidHbO8pPDTmR8fwRNKqcHTSkp5
hiGr6CFXHVZ/5bmuqYb9Xv58/dUCqf6sHUbyTSseRjTv4+RcI4YYaxcrf51ZG5DaZJa8RKDxs
IfLF2jcG9IUzDOPSfYXpUo0gsQJQ==
# (0x4200 = auth-only host-level, 4 = IPSec, 1 = RSA)
Modulus:
0x7f29e6e3be417fc5cec8761c0903fe3a161b87be7d5b53b5066c2c2886c0adb56a22747
6cef293c34e647c7f044d2aa7074d2929e61886afa0855c7559ff96e6baa61bf57bf9f3f7
540aa7fab0751bc934ac7918d3bf8f91708e1861ac5cadfe75646e4369925af11283c6c21
f2c5da3706f485330ce3d27d85e9528d20b1025
```

```
PublicExponent: 0x03
# everything after this point is secret
PrivateExponent:
0x1531a67b4a603ff64d216904ac2b5509ae59ebf514e48df38112075c16757248e705be1
3cd286df5e26614bfd60cdc712be23186fbaec11d456b8f68e45543d0e28f25720c0012db
035b0b89e8e174e1b73831fe4ee39184e6c193df049b9b7d98b1b069ab4dda5dd8cdfb8b7
8a4d89c912ddb363f11c71d5f93a253472c5aab
Prime1:
0xcaa9ed7a02b9f0f252990304950d8b819c6e323e5062e9fa36d4843d8b07ca98d1c2fbc
d0ecc6104498fcfb864e0d1793f04cc6270e7ff940f85a1da43704801
Prime2:
0xa0a14dcf313f91e2ed4f5fbaa61ed2fd4ced1ae4aa073c79d1301cea05af3e740f774ff
c56f2dbb9b42011c4e66e787eca5758ab457b92e38b63255ae390a825
Exponent1:
0x871bf3a6ac7bf5f6e1bb5758635e5d0112f4217ee041f15179e302d3b20531bb3681fd3
35f32eb58310a8a7aedeb3650d4addd96f5efffb80a591691824adaab
Exponent2:
0x6b1633df762a6141f38a3fd1c4148ca8ddf367431c04d2fbe0cabdf1591f7ef80a4f8aa
839f73d267815612deef4505486e4e5c783a7b7425cecc391ed0b1ac3
Coefficient:
0xc29527035094a396b88b7bb586ee1add3086689060ff20e4f29277681309f2cd887263a
7a72867eeb7757a5f53a3803e33b1bea237c92a6104abdf9fdfbff157
```

и в файле/root/yubileyny-key:

```
# RSA 1024 bits   drwalbr.und   Mon Mar 10 17:43:07 2003
# for signatures only, UNSAFE FOR ENCRYPTION
#pubkey=0sAQPBVNukXMmREo55ChGtFKj+64+TW1P1lqSZtI8+WEvVAu2ua0Pdxz39Wpw4zxt
O+RzRCUljwoeEWu4KBXJa9uqtTtBtfN7inMz2KhF0wxugE3B+PC19WdcL3YU1P8pYAvtwjMk/
GHi3STbza8+IxDRewV4klEDTHvNgL3E/ReJcuw==
#IN KEY 0x4200 4 1
AQPBVNukXMmREo55ChGtFKj+64+TW1P1lqSZtI8+WEvVAu2ua0Pdxz39Wpw4zxtO+RzRCUljw
oeEWu4KBXJa9uqtTtBtfN7inMz2KhF0wxugE3B+PC19WdcL3YU1P8pYAvtwjMk/GHi3STbza8
+IxDRewV4klEDTHvNgL3E/ReJcuw==
# (0x4200 = auth-only host-level, 4 = IPSec, 1 = RSA)
Modulus:
0xc154dba45cc991128e790a11ad14a8feeb8f935b53f596a499b48f3e584bd502edae6b4
3ddc73dfd5a9c38cf1b4ef91cd1094963c287845aee0a05725af6eaad4ed06d7cdee29ccc
f62a1174c31ba013707e3c2d7d59d70bdd85353fca5802fb708cc93f1878b74936f36bcf8
8c4345ec15e249440d31ef3602f713f45e25cbb
PublicExponent: 0x03
# everything after this point is secret
PrivateExponent:
0x015f035f93b8ce3127235ad9ff697394df2c97bd786cdcc19f0c2c97231f672f39f828b
439db4910525841c3bd0430f8f12460bf588750d3413bfc684ce68463425eb7a25e6a719f
82328b396297c421641b80d6d03e6fa02daaa948a614d712ffeae3f7782709de6ebb80949
2aa5c1d5d0eb545b1bf68fde29ffe819543c29b
Prime1:
0xfd1877406f2f1d7e72fe0f87b5bca2efee80c6306865b48a5d9da420720d5ecf1f97bef
0b39e7cd0a57e0a51cac82aaffb1e096d0b5e55734b9546cd37f13f59
Prime2:
0xc38cd1ce6f12ea73cd555351bfc7f6bf5ed77fac6290a74858e8541bded02eb55c957b0
13759caf5942f8fa8f6274d82852643c44f07f5aa427afd12d79eee33
Exponent1:
0xa8bafa2af4ca13a9a1feb50523d3174a9f00842045992306e913c2c04c08e9df6a6529f
5cd145335c3a95c3687301c7552140648b23ee3a232638488cff62a3b
Exponent2:
0x825de1344a0c9c4d338e378bd52ff9d4e9e4ffc841b5c4dae5f03812948ac9ce3db8fca
b7a3bdca3b81fb51b4ec4de57036ed7d834aff91c2c51fe0c8fbf4977
Coefficient:
0x0b474a89523b664841d5332d57588a6e31a602d59570d615bcf3728f9c9e403fa19b4c8
e8d7a9c32c02c076d7f4fda73341978746da9e411766a622b4d586210
```

Вставьте открытые ключи в файлы /root/moscow-key и /root/yubileyny-key. В файле /etc/ipsec.conf замените строку:

```
leftrsasigkey=<Public key of 212.45.28.123>
```
на:
leftrsasig-
key="0sAQN/KebjvkF/xc7IdhwJA/46FhuHvn1bU7UGbCwohsCttWoidHbO8pPDTmR8fwRNKq
cHTSkp5hiGr6CFXHVZ/5bmuqYb9Xv58/dUCqf6sHUbyTSseRjTv4+RcI4YYaxcrf51ZG5DaZJ
a8RKDxsIfLF2jcG9IUzDOPSfYXpUo0gsQJQ=="

строку:
```
rightrsasigkey=<Public key of 212.111.80.21>
```
на:
rightrsasig-
key="0sAQPBVNukXMmREo55ChGtFKj+64+TW1P1lqSZtI8+WEvVAu2ua0Pdxz39Wpw4zxtO+R
zRCUl-
jwoeEWu4KBXJa9uqtTtBtfN7inMz2KhF0wxugE3B+PC19WdcL3YU1P8pYAvtwjMk/GHi3STbz
a8+IxDRewV4klEDTHvNgL3E/ReJcuw=="

ЗАМЕЧАНИЕ Значения ключей должны быть заключены в кавычки.

Поместите закрытые ключи в файлы `/etc/ipsec.secrets` на обоих шлюзах.
На шлюзе 212.45.28.123 файл `/etc/ipsec.secrets` отредактируйте следующим образом:
```
212.45.28.123 212.111.80.21: RSA {
Modulus:
0x7f29e6e3be417fc5cec8761c0903fe3a161b87be7d5b53b5066c2c2886c0adb56a22747
6cef293c34e647c7f044d2aa7074d2929e61886afa0855c7559ff96e6baa61bf57bf9f3f7
540aa7fab0751bc934ac7918d3bf8f91708e1861ac5cadfe75646e4369925af11283c6c21
f2c5da3706f485330ce3d27d85e9528d20b1025
PublicExponent: 0x03
# everything after this point is secret
PrivateExponent:
0x1531a67b4a603ff64d216904ac2b5509ae59ebf514e48df38112075c16757248e705be1
3cd286df5e26614bfd60cdc712be23186fbaec11d456b8f68e45543d0e28f25720c0012db
035b0b89e8e174e1b73831fe4ee39184e6c193df049b9b7d98b1b069ab4dda5dd8cdfb8b7
8a4d89c912ddb363f11c71d5f93a253472c5aab
Prime1:
0xcaa9ed7a02b9f0f252990304950d8b819c6e323e5062e9fa36d4843d8b07ca98d1c2fbc
d0ecc6104498fcfb864e0d1793f04cc6270e7ff940f85a1da43704801
Prime2:
0xa0a14dcf313f91e2ed4f5fbaa61ed2fd4ced1ae4aa073c79d1301cea05af3e740f774ff
c56f2dbb9b42011c4e66e787eca5758ab457b92e38b63255ae390a825
Exponent1:
0x871bf3a6ac7bf5f6e1bb5758635e5d0112f4217ee041f15179e302d3b20531bb3681fd3
35f32eb58310a8a7aedeb3650d4addd96f5efffb80a591691824adaab
Exponent2:
0x6b1633df762a6141f38a3fd1c4148ca8ddf367431c04d2fbe0cabdf1591f7ef80a4f8aa
839f73d267815612deef4505486e4e5c783a7b7425cecc391ed0b1ac3
Coefficient:
0xc29527035094a396b88b7bb586ee1add3086689060ff20e4f29277681309f2cd887263a
7a72867eeb7757a5f53a3803e33b1bea237c92a6104abdf9fdfbff157
}
```

На шлюзе 212.111.80.21 файл `/etc/ipsec.secrets` отредактируйте следующим образом:
```
212.45.28.123 212.111.80.21: RSA {
Modulus:
0xc154dba45cc991128e790a11ad14a8feeb8f935b53f596a499b48f3e584bd502edae6b4
3ddc73dfd5a9c38cf1b4ef91cd1094963c287845aee0a05725af6eaad4ed06d7cdee29ccc
f62a1174c31ba013707e3c2d7d59d70bdd85353fca5802fb708cc93f1878b74936f36bcf8
8c4345ec15e249440d31ef3602f713f45e25cbb
PublicExponent: 0x03
# everything after this point is secret
PrivateExponent:
0x015f035f93b8ce3127235ad9ff697394df2c97bd786cdcc19f0c2c97231f672f39f828b
439db4910525841c3bd0430f8f12460bf588750d3413bfc684ce68463425eb7a25e6a719f
```

```
82328b396297c421641b80d6d03e6fa02daaa948a614d712ffeae3f7782709de6ebb80949
2aa5c1d5d0eb545b1bf68fde29ffe819543c29b
Prime1:
0xfd1877406f2f1d7e72fe0f87b5bca2efee80c6306865b48a5d9da420720d5ecf1f97bef
0b39e7cd0a57e0a51cac82aaffb1e096d0b5e55734b9546cd37f13f59
Prime2:
0xc38cd1ce6f12ea73cd555351bfc7f6bf5ed77fac6290a74858e8541bded02eb55c957b0
13759caf5942f8fa8f6274d82852643c44f07f5aa427afd12d79eee33
Exponent1:
0xa8bafa2af4ca13a9a1feb50523d3174a9f00842045992306e913c2c04c08e9df6a6529f
5cd145335c3a95c3687301c7552140648b23ee3a232638488cff62a3b
Exponent2:
0x825de1344a0c9c4d338e378bd52ff9d4e9e4ffc841b5c4dae5f03812948ac9ce3db8fca
b7a3bdca3b81fb51b4ec4de57036ed7d834aff91c2c51fe0c8fbf4977
Coefficient:
0x0b474a89523b664841d5332d57588a6e31a602d59570d615bcf3728f9c9e403fa19b4c8
e8d7a9c32c02c076d7f4fda73341978746da9e411766a622b4d586210
}
```

Шаг 3

На обоих шлюзах в файлах `/etc/sysctl.conf` измените или проверьте наличие строки:

```
net.ipv4.ip_forward = 1
```

Для вступления изменений в силу перезагрузите сеть:

```
[root@yubileyny /]# /etc/init.d/network restart
Деактивируется интерфейс eth0:        [OK]
Деактивируется интерфейс-петля:       [OK]
Устанавливаются параметры сети:       [OK]
Активируется интерфейс loopback:      [OK]
Активируется интерфейс eth0:          [OK]
```

или выполните команду, что не потребует перезагрузки:

```
[root@yubileyny /]# sysctl –w IP_forward =1
```

Шаг 4

Настройте систему сетевой защиты, руководствуясь рекомендациями глав 9 и 10.

Система сетевой защиты, как минимум, должна иметь правила, разрешающие:

- поддержку канала обмена ключами (работу демона `pluto`) – порт 500, протокол UDP;
- поддержку шифрования данных по протоколу ESP – протокол 50;
- поддержку протокола контроля целостности и аутентификации по протоколу AH – протокол 51.

Для реализации этих правил, если вы используете систему сетевой защиты IPTables, в стартовый скрипт `iptables` нужно добавить строки:

```
# allow IPsec
#
# Канал обмена ключами
iptables -A INPUT  -p udp --sport 500 --dport 500 -j ACCEPT
iptables -A OUTPUT -p udp --sport 500 --dport 500 -j ACCEPT
# Шифрование данных по протоколу ESP
iptables -A INPUT  -p 50 -j ACCEPT
iptables -A OUTPUT -p 50 -j ACCEPT
# Контроль за целостностью и аутентичностью данных по протоколу AH
iptables -A INPUT  -p 51 -j ACCEPT
iptables -A OUTPUT -p 51 -j ACCEPT
```

Шаг 5

Для нормальной работы IPSec на обоих шлюзах должна быть выключена подсистема `rp_filter`, используемая для защиты от подмены IP-адреса. Для этого на каждом из шлюзов выполните:

```
[root@yubileyny /]# echo 0 > /proc/sys/net/ipv4/conf/IPSEC0/rp_filter
[root@yubileyny /]# echo 0 > /proC/sys/net/ipv4/conf/eth0/rp_filter
```

Для того, чтобы требуемое значение параметра устанавливалось автоматически при загрузке системы, добавьте в файлы `/etc/rc.d/init.d/iptables` на каждом из шлюзов следующие строки:

```
# Disable IP spoofing protection to allow IPSEC to work properly
```

```
echo 0 > /proc/sys/net/ipv4/conf/IPSEC0/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
```

В противном случае в файл `/var/log/messagess` будут выданы следующие сообщения:

```
Map 10 17:24:40 moscow ipsec: ipsec_setup: WARNING: eth0 has route fil-
tering turned on, KLIPS may not work
Map 10 17:24:40 moscow ipsec_setup:
(/proc/sys/net/ipv4/conf/eth0/rp_filter = `1', should be 0)
```

Тестирование FreeS/WAN

Шаг 1

Перезагрузите оба шлюза, чтобы запустить FreeS/WAN.

Шаг 2

Проверьте отсутствие ошибок в файлах регистрации на каждом из шлюзов. В файлах `/var/log/messages` должны быть строки примерно следующего содержания:

```
Mar 10 17:24:39 moscow kernel: klips_info:ipsec_init: KLIPS startup,
FreeS/WAN IPSec version: 1.99
Map 10 17:24:39 moscow ipsec: ipsec_setup: Starting FreeS/WAN IPsec
1.99...
Map 10 17:24:39 moscow ipsec_setup: Starting FreeS/WAN IPsec 1.99...
Mar 10 17:24:40 moscow ipsec_setup: KLIPS debug `none'
Mar 10 17:24:40 moscow ipsec_setup: KLIPS ipsec0 on eth0
212.45.28.123/255.255.255.255 broadcast 0.0.0.0
Mar 10 17:24:41 moscow ipsec_setup: ...FreeS/WAN IPsec started
Map 10 17:24:41 moscow rc: Starting ipsec:  succeeded
```

В файлах `/var/log/secure` должны быть строки примерно следующего содержания:

```
Mar 10 17:24:40 moscow ipsec__plutorun: Starting Pluto subsystem...
Mar 10 17:24:41 moscow pluto[13069]: Starting Pluto (FreeS/WAN Version
1.99)
Mar 10 17:24:41 moscow pluto[13069]: added connection description "Mos-
cow_ Yubileyny"
Mar 10 17:24:41 moscow pluto[13069]: listening for IKE messages
Mar 10 17:24:42 moscow pluto[13069]: adding interface ipsec0/eth0
212.45.28.123
Mar 10 17:24:42 moscow pluto[13069]: loading secrets from
"/etc/ipsec.secrets"
Mar 10 17:24:42 moscow pluto[13069]: "Moscow-Yubileyny" #l: initiating
Main Mode
Mar 10 17:24:42 moscow pluto[13069]: "Moscow-Yubileyny" #l: ISAKMP SA es-
tablished
Mar 10 17:24:45 moscow pluto[13069]: "Moscow-Yubileyny" #2: initiating
Quick
Mode_POLICY_RSASIG+POLICY_ENCRYPT+POLICY_AUTHENTICATE+POLICY_TUNNEL+POLIC
Y_PFS
Mar 10 17:24:46 moscow pluto[13069]: "Moscow-Yubileyny" #2: sent Q12, IP-
Sec SA
Mar 10 17:24:49 moscow pluto[13069]: "Moscow-Yubileyny"  #3: responding
to Main Mode
Mar 10 17:24:49 moscow pluto[13069]: "Moscow-Yubileyny" " #3: sent MR3,
ISAKMP SA
Mar 10 17:24:50 moscow pluto[13069]: "Moscow-Yubileyny" #4: responding to
Quick Mode established
Mar 10 17:24:50 moscow pluto[13069]: "Moscow-Yubileyny"#4: IPSEC SA es-
tablished
```

На обоих шлюзах в каталоге `/proc/net/` должны содержаться следующие псевдофайлы:

```
[root@yubileyny /]# ls –l /proc/net/ipsec_*
-r--r--r--    1 root     root 0 Map 10 18:03 /proc/net/ipsec_eroute
-r--r--r--    1 root     root 0 Map 10 18:03 /proc/net/ipsec_klipsdebug
-r--r--r--    1 root     root 0 Map 10 18:03 /proc/net/ipsec_spi
```

```
-r--r--r--    1 root     root 0 Map 10 18:03 /proc/net/ipsec_spigrp
-r--r--r--    1 root     root 0 Map 10 18:03 /proc/net/ipsec_tncfg
-r--r--r--    1 root     root 0 Map 10 18:03 /proc/net/ipsec_version
```

Интерфейсы IPSec должны быть описаны ранее физических интерфейсов:

```
[root@yubileyny /]# cat /proc/net/ipsec_tncfg
ipsec0 -> eth0 mtu=16260 -> 1500
ipsec1 -> NULL mtu=0 -> 0
ipsec2 -> NULL mtu=0 -> 0
ipsec3 -> NULL mtu=0 -> 0
```

Шаг 3

Тестирование работоспособности созданного туннеля и виртуальной частной сети может быть осуществлено путем проверки связи между системами, находящимися в разных локальных сетях. В нашем случае, система `drwalbr.und` (192.168.1.105) находилась в локальной сети офиса в г. Юбилейном, а система `karlnext.und` (192.168.1.35) – в локальной сети офиса в г. Москве. Для проверки связи наберите:

```
[karlnext@karlnext /]$ ping –c 3 192.168.1.105
PING 192.168.1.105 (192.168.1.105) from 192.168.1.35: 56(84) bytes of
data.
64 bytes from 192.168.1.105 (192.168.1.105): icmp_seq=1 ttl=249 time=4.17
ms
64 bytes from 192.168.1.105 (192.168.1.105): icmp_seq=2 ttl=249 time=4.73
ms
64 bytes from 192.168.1.105 (192.168.1.105): icmp_seq=3 ttl=249 time=4.56
ms

--- 192.168.1.105 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2021ms
rtt min/avg/max/mdev = 4.170/4.490/4.731/0.235 ms
```

и:

```
[drwalbr@drwalbr /]$ ping –c 3 karlnext.und
PING karlnext.und (192.168.1.35) from 192.168.1.105: 56(84) bytes of
data.
64 bytes from karlnext.und (192.168.1.105): icmp_seq=1 ttl=249 time=4.17
ms
64 bytes from karlnext.und (192.168.1.105): icmp_seq=2 ttl=249 time=4.73
ms
64 bytes from karlnext.und (192.168.1.105): icmp_seq=3 ttl=249 time=4.56
ms

--- karlnext.und ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2021ms
rtt min/avg/max/mdev = 4.170/4.490/4.731/0.235 ms
```

Шаг 4

Протестируйте предназначенные для работы в локальной сети приложения, обращающиеся к системам, расположенным в локальной сети другого офиса.

Выше рассмотрен тривиальный вариант использования и настройки FreeS/WAN. Более сложные случаи рассмотрены в файлах документации, содержащихся в каталоге `/doc` исходных кодов FreeS/WAN и страницах документации.

Подключение к MS WINDOWS NT VPN-серверу с помощью PPTP-клиента

PPTP-клиент реализует PPTP (Point-to-Point Tunneling Protocol) протокол, предназначенный для подключения систем с Linux, FreeBSD и NetBSD к виртуальным частным сетям через MS Windows NT VPN-сервер. PPTP позволяет шифровать передаваемую информацию с ключом длиной 128 бит. Кроме того, этот протокол, не смотря на известные проблемы с безопасностью, используется некоторыми провайдерами для реализации доступа в Интернет через локальные сети общего пользования, и в некоторых случаях является единственной возможностью подключения Linux-системы к Интернет. В такой ситуации оказались жители г. Юбилейного Московской области. В этом городе ЗАО «Инфолайн» имеет сеть и шлюз в Интернет, реализованный на базе Windows NT VPN-сервера. С их помощью и предоставляются услуги доступа в Интернет.

Укрупненная схема сопряжения компьютеров клиентов ЗАО «Инфолайн» с Интернет представлена на рис. 26.2.

> **ЗАМЕЧАНИЕ** К сожалению, информация представленная на рис. 26.2 получена не от ЗАО «Инфолайн» (авторы являются клиентами компании, но в течение двух лет не получили ни одного ответа из службы поддержки на свои вопросы), а путем анализа сообщений стандартных утилит, используемых для тестирования работоспособности сетей. Схема не претендует на полноту и полную достоверность и может содержать ошибки из-за неверного использования утилит, неверной интерпретации выводов результатов их работы и др. причин. Тем не менее, полученные авторами данные позволили настроить доступ в Интернет с Linux-систем. Вопросы, касающиеся некоторых особенностей использования адресного пространства в локальной сети ЗАО «Инфолайн» просьба адресовать службе сервисной поддержки, а не авторам этой книги.

Учитывая, что подключение Linux-системы к MS Windows NT VPN-серверу с помощью PPTP-клиента представляет интерес, в основном, для начинающих пользователей, ниже описывается процедура установки необходимого программного обеспечения из rpm-пакетов с некоторыми подробностями, которые могут показаться излишними для опытных пользователей.

Ограничения и допущения

rpm-пакеты находятся в каталоге `/usr/src`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Используется ядро версии 2.4.18-5asp, или 2.4.18 или 2.4.19, собранные из исходных кодов в соответствии с рекомендациями главы 6. Работоспособность приведенных ниже рекомендаций протестирована для ядер версии 2.4.18 или 2.4.19, собранных из исходных кодов, модифицированных соответствующим патчем Grsecurity.

Для ядра версии 2.4.18-5asp, входящего в комплект поставки ASPLinux 7.3 (Vostok) перекомпиляция не требуется.

По данным, полученным клиентами ЗАО «Инфолайн», процедура, описанная в этой главе, применима без внесения изменений к Red Hat Linux 7.3, а с незначительными изменениями – и для последних версий Linux Slackware и AltLinux.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта PPTP Client по состоянию на 01.02.2003. Регулярно посещайте домашнюю страницу проекта `http://pptpclient.sourceforge.net` и отслеживайте обновления. Для организации подключения системы с ASPLinux 7.3 к MS Windows NT VPN-серверу необходимы пакет `ppp-mppe-2.4.0-4.i386.rpm`, реализующий протокол MPPE (Microsoft Point-To-Point Encryption) и `pptp-linux-1.1.0-1.i386.rpm`, содержащий клиент PPTP.

Инсталляция MPPE и PPTP-клиента

Шаг 1

Проверьте параметры настройки ядра. Если вы используете ядро версии 2.4.18-5asp, поставляемое в составе ASPLinux 7.3, то можете пропустить этот шаг. В противном случае проверьте, что в вашей конфигурации ядра установлены следующие опции:

```
IP: tunneling (CONFIG_NET_IPIP) [N/y/?] <y>
IP: GRE tunnels over IP (CONFIG_NET_IPGRE) [N/y/?] <y>
Dummy net driver support (CONFIG_DUMMY) [Y/n/?] <y>
PPP (point-to-point protocol) support (CONFIG_PPP) [N/y/?] <y>
```

Если опции не были установлены, то перекомпилируйте и проинсталлируйте новое ядро.

Шаг 2

Скачайте `ppp-mppe-2.4.0-4.i386.rpm`, `pptp-linux-1.1.0-1.i386.rpm` в каталог `/var/tmp`, осуществите проверку подлинности и целостности пакетов с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

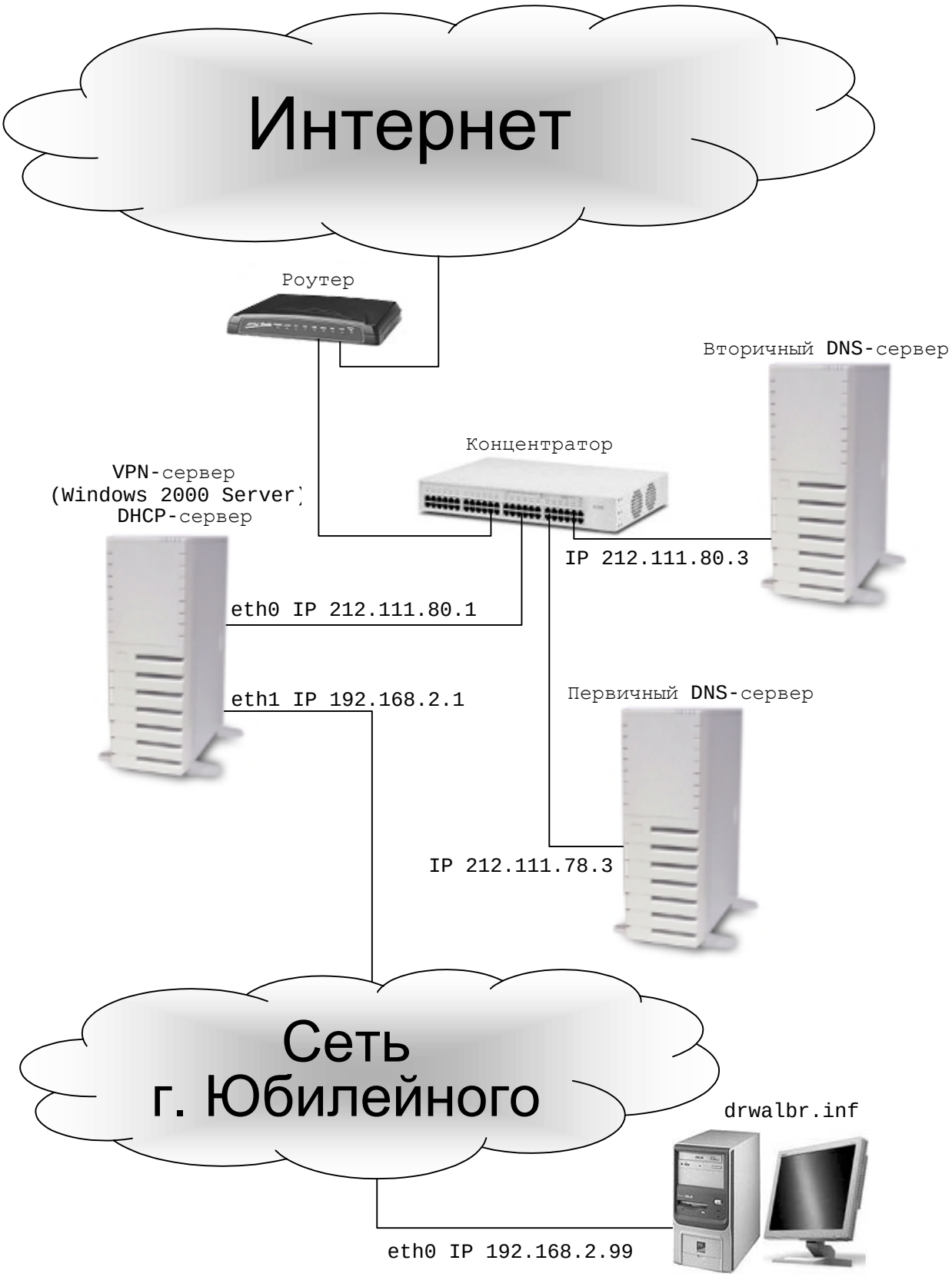


Рис. 26.2. Схема сопряжения компьютеров клиентов ЗАО «Инфолайн» с Интернет.

Шаг 3

Создайте и установите модуль поддержки MPPE. Для этого установите пакет `ppp-mppe-2.4.0-4.i386.rpm`, игнорируя зависимости:

```
[root@drwalbr /]# cd /var/tmp
[root@drwalbr tmp]# rpm -Uhv --nodeps ppp-mppe-2.4.0-4.i386.rpm.
```

В результате получите сообщение о том, что модуль ядра нужно собрать самостоятельно.

Шаг 4

Для создания модуля нужны исходные коды ядра. Если вы используете стандартное ядро версии 2.4.18-5asp, установите пакет `kernel-source-2.4.18-5asp.rpm`. Для этого вставьте третий диск дистрибутива ASPLinux 7.3 в привод CD-ROM и выполните:

```
[root@drwalbr /]# mount /mnt/cdrom
[root@drwalbr /]# cd /mnt/cdrom/ASPLinux/RPMS/
[root@drwalbr RPMS]# rpm -ihv kernel-source-2.4.18-5asp.rpm
[root@drwalbr RPMS]# cd /
[root@drwalbr /]# umount /mnt/cdrom
```

Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то вместо выше перечисленных команд, выполните:

```
[root@drwalbr /]# cd /home/distrib
[root@drwalbr distrib]# rpm -ihv kernel-source-2.4.18-5asp.rpm
```

Далее выполните:

```
[root@drwalbr distrib]# cd /usr/src/linux-2.4.18-5asp/
[root@drwalbr linux-2.4.18-5asp]# cp /boot/config-2.4.18-5asp ./config
```

Если вы используете ядро, созданное из исходных кодов, и придерживались рекомендаций главы 6, то исходные коды содержатся в каталоге `/usr/src/linux-2.4.x`. Если вы уже удалили исходные коды, то выполните:

```
[root@drwalbr /]# cp linux-2.4.x.tar.gz /usr/src/
[root@drwalbr /]# tar xzpf linux-2.4.x.tar.gz
[root@drwalbr /]# cd /usr/src/linux-2.4.x/
```

Шаг 5

Соберите модуль ядра:

```
[root@drwalbr linux-2.4.x]# make dep
[root@drwalbr linux-2.4.x]# cd /usr/lib/ppp-mppe-2.4.0/linux/
[root@drwalbr linux-2.4.x]# ./kmodbuild.sh /usr/src/linux-2.4.x
```

После выполнения этой команды могут появиться различные предупреждения, которые следует проигнорировать.

Шаг 6

Проинсталлируйте модуль ядра:

```
[root@drwalbr linux-2.4.x]# kernel-modules/kmodinst.sh kernel-
modules/new-2.4.x
```

Откорректируйте ссылки в файле `/etc/modules.conf`. Для этого строку:

```
alias char-major-108 ppp
```

замените на:

```
alias char-major-108 ppp_generic
```

и добавьте строку:

```
alias ppp-compress-18 mppe
```

Шаг 7

Установите PPTP-клиента:

```
[root@drwalbr linux-2.4.x]# cd /var/tmp
[root@drwalbr tmp]# rpm -Uhv pptp-linux-1.1.0-1.i386.rpm
```

Конфигурирование PPTP-клиента

Передача параметров PPTP-клиенту возможна через интерфейс командной строки и конфигурационные файлы. Наиболее простым способом конфигурирования клиента является использование скрипта, написанного на языке Perl, с именем `pptp-command`, входящего в дистрибутив PPTP-клиента. Для настройки необходимы следующие исходные данные:

- IP-адрес в локальной сети провайдера и имя вашей системы;
- имя учетной записи (логин) и пароль на VPN-сервере провайдера;
- IP-адрес VPN-сервера в локальной сети провайдера;
- IP-адреса первичного и вторичного DNS-серверов;
- IP-адрес внешнего шлюза.

Рассмотрим конфигурирование PPTP-клиента при следующих исходных данных:

- ваш IP-адрес: 192.168.2.99;
- имя компьютера: `drwalbr.inf`;
- логин: `sv_bambr`;
- пароль: sEcReTnOe_Sl0v0;
- IP-адрес шлюза в локальной сети: 192.168.2.1;
- IP-адрес первичного DNS: 212.111.78.3;
- IP-адрес вторичного DNS: 212.111.80.3;
- IP-адрес внешнего шлюза: 212.111.80.10.

Шаг 1

Войдите в систему в качестве обычного пользователя и запустите скрипт `pptp-command` от имени пользователя root:

```
[drwalbr@drwalbr /$ sudo /usr/sbin/pptp-command
Password: drwalbr_secretnoe_slovo
1.) start
2.) stop
3.) setup
4.) quit
```

Выберите пункт 3:

```
What task would you like to do?: 3 <Enter>
```

Шаг 2

Введите информацию, необходимую для аутентификации на сервере VPN:

```
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
```

Выберите пункт 1:

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

Выберите пункт 2:

```
?: 2 <Enter>
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
```

Введите имя вашей системы:

```
Local Name: sv_bambr <Enter>
```

Установите предлагаемое по умолчанию имя удаленной системы:

```
This is the 'remote' identifier for CHAP authentication.
In most cases, this can be left as the default. If 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]: <Enter>

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

Password: sEcReTnOe_Sl0v0 <Enter>
Adding sv_bambr PPTP *****
```

Шаг 3

Добавьте новый туннель:

```
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
```

Выберите пункт 4:

```
?: 4 <Enter>
Add a NEW PPTP Tunnel.

1.) Other
```

Выберите пункт 1:

```
Which configuration would you like to use?: 1 <Enter>
```

Введите имя туннеля (любая строка):

```
Tunnel Name: drwalbr_internet <Enter>
```

Введите IP-адрес шлюза в локальной сети:

```
Server IP: 192.168.2.1 <Enter>
```

Добавьте, в случае необходимости, опции команды `route`, обеспечивающие прохождение пакетов с вашей системы в Интернет:

```
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( command.
Enter a blank line to stop.
route: del default <Enter>
route: add default gw 212.111.80.10 <Enter>
route: <Enter>
```

Шаг 4

Задайте IP-адреса DNS-серверов:

```
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
```

Выберите пункт 6:

```
?: 6 <Enter>
```

Если вы для всех соединений используйте одни и те же сервера:

```
Use a PPTP-specific resolv.conf during tunnel connections? [Y/n]: n <En-
ter>
```

Выберите один из файлов, содержащих IP-адреса DNS-серверов (у вас не выбран ни один из файлов):

```
1.) Other
Which configuration do you want to use?: 1 <Enter>
```

Введите IP-адреса DNS-серверов:

```
What domain names do you want to search for partially specified names?
Enter all of them on one line, seperated by spaces.
Domain Names: inf <Enter>
Enter the IP addresses of your nameservers
Enter a blank IP address to stop.
Nameserver IP Address:212.111.78.3 <Enter>
Nameserver IP Address:212.111.80.3 <Enter>
Copying /etc/resolv.conf to /etc/resolv.conf.real...
Creating link from /etc/resolv.conf.real to /etc/resolv.conf
```

ЗАМЕЧАНИЕ Если вы не являетесь клиентом ЗАО «Инфолайн», не используйте приведенные выше IP-адреса DNS-серверов. Использование DNS-серверов без разрешения их владельцев – признак плохого тона.

Выберите туннель, используемый по умолчанию:

```
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
```

Выберите пункт 7:

```
?: 7 <Enter>
1.) drwalbr_internet
2.) cancel
```

Выберите пункт 1:

```
Which tunnel do you want to be the default?: 1 <Enter>
```

Завершите конфигурирование PPTP:

```
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
```

Выберите пункт 8:

```
?: 8 <Enter>
```

Тестирование подключения к MS WINDOWS NT VPN-серверу с помощью PPTP-клиента

Шаг 1

Снова запустите `pptp-command` от имени пользователя `root`:

```
 [drwalbr@drwalbr drwalbr]$ sudo /usr/sbin/pptp-command
Password:drwalbr_$e(retnoe_(l0vo
1.) start
2.) stop
3.) setup
4.) quit
What task would you like to do?: 1 <Enter>
1.)VPN
```

Установите соединение с VPN-сервером, выбрав пункт 1:

```
Start a tunnel to which server?: 1 <Enter>
```

Через несколько секунд должно появиться сообщение на экране:

```
Route: del default added
Route: add default gw 212.111.80.10 added
All routes added.
Tunnel VPN is active on ppp0.  IP Address: 212.111.80.221
```

и в файле `/var/log/messages`:

```
Mar 15 22:21:00 drwalbr pptp[22863]:
log[pptp_dispatch_ctrl_packet:pptp_ctrl.c:580]: Client connection estab-
lished.
Mar 15 22:21:01 drwalbr pptp[22863]:
log[pptp_dispatch_ctrl_packet:pptp_ctrl.c:708]: Outgoing call established
(call ID 0, peer's call ID 17326).
Mar 15 22:21:01 drwalbr kernel: CSLIP: code copyright 1989 Regents of the
University of California
Mar 15 22:21:01 drwalbr kernel: PPP generic driver version 2.4.2
Mar 15 22:21:01 drwalbr pppd[8100]: pppd 2.4.0 started by root, uid 0
Mar 15 22:21:01 drwalbr pppd[8100]: Using interface ppp0
Mar 15 22:21:01 drwalbr pppd[8100]: Connect: ppp0 <--> /dev/pts/0
Mar 15 22:21:03 drwalbr pptp[22863]:
log[pptp_dispatch_ctrl_packet:pptp_ctrl.c:757]: PPTP_SET_LINK_INFO re-
cieved from peer_callid 0
Mar 15 22:21:03 drwalbr pptp[22863]:
log[pptp_dispatch_ctrl_packet:pptp_ctrl.c:760]:   send_accm is 00000000,
recv_accm is FFFFFFFF
Mar 15 22:21:03 drwalbr pppd[8100]: Remote message:
S=7FECC7F871AD80E87A2B7F1048D9FE915BC917DA
Mar 15 22:21:03 drwalbr kernel: PPP MPPE compression module registered
Mar 15 22:21:03 drwalbr insmod: Warning: loading /lib/modules/2.4.19-
grsec/misc/mppe.o will taint the kernel: no license
Mar 15 22:21:03 drwalbr insmod:   See http://www.tux.org/lkml/#s1-18 for
information about tainted modules
Mar 15 22:21:03 drwalbr insmod: Module mppe loaded, with warnings
Mar 15 22:21:03 drwalbr pppd[8100]: MPPE 128 bit, stateless compression
enabled
Mar 15 22:21:03 drwalbr pppd[8100]: local  IP address 212.111.80.221
Mar 15 22:21:03 drwalbr pppd[8100]: remote IP address 212.111.80.10
```

Шаг 2

Проверьте наличие доступа в Интернет:

```
[root@drwalbr drwalbr]# ping –c 3 omega2.infline.ru
```

Если получены сообщения, подобные этим:

```
PING (212.111.78.6) from 212.111.80.221: 56(84) bytes of data.
64 bytes from omega2.infline.ru (212.111.78.6): icmp_seq=1 ttl=126
time=4.88 ms
```

```
64 bytes from omega2.infline.ru (212.111.78.6): icmp_seq=2 ttl=126
time=3.14 ms
64 bytes from omega2.infline.ru (212.111.78.6): icmp_seq=3 ttl=126
time=4.89 ms
--- omega2.infline.ru ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2021ms
rtt min/avg/max/mdev = 3.145/4.306/4.891/0.822 ms
```

то соединение установлено и работоспособно. В противном случае проверьте правильность сетевых настроек вашей системы и ознакомьтесь с документацией по диагностике PPTP-клиента, которая может быть получена с `http://pptpclient.sourceforge.net/howto-diagnosis.phtml`.

Проверьте наличие доступа к Web-ресурсам:

```
[root@drwalbr drwalbr]$ lynx www.infline.ru
```

Если вы увидите индексную страницу сервера:

```
                                                    Инфолайн» (p1 of 6)
   left_part_logo center_part_logo right_part_logo
   [naviarr.gif] [spacer.gif] Навигация [spacer.gif] [adrarr.gif]
   [spacer.gif] www.infline.ru [spacer.gif] [adrarr.gif] [spacer.gif]
   Новости
   О компании
   Интернет
   Телефонная связь
   Кабельное ТВ
   Оборудование
   Вакансии
   Наши адреса
   …
```

то процесс настройки подключения к MS WINDOWS NT VPN-серверу с помощью PPTP-клиента можно считать завершенным.

Шаг 3

Завершите соединение:

```
[root@drwalbr $]# sudo /usr/sbin/pptp-command
1.) start
2.) stop
3.) setup
4.) quit
```

Выберите пункт **4**:

```
What task would you like to do?: 4 <Enter>
Sending HUP signal to PPTP processes...
pptp: no process killed
```

В файле `/var/log/messages` должны появиться сообщения:

```
Мар 15 22:24:10 drwalbr pptp: Sending HUP signal to PPTP processes...
Mar 15 22:24:10 drwalbr pptp[22863]:
log[callmgr_main:pptp_callmgr.c:245]: Closing connection
Mar 15 22:24:10 drwalbr pptp[22863]:
log[pptp_conn_close:pptp_ctrl.c:307]: Closing PPTP connection
Mar 15 22:24:10 drwalbr pppd[8100]: Hangup (SIGHUP)
Mar 15 22:24:10 drwalbr pppd[8100]: Modem hangup
Mar 15 22:24:10 drwalbr pppd[8100]: Connection terminated.
Mar 15 22:24:10 drwalbr pppd[8100]: Connect time 3.2 minutes.
Mar 15 22:24:10 drwalbr pppd[8100]: Sent 4816 bytes, received 29486 bytes
```

Приведенные сообщения указывают на корректное завершение соединения и содержат информацию о времени соединения – 3,2 минуты, объеме исходящего и входящего трафика, соответственно – 4816 и 29486 Байт.

Часть 7

Программное обеспечение для организации службы электронной почты

Глава 27

Exim – почтовый транспортный агент

В этой главе:

Exim – почтовый транспортный агент (Mail Transport Agent, MTA), разработанный в университете г. Кембридж (University of Cambridge). Данное программное обеспечение предназначено для:

- доставки (приема и отправки) почтовых сообщений;
- фильтрации нежелательных сообщений;
- управления очередью сообщений, в том числе, доставка которых в данное время невозможна.

Exim является одним из самых безопасных почтовых транспортных агентов, именно поэтому авторы и предлагают устанавливать его на Linux-серверах вместо штатного агента Sendmail.

В этой главе рассматривается установка Exim в следующих двух конфигурациях:

- центрального почтового концентратора, т. е. сервера, предназначенного для приема, отправки и перенаправления почтовых сообщений со всех систем вашей локальной сети;
- локального почтового сервера, принимающего сообщения только от собственных локальных пользователей и перенаправляющего их на центральный почтовый концентратор сети.

В последнем случае Exim должен быть установлен на всех Linux-системах вашей сети. Даже если вы не собираетесь отсылать или получать почту с Linux-системы, то установка почтового сервера все равно необходима для обеспечения возможности получения служебных сообщений, адресованных пользователю `root` и другим специальным пользователям.

Exim, являясь почтовым транспортным агентом, не предназначен для чтения почты. Локальные пользователи почтового сервера могут просматривать, редактировать сообщения и выполнять другие элементарные операции по работе с почтой с помощью программы mail. Для получения почты пользователями вашей сети необходима установка дополнительного программного обеспечения, реализующего протоколы POP (Post Office Protocol) или IMAP (Internet Message Access Protocol), непосредственно взаимодействующего с клиентскими почтовыми программами (Mail User Agent, MUA). Принципиальная схема организации службы электронной почты представлена на рис. 27.1.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта Exim по состоянию на 06.06.2003. Регулярно посещайте домашнюю страницу проекта `http://www.exim.org/` и отслеживайте обновления.

Исходные коды Exim содержатся в архиве `exim-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `exim-4.20.tar.gz`). Подробная документация в формате HTML содержится в архиве `exim-html-version.tar.gz`.

Компиляция, оптимизация и инсталляция Exim

Для инсталляции Exim необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами, используя процедуры, описанные в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами Exim и документацией в каталоге `/var/tmp`:

```
[root@test tmp]# tar xzpf exim-4.20.tar.gz
[root@test tmp]# tar xzpf exim-html-4.10.tar.gz
```

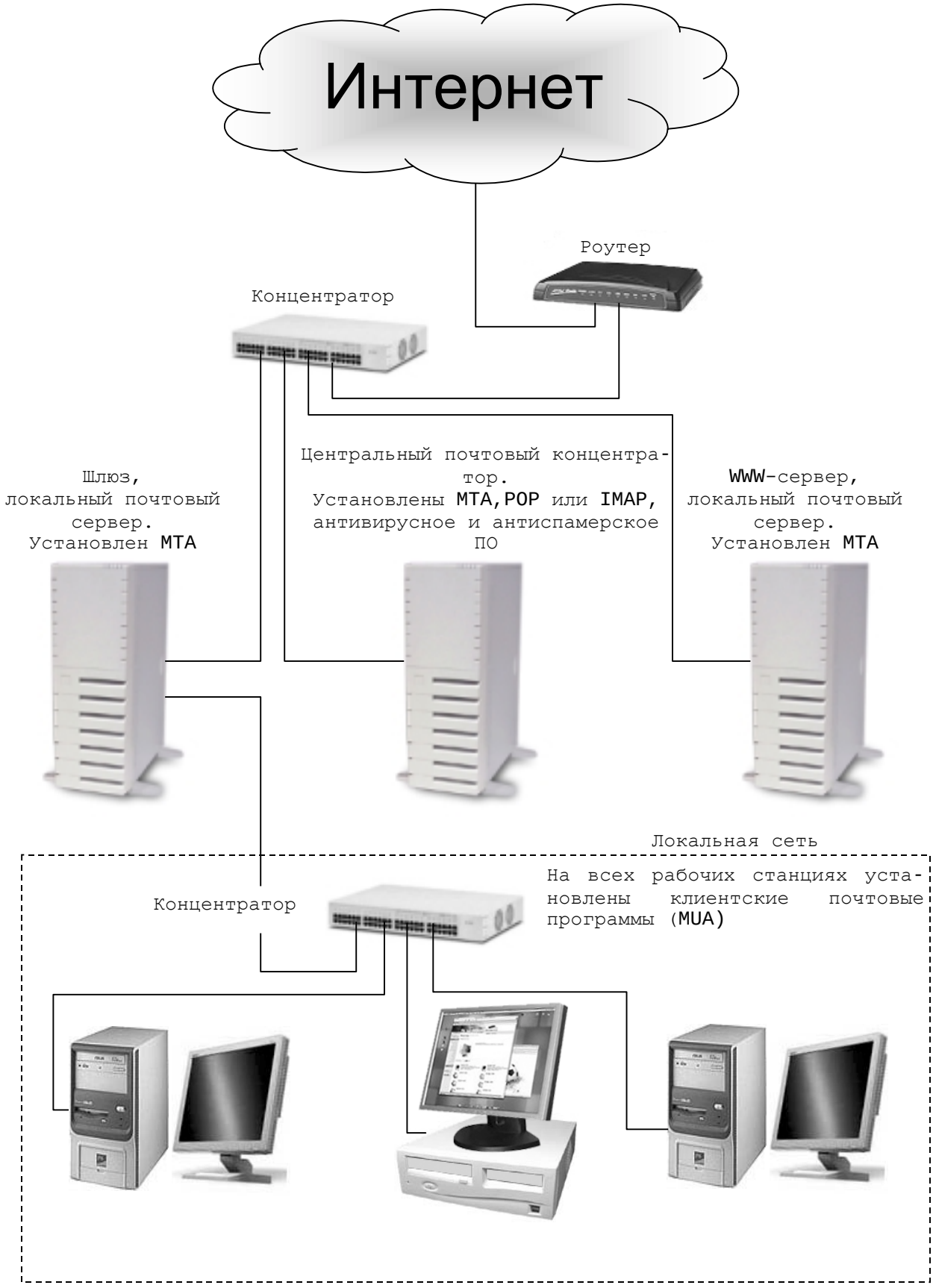


Рис. 27.1. Принципиальная схема организации службы электронной почты.

Шаг 3

Создайте специального пользователя `mail`, от имени которого будет запускаться Exim:

```
[root@test tmp]# groupadd -g 12 mail > /dev/null 2>&1 || :
[root@test tmp]# useradd -u 8 -g 12 -s /bin/false -M -r -d
/var/spool/mqueue mail > /dev/null 2>&1 || :
```

Шаг 4

Для добавления несуществующего командного интерпретатора добавьте в файл `/etc/shells` строку:

```
/bin/false/
```

Шаг 5

Процедура установки Exim несколько отличается от обычной процедуры установки программ с открытыми исходными кодами, в которой `Makefile` создается полуавтоматически с использованием команды `configure`. В комплект поставки входит файл `src/EDITME`, который может быть использован в качестве шаблона для создания собственной версии `Makefile`, оптимизированной под вашу операционную систему и решаемые задачи. Для создания `Makefile` скопируйте `src/EDITME` в файл `Local/Makefile`:

```
[root@test tmp]# cd exim-4.20
[root@test exim-4.20]# cp src/EDITME Local/Makefile
```

Для изменения заданного по умолчанию расположения исполняемых файлов в файле `/var/tmp/exim-4.20/Local/Makefile` замените строку:

```
BIN_DIRECTORY=/usr/exim/bin
```

на:

```
BIN_DIRECTORY=/usr/sbin
```

Для изменения заданного по умолчанию расположения конфигурационного файла замените строку:

```
CONFIGURE_FILE=/usr/exim/configure
```

на:

```
CONFIGURE_FILE=/etc/mail/exim.conf
```

Для определения пользователя, от имени которого будет запускаться Exim, замените строку:

```
# EXIM_USER=
```

на:

```
EXIM_USER=8
```

Для определения группы пользователей замените строку:

```
# EXIM_GROUP=
```

на:

```
EXIM_GROUP=12
```

Для изменения заданного по умолчанию каталога, в котором находятся пересылаемые сообщения, замените строку:

```
SPOOL_DIRECTORY=/var/spool/exim
```

на:

```
SPOOL_DIRECTORY=/var/spool/mqueue
```

Для отключения поддержки монитора, требующего наличия графического интерфейса, который не установлен из соображений безопасности, замените строку:

```
EXIM_MONITOR=eximon.bin
```

на:

```
# EXIM_MONITOR=eximon.bin
```

Для включения поддержки различных протоколов аутентификации пользователей замените строки:

```
# AUTH_CRAM_MD5=yes
# AUTH_PLAINTEXT=yes
```

на:

```
AUTH_CRAM_MD5=yes
AUTH_PLAINTEXT=yes
```

Для ведения файлов регистрации Exim с использованием службы `syslog` замените строку:

```
# LOG_FILE_PATH=syslog:/var/log/exim_%slog
```

на:
```
LOG_FILE_PATH=syslog
```

Для указания пути к программе, используемой Exim для разархивирования файлов, замените строку:
```
ZCAT_COMMAND=/usr/bin/zcat
```
на:
```
ZCAT_COMMAND=/usr/bin/gunzip
```

Для включения поддержки интерпретатора Perl замените строку:
```
# EXIM_PERL=perl.o
```
на:
```
EXIM_PERL=perl.o
```

Для изменения заданных по умолчанию путей к программам, необходимым для функционирования Exim, замените строки:
```
# CHOWN_COMMAND=/usr/bin/chown
# CHGRP_COMMAND=/usr/bin/chgrp
# MV_COMMAND=/bin/mv
# RM_COMMAND=/bin/rm
# PERL_COMMAND=/usr/bin/perl
```
на:
```
CHOWN_COMMAND=/bin/chown
CHGRP_COMMAND=/bin/chgrp
MV_COMMAND=/bin/mv
RM_COMMAND=/bin/rm
PERL_COMMAND=/usr/bin/perl
```

Для обеспечения возможности перемещения «замороженных» сообщений замените строку:
```
# SUPPORT_MOVE_FROZEN_MESSAGES=yes
```
на:
```
SUPPORT_MOVE_FROZEN_MESSAGES=yes
```

Шаг 6

Для оптимизации компиляции исходных кодов Exim применительно к архитектуре вашего процессора в файле `/var/tmp/exim-4.20/OS/Makefile-Linux` замените строку:
```
CFLAGS=-0
```
на:
```
CFLAGS=-O2 -march=i686 -funroll-loops
```

Шаг 7

Откомпилируйте, проинсталлируйте Exim, создайте и сохраните в надежном месте список установленных файлов:
```
[root@test exim-4.20]# make
[root@test exim-4.20]# find /* > /root/exim1
[root@test exim-4.20]# make install
[root@test exim-4.20]# ln -fs /usr/sbin/exim-4.20-1 /usr/lib/sendmail
[root@test exim-4.20]# ln -fs /usr/sbin/exim-4.20-1 /usr/lib/sendmail
[root@test exim-4.20]# ln -fs /usr/sbin/exim-4.20-1 /usr/sbin/sendmail
[root@test exim-4.20]# ln -fs /usr/sbin/exim-4.20-1 /usr/bin/mailq
[root@test exim-4.20]# ln -fs /usr/sbin/exim-4.20-1 /usr/bin/runq
[root@test exim-4.20]# mv /etc/aliases /etc/exim-4.20
[root@test exim-4.20]# strip /usr/sbin/exim-4.20-1
[root@test exim-4.20]# chown 0.mail /var/spool/mail
[root@test exim-4.20]# chmod 1777 /var/spool/mail
[root@test exim-4.20]# find /* > /root/exim2
[root@test exim-4.20]# diff /root/exim1 /root/exim2 > exim.installed
[root@test exim-4.20]# mv /root/exim.installed
/very_reliable_place/exim.installed.YYYYMMDD
```

Шаг 8

Удалите архивы и каталоги с исходными кодами программ и документацией:
```
[root@test exim-4.20]# cd /var/tmp/
[root@test tmp]# rm -rf exim-4.20/
```

```
[root@test tmp]# rm -f exim-4.20.tar.gz
[root@test tmp]# rm -rf exim-html-4.10/
[root@test tmp]# rm -f exim-html-4.10.tar.gz
```

Конфигурирование Exim

Конфигурирование Exim осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/mail/exim.conf`;
- файла `/etc/mail/localdomains`, содержащего имена ваших доменов;
- файла `/etc/mail/relaydomains`, содержащего имена доменов, которым разрешена рассылка почты с использованием вашего сервера;
- файла псевдонимов `/etc/mail/aliases`;
- файла доступа `/etc/mail/access`;
- файла фильтров `/etc/mail/system-filter`;
- системного конфигурационного файла `/etc/sysconfig/exim`, необходимого для передачи опций, с которыми должен запускаться Exim;
- файла инициализации `/etc/init.d/exim`, необходимого для запуска Exim.

Конфигурирование Exim в режиме центрального почтового концентратора

Конфигурационный файл /etc/mail/exim.conf

Шаг 1

Создайте файл `/etc/mail/exim.conf`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
######################################################################
#                    MAIN CONFIGURATION SETTINGS                     #
######################################################################
primary_hostname = test.bruy.info
acl_smtp_rcpt = check_recipient
acl_smtp_data = check_message

domainlist local_domains = @ : lsearch;/etc/mail/localdomains
hostlist relay_hosts = lsearch;/etc/mail/relaydomains
hostlist auth_relay_hosts = *

log_selector =  \
        +all_parents \
        +received_sender \
        +received_recipients \
        +smtp_confirmation \
        +smtp_syntax_error

allow_domain_literals = false
never_users = root:daemon:bin:sync:named
host_lookup = *
trusted_users = mail
gecos_pattern = ^([^,:]*)
gecos_name = $1
freeze_tell = postmaster
auto_thaw = 1h
ignore_bounce_errors_after = 30m
timeout_frozen_after = 7d

received_header_text = "Received: \
        ${if def:sender_rcvhost {from ${sender_rcvhost}\n\t}\
        {${if def:sender_ident {from ${sender_ident} }}\
        ${if def:sender_helo_name {(helo=${sender_helo_name})\n\t}}}}\
        by ${primary_hostname} \
        ${if def:received_protocol {with ${received_protocol}}} \
        (Exim ${version_number} #${compile_number})\n\t\
```

```
        id ${message_id}\
        ${if def:received_for {\n\tfor <$received_for>}}"

system_filter = /etc/mail/system-filter
message_body_visible = 5000
message_size_limit = 10M
smtp_accept_max = 2048
smtp_connect_backlog = 256
queue_only
split_spool_directory
queue_run_max = 1
remote_max_parallel = 1
rfc1413_hosts = *
rfc1413_query_timeout = 0s

smtp_banner = "Welcome on our mail server!\n\
        This system does not accept Unsolicited \
        Commercial Email\nand will blacklist \
        offenders via our spam processor.\nHave a \
        nice day!\n\n${primary_hostname} ESMTP Exim \
        ${version_number} ${tod_full}"

#############################################################################
#                       ACL CONFIGURATION                                   #
#         Specifies access control lists for incoming SMTP mail             #
#############################################################################

begin acl

check_recipient:
  accept  hosts = :

  deny    local_parts   = ^.*[@%!/|]

  deny    senders       = *@dbm;/etc/mail/access.db : \
                          dbm;/etc/mail/access.db

  require verify        = sender

  deny    message       = unrouteable address
          hosts         = !127.0.0.1/8:0.0.0.0/0
         !verify        = recipient

  accept  domains       = +local_domains
          endpass
          message       = unknown user
          verify        = recipient

  accept  hosts         = +relay_hosts

  accept  hosts         = +auth_relay_hosts
          endpass
          message       = authentication required
          authenticated = *

  deny    message       = relay not permitted


check_message:
  accept


#############################################################################
#                       ROUTERS CONFIGURATION                               #
```

```
#               Specifies how addresses are handled                  #
#########################################################################
#     THE ORDER IN WHICH THE ROUTERS ARE DEFINED IS IMPORTANT!         #
# An address is passed to each router in turn until it is accepted.    #
#########################################################################

begin routers

dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  transport = remote_smtp
  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
  no_more

system_aliases:
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup{$local_part}lsearch{/etc/mail/aliases}}
  user = mail
  file_transport = address_file
  pipe_transport = address_pipe

userforward:
  driver = redirect
  check_local_user
  file = $home/.forward
  no_verify
  no_expn
  check_ancestor
  allow_filter
  modemask = 002
  file_transport = address_file
  pipe_transport = address_pipe
  reply_transport = address_reply

localuser:
  driver = accept
  check_local_user
  transport = local_delivery

#########################################################################
#                      TRANSPORTS CONFIGURATION                         #
#########################################################################
#                       ORDER DOES NOT MATTER                           #
#     Only one appropriate transport is called for each delivery.      #
#########################################################################

begin transports

remote_smtp:
  driver = smtp

local_delivery:
  driver = appendfile
  file = /var/mail/$local_part
  delivery_date_add
  envelope_to_add
  return_path_add
  group = mail
  mode = 0600

address_pipe:
```

```
  driver = pipe
  return_output

address_file:
  driver = appendfile
  delivery_date_add
  envelope_to_add
  return_path_add

address_reply:
  driver = autoreply
#############################################################################
#                       RETRY CONFIGURATION                                 #
#############################################################################

begin retry

# Domain               Error       Retries
# ------               -----       -------

*                      *           F,2h,15m; G,16h,1h,1.5; F,4d,6h

#############################################################################
#                       REWRITE CONFIGURATION                               #
#############################################################################

begin rewrite

#############################################################################
#                   AUTHENTICATION CONFIGURATION                            #
#############################################################################

begin authenticators
```

Рассмотрим более подробно настройки каждого раздела главного конфигурационного файла.

В разделе `MAIN CONFIGURATION SETTINGS` определяются основные настройки Exim.

В строке:

```
primary_hostname = test.bruy.info
```

определяется полное имя вашего сервера. Возможно, это единственный параметр, который необходимо изменить в данном файле для нормальной работы Exim.

Строки:

```
acl_smtp_rcpt = check_recipient
acl_smtp_data = check_message
```

определяют имена списков контроля доступа, используемые в дальнейшем для определения правил работы с входящей почтой.

Строки:

```
domainlist local_domains = @ : lsearch;/etc/mail/localdomains
hostlist relay_hosts = lsearch;/etc/mail/relaydomains
hostlist auth_relay_hosts = *
```

определяют имена файлов, используемых для принятия решения о возможности разрешения или отмены пересылки сообщений с использованием SMTP-сервера Exim.

В первой строке определяется имя домена, который обслуживается SMTP-сервером, при этом знак `@` означает домен, указанный в строке `primary_hostname =`..., т. е. `test.bruy.info`. Директива `lsearch` добавляет к множеству обслуживаемых доменов список из файла `/etc/mail/localdomains`.

Во второй строке определяются хосты, которые могут использовать ваш почтовый сервер для отправки почты на любой почтовый адрес в Интернет. Директива `lsearch` указывает на то, что список хостов содержится и может быть получен вашим почтовым сервером из файла `/etc/mail/relaydomains`.

ЗАМЕЧАНИЕ В файл следует включать только названия хостов, которые отправляют почту в Интернет, используя ваш SMTP-сервер Exim. Хосты, которые отправляют почту на локальные почтовые адреса, например, служебные сообщения, адресуемые администратору системы на локальный почтовый адрес `root@test.bruy.info`, не следует включать в файл `/etc/mail/relaydomains`.

Строки:

```
log_selector =  \
        +all_parents \
        +received_sender \
        +received_recipients \
        +smtp_confirmation \
        +smtp_syntax_error
```

используются для определения опций регистрации, необходимых для использования с Exim. В рассматриваемом примере регистрируются все события, связанные с почтовым сервером. Это означает, что если вы посылаете, получаете, отправляете и т. д. почту, то все действия будут зарегистрированы в файле `/var/log/maillog`.

Строка:

```
allow_domain_literals = false
```

используется для запрещения обработки почтовых адресов в формате `mailbox@212.111.80.33`, который может быть использован для рассылки спама, задействуя ваш почтовый сервер.

Строка:

```
never_users = root:daemon:bin:sync:named
```

определяет список локальных пользователей, которым запрещено получать почту. В рассматриваемом примере пользователи `root`, `daemon`, `bin`, `sync` и `named` не смогут получать почту. Для доставки служебных сообщений, адресованных этим пользователям, используется файл `/etc/mail/aliases`.

Строка:

```
host_lookup = *
```

указывает на необходимость преобразования всех IP-адресов, содержащихся в заголовках входящей почты, в имена хостов. Эта опция снижает производительность почтового сервера. На сильно загруженных серверах эта строка должна быть закомментирована.

Строка:

```
trusted_users = mail
```

определяет список пользователей, от имени которых запущенны процессы, которые имеют возможность отправлять сообщения без указания поля `Sender`. Эта опция используется для обеспечения нормальной работы антивирусного и антиспамерского программного обеспечения. Элементы списка пользователей разделяются двоеточием.

Строки:

```
gecos_pattern = ^([^,:]*)
gecos_name = $1
```

обеспечивают добавление в заголовки сообщений дополнительных сведений, содержащихся в поле `gecos`.

Строка:

```
freeze_tell = postmaster
```

указывает на необходимость сообщения на некоторый почтовый адрес - в рассматриваемом примере `postmaster@test.bruy.info` - о «замороженных» сообщениях (т. е. сообщениях, которые невозможно доставить).

Строка:

```
auto_thaw = 1h
```

определяет интервал времени, по истечении которого производится повторная попытка доставки «замороженного» сообщения.

Строка:

```
ignore_bounce_errors_after = 30m
```

определяет интервал времени, по истечении которого производится повторная попытка доставки «замороженного» сообщения с игнорированием всех ошибок.

Строка:

```
timeout_frozen_after = 7d
```

определяет интервал времени, в течение которого «замороженные» сообщения должны быть удалены.

Строки:

```
received_header_text = "Received: \
        ${if def:sender_rcvhost {from ${sender_rcvhost}\n\t}\
        {${if def:sender_ident {from ${sender_ident} }}\
        ${if def:sender_helo_name {(helo=${sender_helo_name})\n\t}}}}\
        by ${primary_hostname} \
```

```
        ${if def:received_protocol {with ${received_protocol}}} \
        (Exim ${version_number} #${compile_number})\n\t\
        id ${message_id}\
        ${if def:received_for {\n\tfor <$received_for>}}"
```

определяют содержание заголовков, добавляемых к каждому входящему сообщению.

Строка:

```
system_filter = /etc/mail/system-filter
```

определяют имя и местоположение файла, содержащего фильтры, используемые для блокирования доставки нежелательных сообщений.

Строка:

```
message_body_visible = 5000
```

определяет максимальное количество строк сообщения, просматриваемое фильтрами.

Строка:

```
message_size_limit = 10M
```

определяет максимально допустимый размер обрабатываемых сообщений.

Строка:

```
smtp_accept_max = 2048
```

определяет максимальное число обрабатываемых подключений к SMTP-серверу. На небольших почтовых серверах с целью предотвращения DoS-атак это значение следует уменьшить, например, до 512.

Строка:

```
smtp_connect_backlog = 256
```

определяет максимальное число ожидаемых SMTP-соединений. В случае, если число установленных соединений превысит величину, определенную в этой строке, последующие попытки будут отменены на уровне TCP/IP.

Строка:

```
queue_only
```

отменяет немедленную доставку новых сообщений и помещает их в очередь.

Строка:

```
split_spool_directory
```

предписывает разбить каталог для входящей почты на 62 подкаталога, что повышает производительность системы.

Строка:

```
queue_run_max = 1
```

определяет максимальное количество процессов, обслуживающих очередь. Если установлено значение больше единицы, то возможна одновременная обработка сообщений в очереди несколькими процессами.

Строка:

```
remote_max_parallel = 1
```

определяет максимальное количество процессов, которые могут быть использованы для доставки сообщений. Если установлено значение больше единицы, то возможна одновременная доставка нескольких сообщений.

Строки:

```
rfc1413_hosts = *
rfc1413_query_timeout = 0s
```

повышают производительность сервера за счет запрета идентификационных соединений, описанных в RFC 1413.

Строки:

```
smtp_banner = "Welcome on our mail server!\n\
        This system does not accept Unsolicited \
        Commercial Email\nand will blacklist \
        offenders via our spam processor.\nHave a \
        nice day!\n\n${primary_hostname} ESMTP Exim \
        ${version_number} ${tod_full}"
```

определяют содержание сообщения, получаемого удаленной системой при установке соединения с SMTP-сервером.

В разделе `ACL CONFIGURATION` описываются списки контроля доступа для входящих сообщений.

Каждый раздел главного конфигурационного файла, кроме `MAIN CONFIGURATION SETTINGS`, начинается со строки, содержащей ключевое слово `begin` и название раздела. Для рассматриваемого раздела - это `begin acl`.

Строка:

```
check_recipient:
```

начинает описание свода правил для входящих сообщений.

Строка:

```
  accept  hosts = :
```

разрешает прием сообщений, отправителем которых является локальный SMTP-сервер.

Строка:

```
  deny    local_parts   = ^.*[@%!/|]
```

запрещает получать сообщения, содержащие в локальной части почтового адреса символы `@`, `%`, `!`, `/` и `|`. Эти символы практически никогда не используются в локальной части почтового адреса, но могут использоваться при попытках обхода правил блокирования сообщений.

Строки:

```
  deny    senders       = *@dbm;/etc/mail/access.db : \
                          dbm;/etc/mail/access.db
```

запрещают получать сообщения с почтовых адресов, содержащихся в файле базы данных `/etc/mail/access.db`.

Строка:

```
  require verify        = sender
```

запрещает получать почту, если адрес отправителя не определен.

Строки:

```
  deny    message       = unrouteable address
        hosts         = !127.0.0.1/8:0.0.0.0/0
      !verify         = recipient
```

запрещают получение сообщений, если они не адресованы локальному хосту, и запрещают проверку отправителя сообщения с локального хоста.

Строки:

```
  accept  domains       = +local_domains
          endpass
          message       = unknown user
          verify        = recipient
```

разрешают прием входящих сообщений только для локального хоста в случае, когда пользователь, которому адресовано сообщение, существует.

Строка:

```
accept  hosts         = +relay_hosts
```

разрешает прием сообщений с внешних хостов, обслуживаемых конфигурируемым SMTP-сервером.

Строки:

```
  accept  hosts         = +auth_relay_hosts
          endpass
          message       = authentication required
          authenticated = *
```

разрешают прием сообщений откуда угодно, в случае успешной аутентификации.

Строка:

```
  deny    message       = relay not permitted
```

служит признаком окончания свода правил списка контроля доступа `check_recipient`.

Строки:

```
check_message:
accept
```

разрешают прием сообщений, прошедших фильтрацию правилами, установленными в списке контроля доступа с именем `check_recipient`.

Дополнительная информация об опциях, используемых в этом разделе, может быть получена из файла документации `/var/tmp/exim-html-4.10/doc/html/spec_37.html`.

В разделе `ROUTERS CONFIGURATION` определяются способы обработки почтовых адресов и способы доставки сообщений.

Строка:

```
begin routers
```

определяет начало раздела.

Строки:

```
dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  transport = remote_smtp
  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
  no_more
```

описывают маршрутизатор, предназначенный для определения имени удаленных хостов-отправителей сообщений.

Строки:

```
system_aliases:
```

```
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup{$local_part}lsearch{/etc/mail/aliases}}
  user = mail
  file_transport = address_file
  pipe_transport = address_pipe
```

описывают маршрутизатор, предназначенный для пересылки сообщений в соответствии с определенными ранее псевдонимами.

Строки:

```
userforward:
  driver = redirect
  check_local_user
  file = $home/.forward
  no_verify
  no_expn
  check_ancestor
  allow_filter
  modemask = 002
  file_transport = address_file
  pipe_transport = address_pipe
  reply_transport = address_reply
```

описывают маршрутизатор, предназначенный для отправки сообщений. При этом строка:

```
file = $home/.forward
```

разрешает использование для перенаправления сообщений файлов `.forward`, находящихся в домашних каталогах пользователей. Эти файлы также могут быть использованы для создания пользовательских фильтров, например, помещающих письма из спамерских рассылок в отдельный почтовый ящик или выполняющих функции автоответчика.

Строки:

```
localuser:
  driver = accept
  check_local_user
  transport = local_delivery
```

описывают маршрутизатор, предназначенный для доставки сообщений локальным пользователям.

Дополнительная информация об опциях, используемых в этом разделе, может быть получена из файла документации `/var/tmp/exim-html-4.10/doc/html/spec_14.html`.

В разделе `TRANSPORTS CONFIGURATION` определяются механизмы доставки сообщений адресатам.

Строка:

```
begin transports
```

определяет начало раздела.

Строки:

```
remote_smtp:
  driver = smtp
```

описывают транспорт, ответственный за доставку сообщений с помощью SMTP-соединений.

Строки:

```
local_delivery:
  driver = appendfile
  file = /var/mail/$local_part
  delivery_date_add
  envelope_to_add
  return_path_add
  group = mail
  mode = 0600
```

описывают транспорт, ответственный за локальную доставку сообщений в пользовательские почтовые ящики традиционного BSD-формата.

Строки:

```
address_pipe:
  driver = pipe
  return_output
```

описывают транспорт, ответственный за доставку сообщений в соответствии с настройками псевдонимов и файлами `$home/.forward`.

Строки:

```
address_file:
  driver = appendfile
  delivery_date_add
  envelope_to_add
  return_path_add
```

описывают транспорт, ответственный за доставку сообщений в файлы, создаваемые при использовании псевдонимов и автоответов.

Строки:

```
address_reply:
  driver = autoreply
```

описывают транспорт, ответственный за доставку автоответов, сгенерированных фильтрами.

Дополнительная информация об опциях, используемых в этом разделе, может быть получена из файла документации `/var/tmp/exim-html-4.10/doc/html/spec_23.html`.

В разделе `RETRY CONFIGURATION` определяются правила повторной доставки сообщений.

Строка:

```
begin retry
```

определяет начало раздела.

Строка:

```
*          *              F,2h,15m; G,16h,1h,1.5; F,4d,6h
```

определяет для всех адресатов порядок повторной доставки сообщений, при отправке которых были получены ошибки. В рассматриваемом примере, попытки повторной отправки сообщений предпринимаются в течение первых двух часов через пятнадцать минут. Затем в течение 16 часов интервалы между попытками повторной доставки изменяются, каждый раз увеличиваясь в 1,5 раза, после этого в течение четырех суток попытки повторной доставки сообщений предпринимаются каждые 6 часов.

Дополнительная информация об опциях, используемых в этом разделе, может быть получена из файла документации `/var/tmp/exim-html-4.10/doc/html/spec_31.html`.

В разделе `REWRITE CONFIGURATION`, признаком начала которого является строка:

```
begin rewrite
```

определяются правила для сообщений, генерирующие во время доставки новые адреса. В рассматриваемом примере этот раздел не используется.

Дополнительная информация об опциях, используемых в этом разделе, может быть получена из файла документации `/var/tmp/exim-html-4.10/doc/html/spec_30.html`.

Раздел `AUTHENTICATION CONFIGURATION`, признаком начала которого является строка:

```
begin authenticators
```

используется для аутентификации пользователей. Особенности его настройки будут рассмотрены чуть ниже.

Шаг 2

После завершения настройки файла `/etc/mail/exim.conf` необходимо определить права доступа к этому файлу и назначить его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/mail/exim.conf
[root@test /]# chown 0.12 /etc/mail/exim.conf
```

Конфигурационный файл /etc/mail/localdomains

В файле `/etc/mail/localdomains` содержатся доменные имена, обслуживаемые конфигурируемым SMTP-сервером.

Шаг 1

Создайте файл `/etc/mail/localdomains`, руководствуясь вашими потребностями и ниже приведенными рекомендациями:

```
# localdomains - include all of your local domains name here.
# Virtual domains must be listed here to be recognized as local.
# N.B.: Exim must be restarted after this file is modified.
bruy.info
```

Шаг 2

Определите права доступа к файлу /etc/mail/localdomains и назначьте его владельцем пользователя root:

```
[root@test /]# chmod 640 /etc/mail/localdomains
[root@test /]# chown 0.12 /etc/mail/localdomains
```

Конфигурационный файл /etc/mail/relaydomains

В файле /etc/mail/relaydomains содержится список доменов, с которых разрешена отправка сообщений.

Шаг 1

Создайте файл /etc/mail/relaydomains, руководствуясь вашими потребностями и ниже приведенными рекомендациями:

```
# This file handle all domains from which relaying is allowed.
# By default we include the localhost of the server or nothing will work.
# Virtual Domains must be added to this list or relaying will be denied.
# N.B.: Exim must be restarted after this file is modified.
 localhost
```

Шаг 2

Определите права доступа к файлу /etc/mail/relaydomains и назначьте его владельцем пользователя root:

```
[root@test /]# chmod 640 /etc/mail/relaydomains
[root@test /]# chown 0.12 /etc/mail/relaydomains
```

Конфигурационный файл /etc/mail/aliases

Файл /etc/mail/aliases содержит правила для преобразования адреса получателя в другой. Совмещение имен в среде почтового сервера – это процесс преобразования одного локального имени получателя в другое. Из соображений безопасности Exim никогда не доставляет почту пользователю root. Для получения служебных сообщений, адресованных этому пользователю, и переадресации их пользователю, администрирующему систему, может быть использован файл /etc/mail/aliases. В RFC-2821 и RFC-2822 подробно описан минимальный набор псевдонимов, необходимый для нормальной работы почтовых серверов.

Шаг 1

Создайте файл /etc/mail/aliases, руководствуясь вашими потребностями и ниже приведенными рекомендациями:

```
# The following aliases are required by the mail RFCs 2821 and 2822.
# At least, you should set "postmaster" to the address of a HUMAN
# who deals with this system's mail problems.
#
postmaster:     real_person@test.bruy.info
mailer-daemon:  postmaster
root:           postmaster

# It is a good idea to redirect any messages sent to system accounts
# so that they don't just get ignored.
#
bin:            root
daemon:         root
sync:           root
mail:           root
pop:            root
uucp:           root
ftp:            root
nobody:         root
www:            root
named:          root
postgres:       root
mysql:          root
squid:          root
```

```
amavis:         root
operator:       root
abuse:          root
hostmaster:     root
webmaster:      root
```

ЗАМЕЧАНИЕ Не забудьте изменить `real_person@bruy.info` на действительный почтовый адрес системного администратора.

Шаг 2

Определите права доступа к файлу `/etc/mail/aliases` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/mail/aliases
[root@test /]# chown 0.12 /etc/mail/aliases
```

Шаг 3

Для повышения производительности почтового сервера, в рассматриваемом примере, сведения о псевдонимах пользователей хранятся в файле базы данных `/etc/mail/aliases.db`, а не в конфигурационном файле `/etc/mail/aliases`. Для формирования файла `/etc/mail/aliases.db` необходимо выполнить следующие команды:

```
[root@test /]# cd /etc/mail/
[root@test mail]# /usr/sbin/exim_dbinbuild aliases aliases.db
[root@test mail]# chmod 640 aliases.db
[root@test mail]# chown root.mail aliases.db
```

ЗАМЕЧАНИЕ Процедуру формирования файла базы данных необходимо осуществлять для вступления в силу любых изменений, внесенных в файл `/etc/mail/aliases`.

Конфигурационный файл etc/mail/access

Файл `/etc/mail/access` используется для блокировки получения почты с определенных почтовых адресов.

ЗАМЕЧАНИЕ Для борьбы со спамом лучше использовать программу SpamAssassin, интеграция которой с Exim описана ниже.

Шаг 1

Для блокировки доставки сообщений с нежелательных адресов, создайте файл `/etc/mail/access` и добавьте строки в соответствии с вашими потребностями и приведенными и ниже рекомендациями:

```
# The value part of the file must contain any email addresses from
# which you want to block access for sending mail to your server.
# N.B.: Exim must be restarted after this file is modified.
# Please list each email address one per line.
zlobny_spamer@yaho.com
hhc@email2me.net
```

Шаг 2

Определите права доступа к файлу `/etc/mail/access` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/mail/access
[root@test /]# chown 0.12 /etc/mail/access
```

Шаг 3

Для повышения производительности почтового сервера, в рассматриваемом примере, сведения о блокируемых адресах хранятся в файле базы данных `/etc/mail/access.db`, а не в конфигурационном файле `/etc/mail/access.db`. Для формирования файла `/etc/mail/access.db` необходимо выполнить следующие команды:

```
[root@test /]# cd /etc/mail/
[root@test mail]# /usr/sbin/exim_dbinbuild access access.db
[root@test mail]# chmod 640 access.db
[root@test mail]# chown root.mail access.db
```

ЗАМЕЧАНИЕ Формирование файла базы данных необходимо осуществлять для вступления в силу любых изменений, внесенных в файл `/etc/mail/access`.

Конфигурационный файл /etc/mail/system-filter

Файл `/etc/mail/system-filter` используется для настройки правил фильтрации сообщений.

Шаг 1

Для блокировки доставки сообщений с нежелательных адресов создайте файл `/etc/mail/system-filter` в соответствии с вашими потребностями и приведенными ниже рекомендациями:

```
## ----------------------------------------------------------------------
# Only run any of this stuff on the first pass through the filter - this
# is an optimization for messages that get queued and have several
# delivery attempts. We express this in reverse so we can just bail out
# on inappropriate messages.
#
if not first_delivery
then
  finish
endif

## ----------------------------------------------------------------------
# Check for MS buffer overruns as per BUGTRAQ.
# This could happen in error messages, hence its placing here...
# We substract the first n characters of the date header and test if its
# the same as the date header... which is a lousy way of checking if the
# date is longer than n chars long.
#
if ${length_80:$header_date:} is not $header_date:
then
  fail text "This message has been rejected because it has\n\
      an overlength date field which can be used\n\
      to subvert Microsoft mail programs\n\
             The following URL has further information\n\

http://www.securityfocus.com/frames/?content=/templates/article.html%3Fid
%3D61"
  seen finish
endif

## ----------------------------------------------------------------------
# These messages are now being sent with a <> envelope sender, but
# blocking all error messages that pattern match prevents bounces
# getting back.... so we fudge it somewhat and check for known
# header signatures. Other bounces are allowed through.
#
if $header_from: contains "@sexyfun.net"
then
  fail text "This message has been rejected since it has\n\
      the signature of a known virus in the header."
  seen finish
endif
if error_message and $header_from: contains "Mailer-Daemon@"
then
  # looks like a real error message - just ignore it
  finish
endif

## ----------------------------------------------------------------------
# Look for single part MIME messages with suspicious name extensions.
# Check Content-Type header using quoted filename [con-
tent_type_quoted_fn_match]
#
```

```
if $header_content-type: matches
"(?:file)?name=(\"[^\"]+\\\\.(?:ad[ep]|ba[st]|chm|cmd|com|cpl|crt|eml|exe
|hlp|hta|in[fs]|isp|jse?|lnk|md[be]|ms[cipt]|pcd|pif|reg|scr|sct|shs|url|
vb[se]|ws[fhc])\")"
then
  fail text "This message has been rejected because it has\n\
      potentially executable content $1\n\
      This form of attachment has been used by\n\
             recent viruses or other malware.\n\
      If you meant to send this file then please\n\
      package it up as a zip file and resend it."
  seen finish
endif

# Same again using unquoted filename [content_type_unquoted_fn_match]
#
if $header_content-type: matches
"(?:file)?name=(\\\\S+\\\\.(?:ad[ep]|ba[st]|chm|cmd|com|cpl|crt|eml|exe|h
lp|hta|in[fs]|isp|jse?|lnk|md[be]|ms[cipt]|pcd|pif|reg|scr|sct|shs|url|vb
[se]|ws[fhc]))"
then
  fail text "This message has been rejected because it has\n\
      potentially executable content $1\n\
      This form of attachment has been used by\n\
             recent viruses or other malware.\n\
      If you meant to send this file then please\n\
      package it up as a zip file and resend it."
  seen finish
endif

## ---------------------------------------------------------------------
# Attempt to catch embedded VBS attachments in emails. These were
# used as the basis for the ILOVEYOU virus and its variants - many
# many varients. Quoted filename - [body_quoted_fn_match].
#
if $message_body matches "(?:Content-(?:Type:(?>\\\\s*)[\\\\w-]+/[\\\\w-
]+|Disposition:(?>\\\\s*)attachment);(?>\\\\s*)(?:file)?name=|begin(?>\\\
\s+)[0-
7]{3,4}(?>\\\\s+))(\"[^\"]+\\\\.(?:ad[ep]|ba[st]|chm|cmd|com|cpl|crt|eml|
exe|hlp|hta|in[fs]|isp|jse?|lnk|md[be]|ms[cipt]|pcd|pif|reg|scr|sct|shs|u
rl|vb[se]|ws[fhc])\")[\\\\s;]"
then
  fail text "This message has been rejected because it has\n\
      a potentially executable attachment $1\n\
      This form of attachment has been used by\n\
             recent viruses or other malware.\n\
      If you meant to send this file then please\n\
      package it up as a zip file and resend it."
  seen finish
endif

# Same again using unquoted filename [body_unquoted_fn_match].
if $message_body matches "(?:Content-(?:Type:(?>\\\\s*)[\\\\w-]+/[\\\\w-
]+|Disposition:(?>\\\\s*)attachment);(?>\\\\s*)(?:file)?name=|begin(?>\\\
\s+)[0-
7]{3,4}(?>\\\\s+))(\\\\S+\\\\.(?:ad[ep]|ba[st]|chm|cmd|com|cpl|crt|eml|ex
e|hlp|hta|in[fs]|isp|jse?|lnk|md[be]|ms[cipt]|pcd|pif|reg|scr|sct|shs|url
|vb[se]|ws[fhc]))[\\\\s;]"
then
  fail text "This message has been rejected because it has\n\
      a potentially executable attachment $1\n\
      This form of attachment has been used by\n\
             recent viruses or other malware.\n\
      If you meant to send this file then please\n\
```

```
        package it up as a zip file and resend it."
    seen finish
endif

## ------------------------------------------------------------------
```

ЗАМЕЧАНИЕ: Этот файл может быть модифицирован для фильтрации сообщений, содержащих вирусы и спам. Кроме того, он может быть использован вами в качестве примера при создании собственных фильтров.

Шаг 2

Определите права доступа к файлу `/etc/mail/system-filter` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/mail/system-filter
[root@test /]# chown 0.12 /etc/mail/system-filter
```

Конфигурационный файл /etc/sysconfig/exim

Файл `/etc/sysconfig/exim` используется для передачи Exim необходимых опций при запуске.

Шаг 1

Создайте файл `/etc/sysconfig/exim`, отредактируйте строки в соответствии с вашими потребностями и приведенными ниже рекомендациями:

```
# Run Exim as a daemon on the system. Remove the "-bd" option
# to run Exim as a Null Client Mail Server.
DAEMON="-bd "

# Procede the queue every 1 minutes.
QUEUE="-q1m"
```

В этом файле строка:

```
DAEMON=""
```

предписывает выполнять Exim в качестве службы и принимать внешние сообщения.

Строка:

```
UEUE="-q1m"
```

предписывает предпринимать попытки постановки сообщений в очередь с интервалом в 1 минуту.

Шаг 2

Определите права доступа к файлу `/etc/sysconfig/exim` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 644 /etc/sysconfig/exim
[root@test /]# chown 0.0 /etc/sysconfig/exim
```

Файл инициализационный /etc/init.d/exim

Шаг 1

Создайте `/etc/init.d/exim`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping Exim.
#
# chkconfig: 2345 80 30
# description: Exim is a Mail Transport Agent, which is the program \
#              that moves mail from one machine to another.
#
# processname: exim
# config: /etc/mail/exim.conf
# pidfile: /var/run/exim.pid

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
```

```
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/exim ] ; then
        . /etc/sysconfig/exim
fi

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If Exim is not available stop now.
[ -f /usr/sbin/exim ] || exit 0

# Path to the Exim binary.
exim=/usr/sbin/exim

RETVAL=0
prog="Exim"

start() {
        echo -n $"Starting $prog: "
        daemon $exim $DAEMON $QUEUE
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/exim
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $exim
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/exim
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $exim
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/exim ]; then
                stop
                start
                RETVAL=$?
        fi
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
```

```
esac
exit $RETVAL
```

Шаг 2

Сделайте файл исполняемым и определите его владельцем суперпользователя `root`:

```
[root@test /]# chmod 700 /etc/init.d/exim
[root@test /]# chown 0.0 /etc/init.d/exim
```

Шаг 3

Для автоматического запуска Exim при загрузке системы создайте необходимые символьные ссылки:

```
[root@test /]# chkconfig --add exim
[root@test /]# chkconfig --level 2345 exim on
```

Шаг 4

Проверьте наличие и при необходимости добавьте соответствующие записи в файлы зоны и обратной зоны вашего DNS-сервера.

Тестирование Exim

Шаг 1

Запустите Exim:

```
[root@test /]# /etc/init.d/exim start
Запускается Exim:                          [OK]
```

Шаг 2

Проверьте правильность синтаксиса конфигурационных файлов:

```
[root@test /]# /usr/sbin/exim -bV
```

Если вы получите сообщение, не содержащее ошибок, аналогичное приведенному ниже:

```
Exim version 4.20 #1 built 06-Jun-2003 13:46:13
Copyright (c) University of Cambridge 2003
Berkeley DB: Sleepycat Software: Berkeley DB 3.3.11: (July 12, 2001)
Authenticators: cram_md5 plaintext
Routers: accept dnslookup ipliteral manualroute queryprogram redirect
Configuration file is /etc/mail/exim.conf
```

то, скорее всего, конфигурационные файлы не содержат синтаксических ошибок.

Шаг 3

Проверьте, возможна ли доставка сообщений локальным пользователям:

```
[root@test /]# /usr/sbin/exim -bt postmaster
real_person@test.bruy.info
    <-- postmaster@test.bruy.info
  router = localuser, transport = local_delivery
```

Шаг 4

Проверьте, возможна ли доставка сообщений пользователям на удаленных системах в Интернет:

```
[root@test /]# /usr/sbin/exim -bt karloff@mtu.ru
karloff@mtu.ru
  router = dnslookup, transport = remote_smtp
  host mx.mtu.ru               [195.34.32.57]  MX=3
  host hueymiccailhuitl.mtu.ru [195.34.32.122] MX=5
  host mtu.ru                  [195.34.32.10]  MX=20
```

Шаг 5

Проверьте доставку сообщений локальным пользователям. Для этого отправьте письмо локальному пользователю, например, `postmaster`:

```
[root@test /]# /usr/sbin/exim -v postmaster
To: postmaster@test.bruy.info <Enter>
From: root@test.bruy.info <Enter>
Subject: Проверка <Enter>
Проверка доставки локальной почты с помощью Exim <Enter>
<Ctrl>+<D>
```

```
LOG: MAIN
  <= root@test.bruy.info U=root P=local S=350
```

Проверьте наличие сообщения в очереди на доставку:

```
[root@test /]# /usr/bin/mailq
 0m  376 19OEfY-0002FA-7s <>
        real_person@test.bruy.info
```

Посмотрите тело сообщения:

```
[root@test /]# /usr/sbin/exim -Mvb 19OEfY-0002FA-7s
19OEfY-0002FA-7s-D
Проверка доставки локальной почты с помощью Exim
```

После исчезновения сообщения из очереди, т. е. получения пустого вывода команды `mailq`, проверьте почту:

```
[root@test /]# mail –u real_person
From root@test.bruy.info Fri Jun 06 14:31:00 2003
Return-path: <root@test.bruy.info>
Envelope-to: postmaster@test.bruy.info
Delivery-date: Fri, 06 Jun 2003 14:31:00 +0400
Received: from root by test.bruy.info with local (Exim 4.20 #1 )
 id 19OEfY-0002FA-7s
 for <postmaster@test.bruy.info>; Fri, 06 Jun 2003 14:30:50 +0400
To: postmaster@test.bruy.info
From:root@test.bruy.info
Subject: Проверка
Message-Id: <19OEfY-0002FA-7s@test.bruy.info>
Date: Fri, 06 Jun 2003 14:30:50 +0400
Status: RO
Проверка доставки локальной почты с помощью Exim
```

Шаг 6

Проверьте (по аналогии с шагом 5) доставку сообщений пользователям удаленных систем. Для этого отправьте сообщение удаленному пользователю и проверьте его почту.

Шаг 7

Проверьте (по аналогии с шагом 5) возможность получения почты локальными пользователями от пользователей удаленных систем.

Аутентификация пользователей перед отправкой сообщений

По умолчанию Exim не позволяет отправлять почту с помощью клиентских почтовых программ (Mail User Agent, MUA), установленных на удаленных системах. Попробуйте с помощью клиентской почтовой программы, установленной на удаленной системе и настроенной на отправку почты через ваш SMTP-сервер, отправить сообщение какому-нибудь адресату. У вас ничего не получится. Не стоит расстраиваться по этому поводу, т. к. это не получится и у спамеров, которые захотят использовать ваш SMTP-сервер для отправки своих сообщений. Для разрешения отправки почты через ваш SMTP-сервер и затруднения его использования для рассылок спама следует разрешить отправку сообщений только после удачной аутентификации пользователя.

Для настройки такого режима отправки сообщений (с аутентификацией пользователей на основе стандартных модулей PAM) необходимо выполнить следующие операции.

Шаг 1

В файле `/etc/mail/exim.conf` в конец раздела `AUTHENTICATION CONFIGURATION` добавьте следующие строки:

```
# AUTH PLAIN authentication meth0d used by Netscape Messenger.
#
plain:
driver = plaintext
public name = PLAIN
server_condition = "${if and {{!eq{$2}{}}{!eq{$3}{}} \
{crypteq{$3}{${extract{l}{:} \
{${lookup{$2}lsearch{/etc/mail/exim.auth} \
```

```
{$value }{*:*}}}}}}}{ 1} (0}}"
# AUTH LOGIN authentication meth0d used by Outlook Express.
#
login:
driver = plaintext
public name = LOGIN
server prompts = "Username:: : Password::"
server_condition = "${if and {{!eq{$l}{}}{!eq{$2}{}} \
{crypteq{$2} ${extract{l}(:} \
{$ { lookup ( $1 } lsearch{ /etc/mail/exim.auth} \
{$value}{*:*}}}}}}}{l}{0}}"
```

Шаг 2

На предыдущем шаге с использованием директивы:

```
lsearch{/etc/mail/exim.auth}
```

в качестве файла, в котором хранятся имена пользователей и их пароли (естественно, в зашифрованном виде), был определен файл `/etc/mail/exim.auth`. Для его создания добавьте в систему всех пользователей, которым будет разрешена отправка сообщений, путем добавления их в файл `/etc/shadow`. Скопируйте его в `/etc/mail/exim.auth` и из файла `/etc/mail/exim.auth` удалите все записи, не соответствующие пользователям, имеющим почтовые учетные записи, например:

```
root:$1$HdSo$8WIF.7SSXO4Gwhf28p6Bt0:12146:0:99999:7:::
bin:*:12146:0:99999:7:::
daemon:*:12146:0:99999:7:::
…
sshd:!!:12147:0:99999:7:::
chuser:$1$h5hX2qaO$xVyh0q4MA1RoEmkCTuv.I1:12147:0:99999:7:::
karlnext:$1$hpxGHH8U$rKTw/hL7FDOSvzA5qJCUx/:12148:0:99999:7:::
snort:!!:12149:0:99999:7:::
urbanoff:$1$zzLYrxBE$dhZrm7lVg90di2sR1S8RB.:12157:0:99999:7:::
ntp:!!:12172:0:99999:7:::
named:!!:12181:0:99999:7:::
drwalbr:$1$XklGtSxx$3oJXwKxCLzFzpw9jY4BtR0:12209:0:99999:7:::
karlnext:$1$hpxGHH8U$rKTw/hL7FDOSvzA5qJCUx/:12148:0:99999:7:::
goldfish:!!:12209:0:99999:7:::
…
```

Шаг 3

Установите права доступа к файлу `/etc/mail/exim.auth` и определите его владельцем пользователя `root` и группы-владельца `mail`:

```
[root@test /]# chmod 640 /etc/mail/exim.auth
[root@test /]# chown root.mail /etc/mail/exim.auth
```

Шаг 4

Для того, чтобы изменения вступили в силу, перегрузите SMTP-сервер:

```
[root@test /]# /etc/init.d/exim restart
Останавливается Exim:                [OK]
Запускается Exim:                    [OK]
```

Шаг 5

В почтовых клиентах, используемых пользователями вашего сервера для отправки почтовых сообщений, сначала необходимо настроить режим аутентификации пользователей. Например, в Microsoft OutLook Express 6 для отправки сообщений с предварительной аутентификацией пользователей в свойствах учетной записи необходимо для сервера исходящей почты включить проверку подлинности пользователя (рис. 27.2).

С настройками других почтовых программ можно ознакомится в их документации.

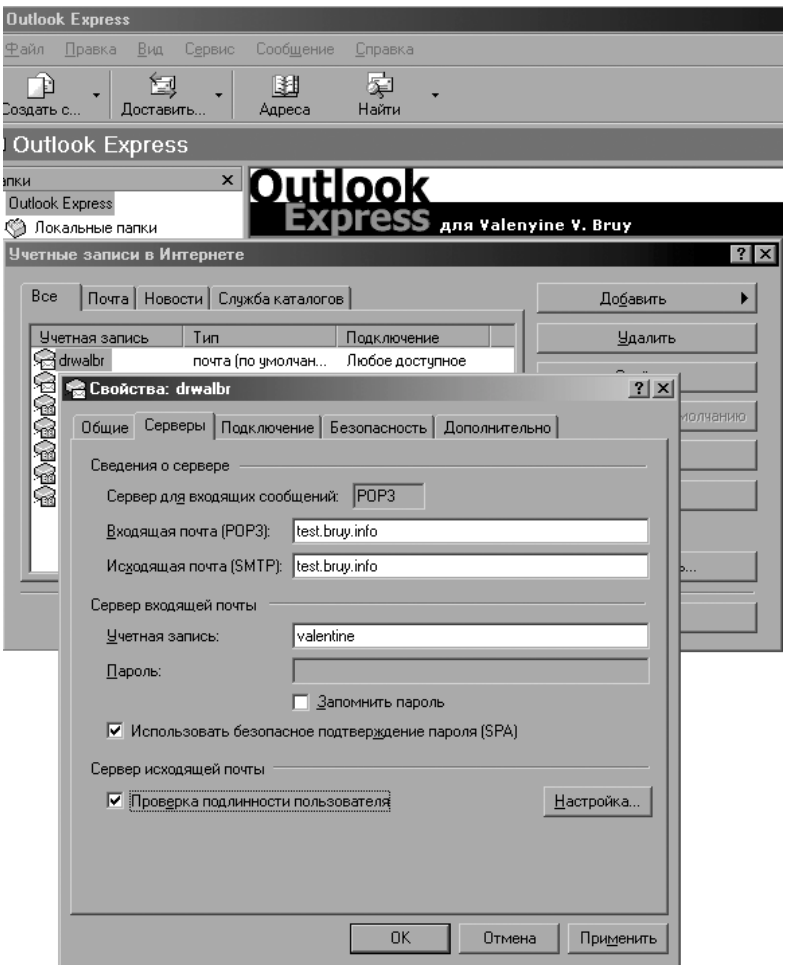


Рис. 27.2 Включение проверки подлинности пользователя.

Запуск Exim с поддержкой SSL

При работе Exim с поддержкой протокола SSL расшифровка почтовых сообщений, логинов и паролей в случае попытки перехвата сообщений между клиентской почтовой программой и SMTP-сервером практически невозможна. Однако следует учесть, что в этом случае сообщение может быть перехвачено на других стадиях его доставки, при передаче с SMTP-сервера получателя клиентской почтовой программе. Таким образом, использование Exim с поддержкой SSL защищает аутентификационную информацию пользователей, но не гарантирует конфиденциальность пересылки сообщений. Нужна ли вам поддержка SSL в Exim, решайте сами.

Для запуска Exim с поддержкой протокола SSL необходимо выполнить следующие операции.

Шаг 1

Для создания самостоятельно подписанного сертификата необходимо наличие собственного сертификационного центра. Если вы его уже создали, то перейдите к следующему шагу. В противном случае ознакомьтесь с рекомендациями раздела «Тестирование OpenSSL» главы 12 и создайте собственный сертификационный центр.

Шаг 2

Создайте закрытый ключ, незащищенный паролем, для чего перейдите в каталог `/usr/share/ssl`:

```
[root@test /]# cd /usr/share/ssl
```

Выберите пять любых больших файлов со случайным (уникальным) содержанием, скопируйте их в каталог `/usr/share/ssl` и переименуйте в `random1`, `random2`, `random3`, `random4`, `random5`, после чего выполните команду:

```
[root@test ssl]# openssl genrsa -rand ran-
dom1:random2:random3:random4:random5 -out smtp.key 1024
2019245 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.++++++
```

```
.................++++++
e is 65537 (0x10001)
```

Шаг 3

Создайте запрос на подтверждение сертификата:

```
[root@test ssl]# openssl req -new -key smtp.key -out smtp.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]: <Enter>
State or Province Name (full name) [Moscow]: <Enter>
Locality Name (eg, city) [Yubileyniy]: <Enter>
Organization Name (eg, company) [Valentine Bruy]: <Enter>
Organizational Unit Name (eg, section) [Home]: <Enter>
Common Name (eg, YOUR name) [test.bruy.info]: <Enter>
Email Address [drwalbr@bruy.info]: <Enter>

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: <Enter>
An optional company name []: <Enter>
```

Шаг 4

Подпишите сертификат:

```
[root@test ssl]# /usr/share/ssl/misc/sign smtp.csr
CA signing: smtp.csr -> smtp.crt:
Using configuration from ca.config
Enter pass phrase for /usr/share/ssl/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :PRINTABLE:'Moscow'
localityName          :PRINTABLE:'Yubileyniy'
organizationName      :PRINTABLE:'Valentine Bruy'
organizationalUnitName:PRINTABLE:'Home'
commonName            :PRINTABLE:'test.bruy.info'
emailAddress          :IA5STRING:'drwalbr@bruy.info'
Please enter the following 'extra' attributes to be sent with your cer-
tificate request
A challenge password [] : <Enter>
An optional company name [ ] : <Enter>
Certificate is to be certified until Jun 21 16:56:10 2004 GMT (365 days)
Sign the certificate? [y/n]: <y>



1 out of 1 certificate requests certified, commit? [y/n] <y>
Write out database with 1 new entries
Data Base Updated
CA verifying: smtp.crt <-> CA cert
smtp.crt: OK
```

ЗАМЕЧАНИЕ Если вы получите сообщение об ошибке, вызванной тем, что такой сертификат уже существует, слегка измените информацию, вводимую при создании запроса на подтверждение сертификата, например, введите

```
An optional company name []: SMTP <Enter>
```

Шаг 5

Создайте необходимые каталоги, разместите в них файлы с сертификатами, определите владельцев и права доступа к ним, удалите ненужный более файл `smtp.csr`:

```
[root@test ssl]# mkdir -p /etc/mail/certs
[root@test ssl]# chmod 700 /etc/mail/certs/
[root@test ssl]# chown mail.mail /etc/mail/certs/
[root@test ssl]# mv smtp.key /etc/mail/certs/
[root@test ssl]# mv smtp.crt /etc/mail/certs/
[root@test ssl]# chmod 400 /etc/mail/certs/smtp.key
[root@test ssl]# chmod 400 /etc/mail/certs/smtp.crt
[root@test ssl]# chown mail.mail /etc/mail/certs/smtp.key
[root@test ssl]# chown mail.mail /etc/mail/certs/smtp.crt
[root@test ssl]# rm -f smtp.csr
```

Шаг 6

Внесение изменения в файл `/etc/mail/exim.conf`:

```
#####################################################################
#                    MAIN CONFIGURATION SETTINGS                    #
#####################################################################

######1111111primary_hostname = smtp.domain.com
primary_hostname = test.bruy.info
acl_smtp_rcpt = check_recipient
acl_smtp_data = check_message
acl_smtp_auth = check_auth


domainlist local_domains = @ : lsearch;/etc/mail/localdomains
hostlist relay_hosts = lsearch;/etc/mail/relaydomains
hostlist auth_relay_hosts = *

hostlist auth_over_tls_hosts = *
hostlist tls_relay_hosts = *

log_selector =  \
        +all_parents \
        +received_sender \
        +received_recipients \
        +smtp_confirmation \
        +smtp_syntax_error

allow_domain_literals = false
never_users = root:daemon:bin:sync:named
host_lookup = *
trusted_users = mail

gecos_pattern = ^([^,:]*)
gecos_name = $1
freeze_tell = postmaster
auto_thaw = 1h
ignore_bounce_errors_after = 30m
timeout_frozen_after = 7d

received_header_text = "Received: \
        ${if def:sender_rcvhost {from ${sender_rcvhost}\n\t}\
        {${if def:sender_ident {from ${sender_ident} }}\
        ${if def:sender_helo_name {(helo=${sender_helo_name})\n\t}}}}\
        by ${primary_hostname} \
        ${if def:received_protocol {with ${received_protocol}}} \
        (Exim ${version_number} #${compile_number} )\n\t\
        id ${message_id}\
        ${if def:received_for {\n\tfor <$received_for>}}"

system_filter = /etc/mail/system-filter
```

```
message_body_visible = 5000
message_size_limit = 10M
smtp_accept_max = 2048
smtp_connect_backlog = 256
queue_only
split_spool_directory
queue_run_max = 1
remote_max_parallel = 1
rfc1413_hosts = *
rfc1413_query_timeout = 0s

smtp_banner = "Welcome on our mail server!\n\
        This system does not accept Unsolicited \
        Commercial Email\nand will blacklist \
        offenders via our spam processor.\nHave a \
        nice day!\n\n${primary_hostname} ESMTP Exim \
        ${version_number} ${tod_full}"
tls_advertise_hosts = *
tls_certificate = /etc/mail/certs/smtp.crt
tls_privatekey = /etc/mail/certs/smtp.key


#############################################################################
#                       ACL CONFIGURATION                                   #
#         Specifies access control lists for incoming SMTP mail             #
#############################################################################

begin acl

check_recipient:
  accept  hosts = :

  deny    local_parts   = ^.*[@%!/|]

  deny    senders       = *@dbm;/etc/mail/access.db : \
                          dbm;/etc/mail/access.db

  require verify        = sender

  deny    message       = unrouteable address
          hosts         = !127.0.0.1/8:0.0.0.0/0
         !verify        = recipient

  accept  domains       = +local_domains
          endpass
          message       = unknown user
          verify        = recipient

  accept  hosts         = +relay_hosts

  accept  hosts         = +auth_relay_hosts
          endpass
          message       = authentication required
          authenticated = *
accept  hosts = +tls_relay_hosts
          endpass
          message = encryption required
          encrypted = *

  deny    message       = relay not permitted


check_message:
  accept
```

```
check_auth:
  accept hosts = +auth_over_tls_hosts
  endpass
  message = STARTTLS required before AUTH
  encrypted = *

###############################################################################
#                      ROUTERS CONFIGURATION                                  #
#               Specifies how addresses are handled                           #
###############################################################################
#     THE ORDER IN WHICH THE ROUTERS ARE DEFINED IS IMPORTANT!                 #
# An address is passed to each router in turn until it is accepted.           #
###############################################################################

begin routers


dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  transport = remote_smtp
  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
  no_more

system_aliases:
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup{$local_part}lsearch{/etc/mail/aliases}}
  user = mail
  file_transport = address_file
  pipe_transport = address_pipe

userforward:
  driver = redirect
  check_local_user
  file = $home/.forward
  no_verify
  no_expn
  check_ancestor
  allow_filter
  modemask = 002
  file_transport = address_file
  pipe_transport = address_pipe
  reply_transport = address_reply

localuser:
  driver = accept
  check_local_user
  transport = local_delivery

###############################################################################
#                      TRANSPORTS CONFIGURATION                               #
###############################################################################
#                       ORDER DOES NOT MATTER                                 #
#     Only one appropriate transport is called for each delivery.             #
###############################################################################

begin transports

remote_smtp:
  driver = smtp
```

```
local_delivery:
  driver = appendfile
  file = /var/mail/$local_part
  delivery_date_add
  envelope_to_add
  return_path_add
  group = mail
  mode = 0600

address_pipe:
  driver = pipe
  return_output

address_file:
  driver = appendfile
  delivery_date_add
  envelope_to_add
  return_path_add

address_reply:
  driver = autoreply
##########################################################################
#                       RETRY CONFIGURATION                              #
##########################################################################

begin retry

# Domain               Error       Retries
# ------               -----       -------

*                      *           F,2h,15m; G,16h,1h,1.5; F,4d,6h

##########################################################################
#                       REWRITE CONFIGURATION                            #
##########################################################################

begin rewrite

##########################################################################
#                    AUTHENTICATION CONFIGURATION                        #
##########################################################################

begin authenticators
```

Шаг 7

Перезапустите Exim:

```
[root@test /]# /etc/init.d/exim restart
Останавливается Exim:                      [OK]
Запускается Exim:                          [OK]
```

Шаг 8

Включите поддержку SSL в клиентских почтовых программах, используемых пользователями SMTP-сервера. Например, в Microsoft Outlook Express 6 для этого нужно в свойствах учетной записи в настройках SMTP-сервера выбрать опцию "Подключаться через безопасное соединение SSL" (рис.27.3).

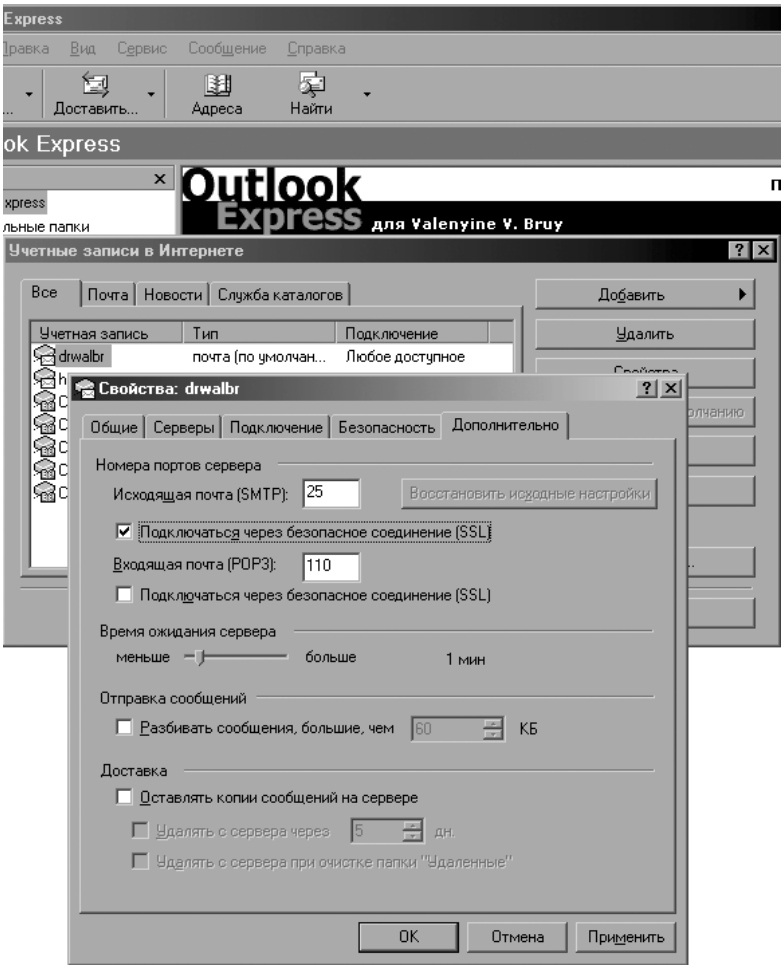


Рис. 27.3 Включение поддержки безопасного соединения с использованием протокола SSL в Microsoft Outlook Express 6.

Конфигурирование Exim в качестве локального почтового сервера

В данном случае под локальным (т. е. обслуживающим только локальных пользователей) почтовым сервером понимается почтовый сервер, который выполняет следующие функции:

- принимает сообщения от локальных пользователей, генерируемых запущенными на сервере службами;
- отправляет сообщения от локальных пользователей на центральный почтовый концентратор сети или другой почтовый сервер, настроенный для доставки сообщений администратору сервера;
- не принимает входящих сообщений от внешних пользователей.

Эта конфигурация для повышения безопасности обычно используется на всех серверах, не являющихся центральными почтовыми концентраторами.

Конфигурирование Exim для использования в режиме локального почтового сервера осуществляется аналогично конфигурированию центрального почтового концентратора.

Для того, чтобы сервер не принимал сообщений из вне в файле `/etc/sysconfig/exim` строку:

```
DAEMON= "-bd"
```

замените на:

```
daemon=""
```

Глава 28

Qpopper –программное обеспечение для организации получения почтовыми клиентскими программами сообщений электронной почты

В этой главе:

Qpopper – популярный, высокопроизводительный и надежный сервер от QUALCOMM Incorporated, предназначенный для организации получения сообщений электронной почты клиентскими почтовыми программами с использованием протокола POP3. Вам необходимо установить эту программу для того, чтобы пользователи с удаленных систем могли получать почту с вашего центрального почтового концентратора, используя установленные на рабочих станциях клиентские почтовые программы (Mail User Agent, MUA).

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта Qpopper по состоянию на 22.06.2003. Регулярно посещайте домашнюю страницу проекта `http://www.qpopper.org/qpopper/` и отслеживайте обновления.

Исходные коды Qpopper содержатся в архиве `qpopperversion.tar.gz` (последняя доступная на момент написания главы стабильная версия `qpopper4.0.5.tar.gz`).

Для нормальной инсталляции и работы Qpopper необходима установка DNS-сервера ISC BIND и почтового транспортного агента Exim. Для использования Qpopper с поддержкой протокола TSL/SSL необходима установка программы OpenSSL.

Компиляция, оптимизация и инсталляция Qpopper

Для инсталляции Qpopper необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами, используя процедуры, описанные в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами Qpopper в каталоге `/var/tmp`:

```
[root@test tmp]# tar xzpf qpopper4.0.5.tar.gz
[root@test tmp]# cd qpopper4.0.5
```

Шаг 3

Откнфигурируйте исходные коды Qpopper:

```
[root@test qpopper4.0.5]# CFLAGS="-O2 -march=i686 -funroll-loops"; export
CFLAGS
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--localstatedir=/var \
--mandir=/usr/share/man \
--enable-cache-dir=/var/spool/mail \
--enable-log-login \
--enable-specialauth \
--enable-shy \
--enable-standalone \
--enable-timing \
--enable-uw-kludge \
--enable-servermode \
--enable-fast-update \
--enable-temp-drop-dir=/var/spool/mail \
--disable-old-spool-loc \
--disable-status \
--with-pam \
```

```
--with-openssl
```

Шаг 4

Откомпилируйте, проинсталлируйте Qpopper, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test qpopper4.0.5]# make
[root@test qpopper4.0.5]# find /* > /root/qpopper1
[root@test qpopper4.0.5]# make install
[root@test qpopper4.0.5]# find /* > /root/qpopper2
[root@test qpopper4.0.5]# diff /root/qpopper1 /root/qpopper2>
/root/qpopper.installed
[root@test qpopper4.0.5]# mv /root/qpopper.installed
/very_reliable_place/qpopper.installed.YYYYMMDD
```

Шаг 5

Удалите архивы и каталоги с исходными кодами программ:

```
[root@test qpopper4.0.5]# cd /var/tmp/
[root@test tmp]# rm -rf qpopper4.0.5/
[root@test tmp]# rm -f qpopper4.0.5.tar.gz
```

Конфигурирование Qpopper

Конфигурирование программы Qpopper осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/qpopper.conf`;
- файла поддержки аутентификации пользователей с использованием модулей PAM `/etc/pam.d/pop3`;
- системного конфигурационного файла `/etc/sysconfig/qpopper`;
- файла инициализации `/etc/init.d/qpopper`.

Конфигурационный файл /etc/qpopper.conf

Шаг 1

Создайте файл `/etc/qpopper.conf`, отредактируйте строки, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
set clear-text-password         = default
set reverse-lookup              = false
set tls-support                 = default
set chunky-writes               = never
```

В этом файле строка:

```
set clear-text-password         = default
```

разрешает использование паролей в текстовом формате для всех пользователей. Опция `set clear-text-password` также может принимать следующие значения:

- never – запрещает использование паролей в текстовом формате;
- always – разрешает использовать пароли в текстовом формате;
- local – разрешает использование паролей в текстовом формате только для локальных пользователей;
- tls – означает, что пароли должны шифроваться с использованием протокола TSL/SSL.

Строка:

```
set reverse-lookup              = false
```

для увеличения производительности запрещает определение доменных имен хостов, устанавливающих соединение.

Строка:

```
set tls-support                 = default
```

отключает поддержку протоколов TSL/SSL.

Строка:

```
set chunky-writes               = never
```

запрещает объединение данных, отправляемых клиентам, в большие фрагменты.

Шаг 2

Определите права доступа к файлу `/etc/qpopper.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/qpopper.conf
[root@test /]# chown 0.0 /etc/qpopper.conf
```

Конфигурационный файл /etc/pam.d/pop3

Шаг 1

Создайте файл `/etc/pam.d/pop3`, содержащий следующие строки:

```
#%PAM-1.0
auth            required        /lib/security/pam_pwdb.so shadow
account         required        /lib/security/pam_pwdb.so
password        required        /lib/security/pam_cracklib.so
password        required        /lib/security/pam_pwdb.so nullok
use_authtok md5 shadow
session         required        /lib/security/pam_pwdb.so
```

Шаг 2

Определите права доступа к файлу `/etc/pam.d/pop3` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/pam.d/pop3
[root@test /]# chown 0.0 /etc/pam.d/pop3
```

Конфигурационный файл /etc/sysconfig/qpopper

Шаг 1

Создайте файл `/etc/sysconfig/qpopper`, содержащий следующие строки:

```
# The IP address & port number on which the Qpopper daemon will listen
# can be specified here. The default port number is "110", for POP3 with
# SSL support (POP3s), the port number must be "995" instead of "110".
#IPADDR="127.0.0.1:110"
IPADDR="0.0.0.0:110"
# IPADDR="0.0.0.0:995"
# Where our Qpopper configuration file (qpopper.conf) is located.
OPTIONS="-f /etc/qpopper.conf"
```

Шаг 2

Определите права доступа к файлу `/etc/sysconfig/qpopper` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/sysconfig/qpopper
[root@test /]# chown 0.0 /etc/sysconfig/qpopper
```

Файл инициализации /etc/init.d/qpopper

Шаг 1

Создайте файл `/etc/init.d/qpopper`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping Qpopper POP3 pro-
tocol.
#
# chkconfig: 345 50 50
# description: Qpopper supports the widely used POP3 protocol for down-
loading \
#              Internet e-mail used by many popular e-mail clients.
#
# processname: popper
# config: /etc/qpopper.conf
# pidfile: /var/run/popper.pid

# Source function library.
. /etc/init.d/functions
```

```
# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/qpopper ] ; then
        . /etc/sysconfig/qpopper
fi

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If Qpopper is not available stop now.
[ -f /usr/sbin/popper ] || exit 0

# Path to the Qpopper binary.
popper=/usr/sbin/popper

RETVAL=0
prog="Qpopper"

start() {
        echo -n $"Starting $prog: "
        daemon $popper $IPADDR $OPTIONS
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/popper
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $popper
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/popper
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $popper
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/popper ]; then
                stop
                start
                RETVAL=$?
        fi
        ;;
  *)
```

```
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 2

Определите права доступа к файлу `/etc/init.d/qpopper` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 700 /etc/init.d/qpopper
[root@test /]# chown 0.0 /etc/init.d/qpopper
```

Шаг 3

Для автоматического запуска Qpopper при загрузке системы создайте необходимые ссылки:

```
[root@test /]# chkconfig --add qpopper
[root@test /]# chkconfig --level 345 qpopper on
```

Тестирование Qpopper

Шаг 1

Проверьте наличие, а при необходимости добавьте в файл `/etc/shells` строку:

```
/bin/false/
```

Шаг 2

На центральном почтовом концентраторе создайте пользователя, которому разрешается получение сообщений:

```
[root@test /]# useradd -g users -s /bin/false polyakoff
[root@test /]# passwd polyakoff
Changing password for user polyakoff
New UNIX password: Secretnoe_$L0VO
Retype new UNIX password: Secretnoe_$L0VO
passwd: all authentication tokens updated successfully
```

Шаг 3

Запустите Qpopper:

```
[root@test /]# /etc/init.d/qpopper start
Запускается Qpopper:           [OK]
```

Шаг 4

Просканируйте порты вашего почтового концентратора с помощью сканера портов, например, `nmap` (`http:// www.insecure.org/nmap/`):

```
[root@test root]# nmap test.bruy.info
```

Если POP-сервер ожидает подключений на 110 порту, то вы получите сообщение следующего вида:

```
Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Interesting ports on test.bruy.info (212.111.80.127):
(The 1554 ports scanned but not shown below are in state: closed)
Port       State       Service
110/tcp    open        pop-3

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

Шаг 5

На удаленной системе настройте клиентскую почтовую программу на использование в качестве SMTP и POP-сервера вашего почтового концентратора. Отправьте с ее помощью сообщение пользователю, например, `polyakoff`. Через некоторое время проверьте почту. Если вы получили сообщение, то POP-сервер работает нормально.

Запуск Qpopper с поддержкой SSL

По умолчанию Qpopper использует пароли в обычном текстовом формате. Злоумышленник, перехватывая пакеты с помощью программы-снифера, может определить имена и пароли пользователей вашего

центрального почтового концентратора и использовать их для получения доступа к почте и выполнения других несанкционированных действий. Для установки шифрования трафика между клиентской почтовой программой и POP-сервером необходимо включить поддержку протокола SSL. Для этого предлагается выполнить следующие операции.

Шаг 1

Для создания самостоятельно подписанного сертификата необходимо наличие собственного сертификационного центра. Если вы его уже создали, то перейдите к следующему шагу. В противном случае ознакомьтесь с рекомендациями раздела «Тестирование OpenSSL» главы 12 и создайте собственный сертификационный центр.

Шаг 2

Создайте самостоятельно подписанный незащищенный паролем сертификат:

```
[root@test /]# cd /usr/share/ssl
[root@test ssl]# openssl req -new -x509 -nodes -days 365 -out tmp.pem
Generating a 1024 bit RSA private key
.....................................................++++++
.....................................................................
.............++++++
writing new private key to 'privkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:<Enter>
State or Province Name (full name) [Moscow]:<Enter>
Locality Name (eg, city) [Yubileyniy]:<Enter>
Organization Name (eg, company) [Valentine Bruy]:<Enter>
Organizational Unit Name (eg, section) [Home]:<Enter>
Common Name (eg, YOUR name) [test.bruy.info]:<Enter>
Email Address [drwalbr@bruy.info]: drwalbr@test.bruy.info <Enter>
```

Шаг 3

Добавьте в конец файла `privkey.pem` раздел "certificate" из файла `tmp.pem`:

```
[root@test ssl]# cat tmp.pem >> privkey.pem
```

Шаг 4

Поместите файл `/usr/share/ssl/privkey.pem` сертификата в каталог `certs`, переименуйте его в `pop3.pem`, установите права доступа к файлу и удалите более ненужный файл `tmp.pem`:

```
[root@test ssl]# mv privkey.pem certs/pop3.pem
[root@test ssl]# chmod 400 certs/pop3.pem
[root@test ssl]# rm -f tmp.pem
```

Шаг 5

Файл `/etc/qpopper.conf` отредактируйте следующим образом:

```
set clear-text-password         = tls
set reverse-lookup              = false
set tls-support                 = alternate-port
set tls-server-cert-file        = "/usr/share/ssl/certs/pop3.pem"
set chunky-writes               = tls
```

Шаг 6

В файле `/etc/sysconfig/qpopper`:

Замените строку:

```
IPADDR = "0.0.0.0:110"
```

на:

```
IPADDR = "0.0.0.0:995"
```

Шаг 7

Перезапустите Qpopper:

```
[root@test /]# /etc/init.d/qpopper restart
Останавливается Qpopper:                          [OK]
Запускается Qpopper:                              [OK]
```

Шаг 8

Просканируйте порты вашего почтового концентратора с помощью сканера портов, например, `nmap` (`http:// www.insecure.org/nmap/`):

```
[root@test /]# nmap test.bruy.info
```

Если POP-сервер ожидает подключений с поддержкой протокола SSL на 995 порту, то вы получите сообщение следующего вида:

```
Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Interesting ports on test.bruy.info (212.111.80.127):
(The 1554 ports scanned but not shown below are in state: closed)
Port       State       Service
995/tcp    open        pop3s

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

Шаг 9

Проверьте работоспособность сертификата:

```
[root@test /]# cd /usr/share/ssl
[root@test ssl]# openssl
OpenSSL> s_client –host test.bruy.info –port 995
```

Если вы получите сообщение такого вида:

```
CONNECTED(00000003)
depth=0 subject=/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
issuer=/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
verify error:num=18:self signed certificate
verify return:1 =/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
issuer=/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info

---
Certificate chain
 0 s:/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
issuer=/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info

   i: :/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
issuer=/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDqjCCAxOgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBmzELMAkGA1UEBhMCUlUx
DzANBgNVBAgTBk1vc2NvdzETMBEGA1UEBxMKWXViaWxleW5peTEXMBUGA1UEChMO
VmFsZW50aW5lIEJydXkxDTALBgNVBAsTBEhvbWUxFzAVBgNVBAMTDnRlc3QuYnJ1
eS5pbmZvMSUwIwYJKoZIhvcNAQkBFhZkcndhbGJyQHRlc3QuYnJ1eS5pbmZvMB4X
DTAzMDYwNjEyMjc0M1oXDTA0MDYwNTEyMjc0M1owgZsxCzAJBgNVBAYTAlJVMQ8w
DQYDVQQIEwZNb3Njb3cxEzARBgNVBAcTCll1YmlsZXluaXkxFzAVBgNVBAoTDlZh
bGVudGluZSBCcnV5MQ0wCwYDVQQLEwRIb21lMRcwFQYDVQQDEw50ZXN0LmJydXku
aW5mbzElMCMGCSqGSIb3DQEJARYWZHJ3YWxickB0ZXN0LmJydXkuaW5mbzCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAzvmLMuOeBKpoCi87tzsd9Q3J6g1gWHFQ
FFI8dTR9Wpnn4UZfOsUg7c01PR7vEZSkap5X1wkJ3mQRYB+7XnDHfcQ34jjqUXyj
```

```
Y7xCRy5mVr8vg5qsTn2uG6vePThci8Lgjz1cEbafh+k2o/W73RIrYJou4x3YNUs1
BbvKUSahFdsCAwEAAaOB+zCB+DAdBgNVHQ4EFgQUtJuuHibUU9UUJOalwV+Eg1Kg
KfIwgcgGA1UdIwSBwDCBvYAUtJuuHibUU9UUJOalwV+Eg1KgKfKhgaGkgZ4wgZsx
CzAJBgNVBAYTAlJVMQ8wDQYDVQQIEwZNb3Njb3cxEzARBgNVBAcTCll1YmlsZXlu
aXkxFzAVBgNVBAoTDlZhbGVudGluZSBCcnV5MQ0wCwYDVQQLEwRIb21lMRcwFQYD
VQQDEw50ZXN0LmJydXkuaW5mbzElMCMGCSqGSIb3DQEJARYWZHJ3YWxickB0ZXN0
LmJydXkuaW5mb4IBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAKL1
il+jCyUEtfWjwsg93r8HysD16FO8ort74h9tJIqjoVSazuOR957J5RfPpakTW86X
rDW66NdLDRzRdmAyDGfrY2gCYQMYyG5StPJChys8Xwgz1TcuaC9W/B3j1xVotOTh
6sZcya6zKHw3hDD6CegMe5WsFeolx9REb1FPG2Af

-----END CERTIFICATE-----

subject=/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
issuer=/C=RU/ST=Moscow/L=Yubileyniy/O=Valentine
Bruy/OU=Home/CN=test.bruy.info/emailAddress=drwalbr@test.bruy.info
---
No client certificate CA names sent
---
SSL handshake has read 1104 bytes and written 346 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES256-SHA
    Session-ID:
5B5265419B1696D549F5164FCCA3399970D573009A27AD5D2FE45026C661C3DB    Ses-
sion-ID-ctx:
    Master-Key:
295C9CBCDF2BBC8851AB64CA1807125DB2705DBE73BA506B88D2FEEA61B1F8DF15F2443C6
00105E56D810B71A48445EA
    Key-Arg   : None
    Start Time: 1056267322
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
+OK ready
```

то ваш сертификат работает правильно.

Завершите соединение с POP-сервером:

```
Pop > quit
+OK Pop server at test.bruy.info signing off.
closed
```

Шаг 10

На удаленной системе настройте клиентскую почтовую программу на использование в качестве SMTP и POP-сервера вашего почтового концентратора. Включите поддержку безопасного соединения с использованием протокола SSL. Например, в Microsoft Outlook Express 6 для этого нужно в свойствах учетной записи в настройках POP-сервера выбрать опцию "Подключаться через безопасное соединение SSL" (рис. 28.1).

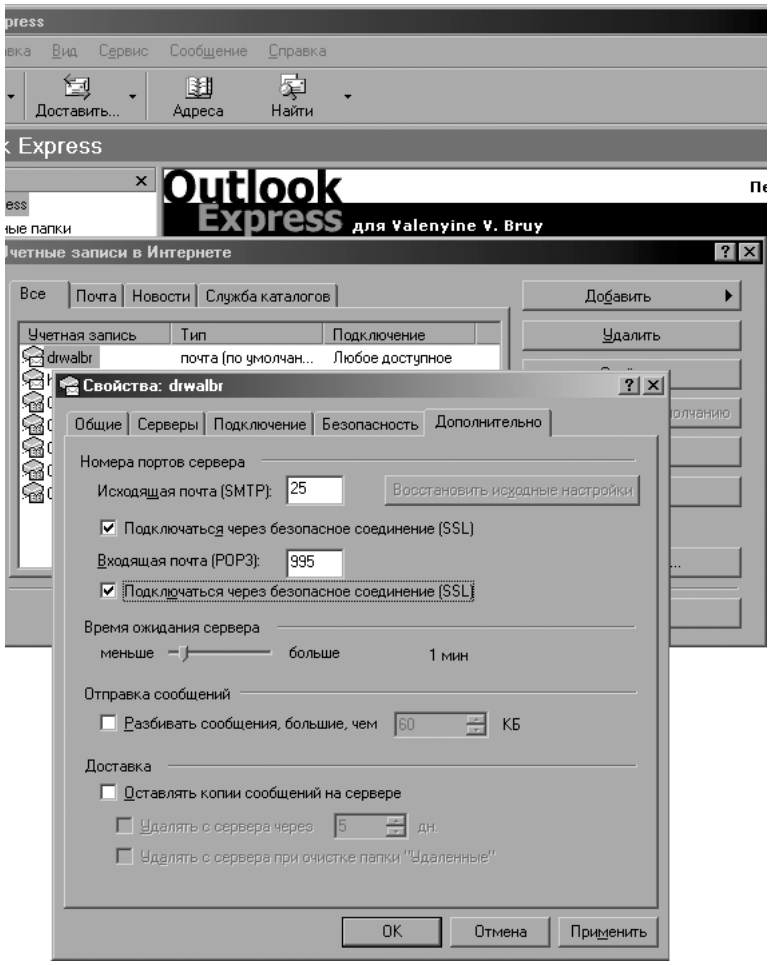


Рис. 28.1 Включение поддержки безопасного соединения с использованием протокола SSL в Microsoft Outlook Express 6.

С настройками других почтовых программ можно ознакомится в их документации.

Отправьте с помощью клиентской почтовой программы сообщение пользователю `polyakoff`. Через некоторое время проверьте почту. Если вы получили сообщение, то POP-сервер работает нормально и поддерживает протокол SSL.

Глава 29

SpamAssassin – программное обеспечение для фильтрации сообщений, содержащих спам

В этой главе:

Спам – электронная почта, содержащая нежелательные сообщения рекламного характера – не только раздражает пользователей и системных администраторов, но и приносит существенные убытки. Несколько лет назад к авторам этой книги как-то обратился директор дружественной туристической фирмы с жалобой на то, что поиск нескольких сообщений от партнеров фирмы, требующих немедленной и адекватной реакции, в нескольких десятках ежедневно поступающих спамерских сообщениях занимают у него не менее часа в день. Ориентировочные оценки показали, что убытки фирмы (затраты на оплату части рабочего времени директора, затрачиваемую на фильтрацию спама) составляют порядка 1500…2000 долларов США в год. Желание помочь хорошему человеку постепенно вылилось в хобби одного из авторов этой книги – изучение российского спама. В настоящее время в нескольких почтовых ящиках, специально отданных на растерзание спамерам путем публикации их на различных российских интернет-ресурсах, собирается несколько тысяч сообщений в месяц. Эти сообщения анализируются как на предмет их содержания, так и технологий, используемых спамерами для маскировки своих рассылок под обычные сообщения.

ЗАМЕЧАНИЕ Очень хотелось бы, что бы эту главу прочитали руководители организаций, финансирующие рекламу своих услуг с использованием спамерских технологий.

Наши программы внимательно читают тексты и заголовки ваших сообщений и классифицируют их по множеству признаков, при этом все сообщения сохраняются в единой базе данных.

В рамках выполнения заказов в области конкурентной интернет-разведки анализируется и смысловая часть сообщений, также сохраняющаяся в базе данных, при этом к вашим конкурентам попадает как статистические результаты, характеризующие основные показатели вашей деятельности, так и (в качестве приложения) тексты рассылаемых вами сообщений.

Можно предположить, что анализом спамерских рассылок занимаются и соответствующие силовые ведомства, заинтересованные в выявлении случаев незаконной предпринимательской деятельности, уклонения от оплаты налогов и т. п.

Следует отметить, что спамеры постоянно совершенствуют свою технологическую базу и пополняют базы адресов, используемых для рассылки. Вполне возможно, что для тестирования своих технологий они используют то же программное обеспечение, что и вы для защиты от спама. Это обстоятельство требует для проверки на принадлежность к спаму сообщений электронной почты уникальных (применительно к потребностям ваших пользователей) постоянно модифицируемых тестов. Разработка перечня тестов, с высокой степенью достоверности фильтрующих спам в масштабах страны, отдельно взятой области или города в современных условиях, по-видимому, невозможна. Однако, как показывает опыт авторов, для удовлетворения потребностей пользователей сети небольшой фирмы это является вполне разрешимой задачей.

В качестве программного обеспечения для фильтрации спама авторы рекомендуют использовать SpamAssassin. Это программное обеспечение с использованием многочисленных тестов проверяет каждое почтовое сообщение на содержание признаков, позволяющих идентифицировать сообщение как спам. В качестве критерия принадлежности к спаму используется величина hits, определяемая как сумма коэффициентов значимости каждого из условий (тестов), которому удовлетворяет проверяемое сообщение. При превышении некоторого порогового значения сообщение признается содержащим спам. Дальнейшая судьба спама зависит от настроек SpamAssassin, почтового транспортного агента и клиентской почтовой программы.

SpamAssassin позволяет:

- проверять сообщения на предмет выявления различных уловок, обычно используемых спамерами для того, чтобы сообщение выглядело бы, как отправленное обычным отправителем, либо относилось к списку рассылки, подписчиком которого вы являетесь;
- анализировать текст сообщения на предмет выявления идиом, содержащих неоправданно выгодные предложения, различные заверения для удовлетворения требованиям действующего законодательства и сетевого этикета и т. п.;
- осуществлять поддержку пользовательских и глобальных стоп-листов;
- создавать пользовательские тесты для фильтрации сообщений.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта SpamAssassin по состоянию на 23.06.2003. Регулярно посещайте домашнюю страницу проекта `http://www.spamassassin.org` и отслеживайте обновления.

Исходные коды SpamAssassin содержатся в архиве `Mail-SpamAssassin-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `Mail-SpamAssassin-2.55.tar.gz`).

Для нормальной инсталляции и работы SpamAssassin необходима установка модулей Perl-`HTML::Parser`, `HTML::Tagset` и почтовый транспортный агент, например, Exim.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет программы SpamAssassin с помощью следующей команды:

```
[root@drwalbr /]# rpm –iq spamassassin
```

Шаг 2

Перейдите в каталог, где находится пакет `spamassassin-2.20-2.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@test /]# cd /home/distrib
```

и установите:

```
[root@test distrib]# rpm -ihv spamassassin-2.20-2.asp.i386.rpm
```

или обновите пакет:

```
[root@test distrib]# rpm –Uhv spamassassin-2.20-2.asp.i386.rpm
```

После установки пакета перейдите к настройке программы.

Компиляция, оптимизация и инсталляция SpamAssassin

Для инсталляции SpamAssassin из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1, раздела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Установите модули Perl `HTML::Parser` и `HTML::Tagset`:

```
[root@test distrib]# rpm -ihv perl-HTML-Parser-3.26-2.i386.rpm\
perl-HTML-Tagset-3.03-14.i386.rpm
```

Шаг 3

Распакуйте архивы с исходными кодами SpamAssassin в каталоге `/var/tmp`:

```
[root@test /]# cd /var/tmp/
[root@test tmp]# tar xzpf Mail-SpamAssassin-2.55.tar.gz
```

Шаг 4

Откомпилируйте, проинсталлируйте SpamAssassin, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test tmp]# cd Mail-SpamAssassin-2.55
[root@test Mail-SpamAssassin-2.55]# perl Makefile.PL
[root@test Mail-SpamAssassin-2.55]# make
[root@test Mail-SpamAssassin-2.55]# find /* > /root/spam1
```

```
[root@test Mail-SpamAssassin-2.55]# mkdir -p /etc/mail/spamassassin
[root@test Mail-SpamAssassin-2.55]# make install
[root@test Mail-SpamAssassin-2.55]# chmod 0444 /usr/share/spamassassin/*
[root@test Mail-SpamAssassin-2.55]# chmod 0640 /etc/mail/spamassassin/*
[root@test Mail-SpamAssassin-2.55]# find /* > /root/spam2
[root@test Mail-SpamAssassin-2.55]# diff /root/spam1 /root/spam2 >
/root/spam.installed
[root@test Mail-SpamAssassin-2.55]# mv /root/spam.installed
/very_reliable_place/spam.installed.YYYYMMDD
```

Шаг 5

Удалите архивы и каталоги с исходными кодами программ:

```
[root@test Mail-SpamAssassin-2.55]# cd ..
[root@test tmp]# rm -rf Mail-SpamAssassin-2.55/
[root@test tmp]# rm -f Mail-SpamAssassin-2.55.tar.gz
```

Конфигурирование и интеграция SpamAssassin с почтовым транспортным агентом Exim

Конфигурирование SpamAssassin осуществляется с использованием следующих файлов:

- конфигурационных файлов из каталога `/etc/mail/spamassassin`;
- файла инициализации `/etc/init.d/spamd`.

По умолчанию SpamAssassin сначала просматривает конфигурационные файлы с расширением `*.cf`, находящиеся в первом из найденных каталогов:

- `/usr/share/spamassassin;`
- `/usr/local/share/spamassassin`.

Просмотр файлов осуществляется в алфавитном порядке, т. е. сначала просматривается файл `10_misc.cf`, затем `20_anti_ratware.cf`, затем `20_body_tests.cf` и т. д. Значения для некоторого параметра, установленного в предыдущем файле, переопределяются значением этого же параметра, установленного в последующем файле.

Далее SpamAssassin просматривает конфигурационные файлы, находящиеся в первом из найденных каталогов:

- `/etc/mail/spamassassin`;
- `/usr/etc/mail/spamassassin`;
- `/usr/etc/spamassassin`;
- `/usr/local/etc/spamassassin`;
- `/usr/pkg/etc/spamassassin`;
- `/usr/etc/spamassassin`;
- `/etc/mail/spamassassin`;
- `/etc/spamassassin`.

Просмотр файлов также осуществляется в алфавитном порядке. В этом случае значения для некоторого параметра, установленного в предыдущем файле, переопределяются значением этого же параметра, установленного в последующем файле.

По умолчанию SpamAssassin просматривает пользовательские предпочтения в домашнем каталоге пользователя в файле `~/.spamassassin/user_prefs`. Если такого файла не существует, осуществляется последовательный просмотр следующих каталогов:

- `/etc/mail/spamassassin;`
- `/usr/etc/mail/spamassassin;`
- `/usr/share/spamassassin;`
- `/etc/spamassassin;`
- `/etc/mail/spamassassin;`
- `/usr/local/share/spamassassin;`
- `/usr/share/spamassassin`

на предмет наличия `user_prefs.template`. При работе программы используются пользовательские предпочтения из первого найденного файла `user_prefs.template`. При этом значения для некоторого параметра, установленного ранее в конфигурационных файлах, переопределяются значением этого же параметра, установленного в файле `user_prefs` или `user_prefs.template`.

ЗАМЕЧАНИЕ Для конфигурирования SpamAssassin не следует изменять файлы в каталоге `/usr/share/spamassassin`, т. к. при обновлении SpamAssassin будут утрачены все изменения, внесенные вами в конфигурацию. Внесение изменений в конфигурацию SpamAssassin следует осуществлять с использованием конфигурационных файлов в каталоге `/etc/mail/spamassassin`. Файлы из каталога `/usr/share/spamassassin` следует использовать в качестве образца при создании собственных конфигурационных файлов.

Таким образом, для создания простейшего варианта конфигурации SpamAssassin необходимо выполнить следующие операции.

Шаг 1

Создайте и отредактируйте файл `/etc/mail/spamassassin/local.cf`, руководствуясь ниже приведенными рекомендациями и вашими потребностями:

```
required_hits           5.0
rewrite_subject         1
subject_tag             >(;-(SPAM*****
report_safe             1
score HEADER_8BITS            0
score HTML_COMMENT_8BITS      0
score SUBJ_FULL_OF_8BITS      0
clear_report_template
report Возможно, отправленное  Вам сообщение содержало спам.
report С его содержанием  вы можете ознакомится в приложении
report к этому письму.  Настройте вашу почтовую программу на
report помещение сообщений, содержащих в заголовке  префикс:
report                  >(;-(SPAM*****
report в  отдельную папку. Просмотр этой  папки осуществляйте
report при возникновении  подозрений  о  неполучении  вами
report важных сообщений поисковыми средствами вашей почтовой
report программы. Администратор Сергей Панов. т. 26-35
report
report Content preview:  _PREVIEW_
report
report Content analysis details:   (_HITS_ points, _REQD_ required)
report _SUMMARY_
```

В рассматриваемом файле строка:

```
required_hits           5.0
```

определяет минимальное значение величины `hits`, при превышении которого сообщение классифицируется как спам.

Строка:

```
rewrite_subject         1
```

предписывает изменять заголовок сообщения, добавляя туда префикс, определяемый в строке:

```
subject_tag             >(;-(SPAM*****
```

В рассматриваемом примере префикс содержит стилизованное изображение спамера, которого настигло заслуженное возмездие, слово SPAM и пять звездочек, соответствующих установленному значению параметра `required_hits`. Содержание префикса должно быть уникальным, в том смысле, что его появление в нормальном сообщении должно быть маловероятным, т. к. наличие префикса в заголовке может использоваться пользователями для размещения сообщений содержащих спам в отдельных папках.

Строка:

```
report_safe             1
```

предписывает сохранять сообщение, содержащее спам, в виде приложения к генерируемому SpamAssassin письму.

Строки:

```
score HEADER_8BITS            0
score HTML_COMMENT_8BITS      0
score SUBJ_FULL_OF_8BITS      0
```

устанавливают нулевое значение значимости для тестов, проверяющих наличие в сообщениях символов в восьми битных кодировках.

Строки:

```
clear_report_template
report Возможно, отправленное  Вам сообщение содержало спам.
```

```
report С его содержанием  вы можете ознакомится в приложении
report к этому письму.  Настройте вашу почтовую программу на
report помещение сообщений, содержащих в заголовке  префикс:
report                    >(;-(SPAM*****
report в  отдельную папку. Просмотр этой  папки осуществляйте
report при возникновении  подозрений  о  неполучении  вами
report важных сообщений поисковыми средствами вашей почтовой
report программы. Администратор Сергей Панов. т. 26-35
report
report Content preview:  _PREVIEW_
report
report Content analysis details:   (_HITS_ points, _REQD_ required)
report _SUMMARY_
```

определяют содержание сообщения, получаемого пользователем, которому было адресовано письмо, содержащее спам. Текст, используемый по умолчанию, предлагает получившему сообщение пользователю обратиться на сайт разработчиков, где они вряд ли смогут понять, что же им нужно сделать со сгенерированным SpamAssassin сообщением.

Шаг 2

Определите права доступа к файлу `/etc/mail/spamassassin/local.cf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/mail/spamassassin/local.cf
[root@test /]# chown 0.0 /etc/mail/spamassassin/local.cf
```

Шаг 3

Скопируйте файл `local.cf` в `user_prefs.template`:

```
[root@test /]# cp /etc/mail/spamassassin/local.cf /etc/mail/spamassassin/
user_prefs.template
```

Эта операция необходима только, если пользователям вашего почтового сервера разрешено создавать в каталоге `~/.spamassassin/` файлы `user_prefs`, предназначенные для создания собственных правил фильтрации спама. В этом случае в качестве образца для создания пользовательского файла будет использованы правила, заданные вами в файле `/etc/mail/spamassassin/local.cf`, а не используемый по умолчанию файл `/usr/share/spamassassin/user_prefs.template`.

Шаг 4

Создайте инициализационный файл `/etc/init.d/spamd`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping SpamAssassin.
#
# chkconfig: 2345 80 30
# description: spamd is a daemon process which uses SpamAssassin to check
\
#              email messages for SPAM. It is normally called by spamc \
#              from a MDA.
#
# processname: spamd

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If SpamAssassin is not available stop now.
[ -f /usr/bin/spamd ] || exit 0

# Path to the SpamAssassin binary.
spamd=/usr/bin/spamd
```

```
RETVAL=0
prog="Spamd"

start() {
        echo -n $"Starting $prog: "
        daemon $spamd -d -i 0.0.0.0 -x -F0 -u mail
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/spamd
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $spamd
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/spamd
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $spamd
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/spamd ]; then
                stop
                start
                RETVAL=$?
        fi
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 5

Определите права доступа к файлу `/etc/init.d/spamd` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 700 /etc/init.d/spamd
[root@test /]# chown 0.0 /etc/init.d/spamd
```

Шаг 6

Для автоматического запуска SpamAssassin при загрузке системы создайте необходимые ссылки:

```
[root@test /]# chkconfig --add spamd
[root@test /]# chkconfig --level 2345 spamd on
```

Шаг 7

Для интеграции SpamAssassin с Exim внесите в файл `/etc/mail/exim.conf` следующие изменения:

```
##########################################################################
#                    MAIN CONFIGURATION SETTINGS                         #
##########################################################################

primary_hostname = test.bruy.info
acl_smtp_rcpt = check_recipient
acl_smtp_data = check_message

domainlist local_domains = @ : lsearch;/etc/mail/localdomains
hostlist relay_hosts = lsearch;/etc/mail/relaydomains
hostlist auth_relay_hosts = *

log_selector =  \
        +all_parents \
        +received_sender \
        +received_recipients \
        +smtp_confirmation \
        +smtp_syntax_error

allow_domain_literals = false
never_users = root:daemon:bin:sync:named
host_lookup = *
trusted_users = mail

gecos_pattern = ^([^,:]*)
gecos_name = $1
freeze_tell = postmaster
auto_thaw = 1h
ignore_bounce_errors_after = 30m
timeout_frozen_after = 7d

received_header_text = "Received: \
        ${if def:sender_rcvhost {from ${sender_rcvhost}\n\t}\
        {${if def:sender_ident {from ${sender_ident} }}\
        ${if def:sender_helo_name {(helo=${sender_helo_name})\n\t}}}}\
        by ${primary_hostname} \
        ${if def:received_protocol {with ${received_protocol}}} \
        (Exim ${version_number} #${compile_number} )\n\t\
        id ${message_id}\
        ${if def:received_for {\n\tfor <$received_for>}}"

system_filter = /etc/mail/system-filter

message_body_visible = 5000
message_size_limit = 10M
smtp_accept_max = 2048
smtp_connect_backlog = 256
queue_only
split_spool_directory
queue_run_max = 1
remote_max_parallel = 1
rfc1413_hosts = *
rfc1413_query_timeout = 0s

smtp_banner = "Welcome on our mail server!\n\
        This system does not accept Unsolicited \
        Commercial Email\nand will blacklist \
        offenders via our spam processor.\nHave a \
        nice day!\n\n${primary_hostname} ESMTP Exim \
        ${version_number} ${tod_full}"
```

```
##########################################################################
#                       ACL CONFIGURATION                                #
#         Specifies access control lists for incoming SMTP mail          #
##########################################################################

begin acl

check_recipient:
  accept  hosts = :

  deny    local_parts   = ^.*[@%!/|]

  deny    senders       = *@dbm;/etc/mail/access.db : \
                          dbm;/etc/mail/access.db

  require verify        = sender

  deny    message       = unrouteable address
          hosts         = !127.0.0.1/8:0.0.0.0/0
         !verify        = recipient

  accept  domains       = +local_domains
          endpass
          message       = unknown user
          verify        = recipient

  accept  hosts         = +relay_hosts

  accept  hosts         = +auth_relay_hosts
          endpass
          message       = authentication required
          authenticated = *

  deny    message       = relay not permitted


check_message:
  accept

##########################################################################
#                       ROUTERS CONFIGURATION                            #
#               Specifies how addresses are handled                      #
##########################################################################
#     THE ORDER IN WHICH THE ROUTERS ARE DEFINED IS IMPORTANT!           #
# An address is passed to each router in turn until it is accepted.      #
##########################################################################

begin routers
#SpamAssassin
spamcheck_router:
  no_verify
  check_local_user
  condition = "${if and { {!def:h_X-Spam-Flag:} \
  {!eq {$received_protocol}{spam-scanned}}} {1} {0}}"
  driver = accept
  transport = spamcheck
#SpamAssassin


dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  transport = remote_smtp
  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
```

```
  no_more

system_aliases:
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup{$local_part}lsearch{/etc/mail/aliases}}
  user = mail
  file_transport = address_file
  pipe_transport = address_pipe

userforward:
  driver = redirect
  check_local_user
  file = $home/.forward
  no_verify
  no_expn
  check_ancestor
  allow_filter
  modemask = 002
  file_transport = address_file
  pipe_transport = address_pipe
  reply_transport = address_reply

localuser:
  driver = accept
  check_local_user
  transport = local_delivery

#############################################################################
#                       TRANSPORTS CONFIGURATION                            #
#############################################################################
#                        ORDER DOES NOT MATTER                              #
#     Only one appropriate transport is called for each delivery.           #
#############################################################################

begin transports

remote_smtp:
  driver = smtp

local_delivery:
  driver = appendfile
  file = /var/mail/$local_part
  delivery_date_add
  envelope_to_add
  return_path_add
  group = mail
  mode = 0600

address_pipe:
  driver = pipe
  return_output

address_file:
  driver = appendfile
  delivery_date_add
  envelope_to_add
  return_path_add

address_reply:
  driver = autoreply
#SpamAssassin
spamcheck:
```

```
  driver = pipe
  batch_max =100
  command = /usr/sbin/exim -oMr  spam-scanned -bS
  use_bsmtp = true
  transport_filter=/usr/bin/spamc
  home_directory = "/tmp"
  current_directory = "/tmp"
  user=mail
  group=mail
  log_output = true
  return_fail_output = true
  return_path_add = false
  message_prefix =
  message_suffix =
#SpamAssassin
#########################################################################
#                       RETRY CONFIGURATION                             #
#########################################################################

begin retry

# Domain               Error       Retries
# ------               -----       -------

*                      *           F,2h,15m; G,16h,1h,1.5; F,4d,6h

#########################################################################
#                       REWRITE CONFIGURATION                           #
#########################################################################

begin rewrite

#########################################################################
#                    AUTHENTICATION CONFIGURATION                       #
#########################################################################

begin authenticators
```

Тестирование SpamAssassin

Для тестирования SpamAssassin выполните следующие операции.

Шаг 1

Запустите spamd:

```
[root@test /]# /etc/init.d/spamd start
Запускается Spamd:                         [OK]
```

Шаг 2

Запустите или перезапустите Exim:

```
[root@test /]# /etc/init.d/exim restart
Останавливается Exim:                        [OK]
Запускается Exim:                            [OK]
```

Шаг 3

Отправьте сообщение какому-нибудь пользователю:

```
[root@test /]# mail drwalbr@test.bruy.info
Subject: Обычное сообщение, не содержащее спам. <Enter>
Это обычное сообщение. <Enter>
В нем нет спама. <Enter>
Администратор. <Enter>
<Ctrl+D>
Cc: <Enter>
```

Шаг 4

Через некоторое время получите почту для этого пользователя:

```
[root@test /]# mail -u drwalbr
Mail version 8.1 6/6/93.  Type ? for help.
"/var/mail/drwalbr": 1 message 1 new
>N  1 root@test.bruy.info   Mon Jun 23 16:52  23/832   "Тест"
& 1 <Enter>
Message 1:
From root@test.bruy.info Mon Jun 23 16:52:32 2003
Envelope-to: drwalbr@test.bruy.info
Delivery-date: Mon, 23 Jun 2003 16:52:32 +0400
To: drwalbr@test.bruy.info
Subject: Обычное сообщение, не содержащее спам.
From: root <root@test.bruy.info>
Date: Mon, 23 Jun 2003 16:51:30 +0400
X-Spam-Status: No, hits=0.0 required=5.0
        tests=none
        version=2.55
X-Spam-Level:
X-Spam-Checker-Version: SpamAssassin 2.55 (1.174.2.19-2003-05-19-exp)

Это обычное сообщение.
В нем нет спама.
Администратор.

& q <Enter>
```

Если сообщение выглядит примерно так, как приведено выше, то доставка сообщений без спама и их проверка работает нормально. При этом строки

```
X-Spam-Status: No, hits=0.0 required=5.0
        tests=none
        version=2.55
X-Spam-Level:
X-Spam-Checker-Version: SpamAssassin 2.55 (1.174.2.19-2003-05-19-exp)
```

указывают на то, что сообщение не содержит спама. Значение `hits` для него составляет 0,0 при максимально допустимом значении 5,0. Сообщение проверено SpamAssassin версии 2.55.

Шаг 5

Отправьте сообщение, содержащее спам, какому-нибудь пользователю:

```
[root@test /]# mail drwalbr@test.bruy.info < spam
```

При этом предполагается, что в файле `spam` содержится сообщение со спамом. При таком способе проверки несколько уменьшается значение `hits`, т. к. исходным отправителем является локальный пользователь `root`. Однако в рассматриваемом примере результатов остальных тестов оказалось достаточно для классификации письма как содержащего спам.

Шаг 6

Через некоторое время для наглядности снимите почту с удаленной системы, используя клиентскую почтовую программу. Пользователь получил сообщение, в заголовке которого добавлен префикс:

```
Fw: >(;-(SPAM***** Кондиционеры. Весенние скидки!
В тексте сообщения содержится созданная вами инструкция для пользователя.
Возможно, отправленное  Вам сообщение содержало спам.
С его содержанием  вы можете ознакомится в приложении
к этому письму.  Настройте вашу почтовую программу на
помещение сообщений, содержащих в заголовке  префикс:
>(;-(SPAM*****
в  отдельную паку. Просмотр этой  папки осуществляйте
при возникновении  подозрений  о  неполучении  вами
важных сообщений поисковыми средствами вашей почтовой
программы. Администратор Сергей Панов. т. 26-35
```

Краткая аннотация спамерского сообщения:

```
Content preview: ЗВОНИТЕ НАМ ЗВОНИТЕ НАМ! ДЕШЕВЛЕ НЕТ! Новый прайс! ООО
```

```
"Техносервис" предлагает приобрести и установить кондиционеры [...]
```

Результаты тестов SpamAssassin:

```
Content analysis details: (9.60 points, 5 required)
X_PRIORITY_HIGH (1.9 points) Sent with 'X-Priority' set to high
HTML_80_90 (0.5 points) BODY: Message is 80% to 90% HTML
HTML_FONT_BIG_B (0.5 points) BODY: HTML has a big "font" and "B" tag
combo
HTML_MESSAGE (0.1 points) BODY: HTML included in message
FRONTPAGE (0.7 points) BODY: Frontpage used to create the message
FORGED_HOTMAIL_RCVD (1.1 points) Forged hotmail.com 'Received:' header
found
FORGED_MUA_OUTLOOK (3.5 points) Forged mail pretending to be from MS Out-
look
MIME_HTML_ONLY (0.1 points) Message only has text/html MIME parts
UPPERCASE_25_50 (1.2 points) message body is 25-50% uppercase
```

Предупреждения для пользователя о небезопасности просмотра подозрительных сообщений в почтовой программе:

```
The original message did not contain plain text, and may be unsafe to
open with some email clients; in particular, it may contain a virus,
or confirm that your address can receive spam. If you wish to view
it, it may be safer to save it to a file and open it with an editor.
```

В приложении в целости и сохранности находится исходное отправление, вид которого представлен на рис 29.1.

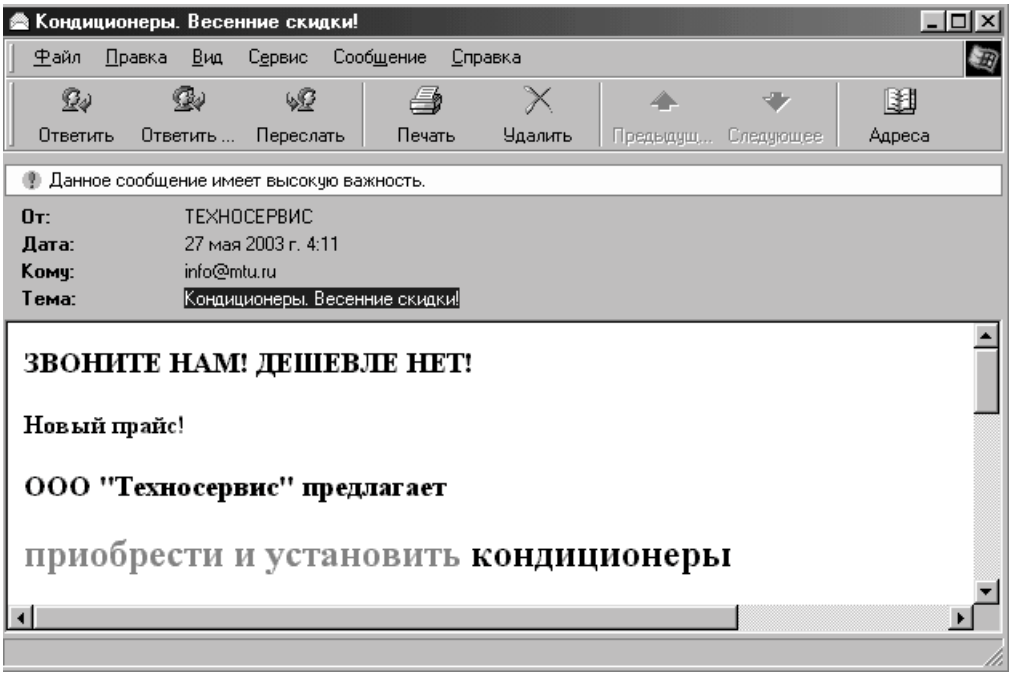


Рис. 29.1 Образец спамерского сообщения, прикрепленного к письму, сгенерированного SpamAssassin.

После того, как пользователи привыкнут к наличию в сети программного обеспечения, осуществляющего фильтрацию спама, текст сообщения, генерируемого SpamAssassin, можно сократить, например, до:

```
Возможно, отправленное Вам сообщение содержало спам.
Администратор Сергей Панов. т. 26-35
```

а отчеты и другую служебную информацию – удалить.

Особенности национального спама

Для тестирования возможностей SpamAssassin с настройками по умолчанию применительно к спаму, попадающему в ящики обычных российских пользователей, было проверена тысяча сообщений, содержа-

щих спам, и тысяча обычных. Сообщения со спамом были отобраны из почтовых ящиков, специально отданных на растерзание спамерам, а обычные сообщения были любезно предоставлены руководством дружественной фирмы. При этом предварительного отбора обычных сообщений по каким-либо признакам – например, степени конфиденциальности – не проводилось.

Для проверки сообщений возможно использование утилиты `spamassassin`, позволяющей определять величину `hits` для сообщений, находящихся в файле, без использования почтового сервера и демона `spamd`. Для проверки сообщения, находящегося в некотором файле, используйте команду:

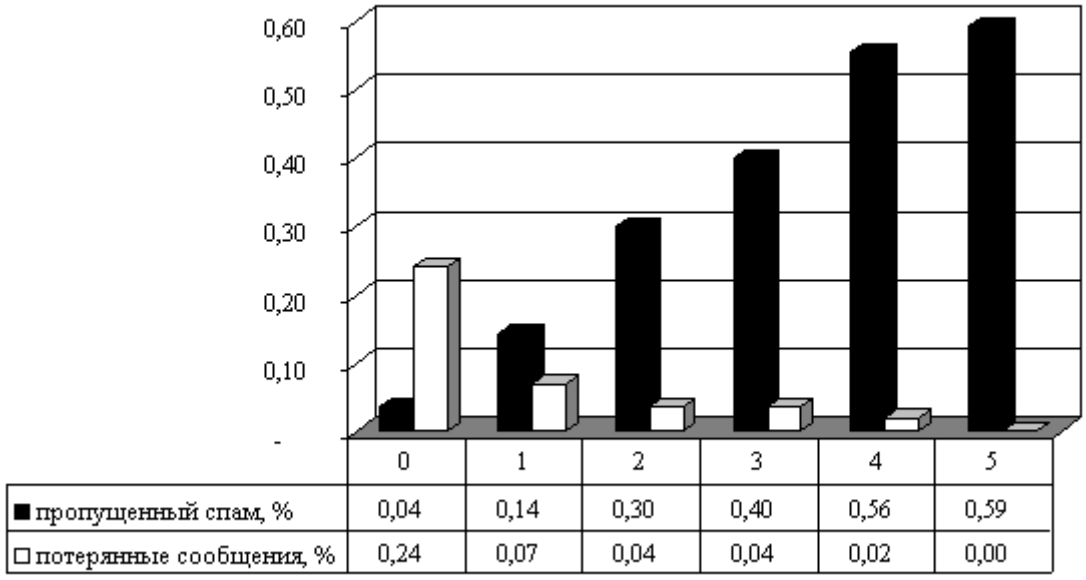
```
[drwalbr@test spam]# spamassassin -t < message_file | less
```

или:

```
[drwalbr@test spam]# spamassassin -t < message_file | grep "X-Spam-
Level:"
X-Spam-Level: *********
```

Для проверки большого числа сообщений лучше написать программу на Perl, использующую класс `Mail::SpamAssassin`.

В результате проверки сообщений были получены зависимости числа ошибочно пропускаемых спамерских сообщений и числа обычных сообщений, ошибочно принимаемых за спамерские, от величины `hits`, при превышении значения которой принимается решение о принадлежности сообщения к спаму. Полученные зависимости представлены на рис. 29.2.



	0	1	2	3	4	5
■ пропущенный спам, %	0,04	0,14	0,30	0,40	0,56	0,59
□ потерянные сообщения, %	0,24	0,07	0,04	0,04	0,02	0,00

Рис. 29.2 Зависимость числа сообщений от величины `hits`.

Из представленных зависимостей видно, что существенное снижение количества спамерских сообщений (на порядок), достигающих своих получателей, имеет место только при значениях `hits` менее или равного единице. При этом теряется не менее семи процентов обычных сообщений, ошибочно принятых за спам. Для проверки обучаемости SpamAssassin были созданы две папки `ham` и `spam`, содержащие, соответственно, по одной тысяче обычных и спамерских сообщений. Обучение SpamAssassin проводилось с использованием утилиты `sa-learn`:

```
[drwalbr@test messages]# /usr/bin/sa-learn --ham --dir ./ham
Learned from 1000 messages.
[drwalbr@test messages]# /usr/bin/sa-learn --spam --dir ./spam
Learned from 1000 messages.
```

После обучения SpamAssassin повторно получены зависимости числа ошибочно пропускаемых спамерских сообщений и числа обычных сообщений, ошибочно принимаемых за спамерские, от величины `hits`. Статистически значимых отклонений от зависимостей, полученных до обучения, обнаружено не было. Очевиден вывод – «чудес не бывает», SpamAssassin не учитывает русскоязычные идиомы. Выход из сложившейся ситуации может быть найден путем создания собственных настроек и тестов, используемых

при принятии решений о принадлежности сообщений к спаму. Двухлетний опыт применения SpamAssassin в пяти организациях показывает, что с использованием достаточно очевидных правил, учитывающих специфику конкретных пользователей, количество спамерских сообщений, достигающих своих получателей, может быть сокращено в 20…30 раз. При этом потерь сообщений, содержащих важную информацию, в течение последнего года не было.

Вы или ваша организация несет затраты (амортизация ресурсов, затраты труда на настройку программного обеспечения, оплата трафика и т. п.) на обработку содержащих спам сообщений. Они все равно поступают к вам, правда, уже в виде, не отвлекающем сотрудников от выполнения своих служебных обязанностей. Для частичной компенсации затрат на организацию борьбы со спамом можно складывать сообщения, сортируя их по датам на внутреннем Web-сервере. Информация, содержащаяся в сообщениях, может оказаться полезной при проведении маркетинговых исследований и решении других задач конкурентной интернет-разведки. Информация, содержащаяся в спаме, по-своему уникальна, т. к., как правило, не публикуется на Web-ресурсах. Для обеспечения оперативного доступа к информации на Web-сервере следует установить поисковую систему, реализующую алгоритм поиска по ключевым словам или с помощью латентно-семантического анализа.

Глава 30

Doctor Web – антивирусное программное обеспечение

В этой главе:

В этой главе рассматривается установка и настройка антивирусного программного обеспечения Doctor Web от Санкт-Петербургской антивирусной лаборатории И. Данилова (ООО «СалД»). Несколько лет назад этот программный продукт был перенесен на платформу Linux. В комплект поставки Doctor Web (Dr. Web) для Linux входят:

- Dr. Web daemon, предназначенный для интеграции с различным программным обеспечением (почтовыми транспортными агентами и файл-серверами), в качестве фильтра;
- сканер Dr. Web, работающий в режиме командной строки.

Кроме демона и сканера в комплект поставки входят исходные тексты программ, необходимых для совместного использования Dr. Web с Sendmail, Exim, QMail Postfix, Communigate Pro, Samba, Courier и ZMailer.

В комплект поставки входит также подробная документация на русском и английском языках.

В отличие от рассмотренного ранее программного обеспечения Doctor Web является коммерческим программным продуктом и не поставляется в исходных кодах. По этой причине авторам не удалось обеспечить работоспособность Dr. Web daemon при его установке в типичные для Linux-систем каталоги. В рассматриваемом ниже варианте инсталляции основные исполняемые файлы устанавливаются в каталог `/opt`, который рекомендуется размещать на отдельном разделе диска. Не смотря на этот недостаток, по мнению авторов, Doctor Web является лучшим программным продуктом для реализации антивирусной защиты на почтовом сервере.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта Doctor Web по состоянию на 29.06.2003. Регулярно посещайте домашнюю страницу проекта `http://` `http://drweb.ru/unix/` и отслеживайте текущие обновления. Doctor Web содержится в архиве `drweb-version-glibc.version.tar.gz` (последняя доступная на момент написания главы стабильная версия `drweb-4.29.2-glibc.2.2.tar.gz`). Клиентское программное обеспечение, предназначенное для интеграции с почтовым транспортным агентом Exim, содержится в архиве `drweb-exim-version-linux.tar.gz` (последняя доступная на момент написания главы стабильная версия `drweb-exim-4.29.10-linux.tar.gz`).

Для нормальной инсталляции и работы Doctor Web необходима установка модуля Perl-`String::CRC32` (`http://www.cpan.org/modules/index.html`) и программы для скачивания файлов Wget (`http://www.gnu.org/software/wget/wget.html`).

Компиляция, оптимизация и инсталляция Doctor Web

Для инсталляции Doctor Web необходимо выполнить следующие операции.

Шаг 1

Распакуйте архив с исходными кодами `String::CRC32` в каталог `/var/tmp` и установите модуль Perl-`String::CRC32`:

```
[root@test tmp]# tar xzpf String-CRC32-1.2.tar.gz
[root@test tmp]# cd String-CRC32-1.2
[root@test String-CRC32-1.2]# perl Makefile.PL
[root@test String-CRC32-1.2]# make
[root@test String-CRC32-1.2]# make test
[root@test String-CRC32-1.2]# make install
```

Шаг 2

Распакуйте архив с исходными кодами Wget в каталоге `/var/tmp`, сконфигурируйте, откомпилируйте, проинсталлируйте Wget, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test tmp]# tar xzpf wget-1.8.2.tar.gz
[root@test tmp]# cd wget-1.8.2
```

```
[root@test wget-1.8.2]# CFLAGS="-O2 -march=i686 -funroll-loops"; export
CFLAGS \
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--localstatedir=/var \
--mandir=/usr/share/man
[root@test wget-1.8.2]# make
[root@test wget-1.8.2]# find /* > /root/wget1
[root@test wget-1.8.2]# make install
[root@test wget-1.8.2]# find /* > /root/wget2
[root@test wget-1.8.2]# diff /root/wget1 /root/wget2 >
/root/wget.installed
[root@test wget-1.8.2]# mv /root/wget.installed
/very_reliable_place/wget.installed.YYYYMMDD
```

Шаг 3

Распакуйте в каталоге `/var/tmp` архивы с Doctor Web и клиентским программным обеспечением:

```
[root@test wget-1.8.2]# cd /var/tmp
[root@test tmp]# tar xzpf drweb-4.29.2-glibc.2.2.tar.gz
[root@test tmp]# tar xzpf drweb-exim-4.29.10-linux.tar.gz
```

Шаг 4

Проинсталлируйте Doctor Web, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test tmp]# find /* > /root/drweb1
[root@test tmp]# drweb-4.29.2-glibc.2.2/install.sh
Enter destination directory (/opt/drweb is default): <Enter>

Select interface language: 0) english  1) russian 1 <Enter>

Dr.Web is installed to /opt/drweb.
Edit /drweb32.ini to complete setup.
[root@test tmp]# find /* > /root/drweb2
[root@test tmp]# diff /root/drweb2 /root/drweb1 > /root/drweb.installed
[root@test tmp]# mv /root/drweb.installed
/very_reliable_place/drweb.installed.YYYYMMDD
```

Шаг 5

Проинсталлируйте клиентское программное обеспечение, необходимое для интеграции Doctor Web с Exim:

```
[root@test tmp]# cp -R drweb-exim/etc/drweb/* /etc/drweb/
[root@test tmp]# cp drweb-exim/opt/drweb/drweb-exim /opt/drweb/
```

Шаг 6

Удалите архивы и каталоги с исходными кодами программ:

```
[root@test tmp]# rm -rf drweb-exim/
[root@test tmp]# rm -f drweb-exim-4.29.10-linux.tar.gz
[root@test tmp]# rm -rf drweb-4.29.2-glibc.2.2/
[root@test tmp]# rm -f drweb-4.29.2-glibc.2.2.tar.gz
```

Конфигурирование и интеграция Doctor Web с почтовым транспортным агентом Exim

Конфигурирование Doctor Web в варианте интеграции его с Exim осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/drweb/drweb32.ini`, единого для демона и сканера;
- главного конфигурационного файла Exim `/etc/mail/exim.conf`;
- конфигурационного файла клиентского программного обеспечения `/etc/drweb/drweb_exim.conf`;
- конфигурационного файла фильтров `/etc/mail/system-filter`;
- конфигурационного файла `/etc/drweb/addresses.conf`;

- конфигурационного файла `/etc/drweb/users.conf`;
- конфигурационного файла `/etc/drweb/viruses.conf`;
- файлов `/etc/drweb/templates/en-ru/*.msg`, содержащих шаблоны сообщений, используемых для информирования получателя, отправителя и администратора системы об обнаружении инфицированных сообщений и принятых к ним мерах.

Конфигурационный файл /etc/drweb/drweb32.ini

Шаг 1

Руководствуясь ниже приведенными рекомендациями и вашими потребностями, отредактируйте файл `/etc/drweb/drweb32.ini`:

```
[Linux]
EnginePath = "/opt/drweb/lib/drweb32.dll"
VirusBase = "/var/drweb/bases/*.vdb", "/var/drweb/bases/*.VDB"
MoveFilesTo = "/var/drweb/infected"
LngFileName = "/opt/drweb/lib/russian.dwl"

Key = "/opt/drweb/drweb.key"
LogFileName = "/var/drweb/log/drweb.log"
RenameFilesTo = #??
FilesTypes =
EXE,COM,SYS,OV?,BAT,BIN,DRV,PRG,BOO,SCR,CMD,VXD,386,DLL,FON,DO?
FilesTypes =
XL?,WIZ,RTF,CL*,HT*,VB*,JS*,INF,AR?,ZIP,R??,PP?,OBJ,LIB,HLP,MD?
FilesTypes = INI,MBR,IMG,CSC,CPL,MBP,SHS,SHB,PIF
ScanFiles = ByFormat
HeuristicAnalysis = Yes
CheckPackedFiles = Yes
CheckArchives = Yes
CheckEMailFiles = Yes
InfectedFiles = Report
SuspiciousFiles = Report
IncurableFiles = Report
ExcludePaths =
LogToFile = Yes
OverwriteLog = No
LogScanned = Yes
LogInfo = Yes
LogPacked = Yes
LogArchived = Yes
LogStatistics = Yes
LogTime = No
ScanSubDirectories = Yes
PromptOnAction = No
LimitLog = No
MaxLogSize = 512
OutputMode = Terminal
FollowLinks = No

UpdatePath = "/opt/drweb/updates"

RecodeNonprintable = Yes
RecodeMode = QuotedPrintable
RecodeChar = "?"

[Linux:Daemon]
EnginePath = "/opt/drweb/lib/drweb32.dll"
VirusBase = "/var/drweb/bases/*.vdb", "/var/drweb/bases/*.VDB"
MoveFilesTo = "/var/drweb/infected"
LngFileName = "/opt/drweb/lib/russian.dwl"

Key = "/opt/drweb/drwebd.key"
LogTime = Yes
```

```
LogFileName = "syslog"
;LogFileName = "/var/drweb/log/drwebd.log"
;BusyFile = "/var/drweb/run/drwebd.bsy"
SocketMode = TCP
SocketFile = "/var/drweb/run/drwebd.socket"
;SocketMode = Unix
;SocketAccess 0666
;Расскоментировать
;PidFile = "/var/drweb/run/drwebd.pid"
DaemonPort = 3000
SocketTimeout = 40
SocketReuseAddr = Yes
FileTimeout = 40
OutputMode = Terminal
LimitLog = No
MaxLogSize = 512
LogScanned = Yes
LogInfo = Yes
LogPacked = Yes
Interfaces = "localhost"
User = mail
;UserID =
;GroupID =
ScanFiles = All
MaxCompressionRatio = 20
MaxChildren = 16
SyslogFacility = "Daemon"
SyslogPriority = "Alert"

FilterRule X-Mailer ".*Mass.*Sender.*" Reject
FilterRule To ".*undisclosed.*recipient.*" Reject
FilterRule Subject ".*free.*xxx.*" Reject

UpdatePath = "/opt/drweb/updates"

RecodeNonprintable = Yes
RecodeMode = QuotedPrintable
RecodeChar = "?"
```

Конфигурационный файл состоит из двух частей. В первой – с заголовком `[Linux]` – содержатся параметры конфигурации сканера, во второй – с заголовком `[Linux:Daemon]` – содержатся параметры конфигурации демона. Вам следует внести изменения в три строки.

Строки (в обоих разделах):

```
LngFileName = "/opt/drweb/lib/russian.dwl"
```

предписывают включение поддержки в сообщениях русского языка.

Строка:

```
User = mail
```

предписывает запускать демон от имени пользователя `mail` – это необходимо для интеграции с Exim.

Назначение остальных используемых в файле опций подробно описано на русском и английском языках в файлах `/opt/drweb/doc/readme.daemon.rus` и `/opt/drweb/doc/readme.daemon`, соответственно. После завершения установки и настройки программного обеспечения каталог с документацией `/opt/drweb/doc/`следует удалить.

Шаг 2

Определите права доступа к файлу `/etc/drweb/drweb32.ini` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/drweb/drweb32.ini
[root@test /]# chown 0.0 /etc/drweb/drweb32.ini
```

Шаг 3

Для обеспечения нормальной работы демона от имени пользователя `mail` (в рассматриваемом примере drwebd запускается от имени пользователя `mail`) определите пользователя `mail` владельцем каталога `/var/drweb`:

```
[root@test /]# chown -R mail.root /var/drweb/
```

Конфигурационный файл /etc/mail/exim.conf

Шаг 1

Добавьте в файл `/etc/mail/exim.conf` параметры транспорта для фильтра, руководствуясь ниже приведенными рекомендациями:

```
##########################################################################
#                    MAIN CONFIGURATION SETTINGS                         #
##########################################################################

primary_hostname = test.bruy.info
acl_smtp_rcpt = check_recipient
acl_smtp_data = check_message

domainlist local_domains = @ : lsearch;/etc/mail/localdomains
hostlist relay_hosts = lsearch;/etc/mail/relaydomains
hostlist auth_relay_hosts = *

log_selector =  \
        +all_parents \
        +received_sender \
        +received_recipients \
        +smtp_confirmation \
        +smtp_syntax_error

allow_domain_literals = false
never_users = root:daemon:bin:sync:named
host_lookup = *
trusted_users = mail
trusted_groups = mail

gecos_pattern = ^([^,:]*)
gecos_name = $1
freeze_tell = postmaster
auto_thaw = 1h
ignore_bounce_errors_after = 30m
timeout_frozen_after = 7d

received_header_text = "Received: \
        ${if def:sender_rcvhost {from ${sender_rcvhost}\n\t}\
        {${if def:sender_ident {from ${sender_ident} }}\
        ${if def:sender_helo_name {(helo=${sender_helo_name})\n\t}}}}\
        by ${primary_hostname} \
        ${if def:received_protocol {with ${received_protocol}}} \
        (Exim ${version_number} #${compile_number} )\n\t\
        id ${message_id}\
        ${if def:received_for {\n\tfor <$received_for>}}"

system_filter = /etc/mail/system-filter
system_filter_pipe_transport =  filter_pipe
system_filter_reply_transport = address_reply
message_body_visible = 5000
message_size_limit = 10M
smtp_accept_max = 2048
smtp_connect_backlog = 256
queue_only
split_spool_directory
queue_run_max = 1
remote_max_parallel = 1
rfc1413_hosts = *
rfc1413_query_timeout = 0s
```

```
smtp_banner = "Welcome on our mail server!\n\
        This system does not accept Unsolicited \
        Commercial Email\nand will blacklist \
        offenders via our spam processor.\nHave a \
        nice day!\n\n${primary_hostname} ESMTP Exim \
        ${version_number} ${tod_full}"


#############################################################################
#                         ACL CONFIGURATION                                 #
#         Specifies access control lists for incoming SMTP mail             #
#############################################################################

begin acl

check_recipient:
  accept  hosts = :

  deny    local_parts   = ^.*[@%!/|]

  deny    senders       = *@dbm;/etc/mail/access.db : \
                          dbm;/etc/mail/access.db

  require verify        = sender

  deny    message       = unrouteable address
          hosts         = !127.0.0.1/8:0.0.0.0/0
         !verify        = recipient

  accept  domains       = +local_domains
          endpass
          message       = unknown user
          verify        = recipient

  accept  hosts         = +relay_hosts

  accept  hosts         = +auth_relay_hosts
          endpass
          message       = authentication required
          authenticated = *

  deny    message       = relay not permitted


check_message:
  accept
#############################################################################
#                        ROUTERS CONFIGURATION                              #
#               Specifies how addresses are handled                         #
#############################################################################
#     THE ORDER IN WHICH THE ROUTERS ARE DEFINED IS IMPORTANT!               #
# An address is passed to each router in turn until it is accepted.         #
#############################################################################

begin routers


dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  transport = remote_smtp
  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
  no_more
```

```
system_aliases:
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup{$local_part}lsearch{/etc/mail/aliases}}
  user = mail
  file_transport = address_file
  pipe_transport = address_pipe

userforward:
  driver = redirect
  check_local_user
  file = $home/.forward
  no_verify
  no_expn
  check_ancestor
  allow_filter
  modemask = 002
  file_transport = address_file
  pipe_transport = address_pipe
  reply_transport = address_reply

localuser:
  driver = accept
  check_local_user
  transport = local_delivery

######################################################################
#                     TRANSPORTS CONFIGURATION                       #
######################################################################
#                       ORDER DOES NOT MATTER                        #
#     Only one appropriate transport is called for each delivery.    #
######################################################################

begin transports

remote_smtp:
  driver = smtp

local_delivery:
  driver = appendfile
  file = /var/mail/$local_part
  delivery_date_add
  envelope_to_add
  return_path_add
  group = mail
  mode = 0600

address_pipe:
  driver = pipe
  return_output

address_file:
  driver = appendfile
  delivery_date_add
  envelope_to_add
  return_path_add

address_reply:
  driver = autoreply

filter_pipe:
  driver = pipe
```

```
  user = mail
  group = mail
  return_fail_output
###############################################################################
#                       RETRY CONFIGURATION                                   #
###############################################################################

begin retry

# Domain               Error       Retries
# ------               -----       -------

*                      *           F,2h,15m; G,16h,1h,1.5; F,4d,6h

###############################################################################
#                       REWRITE CONFIGURATION                                 #
###############################################################################

begin rewrite

###############################################################################
#                     AUTHENTICATION CONFIGURATION                            #
###############################################################################

begin authenticators
```

Вносимые изменения подробно описаны на русском и английском языках в файлах документации `/var/tmp/drweb-exim/opt/drweb/doc/exim/conf_file.rus.txt` и `/var/tmp/drweb-exim/opt/drweb/doc/exim/conf_file.rus.txt`, соответственно.

Конфигурационный файл /etc/drweb/drweb_exim.conf

Шаг 1

Руководствуясь ниже приведенными рекомендациями и вашими потребностями, отредактируйте файл `/etc/drweb/drweb_exim.conf`:

```
#
#  Configuration file for DrWeb Filters
#

#########################
# Communication section #
#########################
[DaemonCommunication]
# Definition of daemons addresses separeted by "," and given
# in a special form {FAMILY}:{ADDRESS}
# where FAMILY one of:
# inet - TCP/IP socket used, then {ADDRESS} is {PORT}@{HOST}
# local - UNIX socket used, then {ADDRESS} is {SOCKETFILE}
# pid - get daemon address from pidfile, then {ADDRESS} is {PIDFILE}
# Examples:
#   Address = inet:3000@localhost
#   Address = local:/usr/local/drweb/run/drwebd.skt
#   Address = pid:/usr/local/drweb/run/drwebd.pid
#   Address = pid:/var/drweb/run/drwebd.pid,
inet:3000@backup_server.example.com
Address = inet:3000@localhost

# Enable/disable caching resolved daemon host
# (useful only if daemon uses TCP/IP communications)
Cache = yes

# Timeout for whole scanning session (in seconds)
Timeout = 120
```

```
########################
# Scan options section #
########################
[Scanning]
# Enable or disable heuristic analizer in virus-finding engine (on/off)
HeuristicAnalysis = on

# Strip the smallest prefix containing StripPath leading slashes
# NOTE: Option works same the -p parameter in patch utility
# StripPath = 2

# Path that prefixes scan paths. Applied to path processed by StripPath.
# NOTE: PrefixPath MUST NOT ends by slash (/)
# PrefixPath = /sandbox/mail

# Include DrWeb report to notifications into $REPORT$
# or as separete macros $DAEMON_REPORT$(yes/no)
IncludeReport = yes

# Include DrWeb extended codes to notifications into $REPORT$
# or as separete macros $SCAN_STAT$ (yes/no)
IncludeStats = yes

# Max size of report that be created if IncludeReport is "yes",
# Specify 0 to non-restrictable size`,' but it is bad idea - report can
grow
# to Mbytes for nested archives
ReportMaxSize = 8192

# Enable or disable local scanning mode (see daemon documentation)
(yes/no)
# LocalScan has affect only on connection with first daemon in Address
list
# If enabled then spool directory must be readable (writeable for EVAL
key)
# for drwebd process (see drweb32.ini option User)
LocalScan = yes

# Enable or disable daemon rule filter (on/off)
RuleFilter = on

# Deny scanning if at least one of recipient or sender address
# present in DenyList with "deny" option (yes/no), if "no" all
# addresses in the message should present in DenyList with "deny"
DenyOnOne = yes

# List with rules for users or domains to block scanning
DenyList = /etc/drweb/users.conf

# Directory used for story temporary files
Spool = /var/drweb/spool

# Permissions for created spool files
SpoolFilesMode = 0600

####################
# Actions section #
####################
[Actions]
# NOTE: If you do not using quarantine action for some causes, please
check
# templates of notification for appropriate case - if need, remove text
about
```

```
# where original message has been storied.
#
# Infected - mean that message is infected one of known virus
# Actions:
#       cure - cure infected attachment or delete infected part of mes-
sage
#              (ONLY FOR REGISTERED USERS)
#       quarantine - move such messages to quarantine and discard
#                    (or reject if discard doesnt supported)
#       discard - discard such messages
#       reject - reject such messages with permanent error
Infected = quarantine

# Suspicious - mean that message possible is infected one of new virus
#              it may be false alarm (can be only if HeuristicAnalysis
on)
# Actions:
#       pass - pass such messages
#       quarantine - move such messages to quarantine and discard
#                    (or reject if discard doesnt supported)
#       discard - discard such messages
#       reject - reject such messages with permanent error
Suspicious = quarantine

# Incureable - mean that file is infected and cannot be cured
# Actions:
#       quarantine - move such messages to quarantine and discard
#                    (or reject if discard doesnt supported)
#       discard - discard such messages
#       reject - reject such messages with permanent error
Incureable = quarantine

# RuleFilterAlert - mean that message are hits to FiltersRule in
drweb32.ini
#                   possible only if RuleFilter = on
# Actions:
#       discard - discard such messages
#       quarantine - move such messages to quarantine and discard
#                    (or reject if discard doesnt supported)
#       reject - reject such messages with permanent error
RuleFilterAlert = quarantine

# EmptyFrom  - mean that SMTP session initiated with empty envelope From:
#              used for mail notifications (reports) and by spammers
# Actions:
#       continue - continue processing such messages
#
#       ATTENTION: Your MTA would not RFC-compliant if you set up
#       non-continue action. The MTA MUST accept messages with <> sender
#       (rfc-2505 see 2.6.1).
#
#       discard - discard such messages
#       reject - reject such messages with permanent error
EmptyFrom = continue

# SkipObject - mean that daemon found object that cannot be checked:
#              password protected archive, broken archive, sym-link,
#              non regular file
# Actions:
#       pass - pass such messages
#       quarantine - move such messages to quarantine and discard
#                    (or reject if discard doesnt supported)
#       reject - reject such messages with permanent error
SkipObject = pass
```

```
# ArchiveRestriction - mean that daemon found object in archive with com-
pression
#                  ratio exceeded MaxCompressionRation, size of object
greater
#                  that MaxFileSizeToExtract or level of nested archive
greater
#                  that MaxArchiveLevelfrom drweb32.ini
# Actions:
#        pass - pass such messages
#        quarantine - move such messages to quarantine and discard
#                     (or reject if discard doesnt supported)
#        reject - reject such messages with permanent error
ArchiveRestriction = reject

# ScanningErrors - mean that daemon fails to scan current object. Example
of
#                  cases: no memory, cannot read file for check (no per-
missions),
#                  timeout (see SocketTimeout and FileTimeout in
drweb32.ini).
# Actions:
#        pass - pass such messages
#        quarantine - move such messages to quarantine and discard
#                     (or reject if discard doesnt supported)
#        reject - reject such messages with permanent error
#        tempfail - reject such message with temporary error
ScanningErrors = quarantine

# ProcessingErrors - errors in proxy-client: no memory, misconfigured,
timeout
#                    on communication with daemon and etc.
# Actions:
#        pass - pass such messages
#        reject - reject such messages with permanent error
#        tempfail - reject such message with temporary error
ProcessingErrors = reject

# Admin mail address (may be unix-local address)
AdminMail = postmaster@bruy.info


# Filter address, that be used in From:
FilterMail = DrWEB-DAEMON@test.bruy.info
# List of unnotificable viruses
UnnotificableVirusesList = /etc/drweb/viruses.conf

# List of unnotificable addresses
UnnotificableAddressesList = /etc/drweb/addresses.conf

# Quarantine directory.
# The infected files could be moved in that dir
# if you stay this field empty or commented then
# infected messages would not been storied
Quarantine = /var/drweb/infected

# Permissions for quarantined files
QuarantineFilesMode = 0660

#########################
# Notifications section #
#########################
[VirusNotifications]
# Enable or disable sending notifications to the persons (yes/no)
```

```
SenderNotify = yes
AdminNotify = yes
RcptsNotify = yes

# Files with notification templates
AdminTemplate = /etc/drweb/templates/en-ru/exim/virus-admin.msg
RcptsTemplate = /etc/drweb/templates/en-ru/exim/virus-rcpts.msg
SenderTemplate = /etc/drweb/templates/en-ru/exim/virus-sender.msg

[SkipNotifications]
SenderNotify = yes
AdminNotify = no
RcptsNotify = no
AdminTemplate =
RcptsTemplate =
SenderTemplate = /etc/drweb/templates/en-ru/exim/skip-sender.msg

[ArchiveRestrictionNotifications]
SenderNotify = yes
AdminNotify = yes
RcptsNotify = no
AdminTemplate = /etc/drweb/templates/en-ru/exim/archive-admin.msg
RcptsTemplate =
SenderTemplate = /etc/drweb/templates/en-ru/exim/archive-sender.msg

[ErrorNotifications]
SenderNotify = yes
AdminNotify = yes
RcptsNotify = no
AdminTemplate = /etc/drweb/templates/en-ru/exim/error-admin.msg
RcptsTemplate =
SenderTemplate = /etc/drweb/templates/en-ru/exim/error-sender.msg

####################
# Logging section #
####################
[Logging]
# Logging detalization ( Quiet, Errors, Alerts, Info, Verbose, Debug )
Level = Info

# Facility used for logging to syslog ( Daemon, Mail, Local0..7 )
SyslogFacility = Mail

# Priority used for logging to syslog ( Debug, Info, Notice, Alert )
SyslogPriority = Info

#################################
# Mail system settings section #
#################################
[Mailer]
# Name of Mail System
MailSystem = Exim

# Submitting program (used to send notifications)
Sendmail = /usr/sbin/exim
```

Вам следует внести изменения, как минимум, в три строки конфигурационного файла.

В строке:

```
AdminMail = postmaster@bruy.info
```

следует указать адрес электронной почты администратора почтового севера.

В строке:

```
FilterMail = DrWEB-DAEMON@test.bruy.info
```

следует указать имя системы, на которой установлен демон Doctor Web.

В строке:

```
Sendmail = /usr/sbin/exim
```

следует указать местоположение исполняемого файла Exim.

Назначение остальных используемых в файле опций подробно описано на русском и английском языках в файлах документации `/var/tmp/drweb-exim/opt/drweb/doc/exim/conf_file.rus.txt` и `/var/tmp/drweb-exim/opt/drweb/doc/exim/conf_file.rus.txt`, соответственно.

Шаг 2

Определите права доступа к файлу `/etc/drweb/drweb_exim.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/drweb/drweb_exim.conf
[root@test /]# chown 0.0 /etc/drweb/drweb_exim.conf
```

Конфигурационный файл /etc/mail/system-filter

Добавьте в файл `/etc/mail/system-filter` строки, определяющие фильтры для сообщений, прошедших проверку на содержание вирусов с использованием Doctor Web:

```
if $received_protocol is "drweb-scanned"
then
  # looks like a already scanned message
  finish
endif

if error_message and $header_from: contains "Mailer-Daemon@"
then
  # looks like a real error message - just ignore it
  finish
endif

if not first_delivery
then
  # not first delivery attempt
  finish
endif

# Dr.Web Filter
pipe "/opt/drweb/drweb-exim --conf=/etc/drweb/drweb_exim.conf -f
$sender_address -- $recipients"

finish
```

Конфигурационный файл /etc/drweb/addresses.conf

Файл `/etc/drweb/addresses.conf` предназначен для блокировки отправки уведомлений на указанные адреса (или группу адресов) в зависимости от контекста, в котором используется адрес (отправителя, получателя или отправителя и получателя), для передачи сообщений.

Первая строка файла должна содержать запись вида:

```
[version=NN]
```

которая означает, что записи содержатся в формате N-й версии файла. Если такой строки нет, то считается, что файл записан в формате 1-й версии.

Остальные строки файла имеют формат:

```
ROLE ADDRESS_EXPRESSION
```

где:

параметр `ROLE` – может принимать значения `from`, `to` или `both` – предназначен для определения контекста, в котором используется адрес, соответственно, отправителя, получателя или отправителя и получателя.

`ADDRESS_EXPRESSION` – регулярное выражение, определяющее адреса.

Более подробно с вариантами и примерами настроек вы можете ознакомиться, прочитав документацию на русском и английском языках в файлах `/var/tmp/drweb-exim/opt/drweb/doc/exim/addresses_list.rus.txt` и `/var/tmp/drweb-exim/opt/drweb/doc/exim/addresses_list.txt`, соответственно.

Шаг 1

Отредактируйте файл `/etc/drweb/addresses.conf`, руководствуясь выше приведенными рекомендациями и вашими потребностями. Авторы настоятельно рекомендуют не вносить в этот файл никаких почтовых адресов.

Шаг 2

Определите права доступа к файлу `/etc/drweb/addresses.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/drweb/addresses.conf
[root@test /]# chown 0.0 /etc/drweb/addresses.conf
```

Конфигурационный файл /etc/drweb/users.conf

Файл `/etc/drweb/users.conf` предназначен для блокировки проверок сообщений на содержание вирусов, отправляемых (или адресуемых) с определенных почтовых адресов. Первая строка файла должна содержать запись вида:

```
[version=NN]
```

которая означает, что записи содержатся в формате N-й версии файла. Если такой строки нет, то считается, что файл записан в формате 1-й версии.

Остальные строки файла имеют следующий формат (для второй версии файла):

```
OPERATION    ROLE    METHOD    ADDRESS_EXPRESSION
```

где:

параметр `OPERATION`, принимая значения `allow` или `deny`, соответственно, разрешает или запрещает проверку на содержание вирусов.

Параметр `ROLE` – может принимать значения `from`, `to` или `any` – предназначен для определения контекста, в котором используется адрес, соответственно, отправителя, получателя или отправителя и получателя.

Параметр `METHOD` – может принимать значения `exact`, `subst`, `regex` – определяет способ обработки соответсвия адреса маске, определенной в `ADDRESS_EXPRESSION`. Значение `exact` требует точного совпадения `ADDRESS_EXPRESSION` с адресом. Значение `subst` требует, чтобы `ADDRESS_EXPRESSION` содержался в адресе в качестве подстроки, `regex` требует, чтобы адрес соответствовал регулярному выражению, определенному в `ADDRESS_EXPRESSION`. При проверке письма содержащиеся в нем адреса отправителей и получателей последовательно сопоставляются с каждой из строк файла. Если найдено соответствие адресов условиям некоторой строки, то поиск прекращается и проверка на содержание вирусов выполняется или не выполняется в соответствии с установленным значением параметра `OPERATION`. Если не найдено ни одной строки, содержащей значение `ADDRESS_EXPRESSION`, соответствующего адресам в сообщении, то осуществляется проверка сообщения на содержание вирусов. Более подробно с вариантами и примерами настроек вы можете ознакомиться в файлах документации на русском и английском языках `/var/tmp/drweb-exim/opt/drweb/doc/exim/users_list.rus.txt` и `/var/tmp/drweb-exim/opt/drweb/doc/exim/users_list.txt`, соответственно.

Шаг 1

Руководствуясь выше приведенными рекомендациями и вашими потребностями, отредактируйте файл `/etc/drweb/users.conf`. Авторы настоятельно рекомендуют не вносить в этот файл никаких почтовых адресов.

Шаг 2

Определите права доступа к файлу `/etc/drweb/users.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/drweb/users.conf
[root@test /]# chown 0.0 /etc/drweb/users.conf
```

Конфигурационный файл /etc/drweb/viruses.conf

Файл `/etc/drweb/viruses.conf` предназначен для блокировки отправки уведомлений администратору, отправителю или получателю сообщения при наличии в сообщении некоторых вирусов.

Первая строка файла должна содержать запись вида:

```
[version=NN]
```

которая означает, что записи содержатся в формате N-й версии файла. Если такой строки нет, то считается, что файл записан в формате 1-й версии.

Остальные строки файла имеют следующий формат:

```
TO_ADMIN TO_SENDER TO_RCPTS VIRUSNAME
```

Параметры TO_ADMIN, TO_SENDER, TO_RCPTS могут принимать значения allow или deny, разрешая или запрещая отправку уведомлений об обнаружении вируса, название которого указано в параметре VIRUSNAME, соответственно, администратору, отправителю и получателю сообщения.

Более подробно с вариантами и примерами настроек вы можете ознакомиться в файлах документации на русском и английском языках /var/tmp/drweb-exim/opt/drweb/doc/exim/viruses_list.rus.txt и /var/tmp/drweb-exim/opt/drweb/doc/exim/viruses_list.txt, соответственно.

Шаг 1

Отредактируйте файл /etc/drweb/viruses.conf, руководствуясь выше приведенными рекомендациями и вашими потребностями. Авторы настоятельно рекомендуют не вносить в этот файл никаких записей.

Шаг 2

Определите права доступа к файлу и назначьте его владельцем пользователя root:

```
[root@test /]# chmod 640 /etc/drweb/viruses.conf
[root@test /]# chown 0.0 /etc/drweb/viruses.conf
```

Конфигурационные файлы шаблонов /etc/drweb/templates/en-ru/*.msg

Файлы шаблонов /etc/drweb/templates/en-ru/*.msg предназначены для редактирования уведомлений – отправляемых администратору, получателю и отправителю – о получении сообщения, содержащего вирус. Шаблон может содержать макросы (ограниченные знаками $), которые заменяются реальными данными в момент создания уведомления.

Более подробно с описанием макросов и примерами их использования вы можете ознакомиться, прочитав документацию на русском и английском языках в файлах /var/tmp/drweb-exim/opt/drweb/doc/exim/notify.rus.txt и /var/tmp/drweb-exim/opt/drweb/doc/exim/notify.txt, соответственно.

Шаг 1

Отредактируйте файлы /etc/drweb/templates/en-ru/*.msg, руководствуясь выше приведенными рекомендациями и вашими потребностями. Авторы рекомендуют сократить текст уведомлений, удалив текст на английском языке и лишние подробности в сообщениях, адресуемых отправителю и получателю сообщения.

Шаг 2

Определите права доступа к файлам и назначьте их владельцем пользователя root:

```
[root@test /]# chmod 550 /etc/drweb/templates/en-ru/*.msg
[root@test /]# chown root.mail /etc/drweb/templates/en-ru/*.msg
```

Тестирование Doctor Web

Для тестирования Doctor Web в варианте интеграции его с почтовым транспортным агентом Exim необходимо выполнить следующие операции.

Шаг 1

Запустите Dr. Web daemon:

```
[root@test /]# /etc/init.d/drwebd start
```

Если вы увидите сообщение, подобное этому:

```
Starting Dr. Web daemon...Демон Dr.Web (R) для Linux, версия 4.29.2 (5
Ноябрь 2002)
Copyright (c) Игорь Данилов, 1992-2002
"Лаборатория Данилова" и «ДиалогНаука"
http://www.drweb.ru, support@drweb.ru: +7 (812) 387-64-08
http://www.dials.ru, antivir@dials.ru: +7 (095) 137-01-50
Ключевой файл: /opt/drweb/drwebd.key
Регистрационные данные:
0100005168
Evaluation Key (ID Anti-Virus Lab. Ltd, St.Petersburg)
ОЗНАКОМИТЕЛЬНАЯ версия! Имеет функциональные ограничения!
Для регистрации обращайтесь к региональному дилеру.
```

```
Загрузка /var/drweb/bases/drwebase.vdb - Ok, вирусных записей: 31578
Демон загружен, TCP-сокет создан на порту 3000
```

то запуск Dr. Web daemon прошел удачно.

Шаг 2

Для проверки работоспособности демона создайте файл, содержащий тестовый вирус EICAR. Для этого удалите из файла `/install/opt/drweb/doc/readme.eicar` лишние строки, оставив только одну:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

и сохраните его в файле `~/virus.com`.

Файл `~/virus.com` не является вирусом, а содержит строку, используемую большинством антивирусных продуктов для тестирования.

Проверьте файл `~/virus.com` на наличие вируса:

```
[root@test /]# /opt/drweb/clients/drwebdc -nlocalhost -p3000 -fvirus.com
```

Если вы получите сообщение, подобное следующему:

```
Results: daemon return code 0x10020 (known virus is found)
```

то Dr. Web daemon функционирует нормально.

Шаг 3

Некоторые ошибки в конфигурационных файлах могут быть обнаружены с помощью запуска из командной строки `drweb-exim`. Протестируйте конфигурационные файлы на предмет наличия ошибок:

```
[root@test /]# /opt/drweb-exim --check_only --check_user=mail
```

Ниже приведен пример сообщения об ошибке в 185 строке конфигурационного файла `/etc/drweb/drweb_exim.conf`:

```
dwlib: conf: filter would use mail account (uid=8, gid=12)
dwlib: conf: configuration will been loaded from
/etc/drweb/drweb_exim.conf
dwlib: read_section(Actions): illegal line 185
dwlib: read_conf(/etc/drweb/drweb_exim.conf): error in section [Actions]
dwlib: conf: configuration loading has been failed
cannot load configuration file
This report created automatically by antivirus software.
Problem: cannot load configuration file
```

Шаг 4

Отравьте письмо, содержащее вирус, какому-нибудь пользователю:

```
[drwalbr@test drwalbr /]$ cat virus.com | mail –s "Вирус" karlnext
```

и через некоторое время проверьте почту отправителя, получателя и администратора. В рассматриваемом примере получатель – `karlnext@test.bruy.info` – должен получить следующее сообщение:

```
From: "DrWeb-DAEMON" <DrWEB-DAEMON@test.bruy.info>
To: "Recipients of original message" <#@[]>
Date: Fri, 27 Jun 2003 21:49:47 +0400
Subject: Undelivered mail:  Вирус
Dear User,
the message sent to you by drwalbr@test.bruy.info (may be forged) with
following
attributes has not been delivered, because contains an infected object.
--- Dr.Web report ---
Following virus(es) has been found:
инфицирован EICAR Test File (NOT a Virus!)

Dr.Web detailed report:
drweb.tmp_X3gj3M/[message body] инфицирован EICAR Test File (NOT a Vi-
rus!)
Dr.Web scanning statistic:
Evaluation key used !Infected : 1
--- Dr.Web report ---
The original message was stored in archive record named:
```

```
drweb.quarantined_8dPLFf
In order to receive the original message, please send request to
<postmaster@bruy.info>, referring to the archive record name
given above.
Antivirus service provided by Dr.Web(R) Daemon for Unix
   (http://www.drweb.ru, http://www.dials.ru/english)
Content-Type: text/plain; charset=koi8-r
Content-Transfer-Encoding: 8bit
Уважаемый Получатель !
Сообщение, посланное Вам с адреса drwalbr@test.bruy.info (возможно подде-
лан)
инфицировано и не было доставлено.
--- Dr.Web report ---
Найден(ы) следующий(е) вирус(ы):
инфицирован EICAR Test File (NOT a Virus!)
Детализированный отчет Dr.Web:
drweb.tmp_X3gj3M/[message body] инфицирован EICAR Test File (NOT a Vi-
rus!)
Статистика сканирования Dr.Web:
Evaluation key used !Infected : 1
--- Dr.Web report ---
Сообщение сохранено в карантине под именем:
drweb.quarantined_8dPLFf
Чтобы получить это сообщение, обратитесь к администратору
по адресу <postmaster@bruy.info>, указав имя, под
которым сохранено сообщение для Вас.
   Антивирусная защита почтовых серверов
   Dr.Web(R) Daemon for Unix (разработан в Daniloff's Labs)
   (http://www.drweb.ru, http://www.DialogNauka.ru)
```

Отправитель – drwalbr@test.bruy.info – должен получить следующее сообщение:

```
From: "DrWeb-DAEMON" <DrWEB-DAEMON@test.bruy.info>
Subject: Undelivered mail:  Вирус
Date: Fri, 27 Jun 2003 21:49:48 +0400
To: drwalbr@test.bruy.info
Dear User,
the message with following attributes has not been delivered,
because contains an infected object.
Sender = drwalbr@test.bruy.info (may be forged)
Recipients = karlnext@test.bruy.info
Subject =  Вирус
Message-ID =  <E19VxLc-0005Mq-Hi@test.bruy.info>
Antivirus filter report:
--- Dr.Web report ---
Following virus(es) has been found:
инфицирован EICAR Test File (NOT a Virus!)
Dr.Web detailed report:
drweb.tmp_X3gj3M/[message body] инфицирован EICAR Test File (NOT a Vi-
rus!)
Dr.Web scanning statistic:
Evaluation key used !Infected : 1
--- Dr.Web report ---
   Antivirus service provided by Dr.Web(R) Daemon for Unix
   (http://www.drweb.ru, http://www.dials.ru/english)
Уважаемый Отправитель drwalbr@test.bruy.info !
Сообщение, отправленное с Вашего адреса (возможно вирусом
с другого компьютера) по адресу(ам) karlnext@test.bruy.info
инфицировано и не было доставлено.
--- Dr.Web report ---
Найден(ы) следующий(е) вирус(ы):
инфицирован EICAR Test File (NOT a Virus!)
Детализированный отчет Dr.Web:
drweb.tmp_X3gj3M/[message body] инфицирован EICAR Test File (NOT a Vi-
rus!)
```

```
Статистика сканирования Dr.Web:
Evaluation key used !Infected : 1
--- Dr.Web report ---
Ваше сообщение сохранено в карантине под именем:
drweb.quarantined_8dPLFf
Чтобы получить это сообщение, обратитесь к администратору
по адресу <postmaster@bruy.info>, указав имя, под которым
Ваше сообщение сохранено в карантине.
---
   Антивирусная защита почтовых серверов
   Dr.Web(R) Daemon for Unix (разработан в Daniloff's Labs)
   (http://www.drweb.ru, http://www.DialogNauka.ru)
```

Администратор – `postmaster@bruy.info` – должен получить сообщение следующего вида:

```
From: "DrWeb-DAEMON" <DrWEB-DAEMON@test.bruy.info>
Subject: A VIRUS HAS BEEN DETECTED !!!
Date: Fri, 27 Jun 2003 21:49:47 +0400
To: "AV-Administrator" <postmaster@bruy.info>

Dear Postmaster,
the message with following attributes has not been delivered, because
contains an infected object.
Sender = drwalbr@test.bruy.info (may be forged)
Recipients = karlnext@test.bruy.info
Subject = Вирус
Message-ID = <E19VxLc-0005Mq-Hi@test.bruy.info>
--- Dr.Web report ---
Following virus(es) has been found:
инфицирован EICAR Test File (NOT a Virus!)
Dr.Web detailed report:
drweb.tmp_X3gj3M/[message body] инфицирован EICAR Test File (NOT a Vi-
rus!)
Dr.Web scanning statistic:
Evaluation key used !Infected : 1
--- Dr.Web report ---
The original message was stored in archive record named:
drweb.quarantined_8dPLFf
Уважаемый Администратор !
Следующее сообщение инфицировано и не было доставлено.
Оправитель = drwalbr@test.bruy.info (возможно подделан)
Получатели = karlnext@test.bruy.info
Тема = Вирус
Идентификатор = <E19VxLc-0005Mq-Hi@test.bruy.info>
--- Dr.Web report ---
Найден(ы) следующий(е) вирус(ы):
инфицирован EICAR Test File (NOT a Virus!)
Детализированный отчет Dr.Web:
drweb.tmp_X3gj3M/[message body] инфицирован EICAR Test File (NOT a Vi-
rus!)
Статистика сканирования Dr.Web:
Evaluation key used !Infected : 1
--- Dr.Web report ---
Сообщение сохранено в карантине под именем:
drweb.quarantined_8dPLFf
```

В каталоге `/var/drweb/infected` должен находиться файл `drweb.quarantined_8dPLFf`, содержащий исходное сообщение, отправленое пользователем `drwalbr` пользователю `karlnext`:

```
From drwalbr@test.bruy.info Fri Jun 27 21:49:47 2003
Received: from drwalbr by test.bruy.info with local (Exim 4.20 #1 )
id 19VxLc-0005Mq-Hi
for <karlnext@test.bruy.info>; Fri, 27 Jun 2003 21:49:20 +0400
To: karlnext@test.bruy.info
Subject: Вирус
Message-Id: <E19VxLc-0005Mq-Hi@test.bruy.info>
```

```
From: drwalbr@test.bruy.info
Date: Fri, 27 Jun 2003 21:49:20 +0400
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Обновление антивирусных баз Doctor Web

Для обновления антивирусных баз данных необходимо запустить скрипт

```
[root@test /]# /opt/drweb/update/update.pl
```

Часть 8

Программное обеспечение для серверов баз данных

Глава 31

MySQL – сервер баз данных

В этой главе:

1. Ограничения и допущения
2. Пакеты
3. Инсталляция MySQL из rpm-пакетов
4. Компиляция, оптимизация и инсталляция MySQL из исходных кодов
5. Конфигурирование MySQL
6. Конфигурационный файл /etc/my.cnf
7. Конфигурационный файл /etc/logrotate.d/mysqld
8. Файл инициализации /etc/init.d/mysqld
9. Установка пароля пользователя root и удаление демонстрационной базы данных test
10. Монтирование раздела баз данных с атрибутом noatime
11. Пример использования MySQL

В настоящее время базы данных находят широкое применение в практически любых информационных системах, начиная с простейшего любительского сайта и заканчивая корпоративными базами данных. Для организации интерфейса между конечными пользователями (клиентскими программами) и базами данных, а также администрирования баз данных используется определенный класс программного обеспечения, называемый серверами баз данных. MySQL – многопользовательский, многопоточный SQL-сервер баз данных, разработанный компанией MySQL AB. К числу достоинств этого сервера следует отнести высокую производительность, устойчивость к ошибкам и простоту в использовании.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции по инсталляции программного обеспечения выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта MySQL по состоянию на 01.07.2003. Регулярно посещайте домашнюю страницу проекта `http://www.mysql.com` и отслеживайте обновления.

MySQL-сервер содержится в пакете `MySQL-server-version.rpm` (последняя доступная на момент написания главы стабильная версия `MySQL-server-4.0.13-0.i386.rpm`), клиентское программное обеспечение – в rpm-пакете `MySQL-client-version.rpm` (последняя доступная на момент написания главы стабильная версия `MySQL-client-4.0.13-0.i386.rpm`). Этих двух пакетов достаточно для стандартной установки сервера и клиентского программного обеспечения. Кроме того, на сервере разработчиков имеются следующие rpm-пакеты:

- пакет `MySQL-bench-VERSION.i386.rpm`, содержащий тесты и контрольные задачи;
- пакет `MySQL-devel-VERSION.i386.rpm`, содержащий библиотеки и другие файлы, необходимые для компиляции некоторых клиентов MySQL, например, модулей Perl.
- пакет `MySQL-shared-VERSION.i386.rpm`, содержащий динамические библиотеки (`libmysqlclient.so*`), используемые в некоторых языках программирования для взаимодействия с MySQL.
- пакет `MySQL-VERSION.src.rpm`, содержащий исходные коды для всех приведенных выше rpm-пакетов.

Исходные коды MySQL содержатся в архиве `mysql-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `mysql-4.0.13.tar.gz`).

ЗАМЕЧАНИЕ В соответствии с рекомендациями разработчиков на Linux-системах с процессором архитектуры x86 и версией компилятора `gcc 2.96` рекомендуется устанавливать MySQL из rpm-пакетов или откомпилированных разработчиками исполняемых файлов. Использование сервера баз данных, скомпилированного из исходных кодов с помощью компилятора `gcc 2.96`, может привести к потере данных. Разработчики также сообщают, что компиляция исходных кодов с помощью компиляторов версий 2.95, 2.91 и 3.2 позволяет получить надежно работающие исполняемые файлы MySQL.

Инсталляция MySQL из rpm-пакетов

Для инсталляция MySQL из rpm-пакетов необходимо выполнить некоторые операции. Следует подчеркнуть, что в состав дистрибутива ASPLinux 7.3 (Vostok) включены лишь часть пакетов из перечисленных выше:

- `mysql-3.23.49-3.asp.i386.rpm;`
- `mysqlclient9-3.23.22-6.i386.rpm;`
- `mysql-server-3.23.49-3.asp.i386.rpm;`
- `mysql-devel-3.23.49-3.asp.i386.rpm`.

Шаг 1

В случае установки MySQL из дистрибутива, перейдите в каталог, где находятся требуемые пакеты. Если вы в соответствии с рекомендациями главы 2 скопировали все исходные rpm-пакеты в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

и установите:

```
[root@drwalbr distrib]# rpm -ihv mysqlclient9-3.23.22-6.i386.rpm\
mysql-server-3.23.49-3.asp.i386.rpm
```

Шаг 2

В случае установки MySQL из более свежих пакетов, загруженных с сервера разработчика, осуществите проверку подлинности имеющихся в вашем распоряжении rpm-пакетов с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 3

Установите и запустите сервер баз данных:

```
[root@drwalbr /]# cd /var/tmp
[root@drwalbr tmp]# rpm -ihv MySQL-client-4.0.13-0.i386.rpm  MySQL-
server-4.0.13-0.i386.rpm
Подготовка...     ########################################### [100%]
   1:MySQL-client ########################################### [ 50%]
   2:MySQL-server ########################################### [100%]
Preparing db table
Preparing host table
Preparing user table
Preparing func table
Preparing tables_priv table
Preparing columns_priv table
Installing all prepared tables
030702 11:15:29  /usr/sbin/mysqld: Shutdown Complete


PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
This is done with:
/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h drwalbr.und password 'new-password'
See the manual for more instructions.

Please report any problems with the /usr/bin/mysqlbug script!

The latest information about MySQL is available on the web at
http://www.mysql.com
Support MySQL by buying support/licenses at https://order.mysql.com

Starting mysqld daemon with databases from /var/lib/mysql
```

ЗАМЕЧАНИЕ Обратите внимание на предупреждающее сообщение о необходимости установки пароля для пользователя `root`. До установки пароля каждый пользователь локальной системы – в рассматриваемом примере `drwalbr.und` – может совершать любые, по своему усмотрению, действия с вашим сервером баз данных. Установить пароль можно с помощью утилиты `mysqladmin`, используемой для администрирования сервера, с помощью команд, приведенных выше или с помощью клиента `mysql` в соответствии с рекомендациями раздела «Конфигурирование MySQL".

Компиляция, оптимизация и инсталляция MySQL из исходных кодов

Напоминаем, использование сервера баз данных, скомпилированного из исходных кодов с помощью компилятора `gcc 2.96`, может привести к потере данных. Для реализации ниже приведенных инструкций необходимо наличие компилятора версии, отличной от 2.96. Установка MySQL из исходных кодов целесообразна лишь в случае предъявления к серверу нестандартных требований по производительности и функциональным возможностям.

Инсталляция MySQL из исходных кодов осуществляется следующим образом.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами MySQL в каталоге `/var/tmp`:

```
[root@drwalbr tmp]# tar xzpf mysql-4.0.13.tar.gz
```

Шаг 3

Создайте специального пользователя `mysql`, от имени которого будет запускаться MySQL:

```
[root@drwalbr tmp]# groupadd -g 27 mysql > /dev/null  2>&1 || :
[root@drwalbr tmp]# useradd -u 27 -g 27 -s /bin/bash -M -r -d
/var/lib/mysql mysql > /dev/null 2>&1 || :
```

Шаг 4

Откonфигурируйте исходные коды MySQL:

```
[root@drwalbr tmp]# cd mysql-4.0.13
[root@drwalbr mysql-4.0.13]# CFLAGS="-static -O2 -march=i686 -funroll-
loops" \
CXXFLAGS="-static -O2 -march=i686 -funroll-loops -felide-constructors -
fno-exceptions -fno-rtti" \
./configure \
--prefix=/usr \
--libexecdir=/usr/sbin \
--sysconfdir=/etc \
--localstatedir=/var/lib/mysql \
--mandir=/usr/share/man \
--disable-shared \
--enable-assembler \
--with-thread-safe-client \
--with-mysqld-user="mysql" \
--with-unix-socket-path=/var/lib/mysql/mysql.sock \
--with-client-ldflags=-all-static \
--with-mysqld-ldflags=-all-static \
--without-readline \
--without-debug \
--without-docs \
--without-bench \
--with-charset=cp1251 \
--with-extra-charsets=all
```

Шаг 5

Откомпилируйте, проинсталлируйте MySQL, создайте и сохраните в надежном месте список установленных файлов:

```
[root@drwalbr mysql-4.0.13]# make
[root@drwalbr mysql-4.0.13]# find /* > /root/mysql1
[root@drwalbr mysql-4.0.13]# make install
[root@drwalbr mysql-4.0.13]# mkdir -p /var/run/mysqld
[root@drwalbr mysql-4.0.13]# chown mysql.mysql /var/run/mysqld
[root@drwalbr mysql-4.0.13]# rm -rf /usr/mysql-test/
[root@drwalbr mysql-4.0.13]# rm -f /usr/share/mysql/mysql-*.spec
[root@drwalbr mysql-4.0.13]# rm -f /usr/share/mysql/mysql-log-rotate
[root@drwalbr mysql-4.0.13]# strip /usr/sbin/mysqld
[root@drwalbr mysql-4.0.13]# find /* > /root/mysql2
[root@drwalbr mysql-4.0.13]# diff /root/mysql1 /root/mysql2
>/root/mysql.installed
[root@drwalbr mysql-4.0.13]# mv /root/mysql.installed
/very_reliable_place/mysql.installed.YYYYMMDD
```

Конфигурирование MySQL

Конфигурирование MySQL осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/my.cnf`;

- файла настройки чередования регистрационных файлов `/etc/logrotate.d/mysqld`;
- файла инициализации `/etc/init.d/mysqld`.

Конфигурационный файл /etc/my.cnf

В комплекте поставки MySQL имеется несколько примеров конфигурационных файлов, оптимизированных для систем различных конфигураций и назначений. В rpm-варианте инсталляции эти файлы находятся в каталоге `/usr/share/mysql`. Файл `my-huge.cnf` содержит пример конфигурации для высокопроизводительных серверов с объемом оперативной памяти более 1…2 Гбайт, используемых исключительно в качестве сервера баз данных. Файл `my-lage.cnf` содержит пример конфигурации для высокопроизводительных серверов с объемом оперативной памяти более 512 Мбайт, используемых исключительно в качестве сервера баз данных. Файл `my-medium.cnf` содержит пример конфигурации для сервера с небольшим объемом оперативной памяти 32…64 Мбайт, преимущественно используемого в качестве сервера баз данных, или серверов с объемом оперативной памяти до 128 Мбайт, на которых MySQL функционирует совместно с другими службами. Файл `my-small.cnf` содержит пример конфигурации для систем с объемом оперативной памяти менее 64 Мбайт, на которых обращение к серверу баз данных осуществляется эпизодически.

Шаг 1

Создайте файл `/etc/my.cnf`, руководствуясь вашими потребностями, техническими характеристиками системы, на которой осуществляется установка, и ниже приведенными рекомендациями:

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
skip-locking
set-variable = key_buffer=16
set-variable = max_allowed_packet=1M
set-variable = table_cache=128
set-variable = sort_buffer=512K
set-variable = net_buffer_length=8k
set-variable = myisam_sort_buffer_size=8M
#Only for RPM installation
default-character-set=cp1251

[mysql.server]
user=mysql
basedir=/var/lib

[safe_mysqld]
err-log=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid

[isamchk]
set-variable = key_buffer=20M
set-variable = sort_buffer=20M
set-variable = read_buffer=2M
set-variable = write_bufer=2M

[myisamchk]
set-variable = key_buffer=20M
set-variable = sort_buffer=20M
set-variable = read_buffer=2M
set-variable = write_bufer=2M
```

Строку:

```
default-character-set=cp1251
```

определяющую кодировку, используемую по умолчанию, следует использовать только в файле `/etc/my.cnf`, создаваемом при инсталляции из rpm-пакета. При инсталляции из исходных кодов указанная опция задается при конфигурировании исходных кодов (см. выше шаг 4 раздела «Компиляция, оптимизация и инсталляция MySQL").

Здесь не рассматривается назначение всех опций, используемых в этом конфигурационном файле, т. к. они подробно описаны во входящей в комплект поставки MySQL документации, находящейся на сервере разработчиков и русскоязычном ресурсе `http://www.mysql.ru`.

Шаг 2

Установите права доступа к файлу `/etc/my.cnf` и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 644 /etc/my.cnf
[root@drwalbr /]# chown 0.0 /etc/my.cnf
```

Конфигурационный файл /etc/logrotate.d/mysqld

Шаг 1

Создайте файл `/etc/logrotate.d/mysqld`, содержащий следующие строки:

```
/var/log/mysqld.log {
    missingok
    create 0640 mysql mysql
    prerotate
        [ -e /var/lock/subsys/mysqld ] && /bin/kill -HUP `/bin/cat
/var/run/mysqld/mysqld.pid` || /bin/true
    endscript
    postrotate
        [ -e /var/lock/subsys/mysqld ] && /bin/kill -HUP `/bin/cat
/var/run/mysqld/mysqld.pid` || /bin/true
    endscript
}
```

При использовании такого варианта конфигурации файлы регистрации будут чередоваться еженедельно.

Шаг 2

Установите права доступа к файлу `/etc/logrotate.d/mysqld` и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 644 /etc/logrotate.d/mysqld
[root@drwalbr /]# chown 0.0 /etc/logrotate.d/mysqld
```

Файл инициализации /etc/init.d/mysqld

Создание файла `/etc/init.d/mysqld` необходимо только в случае инсталляции MySQL из исходных кодов. При инсталляции из rpm-пакетов инициализационный файл `/etc/init.d/mysql` создается автоматически. Если вы устанавливаете MySQL из rpm-пакетов, пропустите этот раздел и перейдите к следующему.

Шаг 1

Создайте файл инициализации `/etc/init.d/mysqld`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping MySQL.
#
# chkconfig: 345 78 12
# description:  MySQL is a fast & secure SQL database server.
#
# processname: mysqld
# config: /etc/my.cnf
# pidfile: /var/run/mysqld/mysqld.pid

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network
# Source for additional options if we have them.
if [ -f /etc/sysconfig/mysql ] ; then
```

```
        . /etc/sysconfig/mysql
fi
# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0
# If MySQL is not available stop now.
[ -f /usr/bin/mysqld_safe ] || exit 0
# Path to the MySQL binary.
safe_mysqld=/usr/bin/mysqld_safe

RETVAL=0
prog="MySQL"
echo "6"
start() {
        if [ ! -d /var/lib/mysql/mysql ] ; then
            action $"Initializing $prog database: "
/usr/bin/mysql_install_db
            ret=$?
            chown -R mysql.mysql /var/lib/mysql
                if [ $ret -ne 0 ] ; then
                        return $ret
                fi
        fi

        chown -R mysql.mysql /var/lib/mysql
        chmod 0755 /var/lib/mysql
        daemon $safe_mysqld --defaults-file=/etc/my.cnf >/dev/null 2>&1 &
        ret=$?

        if [ $ret -eq 0 ]; then
            action $"Starting $prog: " /bin/true
        else
            action $"Starting $prog: " /bin/false
        fi
        [ $ret -eq 0 ] && touch /var/lock/subsys/mysqld
        return $ret
}

stop() {
        kill `cat /var/run/mysqld/mysqld.pid  2> /dev/null ` > /dev/null
2>&1
        ret=$?

        if [ $ret -eq 0 ]; then
            action $"Shutting down $prog: " /bin/true
        else
            action $"Shutting down $prog: " /bin/false
        fi

        [ $ret -eq 0 ] && rm -f /var/lock/subsys/mysqld
        [ $ret -eq 0 ] && rm -f /var/lib/mysql/mysql.sock
        return $ret
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
*)
        echo $"Usage: $0 {start|stop}"
        exit 1
```

```
esac
exit $?
```

Шаг 2

Установите права доступа к файлу `/etc/init.d/mysqld` и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 700 /etc/init.d/mysqld
[root@drwalbr /]# chown 0.0 /etc/init.d/mysqld
```

Шаг 3

Для автоматического запуска MySQL при загрузке системы создайте необходимые ссылки:

```
[root@drwalbr /]# chkconfig --add mysqld
[root@drwalbr /]# chkconfig --level 345 mysqld on
```

Установка пароля пользователя root и удаление демонстрационной базы данных test

Шаг 1

Запустите MySQL. Для запуска сервера баз данных, инсталлированного с помощью rpm-пакетов, используйте команду:

```
[root@drwalbr dymatel]# /etc/init.d/mysql start
[root@drwalbr dymatel]# Starting mysqld daemon with databases from
/var/lib/mysql
```

Для запуска сервера баз данных, инсталлированного посредством компиляции исходных кодов, используйте команду:

```
[root@drwalbr /]# /etc/init.d/mysqld start
Запускается MySQL:                         [OK]
```

Как видно из этих примеров разница заключается только в виде выводимой информации при запуске программы.

Шаг 2

Попытайтесь установить соединение с сервером баз данных с системы, на которой установлен MySQL – в рассматриваемом примере `drwalbr.und`. Для установки соединения с правами администратора сервера баз данных выполните от имени обычного пользователя команду:

```
[drwalbr@drwalbr /]$ mysql -u root mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 0 to server version: 4.0.13

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

Вы подключились к серверу баз данных без ввода пароля. Это также может сделать любой пользователь системы `drwalbr.und`, что очень плохо, с точки зрения безопасности вашей системы. Установите пароль для пользователя `root`:

```
mysql> SET PASSWORD FOR root=PASSWORD('$ecretnoe_sL0vo');
Query OK, 0 rows affected (0.00 sec)
```

Для вступления изменений в силу выполните команду:

```
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Отключитесь от сервера баз данных:

```
mysql> \quit
Bye
```

Шаг 3

Попробуйте вновь установить соединение с сервером баз данных, не вводя пароль:

```
[drwalbr@drwalbr /]$ mysql -u root -h drwalbr.und
```

Вы не сможете установить подключение:

```
ERROR 1045: Access denied for user: 'root@drwalbr.und' (Using password:
NO)
```

Для подключения к серверу с вводом пароля используйте команду:

```
[drwalbr@drwalbr /]$ mysql -u root -h drwalbr -p
Enter password: $ecretnoe_sL0vo
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6 to server version: 4.0.13

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.


Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

Шаг 4

Выведите список баз данных, установленных на вашем сервере:

```
mysql> SHOW DATABASES;
+----------+
| Database |
+----------+
| mysql    |
| test     |
+----------+
2 rows in set (0.00 sec)
```

В комплект поставки MySQL входит база данных с именем `test`, к которой может подключиться без ввода пароля любой пользователь системы, на которой установлен сервер баз данных.

Необходимо удалить базу данных `test`. Для этого выполните:

```
mysql> DROP DATABASE test;
Query OK, 0 rows affected (0.00 sec)
```

Убедитесь в том, что база данных `test` удалена:

```
mysql> SHOW DATABASES;
+----------+
| Database |
+----------+
| mysql    |
+----------+
1 rows in set (0.00 sec)
```

Отключитесь от сервера баз данных:

```
mysql> \quit
Bye
```

и подключитесь к базе данных `test` в качестве произвольного пользователя, например, `xaker`:

```
[drwalbr@drwalbr /]$ mysql -u xaker -h drwalbr.und
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9 to server version: 4.0.13

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

Вы, не вводя пароля, установили соединение с сервером баз данных и можете вновь создать базу данных `test`, то же самое может сделать и любой пользователь системы, имеющий доступ к консоли, на которой установлен сервер баз данных. Это происходит потому что, не смотря на то, что вы удалили базу данных `test`, в базе данных `mysql`, предназначенной для хранения информации о полномочиях пользователей, сохранились записи, разрешающие доступ с локальной системы к базе данных `test`.

Шаг 5

Для удаления этих записей разорвите соединение с сервером баз данных и подключитесь вновь в качестве пользователя `root`:

```
mysql> \quit
Bye
```

```
[drwalbr@drwalbr /]$ mysql -u root -h drwalbr.und –p
Enter password: $ecretnoe_sL0vo
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10 to server version: 4.0.13

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.


Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

Подключитесь к базе данных `mysql`:

```
mysql> USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

Создайте список таблиц базы данных `mysql`:

```
mysql> SHOW TABLES;
+-----------------+
| Tables_in_mysql |
+-----------------+
| columns_priv    |
| db              |
| func            |
| host            |
| tables_priv     |
| user            |
+-----------------+
6 rows in set (0.00 sec)
```

Данные о всех пользователях сервера баз данных хранятся в таблице `user`. С полным перечнем полей таблицы можно ознакомится с помощью команды:

```
mysql> DESCRIBE user;
+------------------+----------------------+------+-----+---------+-------
+
| Field            | Type                 | Null | Key | Default | Extra
|
+------------------+----------------------+------+-----+---------+-------
+
| Host             | varchar(60) binary   |      | PRI |         |
|
| User             | varchar(16) binary   |      | PRI |         |
|
| Password         | varchar(16) binary   |      |     |         |
|
| Select_priv      | enum('N','Y')        |      |     | N       |
|
| Insert_priv      | enum('N','Y')        |      |     | N       |
|
| Update_priv      | enum('N','Y')        |      |     | N       |
|
| Delete_priv      | enum('N','Y')        |      |     | N       |
|
| Create_priv      | enum('N','Y')        |      |     | N       |
|
| Drop_priv        | enum('N','Y')        |      |     | N       |
|
| Reload_priv      | enum('N','Y')        |      |     | N       |
|
| Shutdown_priv    | enum('N','Y')        |      |     | N       |
|
```

```
| Process_priv     | enum('N','Y')        |      |     | N       |
|
| File_priv        | enum('N','Y')        |      |     | N       |
|
| Grant_priv       | enum('N','Y')        |      |     | N       |
|
| References_priv  | enum('N','Y')        |      |     | N       |
|
| Index_priv       | enum('N','Y')        |      |     | N       |
|
| Alter_priv       | enum('N','Y')        |      |     | N       |
|
| Show_db_priv     | enum('N','Y')        |      |     | N       |
|
| Super_priv       | enum('N','Y')        |      |     | N       |
|
| Create_tmp_      | enum('N','Y')        |      |     | N       |
|
| table_priv       |                      |      |     |         |
|
| Lock_tables_priv | enum('N','Y')        |      |     | N       |
|
| Execute_priv     | enum('N','Y')        |      |     | N       |
|
| Repl_slave_priv  | enum('N','Y')        |      |     | N       |
|
| Repl_client_priv | enum('N','Y')        |      |     | N       |
|
| ssl_type         | enum('','ANY','X509' |      |     |         |
|
|                  |  'SPECIFIED')        |      |     |         |
|
| ssl_cipher       | blob                 |      |     |         |
|
| x509_issuer      | blob                 |      |     |         |
|
| x509_subject     | blob                 |      |     |         |
|
| max_questions    | int(11) unsigned     |      |     | 0       |
|
| max_updates      | int(11) unsigned     |      |     | 0       |
|
| max_connections  | int(11) unsigned     |      |     | 0       |
|
+------------------+----------------------+------+-----+---------+-------
+
31 rows in set (0.00 sec)
```

а их назначение подробно описано в документации. С точки зрения решаемой задачи, нас интересуют параметры, содержащиеся в полях `Host`, `User`, `Password` и `*_priv`, в которых находится информация об имени хоста (`Host`), с которого разрешен доступ пользователю (`User`) с паролем (`Password`). В полях `*_priv` содержится информация о привилегиях пользователя.

Для просмотра содержимого таблицы `user` выполните:

```
mysql> SELECT * FROM user;
+-------------+------+----------+-------------+------------...
| Host        | User | Password | Select_priv | Insert_priv
+-------------+------+----------+-------------+------------...
| localhost   | root |          | Y           | Y
| drwalbr.und | root |          | Y           | Y
| localhost   |      |          | N           | N
| drwalbr.und |      |          | N           | N
+-------------+------+----------+-------------+------------...
4 rows in set (0.00 sec)
```

Из полученной информации видно, что установка соединений разрешена любому пользователю (пустые значения в третьей и четвертой строке столбца `User`) локальной системы без ввода пароля (пустые значения в третьей и четвертой строке столбца `Password`). При этом пользователь не имеет никаких привилегий на уровне сервера баз данных в целом (символы `N` в третьей и четвертой строке столбцов `*_priv`). Привилегии в рассматриваемом случае определяются другой таблицей базы данных `mysql – db`. С полным перечнем полей таблицы `db` можно ознакомиться с помощью команды:

```
mysql> DESCRIBE db;
+------------------+-----------------+------+-----+---------+-------+
| Field            | Type            | Null | Key | Default | Extra |
+------------------+-----------------+------+-----+---------+-------+
| Host             | char(60) binary |      | PRI |         |       |
| Db               | char(64) binary |      | PRI |         |       |
| User             | char(16) binary |      | PRI |         |       |
| Select_priv      | enum('N','Y')   |      |     | N       |       |
| Insert_priv      | enum('N','Y')   |      |     | N       |       |
| Update_priv      | enum('N','Y')   |      |     | N       |       |
| Delete_priv      | enum('N','Y')   |      |     | N       |       |
| Create_priv      | enum('N','Y')   |      |     | N       |       |
| Drop_priv        | enum('N','Y')   |      |     | N       |       |
| Grant_priv       | enum('N','Y')   |      |     | N       |       |
| References_priv  | enum('N','Y')   |      |     | N       |       |
| Index_priv       | enum('N','Y')   |      |     | N       |       |
| Alter_priv       | enum('N','Y')   |      |     | N       |       |
| Create_tmp_      | enum('N','Y')   |      |     | N       |       |
| table_priv       | enum('N','Y')   |      |     | N       |       |
| Lock_tables_priv | enum('N','Y')   |      |     | N       |       |
+------------------+-----------------+------+-----+---------+-------+
15 rows in set (0.00 sec)
```

Для просмотра содержимого таблицы `db` наберите:

```
mysql> SELECT * FROM db;
+------+---------+------+-------------+-------------+-------------...
| Host | Db      | User | Select_priv | Insert_priv | Update_priv
+------+---------+------+-------------+-------------+-------------...
| %    | test    |      | Y           | Y           | Y
| %    | test\_% |      | Y           | Y           | Y
+------+---------+------+-------------+-------------+-------------...
2 rows in set (0.01 sec)
```

Из полученного вывода видно, что подключение к базе данных `test` разрешена любому пользователю (пустые значения в первой и второй строках столбца `User`), при этом пользователь имеет все привилегии (символы `Y` в первой и второй строке в столбцах `*_priv`).

Удалите ненужные записи из таблицы `user` и `db`:

```
mysql> DELETE FROM user  WHERE User ="";
Query OK, 2 rows affected (0.00 sec)

mysql> DELETE FROM db WHERE Db ="test";
Query OK, 1 row affected (0.00 sec)

mysql> DELETE FROM db WHERE Db ="test\_%";
Query OK, 1 row affected (0.00 sec)
```

Для вступления изменений в силу выполните команду:

```
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Разорвите соединение с сервером:

```
mysql> \quit
Bye
```

Шаг 6

Попробуйте подключиться к базе данных `test` с полномочиями пользователя `xaker`:

```
[drwalbr@drwalbr /]$ mysql -u xaker -h drwalbr.und
```

Вам не удастся установить соединение, а на экране появится сообщение об ошибке:

```
ERROR 1045: Access denied for user: 'xaker@drwalbr.und' (Using password:
NO)
```

Монтирование раздела баз данных с атрибутом noatime

Если на вашем сервере каталог, в который установлен MySQL – например, `/var/lib` – смонтирован на отдельном разделе диска, то для некоторого повышения производительности сервера баз данных можно перемонтировать этот раздел с атрибутом `noatime`.

Для этого необходимо выполнить следующие операции:

Шаг 1

В файле `/etc/fstab` замените строку, подобную этой:

```
/dev/hdb6     /var/lib    ext3    defaults          0   1
```

на:

```
/dev/hdb6     /var/lib    ext3    defaults,noatime 0   1
```

Шаг 2

Перемонтируйте раздел диска, на котором находится каталог `/var/lib` с атрибутом `noatime`:

```
[root@drwalbr /]# mount /var/lib -oremount
```

Шаг 3

Проверьте атрибуты монтирования дискового раздела с каталогом:

```
[root@drwalbr/]# cat /proc/mounts | grep lib
/dev/hdb6     /var/lib    ext3    defaults,noatime 0   1
```

Пример использования MySQL

Часто при создании интерактивных Web-ресурсов (форумов, поисковых систем и т. п.) начинающие пользователи сталкиваются с проблемой создания единственной базы данных, доступ к которой следует разрешить только определенному пользователю. При этом требуется также вносить некоторые изменения в данные таблиц. Ниже приведен пример создания и модификации данных в такой базе данных.

Шаг 1

Для создания базы данных от имени обычного пользователя установите соединение с сервером баз данных с полномочиями пользователя `root`:

```
[drwalbr@drwalbr /]$ mysql -u root -h drwalbr -p
Enter password: $ecretnoe_sL0vo
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 26 to server version: 4.0.13

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.


Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

Создайте базу данных, например, с именем `friends_book`:

```
mysql> CREATE DATABASE friends_book;
Query OK, 1 row affected (0.00 sec)
```

Проверьте наличие вновь созданной базы данных:

```
mysql> SHOW DATABASES;
+--------------+
| Database     |
+--------------+
| friends_book |
| mysql        |
+--------------+
2 rows in set (0.00 sec)
```

Шаг 2

Для создания пользователя, например, `drwalbr`, обладающего всеми привилегиями по отношению к базе `friends_book`, добавьте соответствующие записи в таблицы привилегий `user` и `db` базы данных `mysql`:

```
mysql> USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

mysql> INSERT INTO user SET
    -> Host='localhost', User='drwalbr', Pass-
word=PASSWORD('Walbr_$_W0rd');
Query OK, 1 row affected (0.01 sec)

mysql> INSERT INTO db
    -> VALUES ('localhost','friends_book', 'drwalbr',
    -> 'Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y');
Query OK, 1 row affected (0.00 sec)
```

Для вступления изменений в силу наберите:

```
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Завершите соединение с сервером баз данных:

```
mysql> \quit
Bye
```

Шаг 3

Для создания таблицы `friends`, содержащей имена и соответствующие им адреса электронной почты, установите соединение с сервером баз данных от имени пользователя `drwalbr` и подключитесь к базе данных `friends_book`:

```
[drwalbr@drwalbr /]$ mysql -u drwalbr -h localhost –p friends_book
Enter password: Dr_Walbr_$_W0rd
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1 to server version: 4.0.13

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

Создайте таблицу:

```
mysql> CREATE TABLE friends
    -> (Name VARCHAR(20),
    -> Email VARCHAR(20));
Query OK, 0 rows affected (0.00 sec)
```

Шаг 4

Если необходимо можете добавить соответствующие записи в таблицу. Для построчного добавления записей выполните:

```
mysql> INSERT INTO friends
    -> VALUES ('Андрусенко Ю.В.', 'andrysenco@domen.ru');
Query OK, 1 row affected (0.00 sec)
```

Для добавления нескольких записей одновременно выполните:

```
mysql> INSERT INTO friends VALUES
    -> ('Карлов С.В.', 'karlnext@domen.ru'),
    -> ('Поляков А.В.', 'polyakov@domen.ru'),
    -> ('Урбанов В.К.', 'urbanoffff@domen.ru');
Query OK, 3 rows affected (0.01 sec)
Records: 3  Duplicates: 0  Warnings: 0
```

Шаг 5

Проверьте правильность внесенных в таблицу `friends` данных:

```
mysql> SELECT * FROM friends;
+-----------------+--------------------+
```

```
| Name             | Email                |
+------------------+----------------------+
| Андрусенко Ю.В. | andrysenco@domen.ru |
| Карлов С.В.      | karlnext@domen.ru    |
| Поляков А.В.     | polyakoff@domen.ru   |
| Урбанов В.К.     | urbanoffff@domen.ru |
+------------------+----------------------+
4 rows in set (0.00 sec)
```

Завершите соединение с сервером баз данных:

```
mysql> \quit
Bye
```

Часть 9

Программное обеспечение для организации службы FTP-сервера

Глава 32

ProFTPD – FTP-сервер

В этой главе:

Протокол передачи файлов (File Transfer Protocol, FTP) остается одним из самых популярных способов передачи файлов по сети с одной системы на другую. В настоящее время для каждой операционной системы существуют клиентские и серверные программы.

ProFTPD – относительно безопасный и легко адаптируемый для решения практически любых задач FTP-сервер для Linux-систем. ProFTPD использует ту же схему построения, что и популярный Web-сервер Apache, имеет аналогичный формат конфигурационных файлов, модульную схему построения и т. д.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, вполне могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта ProFTPD по состоянию на 07.07.2003. Регулярно посещайте домашнюю страницу проекта `http://www.proftp.org/` и отслеживайте обновления.

Исходные коды ProFTPD содержатся в архиве `proftpd-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `proftpd-1.2.8.tar.gz`). Для использования ProFTPD с поддержкой протокола TSL/SSL обязательным условием является наличие установленной программы OpenSSL.

Компиляция, оптимизация и инсталляция ProFTPD

Для инсталляции ProFTPD из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами. Для этого можно воспользоваться процедурой, описанной в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами ProFTPD в каталоге `/var/tmp`:

```
[root@test tmp]# tar xzpf proftpd-1.2.8.tar.gz
```

Шаг 3

Создайте специального пользователя `ftp`, от имени которого будет выполняться ProFTPD:

```
[root@test tmp]# groupadd -g 24 ftp > /dev/null 2>&1 || :
[root@test tmp]# useradd -u 24 -g 24 -s /bin/false -M -r -d /home/ftp ftp
> /dev/null 2>&1 || :
```

Шаг 4

Для добавления несуществующего командного интерпретатора, «используемого» пользователем `ftp`, добавьте (проверьте наличие) в файл `/etc/shells` строку:

```
/bin/false/
```

Шаг 5

Попробуйте увеличить заданное по умолчанию максимально допустимое число открытых дескрипторов файлов, используемых для передачи FTP-данных и выполнения некоторых других задач. К сожалению, эта операция допустима не для всех дистрибутивов. Выполните команду:

```
[root@test tmp]# cd proftpd-1.2.8/

[root@test proftpd-1.2.8]# ulimit -n 8192
```

Если не выводится сообщения вида:

```
bash: ulimit: cannot modify open files limit: Operation not permitted
```

то вам удалось увеличить максимально допустимое число открытых дескрипторов файлов.

Если предыдущая операция прошла удачно, в файле `/tmp/proftpd-1.2.8./include/options.h` замените строку:

```
#define TUNABLE_BUFFER_SIZE    1024
```

на:

```
#define TUNABLE BUFFER SIZE    8192
```

Шаг 6

Откonфигурируйте исходные коды ProFTPD:

```
[root@test proftpd-1.2.8]# CFLAGS="-O2 -march=i686 -funroll-loops"; ex-
port CFLAGS
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--localstatedir=/var/run \
--mandir=/usr/share/man \
--enable-pam \
--with-openssl-dir=/usr/share/ssl \
--with-modules=mod_readme:mod_tls\
```

В рассматриваемом примере исходные коды ProFTPD сконфигурированы с поддержкой стандартных модулей аутентификации PAM и поддержкой подключения модулей `mod_readme` и `mod_tls`. Использование опции `--with-openssl-dir=/usr/share/ssl` и подключение модуля `mod_tls` необходимо только в случае, если вы собираетесь использовать ProFTPD с поддержкой протокола TSL/SSL.

Шаг 7

Откомпилируйте, проинсталлируйте ProFTPD, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test proftpd-1.2.8]# make
[root@test proftpd-1.2.8]# find /* > /root/proftpd1
[root@test proftpd-1.2.8]# make install
[root@test proftpd-1.2.8]# strip /usr/sbin/proftpd
[root@test proftpd-1.2.8]# strip /usr/sbin/ftpshut
[root@test proftpd-1.2.8]# strip /usr/bin/ftpcount
[root@test proftpd-1.2.8]# strip /usr/bin/ftpwho
[root@test proftpd-1.2.8]# find /* > /root/proftpd2
[root@test proftpd-1.2.8]# diff /root/proftpd1 /root/proftpd2 >
/root/proftpd.installed
[root@test proftpd-1.2.8]# mv /root/proftpd.installed
/very_reliable_place/proftpd.installed.YYYYMMDD
```

Шаг 8

Удалите архив и каталог с исходными кодами:

```
[root@test proftpd-1.2.8]# cd /var/tmp/
[root@test tmp]# rm -rf proftpd-1.2.8/
[root@test tmp]# rm -f proftpd-1.2.8.tar.gz
```

Конфигурирование ProFTPD

Конфигурирование ProFTPD осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/proftpd.conf`;
- системного конфигурационного файла `/etc/sysconfig/proftpd`;
- файла поддержки аутентификации пользователей с использованием модулей PAM `/etc/pam.d/ftp`;
- файла `/etc/ftpusers`, содержащего список пользователей, которым запрещен доступ к FTP-серверу;
- файла инициализации `/etc/rc.d/init.d/proftpd`;
- файлов `.ftpaccess`.

Конфигурирование ProFTPD с аутентификацией пользователей

Конфигурационный файл /etc/proftpd.conf

Для конфигурации ProFTPD используется метод директив и контекстов. В настоящее время ProFTPD имеет семь различных контекстов конфигурации: `<General>`, `<Global>`, `<Limit>`, `<Anonymous>`, `<Directory>`, `<VirtualHost>`. В главном конфигурационном файле могут содержаться следующие разделы:

- раздел общей конфигурации FTP-сервера – `General server context`;
- раздел глобальной конфигурации FTP- сервера – `Global Server context`;
- раздел конфигурации ограничений FTP-сервера – `Limit Server context`;
- раздел анонимной конфигурации FTP-сервера – `Anonymous Server Context`.

Шаг 1

Создайте файл `/etc/proftpd.conf`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
# General Server Context.
ServerName                   "Test FTPD BRUY.INFO"
ServerAdmin                  ftpadmin@bruy.info
ServerType                   standalone
DefaultServer                on
Port                         21
tcpBackLog                   10
MaxInstances                 30
CommandBufferSize            50
UseReverseDNS                off
IdentLookups                 off
User                         ftp
Group                        ftp
AccessDenyMsg                "Access for %u has been denied"
AuthPAMAuthoritative         on
DeferWelcome                 on
MultilineRFC2228             on
AllowFilter                  "^[a-zA-Z0-9 ,.,-]*$"
DefaultRoot                  ~ users


# Global Server Context.
<Global>
  DeleteAbortedStores        on
  MaxClients                 3
  MaxLoginAttempts           3
 TransferRate               APPE,RETR,STOR,STOU 56.4:256000
  ServerIdent                on "Ok, Test FTPD BRUY.INFO!"
  Umask                      022
</Global>


# Limit normal user logins, because we only want to allow Guest logins.
<Limit LOGIN>
  DenyAll
</Limit>


# Anonymous Server Context.
#
<Anonymous /home/karl_next>
  User                      karlnext
  Group                     users
AnonRequirePassword         on
```

```
    <Limit LOGIN>
      AllowAll
    </Limit>

    HideUser                  root
    HideGroup                 root

    <Directory /*>
      AllowOverwrite on
    </Directory>
  </Anonymous>
```

Раздел `General Server Contex`.

В разделе General Server Context содержатся наиболее общие (не переопределяемые в других разделах) директивы.

Директива:

```
ServerName                    "Test FTPD BRUY.INFO"
```

используется для определения строкового сообщения, отображаемого пользователям FTP-сервера при подключении.

Директива:

```
ServerAdmin                   ftpadmin@bruy.info
```

используется для определения адреса электронной почты администратора сервера.

Директива:

```
ServerType                    standalone
```

используется для определения режима работы сервера. В рассматриваемом примере сервер работает в режиме автономного сервера без задействования суперсервера xinetd. Это, по мнению авторов, более безопасный режим, обеспечивающий наилучшую производительность.

Директива:

```
DefaultServer                 on
```

используется для выбора конфигурации сервера, выполняемой по умолчанию, т. е. когда входящее FTP соединение предназначено для IP-адреса, не являющегося IP-адресом обычного или виртуального FTP-сервера.

Директива:

```
Port                          21
```

используется для определения номера порта, на котором FTP-сервер ожидает подключений.

Директива:

```
tcpBackLog                    10
```

используется для управления размером неудовлетворенной очереди (backlog queue) TCP соединений при работе ProFTPD в автономном режиме. Другими словами, когда TCP соединение установлено, существует некоторый промежуток времени между моментом фактической установки соединения и началом обработки соединения непосредственно пользовательской программой. Продолжительность этого периода может изменяться в зависимости от различных факторов (конфигурации системы, на которой установлен FTP-сервер, загрузки системы, числа виртуальных хостов и т. п.). В некоторых случаях это может привести к получению пользователями сообщений об отказе подключения (Connection refused). Для устранения этого эффекта осуществляется перераспределение ресурсов, выделяемых для различных модулей FTP-сервера. Чем больше значение параметра, определяемое директивой `tcpBackLog`, тем больше подключений может быть установлено в единицу времени.

Директива:

```
MaxInstances                  30
```

используется для управления максимальным числом одновременно открытых соединений. Это позволяет предотвращать атаки, типа отказа в обслуживании.

Директива:

```
CommandBufferSize             50
```

используется для управления максимальной длиной команды, которая может быть передана для исполнения FTP-серверу. Ограничение длины команды позволяет предотвращать различные атаки, основанные на отказе в обслуживании.

Директива:

```
UseReverseDNS                 off
```

используется для запрета определения имен систем, с которых осуществляется подключение к FTP-серверу с использованием службы DNS, что, в конечном счете, позволяет несколько повысить производительность сервера.

Директива:

```
IdentLookups                  off
```

используется для отключения протокола IDENT, описанного в RFC-1413, обычно применяемого для идентификации имени удаленного пользователя и неиспользуемого FTP-сервером. Отключение протокола IDENT также позволяет добиться некоторого прироста производительности сервера.

Директивы:

```
User                    ftp
```

и

```
Group                   ftp
```

используются для определения пользователя и группы пользователя, от имени которого будет функционировать FTP-сервер.

Директива:

```
AccessDenyMsg           "Access for %u has been denied"
```

используется для определения строкового сообщения, получаемого пользователем при неудачной попытке регистрации на FTP-сервере.

Директива:

```
AuthPAMAuthoritative    on
```

используется для определения способа аутентификации пользователей. В рассматриваемом примере используется аутентификация с помощью стандартных модулей PAM.

Директива:

```
DeferWelcome            on
```

используется для запрета выдачи какой-либо информации пользователям, не прошедшим аутентификацию.

Директива:

```
MultilineRFC2228        on
```

используется для того, чтобы файлы `.message`, расположенные в каталогах FTP и содержащие, например, описание содержимого каталога, были доступными для работы со всеми браузерами.

Директива:

```
AllowFilter             "^[a-zA-Z0-9 ,.,-]*$"
```

используется для определения наборов символов, которые могут быть переданы FTP-серверу в качестве команд. Обычно применяется для защиты FTP-сервера от атак, связанных с использованием некорректных команд.

Директива:

```
DefaultRoot             ~ users
```

используется для определения корневого каталога пользователей и групп пользователей. В рассматриваемом примере для каждого пользователя определяется в качестве корневого его домашний каталог.

Раздел `Global Server Context`.

В универсальном разделе `Global Server Context` определяются наиболее общие параметры конфигурации ProFTPD. Признаком начала и окончания раздела служат директивы `<Global>` и `</Global>`, соответственно.

Директива:

```
DeleteAbortedStores     on
```

используется для запрета сохранения на FTP-сервере частично загруженных и поврежденных при загрузке файлов.

Директива:

```
MaxClients              3
```

используется для ограничения максимального числа клиентов, одновременно обслуживаемых FTP-сервером.

Директива:

```
MaxLoginAttempts        3
```

используется для ограничения максимального числа попыток неудачной регистрации пользователя на FTP-сервере в целях затруднения подбора пароля.

Директива:

```
TransferRate            APPE,RETR,STOR,STOU 56.4:256000
```

используется для ограничения скорости соединения при выполнении различных команд FTP-сервера. В директиве указывается:

- перечень команд (допустимые значения: `APPE` – добавить файл, `RETR` – принять файл, `STOR` – сохранить файл, `STOU` – сохранить файл с уникальным именем), для которых ограничивается скорость соединения;
- максимально допустимая скорость соединения в кБит/с, в рассматриваемом примере 56,4 кБит/с;
- объем трафика в байтах – в рассматриваемом примере 256 кБайт – по превышении которого начинает действовать ограничение на пропускную способность соединения.

Директива:

```
ServerIdent             on "Ok, Test FTPD BRUY.INFO!"
```

используется для определения строкового сообщения, получаемого пользователем при соединении с FTP-сервером.

Директива:

```
Umask                   022
```

используется для задаваемых по умолчанию прав доступа к вновь создаваемым файлам и каталогам.

Раздел `Limit Server Context`.

В разделе `Limit Server Context` определяются различные ограничения. С использованием директив:

```
<Limit LOGIN>
  DenyAll
</Limit>
```

запрещается любой доступ всем пользователям к FTP-серверу, ниже он будет разрешен только специально определенным пользователям.

Раздел `Anonymous Server context`.

В разделе `Anonymous Server context` можно разрешить доступ пользователям к определенным каталогам сервера. Некоторых читателей может дезориентировать название раздела, из которого можно сделать ошибочный вывод, что в нем настраивается анонимный доступ к FTP-серверу. Оставим название раздела на совести разработчиков и перейдем к настройке доступа с аутентификацией пользователей путем использования стандартных модулей PAM.

Директивы:

```
<Anonymous /home/karl_next>
```

и

```
</Anonymous>
```

определяют блок в конфигурационном файле, содержащий все настройки, касающиеся пользователя `karl_next`.

Директивы:

```
  User                  karlnext
  Group                 users
AnonRequirePassword     on
  <Limit LOGIN>
    AllowAll
  </Limit>
```

разрешают доступ к каталогу `/home/karl_next` пользователю `karlnext` из группы `users` после удачной аутентификации с использованием пароля.

Директивы:

```
  HideUser               root
  HideGroup              root
```

используются для скрытия от пользователя каталогов и файлов, владельцами которых являются соответствующий пользователь и группа пользователей, в рассматриваемом примере – `root.`

Директивы

```
  <Directory /*>
    AllowOverwrite on
  </Directory>
</Anonymous>
```

разрешают пользователю `karlnext` осуществлять перезапись файлов в своем домашнем каталоге.

Шаг 2

Установите права доступа к файлу `/etc/proftpd.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/proftpd.conf
[root@test /]# chown 0.0 /etc/proftpd.conf
```

Конфигурационный файл /etc/sysconfig/proftpd

Шаг 1

Создайте файл `/etc/sysconfig/proftpd` и добавьте строки:

```
# Uncomment the following line if you want to debug ProFTPD. All
# log or debug messages will be send to the syslog mechanism.
#
#OPTIONS="-d 5"
```

В этом файле ProFTPD передается единственная опция, включающая отладочный режим, в рассматриваемом примере она закоментирована.

Шаг 2

Установите права доступа к файлу `/etc/sysconfig/proftpd` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 644 /etc/sysconfig/proftpd
[root@test /]# chown 0.0 /etc/sysconfig/proftpd
```

Конфигурационный файл /etc/pam.d/ftp

Этот файл используется для поддержки аутентификации пользователей с использованием стандартных модулей PAM.

Шаг 1

Создайте файл `/etc/pam.d/ftp`, содержащий следующие строки:

```
#%PAM-1.0
auth       required     /lib/security/pam_listfile.so item=user
sense=deny file=/etc/ftpusers onerr=succeed
auth       required     /lib/security/pam_pwdb.so shadow nullok
auth       required     /lib/security/pam_shells.so
account    required     /lib/security/pam_pwdb.so
session    required     /lib/security/pam_pwdb.so
```

Шаг 2

Установите права доступа к файлу `/etc/pam.d/ftp` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/pam.d/ftp
[root@test /]# chown 0.0 /etc/pam.d/ftp
```

Конфигурационный файл /etc/ftpusers

Этот файл используется для определения списка пользователей, для которых доступ к FTP-серверу закрыт. Сюда необходимо внести всех привилегированных пользователей вашей системы.

Шаг 1

Внесите в файл `/etc/ftpusers` всех привилегированных пользователей вашей системы:

- `root`;
- `bin`;
- `daemon`;
- `sync`;
- `mail`;
- `nobody`;
- `named`;
- `rpm`;
- `www`;
- `amavis`;
- `mysql`.

Шаг 2

Установите права доступа к файлу `/etc/ftpusers` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 600 /etc/ftpusers
[root@test /]# chown 0.0 /etc/ftpusers
```

Файл инициализации /etc/init.d/proftpd

Шаг 1

Для запуска и остановки ProFTPD создайте файл `/etc/init.d/proftpd`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping ProFTPD (FTP
server).
#
# chkconfig: 345 85 15
# description: ProFTPD is an enhanced FTP server with a focus toward \
#              simplicity, security, and ease of configuration.
#
# processname: /usr/sbin/proftpd
# config: /etc/sysconfig/network
# config: /etc/proftpd.conf

# Source function library.
. /etc/rc.d/init.d/functions

# Get config.
test -f /etc/sysconfig/network && . /etc/sysconfig/network

if [ -f /etc/sysconfig/proftpd ]; then
      . /etc/sysconfig/proftpd
fi

# Check that networking is up.
[ ${NETWORKING} = "yes" ] || exit 0
[ -f /usr/sbin/proftpd ] || exit 1
[ -f /etc/proftpd.conf ] || exit 1

RETVAL=0

start() {
        echo -n "Starting ProFTPD: "
        daemon proftpd $OPTIONS
        RETVAL=$?
        echo
        touch /var/lock/subsys/proftpd
        return $RETVAL
}

stop() {
        echo -n "Shutting down ProFTPD: "
        killproc proftpd
        RETVAL=$?
        echo
        rm -f /var/lock/subsys/proftpd
        return $RETVAL
}

restart() {
        stop
        start
}

condrestart() {
        [ -e /var/lock/subsys/proftpd ] && restart
        return 0
}
```

```
# See how we were called.
case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    status)
        status /usr/sbin/proftpd
        ;;
    restart)
        restart
        ;;
    condrestart)
        condrestart
        ;;
    *)
        echo "Usage: proftpd {start|stop|status|restart|condrestart}"
        RETVAL=1
esac
exit $RETVAL
```

Шаг 2

Установите права доступа к файлу, назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 700 /etc/init.d/proftpd
[root@test /]# chown 0.0 /etc/init.d/proftpd
```

Шаг 3

Если вы хотите, чтобы демон `proftpd` запускался автоматически при загрузке системы, создайте соответствующие ссылки:

```
[root@test /]# chkconfig --add proftpd
[root@test /]# chkconfig --level 345 proftpd on
```

Создание учетной записи FTP-клиента для соединения с FTP-сервером

Для того, чтобы пользователь смог получить доступ к своему каталогу на FTP-сервере, необходимо наличие соответствующей учетной записи. Для ее создания предлагается выполнить некоторые операции.

Шаг 1

Создайте нового пользователя, например, `karlnext`, не имеющего доступа к командному интерпретатору. Его домашний каталог был определен ранее директивой `<Anonymous ...>` в разделе `Anonymous Server Context` конфигурационного файла `/etc/proftpd.conf`. Выполните команды:

```
[root@test /]# useradd -g users -s /bin/false karlnext
[root@test /]# passwd karlnext
Changing password for user
karlnext New UNIX password:ka4l$ectetn0esl0v0
Retype new UNIX password: ka4l$ectetn0esl0v0
passwd: all authentication tokens updated successfully
```

Шаг 2

Создайте домашний FTP-каталог для нового пользователя:

```
[root@test /]# mkdir /home/karl_next
```

и определите его владельцем пользователя `karlnext` и группу владельца `users`:

```
[root@test /]# chown -R karlnex.users /home/karl_next
```

Тестирование ProFTPD

Шаг 1

Запустите FTP-сервер:

```
[root@test /]# /etc/init.d/proftpd start
```

```
Starting ProFTPD:                          [OK]
```

Шаг 2

Попытайтесь установить соединение с FTP-сервером с помощью FTP-клиента. В комплект поставки ASPLinux 7.3 входит консольный FTP-клиент, находящийся в пакете `ftp-0.17-13.i386.rpm`.

Перейдите в каталог, где находятся требуемые пакеты. Если вы в соответствии с рекомендациями главы 2 скопировали все исходные rpm-пакеты в каталог `/home/distrib`:

```
[root@test /]# cd /home/distrib
[root@drwalbr distrib]# rpm -ihv ftp-0.17-13.i386.rpm
```

Запустите FTP-клиент от имени обычного пользователя, например, `drwalbr`:

```
[drwalbr@test dr_walbr]$ ftp
```

Установите соединение с вашим FTP-сервером:

```
ftp> open test.bruy.info
Connected to test.bruy.info (212.111.80.58).
220 Ok, Test FTPD BRUY.INFO!
```

Шаг 3

Зарегистрируйтесь на FTP-сервере в качестве пользователя `karlnext`:

```
Name (test.bruy.info:drwalbr): karlnext
331 Password required for karlnext.
Password: ka4l$ectetn0esl0v0
230 Anonymous access granted, restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Протестируйте работоспособность всех директив, используемых в файле `/etc/proftpd.conf`. Например, для проверки работоспособности ограничений на пропускную способность соединения сравните время загрузки на сервер предварительно созданных файлов с размером менее и более 256 кБайт:

```
ftp> put lt256
local: lt256 remote: lt256
227 Entering Passive Mode (212,111,80,58,136,28).
150 Opening BINARY mode data connection for lt256
226 Transfer complete.
95434 bytes sent in 0.00149 secs (6.3e+04 Kbytes/sec)
ftp> put gt256
local: gt256 remote: gt256
227 Entering Passive Mode (212,111,80,58,223,196).
150 Opening BINARY mode data connection for gt256
226 Transfer complete.
449817 bytes sent in 17.7 secs (25 Kbytes/sec)
```

Шаг 4

По окончании тестирования завершите сеанс работы с FTP-сервером:

```
ftp> quit
221 Goodbye.
```

Шаг 5

Используя утилиту `ftpwho`, можно получить информацию о состоянии сервера и количестве подключенных к нему клиентов:

```
[drwalbr@test /]$ ftpwho
standalone FTP daemon [29900]:
28402 ftp      [ 1m33s]  0m37s (idle)
Service class                      -   1 user
```

Конфигурирование ProFTPD с поддержкой протокола SSL

Для запуска ProFTPD с поддержкой протокола SSL необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Для включения поддержки протокола SSL исходные коды ProFTPD необходимо сконфигурировать с опцией `--with-openssl-dir=/usr/share/ssl` и подключением модуля `mod_tls`. В версии ProFTPD 1.2.8 использование этого модуля вы можете осуществлять на свой страх и риск. Тем не менее, разработчики ProFTPD планируют включение этого модуля в следующей версии FTP-сервера.

Шаг 1

Для создания самостоятельно подписанного сертификата необходимо наличие собственного сертификационного центра. Если вы его уже создали, то перейдите к следующему шагу. В противном случае ознакомьтесь с рекомендациями раздела «Тестирование OpenSSL» главы 12 и создайте собственный сертификационный центр.

Шаг 2

Создайте закрытый ключ, не защищенный паролем, для чего перейдите в каталог `/usr/share/ssl`:

```
[root@test /]# cd /usr/share/ssl
```

Выберите пять любых больших файлов со случайным (уникальным) содержанием, скопируйте их в каталог `/usr/share/ssl` и переименуйте в `random1`, `random2`, `random3`, `random4`, `random5`, после чего выполните команду:

```
[root@test ssl]# openssl genrsa -rand ran-
dom1:random2:random3:random4:random5 -out ftpd-rsa.key.pem 1024
2019245 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
..................++++++
.....................................................++++++
e is 65537 (0x10001)
```

Шаг 3

Создайте запрос на подтверждение сертификата:

```
[root@test ssl]# openssl req -new -key ftpd-rsa.key.pem -out ftpd-
rsa.csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]: <Enter>
State or Province Name (full name) [Moscow]: <Enter>
Locality Name (eg, city) [Yubileyniy]: <Enter>
Organization Name (eg, company) [Valentine Bruy]: <Enter>
Organizational Unit Name (eg, section) [Home]: <Enter>
Common Name (eg, YOUR name) [test.bruy.info]: <Enter>
Email Address [drwalbr@bruy.info]:ftp@test.bruy.info <Enter>

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: <Enter>
```

Шаг 4

Подпишите сертификат:

```
[root@test ssl]# /usr/share/ssl/misc/sign ftpd-rsa.csr.pem
CA signing: ftpd-rsa.csr.pem -> ftpd-rsa.csr.pem.crt:
Using configuration from ca.config
Enter pass phrase for /usr/share/ssl/private/ca.key:$()VSecretn0eSlovo
Check that the request matches the signature
Signature ok
```

```
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :PRINTABLE:'Moscow'
localityName          :PRINTABLE:'Yubileyniy'
organizationName      :PRINTABLE:'Valentine Bruy'
organizationalUnitName:PRINTABLE:'Home'
commonName            :PRINTABLE:'test.bruy.info'
emailAddress          :IA5STRING:'ftp@test.bruy.info'
Certificate is to be certified until Jul  6 13:15:43 2004 GMT (365 days)
Sign the certificate? [y/n]: y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
CA verifying: ftpd-rsa.csr.pem.crt <-> CA cert
ftpd-rsa.csr.pem.crt: OK
```

Шаг 5

Переместите файл, содержащий закрытый ключ и сертификат, в каталог `/usr/share/ssl/private`. Переименуйте файл `ftpd-rsa.csr.pem.crt` в `ftpd-rsa.pem` и переместите его в каталог `/usr/share/ssl/certs`. Определите права доступа к файлам и удалите ненужный более файл `ftpd-rsa-csr.pem`:

```
[root@test ssl]# mv ftpd-rsa.key.pem private
[root@test ssl]# mv ftpd-rsa.csr.pem.crt certs/ftpd-rsa.pem
[root@test ssl]# chmod 400 private/ftpd-rsa.key.pem
[root@test ssl]# chmod 400 certs/ftpd-rsa.pem
[root@test ssl]#rm -f ftpd-rsa-csr.pem
```

Шаг 6

Внесите в файл `/etc/proftpd.conf` изменения, руководствуясь ниже приведенными рекомендациями:

```
General Server Context.
ServerName                  "Test FTPD BRUY.INFO"
ServerType                  standalone
DefaultServer               on
Port                        990
tcpBackLog                  10
MaxInstances                30
CommandBufferSize           50
UseReverseDNS               off
IdentLookups                off
User                        ftp
Group                       ftp

AccessDenyMsg               "Access for %u has been denied"
AuthPAMAuthoritative        on
DeferWelcome                on
MultilineRFC2228            on
AllowFilter                 "^[a-zA-Z0-9 ,.,-]*$"
DefaultRoot                 ~ users
TLSRSACertificateFile       /usr/share/ssl/certs/ftpd-rsa.pem
TLSRSACertificateKeyFile    /usr/share/ssl/private/ftpd-rsa.key.pem
TlsRequired                 on

# Global Server Context.
<Global>
  DeleteAbortedStores           on
  MaxClients                  3
MaxLoginAttempts            3
#RateReadBPS                  56400
TransferRate              APPE,RETR,STOR,STOU 56.4:256000
```

```
ServerIdent                  on "Ok, Test FTPD BRUY.INFO!"
  Umask                     022
</Global>


# Limit normal user logins, because we only want to allow Guest logins.
<Limit LOGIN>
  DenyAll
</Limit>


# Anonymous Server Context.
<Anonymous /home/karl_next>
  User                      karlnext
  Group                     users
AnonRequirePassword            on
  <Limit LOGIN>
    Order Allow,Deny
      Allow from 212.45.28.123,192.168.1
      Deny from all
  </Limit>

  HideUser                   root
  HideGroup                  root

  <Directory /*>
    AllowOverwrite on
  </Directory>
</Anonymous>
```

В данном файле директива:

```
Port                         990
```

определяет порт, на котором ProFTPD ожидает подключений с поддержкой протокола SSL.

Директивы:

```
TLSRSACertificateFile        ftpd-rsa.pem
```

и

```
TLSRSACertificateKeyFile     ftpd-rsa.key.pem
```

определяют местоположение файлов, содержащих закрытый ключ и сертификат.

Директива:

```
TlsRequired                  on
```

определяет, какие виды соединений должны осуществляться с поддержкой протокола SSL. В рассматриваемом примере – все.

В разделе `Anonymous Server Context` были внесены изменения, не имеющие никакого отношения к поддержке протокола SSL, но существенно повышающие защищенность FTP-сервера:

```
<Limit LOGIN>
    Order Allow,Deny
      Allow from 212.45.28.123,192.168.1
      Deny from all
  </Limit>
```

В рассматриваемом примере доступ к FTP-серверу разрешен только из локальной сети 192.168.1.0/24 и удаленного офиса с IP-адресом шлюза 212.45.28.123. Такой вариант ограничения доступа может использоваться в любом варианте конфигурации ProFTPD (с аутентификацией пользователей, анонимным доступом, поддержкой SSL).

Шаг 7

Установите права доступа к файлу `/etc/proftpd.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/proftpd.conf
[root@test /]# chown 0.0 /etc/proftpd.conf
```

Шаг 8

Создайте остальные конфигурационные файлы в соответствии с рекомендациями раздела «Конфигурирование ProFTPD с аутентификацией пользователей».

Шаг 9

Протестируйте доступ к FTP-серверу с поддержкой протокола SSL в соответствии с рекомендациями раздела «Тестирование ProFTPD». Перечень клиентов и их краткое описание может быть получено со страницы `http://www.ford-hutchinson.com/~fh-1-pfh/ftps-ext.html`.

Конфигурирование ProFTPD в режиме анонимного FTP-сервера

Для конфигурирования ProFTPD в режиме анонимного FTP-сервера необходимо выполнить следующие операции.

Шаг 1

Создайте каталог, в который будет разрешен анонимный доступ, и назначьте его владельцем пользователя `ftp`:

```
[root@test /]# mkdir /home/ftp
[root@test /]# chown ftp.ftp /home/ftp/
```

Шаг 2

Отредактируйте файл `/etc/proftpd.conf`, внесите изменения, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
# General Server Context.
ServerName                  "Anonymous FTP"
ServerType                   standalone
DefaultServer                on
Port                         21
tcpBackLog                   10
MaxInstances                 30
CommandBufferSize            50
UseReverseDNS                off
IdentLookups                 off
User                         ftp
Group                        ftp
AuthPAMAuthoritative         on
MultilineRFC2228             on
AllowFilter                  "^[a-zA-Z0-9 ,.,-]*$"

# Global Server Context.
<Global>
  DeleteAbortedStores        on
  MaxClients                 10000
MaxLoginAttempts             3
TransferRate                 APPE,RETR,STOR,STOU 56.4:256000
  ServerIdent                on "Ok, Test FTPD BRUY.INFO!"
  Umask                      022
</Global>

# We don't want normal users logging in at all.
<Limit LOGIN>
  DenyAll
</Limit>

# Normally, we want files to be overwriteable.
<Directory /*>
  AllowOverwrite             on
</Directory>

# A basic Anonymous configuration, no upload directories.
<Anonymous ~ftp>

# Allow Anonymous logins here since all logging are disabled above.
<Limit LOGIN>
  AllowAll
</Limit>
```

```
AnonRequirePassword          off
RequireValidShell            off
User                         ftp
Group                        ftp

# We want 'welcome.msg' displayed at login, and '.message' displayed
# in each newly chdired directory.
DisplayLogin                  welcome.msg
DisplayFirstChdir             .message

# We want clients to be able to login with "anonymous" as well as "ftp".
UserAlias                     anonymous ftp

# Limit the maximum number of anonymous logins.
MaxClients                    10000

# Limit WRITE everywhere in the anonymous chroot jail.
<Limit WRITE>
  DenyAll
</Limit>
</Anonymous>
```

В данном файле директива:

```
MaxClients                    10000
```

как и в предыдущей конфигурации, определяет максимально возможное число клиентов, подключаемых к FTP-серверу, однако, сейчас их число увеличено до 10000.

Основные директивы конфигурации анонимного FTP-сервера находятся в блоке, ограниченном директивами `<Anonymous ~ftp>` и `</Anonymous>`

Директива:

```
AnonRequirePassword          off
```

в отличие от предыдущей конфигурации, отменяет обязательный ввод пароля, вместо него пользователь сможет ввести все, что угодно.

Директива:

```
RequireValidShell            off
```

используется для разрешения входа в систему пользователей, не имеющих доступа к командному интерпретатору. По умолчанию эта директива устанавливает значение "off" и запрещает вход в систему таким пользователям.

Директивы:

```
User                         ftp
```

и

```
Group                        ftp
```

определяют анонимного пользователя.

Директива:

```
DisplayLogin                  welcome.msg
```

определяет имя файла в корневом каталоге для анонимных пользователей, содержащего текст приветственного сообщения, отображаемого пользователю при входе на FTP-сервер.

Директива:

```
DisplayFirstChdir             .message
```

определяет имя файла в соответствующем каталоге, содержащего текст отображаемого пользователю приветственного сообщения при первом входе в каталог.

Директива:

```
UserAlias                     anonymous ftp
```

для сопоставления реальным пользователям псевдонимов. В рассматриваемом примере анонимный пользователь может зарегистрироваться, используя логин `ftp` или `anonymous`.

Блок директив:

```
<Limit WRITE>
DenyAll
</Limit>
```

запрещает запись всем пользователям.

В приведенном выше примере конфигурации анонимным пользователям не разрешено закладывать файлы на FTP-сервер. Для того, чтобы разрешить им загрузку файлов в некоторый каталог на анонимном FTP-сервере необходимо выполнить следующие операции.

Шаг 3

Создайте каталог, в который будет разрешен анонимный доступ и назначьте его владельцем пользователя `ftp`:

```
[root@test /]# mkdir /home/ftp/uploads
[root@test /]# chown ftp.ftp /home/ftp/uploads
```

Шаг 4

Внесите изменения в файл `/etc/proftpd.conf`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
# General Server Context.
ServerName                  "Anonymous FTP"
ServerType                   standalone
DefaultServer                on
Port                         21
tcpBackLog                   10
MaxInstances                 30
CommandBufferSize            50
UseReverseDNS                off
IdentLookups                 off
User                         ftp
Group                        ftp
AuthPAMAuthoritative         on
MultilineRFC2228             on
AllowFilter                  "^[a-zA-Z0-9 ,.,-]*$"

# Global Server Context.
<Global>
  DeleteAbortedStores        on
  MaxClients                 10000
MaxLoginAttempts             3
TransferRate                 APPE,RETR,STOR,STOU 56.4:256000
  ServerIdent                on "Ok, Test FTPD BRUY.INFO!"
  Umask                      022
</Global>

# We don't want normal users logging in at all.
<Limit LOGIN>
  DenyAll
</Limit>

# Normally, we want files to be overwriteable.
<Directory /*>
  AllowOverwrite             on
</Directory>

# A basic Anonymous configuration, no upload directories.
<Anonymous ~ftp>

# Allow Anonymous logins here since all logging are disabled above.
<Limit LOGIN>
  AllowAll
</Limit>

AnonRequirePassword          off
RequireValidShell            off
User                         ftp
Group                        ftp

# We want 'welcome.msg' displayed at login, and '.message' displayed
# in each newly chdired directory.
DisplayLogin                  welcome.msg
DisplayFirstChdir             .message
```

```
# We want clients to be able to login with "anonymous" as well as "ftp".
UserAlias                    anonymous ftp

# Limit the maximum number of anonymous logins.
MaxClients                   10000

# Limit WRITE everywhere in the anonymous chroot jail.
<Limit WRITE>
  DenyAll
</Limit>
#Upload directory that allows storing files but
#not retrieving or creating directories.
<Directory uploads/*>
  HiddenStor on
  <Limit READ RMD DELE MKD>
    DenyALL
  </Limit>
  <Limit STOR CWD>
    AllowAll
  </Limit>
</Directory>
</Anonymous>
```

В блоке, ограниченном директивами `<Directory uploads/*>` и `</Directory>`, содержатся директивы, используемые для конфигурирования загрузки файлов анонимными пользователями.

Директива:

```
HiddenStor on
```

запрещает сохранение не полностью загруженных и поврежденных файлов.

Блок директив:

```
<Limit READ RMD DELE MKD>
  DenyAll
</Limit>
```

запрещает чтение, перемещение, удаление и создание файлов и подкаталогов в каталоге `/home/ftp/uploads` для всех пользователей.

Блок директив:

```
<Limit STOR CWD>
  AllowAll
</Limit>
```

разрешает всем анонимным пользователям загружать файлы в каталог `/home/ftp/uploads`.

Шаг 5

Установите права доступа к файлу `/etc/proftpd.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/proftpd.conf
[root@test /]# chown 0.0 /etc/proftpd.conf
```

Шаг 6

Создайте остальные конфигурационные файлы в соответствии с рекомендациями раздела «Конфигурирование ProFTPD с аутентификацией пользователей».

Шаг 7

Протестируйте анонимный доступ к FTP-серверу, в соответствии с рекомендациями раздела «Тестирование ProFTPD».

Глава 33

vsftpd – безопасный FTP-сервер

В этой главе:

Если вам необходим высокопроизводительный и безопасный FTP-сервер, не реализующий экзотические варианты настроек, например поддержку протокола SSL, авторы настоятельно рекомендуют использовать программу vsftpd. С нашей точки зрения, vsftpd является идеальным вариантом для реализации сервера анонимного доступа. Он предельно прост в инсталляции и настройке и может быть рекомендован пользователям и системным администраторам, не имеющим опыта организации службы `ftp`.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми и для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта vsftpd по состоянию на 09.07.2003. Регулярно посещайте домашнюю страницу проекта `http://vsftpd.beasts.org` и отслеживайте обновления.

Исходные коды vsftpd содержатся в архиве `vsftpd-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `vsftpd-1.2.0.tar.gz`).

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет программы vsftpd с помощью следующей команды:

```
[root@test /]# rpm –iq vsftpd
```

Шаг 2

Перейдите в каталог, где находится пакет `vsftpd-1.0.1-5.asp.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@test /]# cd /home/distrib
```

и установите:

```
[root@test distrib]# rpm -ihv vsftpd-1.0.1-5.asp.i386.rpm
```

или обновите пакет:

```
[root@test distrib]# rpm –Uhv vsftpd-1.0.1-5.asp.i386.rpm
```

После установки пакета перейдите к настройке программы.

Компиляция, оптимизация и инсталляция vsftpd

Для инсталляции vsftpd из архива с исходными кодами необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами vsftpd в каталоге `/var/tmp`:

```
[root@test tmp]# tar xzpf vsftpd-1.2.0.tar.gz
```

Шаг 3

Создайте специального пользователя `ftp`, от имени которого будет выполняться vsftpd:

```
[root@test tmp]# groupadd -g 24 ftp > /dev/null 2>&1 || :
[root@test tmp]# useradd -u 24 -g 24 -s /bin/false -M -r -d /home/ftp ftp
> /dev/null 2>&1 || :
```

Шаг 4

Для добавления несуществующего командного интерпретатора, «используемого» пользователем `ftp` добавьте (проверьте наличие) в файл `/etc/shells` строку:

```
/bin/false/
```

Шаг 5

Для того, чтобы изменить каталоги, используемые по умолчанию в файле `/var/tmp/vsftpd-1.2.0/Makefile`, замените строки:

```
install:
    if [ -x /usr/local/sbin ]; then \
        $(INSTALL) -m 755 vsftpd /usr/local/sbin/vsftpd; \
    else \
        $(INSTALL) -m 755 vsftpd /usr/sbin/vsftpd; fi
    if [ -x /usr/local/man ]; then \
        $(INSTALL) -D -m 644 vsftpd.8 /usr/local/man/man8/vsftpd.8; \
        $(INSTALL) -D -m 644 vsftpd.conf.5
/usr/local/man/man5/vsftpd.conf.5; \
    elif [ -x /usr/share/man ]; then \
        $(INSTALL) -D -m 644 vsftpd.8 /usr/share/man/man8/vsftpd.8; \
        $(INSTALL) -D -m 644 vsftpd.conf.5
/usr/share/man/man5/vsftpd.conf.5; \
    else \
        $(INSTALL) -D -m 644 vsftpd.8 /usr/man/man8/vsftpd.8; \
        $(INSTALL) -D -m 644 vsftpd.conf.5 /usr/man/man5/vsftpd.conf.5;
fi
    if [ -x /etc/xinetd.d ]; then \
        $(INSTALL) -m 644 xinetd.d/vsftpd /etc/xinetd.d/vsftpd; fi
```

на:

```
install:
    $(INSTALL) -m 0511 vsftpd /usr/sbin/vsftpd
    $(INSTALL) -D -m 644 vsftpd.8 /usr/share/man/man8/vsftpd.8
    $(INSTALL) -D -m 644 vsftpd.conf.5 /usr/share/man/man5/vsftpd.conf.5
```

Шаг 6

Откомпилируйте, проинсталлируйте vsftpd, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test tmp]# cd vsftpd-1.2.0
[root@test vsftpd-1.2.0]# make CFLAGS="-O2 -march=i686 -funroll-loops"
[root@test vsftpd-1.2.0]# find /* > /root/vsftpd1
[root@test vsftpd-1.2.0]# make install
[root@test vsftpd-1.2.0]# find /* > /root/vsftpd2
[root@test vsftpd-1.2.0]# diff /root/vsftpd1 /root/vsftpd2 >
/root/vsftpd.installed
[root@test vsftpd-1.2.0]# mv /root/vsftpd.installed
/very_reliable_place/vsftpd.installed.YYYYMMDD
```

Шаг 7

Удалите архив и каталог с исходными кодами:

```
[root@test vsftpd-1.2.0]# cd /var/tmp/
[root@test tmp]# rm -rf vsftpd-1.2.0/
[root@test tmp]# rm -f vsftpd-1.2.0.tar.gz
```

Конфигурирование vsftpd

Конфигурирование vsftpd осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/vsftpd.conf`;
- файла поддержки аутентификации пользователей с использованием модулей PAM `/etc/pam.d/ftp`;
- файла `/etc/ftpusers`, содержащего список пользователей, которым запрещен доступ к FTP-серверу;
- файла настройки чередования регистрационных файлов `/etc/logrotate.d/vsftpd`;
- файла инициализации `/etc/init.d/vsftpd`.

Конфигурирование vsftpd с аутентификацией пользователей

Конфигурационный файл /etc/vsftpd.conf

Шаг 1

Создайте файл `/etc/vsftpd.conf`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
xferlog_enable=YES
connect_from_port_20=NO
one_process_model=NO
nopriv_user=ftp
ftpd_banner=TEST FTP SERVER TEST.BRUY.INFO
chroot_local_user=YES
```

В нем строка:

```
listen=YES
```

предписывает запускать `vsftpd` в качестве автономного демона.

Строка:

```
anonymous_enable=NO
```

запрещает доступ анонимным пользователям.

Строка:

```
local_enable=YES
```

разрешает доступ пользователям, прошедшим аутентификацию.

Строка:

```
write_enable=YES
```

разрешает осуществлять запись в пользовательские каталоги.

Строка:

```
local_umask=022
```

определяет права доступа к вновь создаваемым пользователями файлам. Значение 022 соответствует правам доступа `-rw-r--r--`.

Строка:

```
xferlog_enable=YES
```

предписывает регистрацию загрузки vsftpd и файлов с FTP-сервера пользователями в файлы каталога `/var/log/messages`.

Строка:

```
connect_from_port_20=NO
```

позволяет выполнять vsftpd с меньшими правами доступа, однако некоторые клиенты могут требовать подключения на 20 порту. Попробуйте запускать свой сервер с отключенной опцией `connect_from_port_20`, если возникнут проблемы, то включите ее.

Строка:

```
one_process_model=NO
```

По умолчанию vsftpd обслуживает соединение двумя процессами. На сильно загруженных FTP-серверах это может привести к падению производительности. Поэтому, если ваш FTP-сервер поддерживает большое число пользователей, лучше разрешить эту опцию, т. е. изменить установленное нами значение "no" на "yes".

Строка:

```
nopriv_user=ftp
```

определяет имя пользователя, от имени которого запускается vsftpd.

Строка:

```
ftpd_banner=TEST FTP SERVER TEST.BRUY.INFO
```

определяет содержание строкового сообщения, отображаемого при подключении FTP-клиента к серверу.

Строка:

```
chroot_local_user=YES
```

предписывает перемещение пользователя сервера в свой домашний каталог сразу же после регистрации на сервере. В этом случае пользователи не смогут заходить в каталоги других пользователей.

Шаг 2

Установите права доступа к файлу `/etc/vsftpd.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 600 /etc/vsftpd.conf
[root@test /]# chown 0.0 /etc/vsftpd.conf
```

Конфигурационный файл /etc/pam.d/ftp

Этот файл используется для поддержки аутентификации пользователей с использованием стандартных модулей PAM.

Шаг 1

Создайте файл `/etc/pam.d/ftp`, содержащий следующие строки:

```
#%PAM-1.0
auth       required     /lib/security/pam_listfile.so item=user
sense=deny file=/etc/ftpusers onerr=succeed
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_shells.so
account    required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Шаг 2

Установите права доступа к файлу `/etc/pam.d/ftp` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/pam.d/ftp
[root@test /]# chown 0.0 /etc/pam.d/ftp
```

Конфигурационный файл /etc/ftpusers

Этот файл используется для определения списка пользователей, для которых доступ к FTP-серверу закрыт. Здесь следует отразить всех привилегированных пользователей вашей системы.

Шаг 1

Внесите в файл `/etc/ftpusers` всех привилегированных пользователей вашей системы:

- `root`;
- `bin`;
- `daemon`;
- `sync`;
- `mail`;
- `nobody`;
- `named`;
- `rpm`;
- `www`;
- `mysql`.

Шаг 2

Установите права доступа к файлу `/etc/ftpusers` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 600 /etc/ftpusers
[root@test /]# chown 0.0 /etc/ftpusers
```

Конфигурационный файл /etc/logrotate.d/vsftpd

Этот файл используется для настройки чередования файлов регистрации. В рассматриваемом примере файлы регистрации будут чередоваться еженедельно.

Шаг 1

Создайте файл `/etc/logrotate.d/vsftpd`, содержащий следующие строки:

```
/var/log/vsftpd.log {
    nocompress
    missingok
```

Шаг 2

Установите права доступа к файлу `/etc/logrotate.d/vsftpd` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 640 /etc/logrotate.d/vsftpd
[root@test /]# chown 0.0 /etc/logrotate.d/vsftpd
```

Файл инициализации /etc/init.d/vsftpd

Шаг 1

Для запуска и остановки демона `vsftpd` создайте файл `/etc/init.d/vsftpd`, содержащий следующие строки:

```
#!/bin/bash

# This shell script takes care of starting and stopping vsftpd.
#
# chkconfig: 345 58 74
# description: vsftpd is the FTP-server.

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/vsftpd ];then
        . /etc/sysconfig/vsftpd
fi
# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If vsftpd is not available stop now.
[ -f /usr/sbin/vsftpd ] || exit 0
[ -f /etc/vsftpd.conf ] || exit 0

# Path to the vsftpd binary.
vsftpd=/usr/sbin/vsftpd

RETVAL=0
prog="vsftpd"
start() {
        echo строка запуска $vsftpd $OPTIONS
        echo -n $"Starting $prog: "
        daemon $vsftpd $OPTIONS &
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/vsftpd
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $vsftpd
        RETVAL=$?
```

```
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/vsftpd
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $vsftpd
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/lock/subsys/vsftpd ]; then
            stop
            start
            RETVAL=$?
        fi
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 2

Установите права доступа к файлу, назначьте его владельцем пользователя `root` и создайте соответствующие ссылки:

```
[root@test /]# chmod 700 /etc/init.d/vsftpd
[root@test /]# chown 0.0 /etc/init.d/vsftpd
```

Шаг 3

Если вы хотите, чтобы `vsftpd` запускался автоматически при загрузке системы, создайте соответствующие ссылки:

```
[root@test /]# chkconfig --add vsftpd
[root@test /]# chkconfig --level 345 vsftpd on
```

Создание учетной записи FTP-клиента для соединения с FTP-сервером

Для того, чтобы пользователь мог установить соединение с FTP-сервером необходимо создать соответствующую учетную запись. Для этого необходимо выполнить следующие операции.

Шаг 1

Создайте учетную запись для пользователя, например `karlnext`, которому будет разрешен доступ к FTP-серверу:

```
[root@test /]# ureradd -g urers -d /home/karl_next -s /bin/false karlnext
```

Шаг 2

Задайте пароль для пользователя `karlnext`:

```
[root@test /]# passwd karlnext
Changing password for user karlnext
New UNIX password:
```

```
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

Конфигурирование vsftpd в режиме анонимного FTP-сервера

Для конфигурирования vsftpd в режиме анонимного FTP-сервера необходимо выполнить следующие операции.

Шаг 1

Создайте каталог для анонимных пользователей:

```
[root@test /]# mkdir /home/ftp/
```

и определите права доступа к нему:

```
[root@test /]# chmod -R 0555 /home/ftp/
```

Назначьте владельцем этого каталога пользователя `ftp`:

```
[root@test /]# chown -R ftp.ftp /home/ftp/
```

Шаг 2

Если вы хотите разрешить анонимным пользователям осуществлять запись файлов в какой-нибудь каталог, то создайте его:

```
[root@test /]# mkdir /home/ftp/uploads
```

и назначьте его владельцем пользователя `ftp`:

```
[root@test /]# chown -R ftp.ftp /home/ftp/uploads/
```

Шаг 3

Отредактируйте файл `/etc/vsftpd.conf`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
listen=YES
anon_root=/home/ftp
#For put files
write_enable=YES
anon_umask=022
anon_upload_enable=YES
chown_uploads=YES
chown_username=ftp
#/For put files
dirmessage_enable=YES
anon_max_rate=33600
max_clients=1000
max_per_ip=2
connect_from_port_20=NO
one_process_model=NO
nopriv_user=ftp
ftpd_banner=TEST FTP SERVER TEST.BRUY.INFO
```

В нем строка:

```
anon_root=/home/ftp
```

определяет местоположение каталога анонимных пользователей.

Строка:

```
dirmessage_enable=YES
```

разрешает использование файла `.messages`, содержимое которого отображается пользователю при первом изменении каталога.

Строка:

```
anon_max_rate=33600
```

ограничивает скорость передачи данных от сервера к клиенту для анонимных пользователей. В рассматриваемом примере установлено ограничение 33600 Бит/с.

Строка:

```
max_clients=1000
```

ограничивает количество клиентов, одновременно подключаемых к серверу.

Строка:

```
max_per_ip=2
```

ограничивает максимальное количество клиентов, подключаемых к серверу с одного IP-адреса.

В строках:

```
write_enable=YES
anon_umask=022
anon_upload_enable=YES
chown_uploads=YES
chown_username=ftp
```

разрешается загрузка файлов для анонимных пользователей. Если вы не собираетесь разрешать анонимным пользователям сохранять на сервере файлы, то удалите эти строки.

Назначение остальных опций описано выше при конфигурировании vsftpd в качестве FTP-сервера с аутентификацией пользователей.

Шаг 4

Установите права доступа к файлу `/etc/vsftpd.conf` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 600 /etc/vsftpd.conf
[root@test /]# chown 0.0 /etc/vsftpd.conf
```

Шаг 5

Создайте остальные конфигурационные файлы в соответствии с рекомендациями раздела «Конфигурирование vsftpd с аутентификацией пользователей».

Тестирование vsftpd

Шаг 1

Запустите FTP-сервер:

```
[root@test /]# /etc/init.d/vsftpd start
Starting vsftpd:                  [OK]
```

Дальнейшие операции осуществлялись в варианте конфигурации анонимного FTP-сервера.

Шаг 2

Попытайтесь установить соединение с FTP-сервером с помощью FTP-клиента, например, входящего в комплект поставки ASPLinux 7.3, находящегося в пакете `ftp-0.17-13.i386.rpm`. Установка данного пакета описана в шаге 2 раздела «Тестирование ProFTPD» главы 32.

Установите соединение с вашим FTP-сервером:

```
[drwalbr@test dr_walbr]$ ftp test.bruy.info Connected to test.bruy.info.
220 TEST FTP SERVER TEST.BRUY.INFO
530 Please login with USER and PASS.
```

Шаг 3

Зарегистрируйтесь на FTP-сервере в качестве анонимного (`anonymous`) пользователя или пользователя `ftp`:

```
Name (test.bruy.info:drwalbr): anonymous
331 Please specify the password.
```

Вместо пароля можно ввести любую, в том числе и пустую, строку:

```
Password:Any_or_empty_string
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Шаг 4

Получите список файлов и каталогов, содержащихся в корневом каталоге сервера:

```
ftp> dir
229 Entering Extended Passive Mode (|||51857|)
150 Here comes the directory listing.
-r-xr-xr-x    1 24       24         700610 Jun 06 13:21 Mail-
SpamAssassin-2.55.tar.gz
dr-xr-xr-x    2 24       24           4096 Jul 07 12:59 uploads
226 Directory send OK.
```

Шаг 5

Проверьте возможность получения файлов с сервера анонимными пользователями и работоспособность установленных вами ограничений на скорость соединения:

```
ftp> get Mail-SpamAssassin-2.55.tar.gz
local: Mail-SpamAssassin-2.55.tar.gz remote: Mail-SpamAssassin-
2.55.tar.gz
229 Entering Extended Passive Mode (|||34124|)
150 Opening BINARY mode data connection for Mail-SpamAssassin-2.55.tar.gz
(700610 bytes).
100% |*********************************************|   684 KB    00:19
226 File send OK.
700610 bytes received in 19.05 seconds (35.91 KB/s)
```

Шаг 6

Проверьте возможность закладки файлов анонимными пользователями в каталог `uploads`. Для этого перейдите в каталог `uploads`:

```
ftp> cd uploads
250 Directory successfully changed.
```

и загрузите какой-нибудь файл:

```
ftp> put mbox
local: mbox remote: mbox
229 Entering Extended Passive Mode (|||38581|)
150 Ok to send data.
100% |*************************************************|  3711
00:00
226 File receive OK.
3711 bytes sent in 0.02 seconds (229.48 KB/s)
```

Проверьте наличие файла в каталоге `uploads`:

```
ftp> dir
229 Entering Extended Passive Mode (|||39129|)
150 Here comes the directory listing.
-rw-------    1 24       24           3711 Jul 09 08:28 mbox
226 Directory send OK.
```

Шаг 7

Завершите работу с ftp-клиентом.

```
ftp> quit
221 Goodbye.
```

Часть 10

Программное обеспечение для организации службы HTTP-сервера

Глава 34

Apache HTTP Server

В этой главе:

1. Ограничения и допущения
2. Пакеты
3. Установка из rpm-пакетов
4. Компиляция, оптимизация и инсталляция Apache
5. Конфигурирование Apache HTTP Server
6. Конфигурационный файл /etc/httpd/conf/httpd.conf
7. Конфигурационный файл /etc/sysconfig/httpd
8. Конфигурационные файлы .htaccess
9. Конфигурационный файл /etc/logrotate.d/httpd
10. Файл инициализации /etc/rc.d/init.d/httpd
11. Конфигурирование Apache HTTP Server с доступом в закрытые каталоги с аутентификацией пользователей (файл /etc/httpd/conf/dbmpasswd)
12. Конфигурирование поддержки протокола SSL в Apache HTTP Server (файлы /usr/share/ssl/certs/www.crt и /usr/share/ssl/private/www.key)
13. Тестирование Apache HTTP Server
14. Выполнение Apache HTTP Server в среде chroot-jail

В настоящее время Apache HTTP Server представляет собой хорошо защищенный, высокопроизводительный сервер, предназначенный для обработки HTTP-запросов. Разработка сервера и некоторых смежных проектов поддерживается Apache Software Foundation. Код сервера имеет модульную структуру и, следовательно, может быть легко модифицирован к решению практически любых задач по организации виртуального общения между сервером и клиентом. В настоящее время разработчики сервера предлагают две версии – 1.3 и 2.0. В этой главе рассматривается установка Web-сервера Apache версии 2.0. Это относительно новая ветвь разработки и, к сожалению, не полностью совместима с предыдущими версиями Web-сервера. Новая генерация Apache появилась относительно недавно, и поэтому не все сторонние разработчики программного обеспечения успели модифицировать его к новой версии Web-сервера. Тем не менее, авторы предполагают, что в ближайшее время Apache 2.0 станет стандартом Web-сервера де-факто. В связи с этим инсталляция и настройка Apache в этой книге рассматривается именно на примере версии 2.0.47. К настоящему времени новые версии Apache, в частности, поддерживают:

- протокол SSL, реализуемый встроенным модулем `mod_ssl`, позволяющий устанавливать защищенное соединение между клиентской программой-браузером и Web-сервером;
- язык PHP, реализуемый модулем сторонних разработчиков `mod_php`;
- модуль `mod_perl` – также разрабатываемый сторонними разработчиками – повышающий производительность сервера применительно к выполнению сценариев, написанных на языке Perl.

Интеграция Apache с этими модулями описана в этой и двух последующих главах.

Потенциальные уязвимости Apache, как и любого другого программного обеспечения, могут использоваться для реализации атак на вашу систему. Поэтому для повышения безопасности вашей системы Apache можно заставить работать в защищенной среде chroot-jail. Запуск Apache в окружении chroot-jail совместно с поддержкой `mod_ssl`, `mod_php` и `mod_perl` описана далее в отдельной главе.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого, к сожалению, не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы Apache HTTP Server Project по состоянию на 10.07.2003. Регулярно посещайте домашнюю страницу проекта `http://httpd.apache.org/`и отслеживайте обновления. Исходные коды Apache HTTP Server содержатся в архиве `httpd-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `httpd-2.0.47.tar.gz`).

Если вы собираетесь использовать Web-сервер с поддержкой протокола SSL, установите OpenSSL в соответствии с рекомендациями главы 12.

Для проведения инсталляции и нормальной работы на вашей системе должны быть установлены входящие в комплект поставки ASPLinux 7.3 rpm-пакеты:

- `autoconf-2.13-17.noarch.rpm`;
- `automake-1.4p5-4.noarch.rpm`;
- `db3-devel-3.3.11-6.i386.rpm`;
- `expat-1.95.2-2.i386.rpm`;
- `expat-devel-1.95.2-2.i386.rpm`;
- `gdbm-devel-1.8.0-14.i386.rpm`;
- `libtool-1.4.2-7.i386.rpm`.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлены ли пакеты программ из списка, представленного выше. Используйте, например, команду:

```
[root@test /]# rpm –iq autoconf
```

Повторите ее для вывода информации об остальных пакетах.

Шаг 2

Перейдите в каталог, где находятся rpm-пакеты. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@test /]# cd /home/distrib
```

Шаг 3

Установите недостающие пакеты. Если вы следовали рекомендациям по установке, описанным в этой книге, вам останется лишь установить:

```
[root@test distrib]# rpm -ihv autoconf-2.13-17.noarch.rpm \
automake-1.4p5-4.noarch.rpm \
expat-1.95.2-2.i386.rpm \
expat-devel-1.95.2-2.i386.rpm
[root@test distrib]# rpm -ihv apache-1.3.23-11.asp.i386.rpm \
apache-devel-1.3.23-11.asp.i386.rpm
```

После установки пакета перейдите к настройке программы Apache.

ЗАМЕЧАНИЕ В комплект поставки дистрибутива ASPLinux 7.3 (Voctok) входят пакеты, содержащие Apache HTTP Server версии 1.3.23. Приведенные ниже в разделе «Конфигурирование Apache HTTP Server рекомендации по настройке относятся к версии 2.0.xx. Поэтому при установке Apache HTTP Server из rpm-пакетов вам придется конфигурировать сервер самостоятельно, руководствуясь комментариями в файле httpd.conf и докуметацией.

Компиляция, оптимизация и инсталляция Apache HTTP Server

Для инсталляции Apache HTTP Server из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами, например, используя процедуры, описанные в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12. Необходимые для проверки исходные данные вы можете получить с `http://www.apache.org/dist/httpd/`.

Шаг 2

Распакуйте архивы с исходными кодами Apache HTTP Server в каталог `/var/tmp`:

```
[root@test tmp]# tar xzpf httpd-2.0.47.tar.gz
```

Шаг 3

Создайте специального пользователя `www`, от имени которого будет выполняться Apache HTTP Server:

```
[root@test tmp]# groupadd -g 48 www
[root@test tmp]# useradd –u 48 -g 48 -s /sbin/nologin -M -r -d /var/www
www
```

Шаг 4

Для добавления несуществующего командного интерпретатора, «используемого» пользователем `www`, добавьте (проверьте наличие) в файл `/etc/shells` строку:

```
/bin/false/
```

Шаг 5

Сконфигурируйте исходные коды Apache HTTP Server :

```
[root@test tmp]# cd httpd-2.0.47
[root@test httpd-2.0.47]# CFLAGS="-O2 -march=i686 -funroll-loops -
D_REENTRANT -D_SINGLE_LISTEN_UNSERIALIZED_ACCEPT -fPIC"
./configure --prefix=/etc/httpd \
```

```
--exec-prefix=/usr \
--bindir=/usr/bin \
--sbindir=/usr/sbin \
--mandir=/usr/share/man \
--sysconfdir=/etc/httpd/conf \
--includedir=/usr/include/httpd \
--libexecdir=/usr/lib/httpd/modules \
--datadir=/var/www \
--localstatedir=/var \
--enable-access=shared \
--enable-actions=shared \
--enable-alias=shared \
--enable-auth=shared \
--enable-auth-dbm=shared \
--enable-auth-digest=shared \
--enable-autoindex=shared \
--enable-cern-meta=shared \
--enable-cgi=shared \
--enable-cgid=shared \
--enable-dav=shared \
--enable-dav-fs=shared \
--enable-dir=shared \
--enable-env=shared \
--enable-expires=shared \
--enable-file-cache=shared \
--enable-headers=shared \
--enable-include=shared \
--enable-log-config=shared \
--enable-mime=shared \
--enable-mime-magic=shared \
--enable-negotiation=shared \
--enable-rewrite=shared \
--enable-setenvif=shared \
--enable-speling=shared \
--enable-ssl=shared \
--enable-unique-id=shared \
--enable-usertrack=shared \
--enable-vhost-alias=shared \
--enable-suexec=shared \
--with-suexec-caller=www \
--with-suexec-docroot=/var/www \
--with-suexec-logfile=/var/log/httpd/suexec_log \
--with-suexec-bin=/usr/sbin/suexec \
--with-suexec-uidmin=500 --with-suexec-gidmin=500 \
--disable-auth-anon \
--disable-charset-lite \
--disable-disk-cache \
--disable-mem-cache \
--disable-cache \
--disable-deflate \
--disable-ext-filter \
--disable-case-filter \
--disable-case-filter-in \
--disable-example \
--disable-proxy \
--disable-proxy-connect \
--disable-proxy-ftp \
--disable-proxy-http \
--disable-status \
--disable-asis \
--disable-info \
--disable-imap \
--disable-userdir \
--with-z \
```

```
--with-ssl \
--with-suexec
```

В рассматриваемом примере изменены каталоги, используемые сервером по умолчанию, и оставлен минимальный набор опций, необходимый для работы сервера. Назначение всех опций прекрасно описано в документации по Apache HTTP Server (`http://httpd.apache.org/docs-2.0/install.html`). Если вы не собираетесь использовать сервер с поддержкой SSL, следует вместо опции:

```
--with-ssl
```

использовать:

```
--disable-ssl
```

Шаг 6

Откомпилируйте, проинсталлируйте Apache HTTP Server , создайте и сохраните в надежном месте список установленных файлов:

```
[root@test httpd-2.0.47]# make
[root@test httpd-2.0.47]# find /* > /root/apache1
[root@test httpd-2.0.47]# make install
[root@test httpd-2.0.47]# strip /usr/sbin/httpd
[root@test httpd-2.0.47]# chmod 0511 /usr/sbin/httpd
[root@test httpd-2.0.47]# strip --strip-debug -R .comment
/usr/lib/httpd/modules/*.so
[root@test httpd-2.0.47]# mkdir -p /var/log/httpd/
[root@test httpd-2.0.47]# mkdir -p /var/lib/dav
[root@test httpd-2.0.47]# rm -rf /var/logs
[root@test httpd-2.0.47]# mv /var/www/build /usr/lib/httpd/build
[root@test httpd-2.0.47]# rm -f  /usr/lib/httpd/build/libtool
[root@test httpd-2.0.47]# ln -s /usr/bin/libtool
/usr/lib/httpd/build/libtool
[root@test httpd-2.0.47]# ln -s /var/log/httpd /etc/httpd/logs
[root@test httpd-2.0.47]# ln -s /var/run /etc/httpd/run
[root@test httpd-2.0.47]# ln -s /usr/lib/httpd/modules /etc/httpd/modules
[root@test httpd-2.0.47]# ln -s /usr/lib/httpd/build /etc/httpd/build
[root@test httpd-2.0.47]# find /* > /root/apache2
[root@test httpd-2.0.47]# diff /root/apache1 /root/apache2 >
/root/apache.installed
[root@test httpd-2.0.47]# mv /root/apache.installed
/very_reliable_place/apache.installed.YYYYMMDD
```

Шаг 7

Удалите архив и каталог с исходными кодами:

```
[root@test httpd-2.0.47]# cd /var/tmp/
[root@test tmp]# rm -rf httpd-2.0.47/
[root@test tmp]# rm -f httpd-2.0.47.tar.gz
```

Конфигурирование Apache HTTP Server

Конфигурирование Apache HTTP Server осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/httpd/conf/httpd.conf`;
- системного конфигурационного файла `/etc/sysconfig/httpd`;
- файлов `.htaccess`, определяющих настройки Web-сервера, применяемые к каталогу, в котором находится файл, и подкаталогам любого уровня каталога, содержащего файл `.htaccess`;
- файла настройки чередования регистрационных файлов `/etc/logrotate.d/httpd`;
- файла инициализации `/etc/rc.d/init.d/httpd`;
- файла с аутентификационной информацией пользователей для доступа в закрытые каталоги сервера `/etc/httpd/conf/dbmpasswd`;
- файлов `/usr/share/ssl/certs/www.crt` и `/usr/share/ssl/private/www.key`, содержащих закрытый ключ и сертификат, необходимые для поддержки протокола SSL.

Конфигурационный файл /etc/httpd/conf/httpd.conf

Главный конфигурационный файл `/etc/httpd/conf/httpd.conf` может содержать большое число различных директив, даже краткое описание которых может послужить темой для отдельной книги.

Поэтому в дальнейшем рассмотрении мы ограничимся простейшими случаями конфигурации сервера, иллюстрирующими возможности сервера по поддержанию виртуальных серверов с доступом по протоколу HTTP или HTTPS (HTTP с поддержкой SSL) и аутентификации пользователей. При этом комментарии будут касаться только наиболее часто используемых при индивидуальной настройке сервера директив. С остальными директивами и вариантами конфигурации вы можете ознакомиться в документации (`http://httpd.apache.org/docs-2.0/`) и кратком руководстве по директивам Apache HTTP Server (`http://httpd.apache.org/docs-2.0/mod/quickreference.html`).

Шаг 1

Создайте файл `/etc/httpd/conf/httpd.conf`, измените в нем строки, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
### Section 1: Global Environment
#
ServerRoot "/etc/httpd"
PidFile /var/run/httpd.pid
ServerTokens Prod
ServerSignature Off

Timeout 60
KeepAlive Off
MaxKeepAliveRequests 0
KeepAliveTimeout 10

# Prefork MPM
#
<IfModule prefork.c>
StartServers        5
MaxClients          512
MinSpareServers     5
MaxSpareServers     10
MaxRequestsPerChild 0
</IfModule>

Listen 212.111.80.127:443
Listen 212.111.80.127:80
# Dynamic Shared Object (DSO) Support
#
LoadModule access_module        modules/mod_access.so
#LoadModule auth_module         modules/mod_auth.so
LoadModule auth_dbm_module      modules/mod_auth_dbm.so
#LoadModule auth_digest_module  modules/mod_auth_digest.so
#LoadModule file_cache_module   modules/mod_file_cache.so
LoadModule include_module       modules/mod_include.so
LoadModule log_config_module    modules/mod_log_config.so
LoadModule env_module           modules/mod_env.so
LoadModule mime_magic_module    modules/mod_mime_magic.so
#LoadModule cern_meta_module    modules/mod_cern_meta.so
#LoadModule expires_module      modules/mod_expires.so
#LoadModule headers_module      modules/mod_headers.so
#LoadModule usertrack_module    modules/mod_usertrack.so
#LoadModule unique_id_module    modules/mod_unique_id.so
LoadModule setenvif_module      modules/mod_setenvif.so
LoadModule ssl_module           modules/mod_ssl.so
LoadModule mime_module          modules/mod_mime.so
#LoadModule dav_module          modules/mod_dav.so
LoadModule autoindex_module     modules/mod_autoindex.so
LoadModule cgi_module           modules/mod_cgi.so
#LoadModule dav_fs_module       modules/mod_dav_fs.so
#LoadModule vhost_alias_module  modules/mod_vhost_alias.so
LoadModule negotiation_module   modules/mod_negotiation.so
LoadModule dir_module           modules/mod_dir.so
#LoadModule actions_module      modules/mod_actions.so
#LoadModule speling_module      modules/mod_speling.so
```

```
LoadModule alias_module         modules/mod_alias.so
LoadModule rewrite_module       modules/mod_rewrite.so
#LoadModule perl_module         modules/mod_perl.so
#LoadModule php4_module         modules/libphp4.so

### Section 2: 'Main' server configuration
#
User www
Group www

ServerAdmin apacheadmin@test.bruy.info
ServerName test.bruy.info
UseCanonicalName Off


DocumentRoot "/var/www/htdocs"
<Directory />
    Options None
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>

<Files .pl>
    Options None
    AllowOverride None
    Order deny,allow
    Deny from all
</Files>

<IfModule mod_file_cache.c>
<IfModule mod_include.c>
    Include /etc/httpd/mmap.conf
</IfModule>
</IfModule>

<IfModule mod_dir.c>
    DirectoryIndex index.htm index.html index.php default.php index.shtml
index.php3
</IfModule>

<IfModule mod_mime.c>
    TypesConfig /etc/httpd/conf/mime.types
    AddEncoding x-compress Z
    AddEncoding x-gzip gz tgz
    AddType application/x-tar .tgz
    AddType application/x-httpd-php .php
    AddType application/x-httpd-php .php3
    AddType application/x-httpd-php .php4
    AddType application/x-httpd-php .phtml
    AddType application/x-httpd-php .shtml
    AddType application/x-httpd-php-source .phps
</IfModule>

DefaultType text/plain

<IfModule mod_mime_magic.c>
    MIMEMagicFile /etc/httpd/conf/magic
</IfModule>

HostnameLookups Off

LogLevel debug
ErrorLog /var/log/httpd/error_log
```

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
combined
CustomLog /var/log/httpd/access_log combined

<IfModule mod_alias.c>
Alias /icons/ "/var/www/icons/"
<Directory "/var/www/icons/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

ScriptAlias /cgi-bin/  "/var/www/cgi-bin/"
 <Directory "/var/www/cgi-bin/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
 </Directory>
</IfModule>

<IfModule mod_autoindex.c>
    IndexOptions FancyIndexing
    AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
    AddIconByType (TXT,/icons/text.gif) text/*
    AddIconByType (IMG,/icons/image2.gif) image/*
    AddIconByType (SND,/icons/sound2.gif) audio/*
    AddIconByType (VID,/icons/movie.gif) video/*
    AddIcon /icons/binary.gif .bin .exe
    AddIcon /icons/binhex.gif .hqx
    AddIcon /icons/tar.gif .tar
    AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
    AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
    AddIcon /icons/a.gif .ps .ai .eps
    AddIcon /icons/layout.gif .html .shtml .htm .pdf
    AddIcon /icons/text.gif .txt
    AddIcon /icons/c.gif .c
    AddIcon /icons/p.gif .pl .py
    AddIcon /icons/f.gif .for
    AddIcon /icons/dvi.gif .dvi
    AddIcon /icons/uuencoded.gif .uu
    AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
    AddIcon /icons/tex.gif .tex
    AddIcon /icons/bomb.gif core
    AddIcon /icons/back.gif ..
    AddIcon /icons/hand.right.gif README
    AddIcon /icons/folder.gif ^^DIRECTORY^^
    AddIcon /icons/blank.gif ^^BLANKICON^^
    DefaultIcon /icons/unknown.gif
    ReadmeName README.html
    HeaderName HEADER.html
    IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
</IfModule>
###Поддержка русского и английского языка
#

AddLanguage en .en
AddLanguage ru .ru
AddDefaultCharset koi8-r
AddCharset ISO-8859-1  .iso8859-1  .latin1
AddCharset ISO-8859-5  .iso8859-5  .latin5 .cyr .iso-ru
AddCharset WINDOWS-1251 .cp-1251   .win-1251
AddCharset CP866       .cp866
```

```
AddCharset KOI8-r      .koi8-r .koi8-ru
AddCharset KOI8-ru     .koi8-uk .ua
AddCharset ISO-10646-UCS-2 .ucs2
AddCharset ISO-10646-UCS-4 .ucs4
AddCharset UTF-8       .utf8


ErrorDocument 400 "Server could not understand this request."
ErrorDocument 401 "Server could not verify your access authorization."
ErrorDocument 403 "Access Forbidden -- Go away."
ErrorDocument 404 "Error! The requested page do not exist"
ErrorDocument 405 "Method not allowed for the requested URL."
ErrorDocument 408 "Server closed the network connection."
ErrorDocument 410 "Requested URL no longer available."
ErrorDocument 411 "Requested method Requires a valid header."
ErrorDocument 412 "Precondition request failed positive evaluation."
ErrorDocument 413 "Method not allowed for the data transmitted."
ErrorDocument 414 "Requested URL exceeds the capacity limit."
ErrorDocument 415 "Server temporarily unavailable -- Maintenance down-
time."
ErrorDocument 500 "Server encountered an internal error."
ErrorDocument 501 "Server does not support the action requested."
ErrorDocument 502 "Proxy server received an invalid response."
ErrorDocument 503 "Server temporarily unavailable -- Maintenance down-
time."
ErrorDocument 506 "Access not possible."

<IfModule mod_setenvif.c>
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redi-
rect-carefully
BrowserMatch "^WebDrive" redirect-carefully
</IfModule>

### Section 3: Virtual Hosts
#
### Виртуальный хост, например, с витриной магазина
### с доступом  по протоколу http
#
NameVirtualHost eshop.bruy.info:80

<VirtualHost eshop.bruy.info:80>
ServerAdmin sales@test.bruy.info
ServerName eshop.bruy.info
DocumentRoot "/var/www/eshop/html/"

#Каталог для html-документов
<Directory "/var/www/eshop/html/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

#Каталог с ограниченным доступом.
#Вряд ли имеет смысл создавать его на этом
#виртуальном хосте так логины и пароли передаются
#по сети в формате обычного текста.
#Каталог с  ограниченным доступом лучше создать на
#виртуальном хосте с поддержкой протокола SSL.
```

```
<Directory "/var/www/eshop/html/private/">
    Options None
    AllowOverride AuthConfig
    AuthName "Restricted Section"
    AuthType Basic
    AuthDBMType GDBM
    AuthDBMUserFile /etc/httpd/conf/dbmpasswd
    Require valid-user
</Directory>

#Каталог для сценариев
ScriptAlias /cgi-bin/  "/var/www/eshop/cgi-bin/"
 <Directory "/var/www/eshop/cgi-bin/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
 </Directory>


ErrorLog /var/log/httpd/error_eshop_log
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
TransferLog /var/log/httpd/access_eshop_log
</VirtualHost>


## SSL Global Context
#
<IfModule mod_ssl.c>
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl

SSLPassPhraseDialog     builtin
SSLSessionCache         none
SSLSessionCacheTimeout  300
SSLMutex                sem
SSLRandomSeed startup   file:/dev/urandom 1024
SSLRandomSeed connect   file:/dev/urandom 1024

## SSL Virtual Host Context
#
### Виртуальный хост, например,
### с информацией для зарегистрированных клиентов
### с доступом  по протоколу https
NameVirtualHost eshop.bruy.info:443

<VirtualHost eshop.bruy.info:443>
ServerAdmin sales@test.bruy.info
ServerName eshop.bruy.info
DocumentRoot "/var/www/eshopssl/html"

#Каталог для html-документов
<Directory "/var/www/eshopssl/html/">
    Options Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
#Каталог с ограниченным доступом
<Directory "/var/www/eshopssl/html/private/">
    Options None
    AllowOverride AuthConfig
    AuthName "Restricted Section"
    AuthType Basic
```

```
    AuthDBMType GDBM
    AuthDBMUserFile /etc/httpd/conf/dbmpasswd
    Require valid-user
</Directory>

#Каталог для сценариев
ScriptAlias /cgi-bin/ "/var/www/eshopssl/cgi-bin/"
 <Directory "/var/www/eshopssl/cgi-bin/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
 </Directory>



ErrorLog /var/log/httpd/error_eshopssl_log
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
TransferLog /var/log/httpd/access_eshopssl_log

SSLEngine on

SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile      /usr/share/ssl/certs/www.crt
SSLCertificateKeyFile   /usr/share/ssl/private/www.key
SSLVerifyClient none
SSLVerifyDepth  10

SetEnvIf User-Agent ".*MSIE.*" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0

CustomLog /var/log/httpd/ssl_request_log \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

</VirtualHost>

</IfModule>
```

В разделе `Section 1: Global Environment` приведенного конфигурационного файла содержатся директивы, определяющие поведение сервера вцелом.

Директива:

```
ServerRoot "/etc/httpd"
```

определяет местоположение каталога с файлом `/etc/httpd`.

Директива:

```
PidFile /var/run/httpd.pid
```

определяет местоположение pid-файла, создаваемого при запуске демона `httpd`.

Директива:

```
ServerTokens Prod
```

предназначена для управления объемом информации, выдаваемой сервером в ответах на запросы клиентов. В принципе, в заголовках запросов может содержаться информация о версии сервера, типе используемой операционной системы, модулях и т. п. С точки зрения обеспечения безопасности, не плохо было бы ограничить объем выдаваемой информации только названием Web-сервера – Apache. Для этого используйте параметр `Prod`.

Директива:

```
ServerSignature Off
```

используется для исключения из сообщений об ошибках информации о версии сервера.

Директива:

```
Timeout 60
```

определяет максимальный интервал времени ожидания, измеряемый в секундах, по истечении которого сервер разрывает соединение. Значение 60, установленное в рассматриваемом примере, позволяет повысить производительность сильно загруженного сервера. Однако при плохих каналах связи, используемых клиентами, это время нужно увеличить до 300, в противном случае они не смогут получить доступ к серверу.

Директива:

```
KeepAlive Off
```

позволяет разрешать или запрещать так называемые постоянные соединения, позволяя при этом за одно соединение удовлетворять несколько запросов. Вам следует включить эту опцию ("on"), если вы устанавливаете Apache на сильно загруженном сервере.

Директива:

```
MaxKeepAliveRequests 0
```

определяет максимально допустимое число запросов, обслуживаемых за одно соединение. Значение 0, используемое в рассматриваемом примере, не ограничивает число запросов, обслуживаемых при одном соединении.

Директива:

```
KeepAliveTimeout 10
```

используется для определения временного интервала (в секундах), в течение которого Apache будет ожидать последующего запроса перед окончанием соединения. После получения запроса к нему применяется значение времени ожидания, указанное в директиве `Timeout`. Значение 10 секунд вполне подходит для нормальной работы сервера. Это значение должно устанавливаться по возможности более низким.

Директива:

```
StartServers        5
```

используется для определения числа дочерних процессов сервера, которые будут создаваться при запуске Apache. Поскольку число процессов для Apache 2.x динамически управляется в зависимости от его загрузки, обычно нет необходимости изменять значение, заданное по умолчанию (т. е. 5).

Директива:

```
MaxClients          512
```

используется для ограничения числа дочерних процессов, которые будут созданы для обслуживания запросов. Значение, установленное по умолчанию, означает, что одновременно могут обрабатываться до 512 HTTP-запросов. Любые дальнейшие запросы соединений ставятся в очередь. Это важный параметр оптимизации производительности Web-сервера Apache. При сильной загруженности значение 512 наиболее оптимально и рекомендуется различными эталонными Internet-тестами. Для обычного использования можно установить значение, равное 256.

Директива:

```
MinSpareServers     5
```

определяет количество неактивных (неиспользуемых запросами клиентов) дочерних процессов. Если количество неактивных процессов упадет менее величины, определенной директивой, сервер сразу же создаст еще один дочерний процесс, готовый немедленно обслужить клиентский запрос.

```
MaxRequestsPerChild 0
```

определяет максимальное число запросов, обрабатываемых каждым из дочерних процессов сервера. В рассматриваемом примере установлено значение 0, т. е. количество запросов не ограничено.

Директивы:

```
Listen 212.111.80.127:443
Listen 212.111.80.127:80
```

определяют IP-адреса и номера портов, на которых httpd-демон ожидает подключений. В рассматриваемом примере используется один IP-адрес и общепринятые значения портов для соединений по протоколу HTTP и HTTPS. Здесь вы должны ввести IP-адрес именно вашего сервера.

Директивы:

```
LoadModule access_module        modules/mod_access.so
#LoadModule auth_module         modules/mod_auth.so
#LoadModule auth_dbm_module     modules/mod_auth_dbm.so

LoadModule rewrite_module       modules/mod_rewrite.so
#LoadModule perl_module         modules/mod_perl.so
#LoadModule php4_module         modules/libphp4.so
```

определяют модули, которые могут быть загружены ядром сервера в случае необходимости. Модули, отвечающие за поддержку SSL, PHP, Perl и аутентификацию пользователей пока закомментированы. Для их подключения необходимо выполнение ряда операций, описанных ниже в этой главе и последующих двух главах.

В разделе `Section 2: 'Main' server configuration` находятся наиболее общие настройки сервера.

Директивы:

```
User www
Group www
```

соответственно, определяют пользователя и группу пользователей, от имени которых запускается Web-сервер Apache.

Директивы:

```
ServerAdmin apacheadmin@test.bruy.info
```

используется для определения адреса электронной почты, куда будут отсылаться любые сообщения об ошибках, возвращаемых клиенту. Не забудьте изменить данное значение на реальный почтовый адрес администратора вашего сервера (авторам этой книги совершенно не интересно получать сообщения об ошибках на чужих серверах).

Директивы:

```
ServerName test.bruy.info
```

используется для определения имени хоста. Здесь вы должны ввести имя именно вашей системы, в соответствии с записями в файле зоны вашего DNS-сервера.

Блок директив:

```
DocumentRoot "/var/www/htdocs"
<Directory />
    Options None
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>
```

запрещает доступ к корневому каталогу вашего сервера. Это сделано, во-первых, потому что в нем содержатся страницы на нескольких языках, устанавливаемые при инсталляции Apache и имеющие ссылку на руководство. Во-вторых, потому что в дальнейшем рассмотрении мы собираемся конфигурировать сервер в режиме поддержки виртуальных серверов. В этом случае, если вы даже разрешите доступ к каталогу `/var/www/htdocs`, при обращении к серверу `test.bruy.info` пользователь будет получать доступ к корневому каталогу первого из упомянутых в конфигурационном файле виртуальных серверов.

После инсталляции и настройки сервера авторы настоятельно рекомендуют удалить все лишние файлы из каталога `/var/www/htdocs` и каталог руководства:

```
[root@test tmp]# rm –f /var/www/htdocs/*
[root@test tmp]# rm –rf /var/www/manual/
```

Блок директив:

```
<Files .pl>
    Options None
    AllowOverride None
    Order deny,allow
    Deny from all
</Files>
```

запрещает доступ к файлам, имеющим разрешение `*.pl`. Это расширение обычно используется для файлов сценариев, написанных на языке Perl. Если в последующем понадобится, можете разрешить доступ к файлам с расширением `*.pl` только в некоторых каталогах.

Блок директив:

```
<IfModule mod_dir.c>
    DirectoryIndex index.htm index.html index.php default.php index.shtml
index.php3
</IfModule>
```

используется для определения последовательности поиска индексных файлов, т. е. файлов, которые выдаются по умолчанию при получении HTTP-запроса, содержащего URL каталога. Для повышения производительности сервера в директиве `DirectoryIndex` рекомендуется включать только те файлы, которые действительно используются в качестве индексных на вашем сервере.

Директива:

```
HostnameLookups Off
```

отключает запросы к DNS-серверам для получения информации об имени хоста, с которого осуществляется запрос к серверу. Для повышения производительности сервера рекомендуется использовать значение "off".

Блок директив:

```
LogLevel debug
ErrorLog /var/log/httpd/error_log
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
combined
CustomLog /var/log/httpd/access_log combined
```

определяет пути к файлам регистрации, объем и содержание записываемой в них информации. Используемое в директиве `LogLevel` значение `debug` соответствует максимальному объему выводимой информации и может быть использовано только на этапе настройки и тестирования сервера. При штатной эксплуатации сервера рекомендуется использовать значение `notice`.

Блоки директив:

```
<IfModule mod_mime_magic.c>
```

```
    MIMEMagicFile /etc/httpd/conf/magic
</IfModule>
```

и

```
<IfModule mod_mime.c>
    TypesConfig /etc/httpd/conf/mime.types
    AddEncoding x-compress Z
    AddEncoding x-gzip gz tgz
    AddType application/x-tar .tgz
    AddType application/x-httpd-php .php
    AddType application/x-httpd-php .php3
    AddType application/x-httpd-php .shtml
    AddType application/x-httpd-php-source .phps
</IfModule>
```

используются для определения типов файлов, обслуживаемых сервером, и для определения алгоритма выдачи их по запросам клиентов.

Блок директив:

```
ScriptAlias /cgi-bin/  "/var/www/cgi-bin/"
 <Directory "/var/www/cgi-bin/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
 </Directory>
</IfModule>
```

определяет общий для всего сервера каталог, в котором могут размещаться файлы сценариев. Этот каталог может использоваться и виртуальными серверами. Однако для большей наглядности в дальнейшем мы определили для каждого виртуального сервера свой собственный каталог для файлов сценариев. Тем не менее, в каталоге `/var/www/cgi-bin/` возможно размещение файлов сценариев. Доступ к ним может быть осуществлен с помощью URL вида: `http://test.bruy.info/cgi-bin/name_script.cgi`.

Блок директив:

```
<IfModule mod_autoindex.c>
    IndexOptions FancyIndexing
    AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
…
    ReadmeName README.html
    HeaderName HEADER.html
    IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
</IfModule>
```

Блок директив:

```
AddLanguage en .en
AddLanguage ru .ru
AddDefaultCharset koi8-r
AddCharset ISO-8859-1  .iso8859-1  .latin1
AddCharset ISO-8859-5  .iso8859-5  .latin5 .cyr .iso-ru
AddCharset WINDOWS-1251 .cp-1251   .win-1251
AddCharset CP866       .cp866
AddCharset KOI8-r      .koi8-r .koi8-ru
AddCharset KOI8-ru     .koi8-uk .ua
AddCharset ISO-10646-UCS-2 .ucs2
AddCharset ISO-10646-UCS-4 .ucs4
AddCharset UTF-8       .utf8
```

используется для поддержки кодировок русского языка. При этом, директива:

```
AddDefaultCharset koi8-r
```

определяет кодировку, выдаваемую в заголовке клиенту. В рассматриваемом примере мы используем кодировку koi8-r, и следовательно, страницы, обслуживаемые сервером, должны быть в этой же кодировке. В настоящее время кодировка windows-1251 является более распространенной и проще интегрируется со многими программами, поэтому может оказаться более удобным страницы сервера выполнять в кодировке windows-1251. Для их корректного отображения измените значение директивы `AddDefaultCharset` на:

```
AddDefaultCharset windows-1251
```

Блок директив:

```
ErrorDocument 400 "Server could not understand this request."
ErrorDocument 401 "Server could not verify your access authorization."
ErrorDocument 403 "Access Forbidden -- Go away."
```

```
…
ErrorDocument 502 "Proxy server received an invalid response."
ErrorDocument 503 "Server temporarily unavailable -- Maintenance down-
time."
ErrorDocument 506 "Access not possible."
```

определяет реакцию сервера на сообщения о различных ошибках. Вместо сообщения, указанного в кавычках, может использоваться путь к файлу, содержащему сообщение об ошибке или URL. Например, переход к странице, выполненной в дизайне вашего сервера, и сообщающей об ошибке 403 может быть выполнен с помощью директивы:

```
ErrorDocument 403 /errors/403.html
```

а переадресация на другой URL (такая переадресация поддерживается, но по мнению авторов, является признаком дурного тона) – с помощью директивы:

```
ErrorDocument 404 http://www.gogle.com
```

Блок директив:

```
<IfModule mod_setenvif.c>
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redi-
rect-carefully
BrowserMatch "^WebDrive" redirect-carefully
</IfModule>
```

используется для более адекватного отображения содержимого обслуживаемых Web-сервером ресурсов в различных браузерах путем изменения соответствующих переменных окружения.

В разделе `Section 3: Virtual Hosts` определяются виртуальные сервера, обслуживаемые основным сервером.

В рассматриваемом примере виртуальный север `eshop.bruy.info` определен с помощью директив:

```
### Виртуальный хост, например, с витриной магазина
### с доступом  по протоколу http
#
NameVirtualHost eshop.bruy.info:80

<VirtualHost eshop.bruy.info:80>
ServerAdmin sales@test.bruy.info
ServerName eshop.bruy.info
DocumentRoot "/var/www/eshop/html/"

#Каталог для html-документов
<Directory "/var/www/eshop/html/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

#Каталог с ограниченным доступом.
#Вряд ли имеет смысл создавать его на этом
#виртуальном хосте так логины и пароли передаются
#по сети в формате обычного текста.
#Каталог с  ограниченным доступом лучше создать на
#виртуальном хосте с поддержкой протокола SSL.
<Directory "/var/www/eshop/html/private/">
    Options None
    AllowOverride AuthConfig
    AuthName "Restricted Section"
    AuthType Basic
    AuthDBMType GDBM
    AuthDBMUserFile /etc/httpd/conf/dbmpasswd
    Require valid-user
</Directory>
```

```
#Каталог для сценариев
ScriptAlias /cgi-bin/  "/var/www/eshop/cgi-bin/"
 <Directory "/var/www/eshop/cgi-bin/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
 </Directory>


ErrorLog /var/log/httpd/error_eshop_log
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
TransferLog /var/log/httpd/access_eshop_log
</VirtualHost>
```

Многие из этих директив уже использовались нами при конфигурировании основного сервера. Кроме того, следует отметить, что виртуальный сервер наследует непереопределенные настройки основного.

Директива:

```
NameVirtualHost eshop.bruy.info:80
```

предписывает прослушивать подключения на 80 порту – используемого по умолчанию – для соединений по протоколу HTTP.

ЗАМЕЧАНИЕ для нормальной работы виртуального сервера необходимо внести соответствующие коррективы в файлы зон DNS-сервера.

Директивы:

```
<VirtualHost eshop.bruy.info:80>
```

и

```
</VirtualHost>
```

ограничивают область описания виртуального сервера.

Блок директив:

```
#Каталог для html-документов
<Directory "/var/www/eshop/html/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

определяет путь к корневому каталогу виртуального сервера eshop.bruy.info:80.

Блок директив:

```
<Directory "/var/www/eshop/html/private/">
    Options None
    AllowOverride AuthConfig
    AuthName "Restricted Section"
    AuthType Basic
    AuthDBMType GDBM
    AuthDBMUserFile /etc/httpd/conf/dbmpasswd
    Require valid-user
</Directory>
```

определяет каталог `/var/www/eshop/html/private/`, доступ в который осуществляется после удачной аутентификации пользователя. Аутентификационную информацию о пользователях (логин и пароль) для повышения производительности лучше хранить в специально созданной базе данных.

Директива:

```
AllowOverride AuthConfig
```

разрешает использование директив авторизации пользователей при доступе к каталогу.

Директива:

```
AuthName "Restricted Section"
```

определяет строковое сообщение, отправляемое клиентской программе при обращении к каталогу перед аутентификацией пользователя. Здесь вы можете ввести строку любого содержания, подсказывающую пользователю, для доступа к какому именно ресурсу он должен ввести аутентификационную информацию.

Директива:

```
AuthType Basic
```

определяет тип используемой аутентификации.

Директива:

```
AuthDBMType GDBM
```

определяет тип базы данных, где хранится аутентификационная информация о пользователях.

Директива:

```
AuthDBMUserFile /etc/httpd/conf/dbmpasswd
```

определяет путь к файлу, в котором хранится аутентификационная информация о пользователях.

Директива:

```
Require valid-user
```

разрешает доступ к каталогу пользователей, удачно прошедших аутентификацию.

ЗАМЕЧАНИЕ Если вы не собираетесь использовать каталоги с ограниченным доступом, закомментируйте или удалите настройки доступа к каталогу из разделов, конфигурирующих виртуальные сервера, а также строку:

```
LoadModule auth_dbm_module     modules/mod_auth_dbm.so
```

из раздела `Section 1: Global Environment`.

Блок директив:

```
#Каталог для сценариев
ScriptAlias /cgi-bin/  "/var/www/eshop/cgi-bin/"
 <Directory "/var/www/eshop/cgi-bin/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
 </Directory>
```

определяет путь к каталогу для файлов сценариев виртуального сервера eshop.bruy.info`:80`.

Настройки, касающиеся поддержки протокола SSL, содержатся в блоке, ограниченном директивами:

```
<IfModule mod_ssl.c>
```

и

```
</IfModule>
```

Общие для основного сервера и виртуальных серверов настройки определяются следующими директивами:

```
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl
SSLPassPhraseDialog     builtin
SSLSessionCache         none
SSLSessionCacheTimeout  300
SSLMutex                sem
SSLRandomSeed startup   file:/dev/urandom 1024
SSLRandomSeed connect   file:/dev/urandom 1024
```

В рассматриваемом примере виртуальный север eshop.bruy.info с поддержкой протокола SSL определен с помощью директив:

```
## SSL Virtual Host Context
#
### Виртуальный хост, например,
### с информацией для зарегистрированных клиентов
### с доступом  по протоколу https
NameVirtualHost eshop.bruy.info:443

<VirtualHost eshop.bruy.info:443>
ServerAdmin sales@test.bruy.info
ServerName eshop.bruy.info
DocumentRoot "/var/www/eshopssl/html"

#Каталог для html-документов
<Directory "/var/www/eshopssl/html/">
    Options Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
#Каталог с ограниченным доступом
<Directory "/var/www/eshopssl/html/private/">
    Options None
```

```
    AllowOverride AuthConfig
    AuthName "Restricted Section"
    AuthType Basic
    AuthDBMType GDBM
    AuthDBMUserFile /etc/httpd/conf/dbmpasswd
    Require valid-user
</Directory>

#Каталог для сценариев
ScriptAlias /cgi-bin/ "/var/www/eshopssl/cgi-bin/"
 <Directory "/var/www/eshopssl/cgi-bin/">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
 </Directory>



ErrorLog /var/log/httpd/error_eshopssl_log
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
TransferLog /var/log/httpd/access_eshopssl_log

SSLEngine on

SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile      /usr/share/ssl/certs/www.crt
SSLCertificateKeyFile   /usr/share/ssl/private/www.key
SSLVerifyClient none
SSLVerifyDepth  10

SetEnvIf User-Agent ".*MSIE.*" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0

CustomLog /var/log/httpd/ssl_request_log \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

</VirtualHost>
```

Многие из этих директив использовались ранее при конфигурировании виртуального сервера без поддержки протокола SSL, поэтому их назначение при конфигурировании виртуального сервера с поддержкой SSL не поясняются.

С помощью директив:

```
NameVirtualHost eshop.bruy.info:443
```

и

```
<VirtualHost eshop.bruy.info:443>
```

виртуальному серверу предписывается ожидать соединений на 443 порту, используемого по умолчанию для протокола HTPPS.

ЗАМЕЧАНИЕ Для нормальной работы виртуального сервера необходимо внести соответствующие коррективы в файлы зон DNS-сервера.

Директивы:

```
SSLCertificateFile      /usr/share/ssl/certs/www.crt
```

и

```
SSLCertificateKeyFile   /usr/share/ssl/private/www.key
```

определяют пути к файлам, содержащих сертификат и закрытый ключ.

ЗАМЕЧАНИЕ Если вы не собираетесь использовать каталоги с ограниченным доступом, закомментируйте или удалите настройки доступа к каталогу из разделов, конфигурирующих виртуальные сервера, а также строку:

```
LoadModule auth_dbm_module     modules/mod_auth_dbm.so
```

из раздела `Section 1: Global Environment`.

Если вы не собираетесь использовать виртуальный сервер с поддержкой протокола SSL, удалите настройки виртуального сервера и удалите или закомментируйте строку:
```
LoadModule ssl_module          modules/mod_ssl.so
```
из раздела `Section 1: Global Environment`.

Шаг 2

Установите права доступа к файлу `/etc/httpd/conf/httpd.conf` и назначьте его владельцем пользователя `root`:
```
[root@test /]# chmod 600 /etc/httpd/conf/httpd.conf
[root@test /]# chown 0.0 /etc/httpd/conf/httpd.conf
```

Конфигурационный файл /etc/sysconfig/httpd

Шаг 1

Создайте файл `etc/sysconfig/httpd`, содержащий следующие строки:
```
# Uncomment the following line to enable SSL support with Apache.
# Certificate should be already configured into httpd.conf file.
#
OPTIONS="-DSSL"
```

ЗАМЕЧАНИЕ Закомментируйте или удалите строку:
`OPTIONS="-DSSL"`
если вы не собираетесь использовать Web-сервер с поддержкой протокола SSL.

Шаг 2

Установите права доступа к файлу /`etc/sysconfig/httpd` и назначьте его владельцем пользователя `root`:
```
[root@test /]# chmod 640 /etc/sysconfig/httpd
[root@test /]# chown 0.0 /etc/sysconfig/httpd
```

Конфигурационные файлы .htaccess

Конфигурационные файлы `.htaccess` не следует использовать без крайней необходимости. Использование этих файлов оправдано только в случае, когда вы не имеете доступа к основному Web-серверу. Для того, чтобы файлы `.htaccess` не игнорировались, а содержащиеся в них директивы выполнялись сервером, необходимо, чтобы это было разрешено директивой `AllowOverride`, действие которой распространяется на каталог, в котором находится файл, например:
```
AllowOverride All
```
Имя файла, используемого для конфигурирования каталога, может быть изменено с помощью директивы `AccessFileName`, например, если вас чем-то не устраивает имя `.htaccess` и вы хотите использовать файл с именем `.myconf`:
```
AccessFileName .myconf
```
Для того, чтобы содержимое файлов не было доступно клиентским пользовательским программам, используйте блок директив:
```
<Files ~ "^\.my">
    Order allow,deny
    Deny from all
</Files>
```
Директивы, используемые внутри файлов `.htaccess`, должны допускать использование в контексте файла `.htacess`.

Например, директива ErrorDocument Directive, в соответсвии с информацией представленной на сервере разработчиков (`http://httpd.apache.org/docs-2.0/mod/core.html#errordocument`) допускает ее использование в файлах `.htacess`:
```
Description: What the server will return to the client in case of an er-
ror
Syntax: ErrorDocument error-code document
Context: server config, virtual host, directory, .htaccess
Override: FileInfo
Status: Core
Module: core
Compatibility: Quoting syntax for text messages is different in Apache
2.0
```

Конфигурационный файл /etc/logrotate.d/httpd

Этот файл используется для настройки чередования файлов регистрации. В рассматриваемом примере файлы регистрации будут чередоваться еженедельно.

Шаг 1

Создайте файл `/etc/logrotate.d/httpd`, содержащий следующие строки:

```
 /var/log/httpd/*_log {
missingok
notifempty
sharedscripts
postrotate
/usr/bin/killall -HUP httpd
endscript
}
```

ЗАМЕЧАНИЕ Обратите внимание, что первая строка файла `/etc/logrotate.d/httpd` должна содержать регулярные выражения, определяющие пути ко всем файлам регистрации, используемым основным и виртуальными серверами. Это обстоятельство следует учитывать при определении имен файлов регистрации для виртуальных серверов.

Шаг 2

Установите права доступа к файлу /`etc/logrotate.d/httpd` и назначьте его владельцем пользователя `root`:

```
[root@test /]# chmod 644 /etc/logrotate.d/httpd
[root@test /]# chown 0.0 /etc/logrotate.d/httpd
```

Файл инициализации /etc/rc.d/init.d/httpd

Шаг 1

Для запуска и остановки Apache HTTP Server создайте файл `/etc/init.d/proftpd`, содержащий следующие строки:

```
#!/bin/bash
# This shell script takes care of starting and stopping Apache.
#
# chkconfig: 345 85 15
# description: Apache is a World Wide Web server. It is used to serve \
#              HTML files and CGI.
#
# processname: httpd
# config: /etc/httpd/conf/httpd.conf
# pidfile: /var/run/httpd.pid

# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/httpd ] ; then
        . /etc/sysconfig/httpd
fi

# This will prevent initlog from swallowing up a pass-phrase prompt if
# mod_ssl needs a pass-phrase from the user.
INITLOG_ARGS=""

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If Apache is not available stop now.
[ -f /usr/sbin/httpd ] || exit 0

# Path to the Apache apachectl script and server binary.
```

```
apachectl=/usr/sbin/apachectl
httpd=/usr/sbin/httpd

RETVAL=0
prog="httpd"

start() {
        echo -n $"Starting $prog: "
        daemon $httpd $OPTIONS
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && touch /var/lock/subsys/httpd
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        killproc $httpd
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && rm -f /var/lock/subsys/httpd
/var/run/httpd.pid
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        status $httpd
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
  condrestart)
        if [ -f /var/run/httpd.pid ] ; then
                stop
                start
                RETVAL=$?
        fi
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 2

Установите права доступа к файлу, назначьте его владельцем пользователя:

```
[root@test /]# chmod 700 /etc/init.d/httpd
[root@test /]# chown 0.0 /etc/init.d/httpd
```

Шаг 3

Если вы хотите, чтобы Apache HTTP Server запускался автоматически при загрузке системы, создайте соответствующие ссылки:

```
[root@test /]# chkconfig --add httpd
```

```
[root@test /]# chkconfig --level 345 httpd on
```

Конфигурирование Apache HTTP Server с доступом в закрытые каталоги с аутентификацией пользователей (файл /etc/httpd/conf/dbmpasswd)

В рассматриваемом примере мы храним аутентификационную информацию пользователей (логины и пароли) в базе данных, содержащейся в файле `/etc/httpd/dbmpasswd`. Альтернативным вариантом является хранение аутентификационной информации в обычном текстовом файле. Однако этот вариант работает более медленно, поэтому мы его не рассматриваем. Для конфигурирования доступа в закрытые каталоги вашего сервера (`/var/www/eshop/html/private/`и `/var/www/eshopssl/html/private/`), необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Если вы не собираетесь включать поддержку доступа к закрытым каталогам с аутентификацией пользователей, пропустите этот раздел и не забудьте удалить или закомментировать в разделе `Section 1: Global Environment` из файла `/etc/httpd/conf/httpd.conf` строку:

```
LoadModule auth_dbm_module      modules/mod_auth_dbm.so.
```

Шаг 1

Для администрирования базы данных, содержащих аутентификационную информацию пользователей сервера, используется утилита `/usr/sbin/dbmmanage`. Для того, чтобы затруднить несанкционированную модификацию базы данных, переопределите права доступа к утилите:

```
[root@test /]# chmod 510 /usr/sbin/dbmmanage
```

Шаг 2

Добавьте пользователя, которому будет разрешен доступ в закрытые каталоги сервера:

```
[root@test /]# /usr/sbin/dbmmanage /etc/httpd/dbmpasswd adduser shoper
New password:Sh()perpa$ <Enter>
Re-type new password: Sh()perpa$ <Enter>
User shoper added with password encrypted to 7Wj/W4BLeZ4uI using crypt
```

Шаг 3

Проверьте наличие в конфигурационном файле `/etc/httpd/conf/httpd.conf` строки:

```
LoadModule auth_dbm_module      modules/mod_auth_dbm.so
```

необходимой для загрузки встроенного модуля `auth_dbm_module`, обеспечивающего поддержку доступа в закрытые каталоги сервера после удачной аутентификации пользователей.

Конфигурирование поддержки протокола SSL в Apache HTTP Server (файлы /usr/share/ssl/certs/www.crt и /usr/share/ssl/private/www.key)

Для того, чтобы ваш сервер поддерживал защищенные соединения по протоколу HTTPS, необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Если вы не собираетесь включать поддержку протокола SSL, пропустите этот раздел и не забудьте удалить или закомментировать в разделе `Section 1: Global Environment` из файла `/etc/httpd/conf/httpd.conf` строку:

```
LoadModule ssl_module           modules/mod_ssl.so.
```

Шаг 1

Для создания самостоятельно подписанного сертификата необходимо наличие собственного сертификационного центра. Если вы его уже создали, то перейдите к следующему шагу. В противном случае ознакомьтесь с рекомендациями раздела «Тестирование OpenSSL» главы 12 и создайте собственный сертификационный центр.

Шаг 2

Создайте закрытый ключ, не защищенный паролем, для чего перейдите в каталог`/usr/share/ssl`:

```
[root@test /]# cd /usr/share/ssl
```

Выберите пять любых больших файлов со случайным (уникальным) содержанием, скопируйте их в каталог `/usr/share/ssl` и переименуйте в `random1`, `random2`, `random3`, `random4`, `random5`, после чего выполните команду:

```
[root@test ssl]# openssl genrsa -rand ran-
dom1:random2:random3:random4:random5 -out www.key 1024
```

```
2019245 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....................................................++++++
...........++++++
e is 65537 (0x10001)
```

ЗАМЕЧАНИЕ Использование закрытого ключа, не защищенного паролем, не очень желательно, с точки зрения безопасности системы. Поэтому авторы настоятельно рекомендуют все-таки использовать закрытый ключ, защищенный паролем, созданный в соответствии с рекомендациями раздела «Тестирование OpenSSL» главы 12. В случае использования закрытого ключа, защищенного паролем, при загрузке Apache HTTP Server потребует ввода пароля для получения доступа к закрытому ключу.

Рассматриваемый пример, в котором используется закрытый ключ, не защищенный паролем, просто иллюстрирует еще один вариант конфигурации поддержки протокола SSL в Apache HTTP Server.

Шаг 3

Сохраните файл `www.key`, содержащий закрытый ключ, в надежном месте:

```
[root@test ssl]# cp www.key /very_reliable_place/eshop_bruy_info/www.key
```

Шаг 4

Создайте запрос на подтверждение сертификата:

```
[root@test ssl]# openssl req -new -key www.key -out www.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]: <Enter>
State or Province Name (full name) [Moscow]: <Enter>
Locality Name (eg, city) [Yubileyniy]: <Enter>
Organization Name (eg, company) [Valentine Bruy]: <Enter>
Organizational Unit Name (eg, section) [Home]: <Enter>
Common Name (eg, YOUR name) [test.bruy.info]: eshop.bruy.info <Enter>
Email Address [drwalbr@bruy.info]: sales@test.bruy.info <Enter>

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: <Enter>
An optional company name []: <Enter>
```

ЗАМЕЧАНИЕ Обратите внимание, что мы запрашиваем сертификат для виртуального сервера eshop.bruy.info, а не для основного сервера test.bruy.info, т. к. в рассматриваемом примере конфигурации поддержка протокола SSL осуществляется только для виртуального сервера.

Шаг 5

Подпишите сертификат:

```
[root@test ssl]# /usr/share/ssl/misc/sign www.csr
CA signing: www.csr -> www.crt:
Using configuration from ca.config
Enter pass phrase for /usr/share/ssl/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :PRINTABLE:'Moscow'
localityName          :PRINTABLE:'Yubileyniy'
organizationName      :PRINTABLE:'Valentine Bruy'
organizationalUnitName:PRINTABLE:'Home'
commonName            :PRINTABLE:'eshop.bruy.info'
emailAddress          :IA5STRING:'sales@test.bruy.info'
Certificate is to be certified until Jul  9 08:12:16 2004 GMT (365 days)
Sign the certificate? [y/n]:y <Enter>
```

```
1 out of 1 certificate requests certified, commit? [y/n]y <Enter>

Write out database with 1 new entries
Data Base Updated
CA verifying: www.crt <-> CA cert
www.crt: OK
```

Шаг 6

Сохраните файл `www.crt`, содержащий сертификат, в надежном месте:

```
[root@test ssl]# cp www.crt /very_reliable_place/eshop_bruy_info/www.crt
```

Шаг 7

Поместите файлы `www.crt` и `www.key` в каталоги, определенные директивами `SSLCertificateFile` и `SSLCertificateKeyFile` в конфигурационном файле `/etc/httpd/conf/httpd.conf`. Определите права доступа к ним и назначьте их владельцем пользователя `www`, от имени которого запускается Apache HTTP Server :

```
[root@test ssl]# mv www.key  private/
[root@test ssl]# mv www.crt  certs/
[root@test ssl]# chmod 400 private/www.key
[root@test ssl]# chmod 400 certs/www.crt
[root@test ssl]# chown www.www private/www.key
[root@test ssl]# chown www.www certs/www.crt
```

Шаг 8

Проверьте наличие в конфигурационном файле `/etc/httpd/conf/httpd.conf` строки:

```
LoadModule ssl_module           modules/mod_ssl.so
```

необходимой для загрузки встроенного модуля `ssl_module`, обеспечивающего поддержку протокола SSL.

Тестирование Apache HTTP Server

Для проверки работоспособности рассматриваемой конфигурации сервера необходимо выполнить следующие операции:

Шаг 1

Создайте каталоги и разместите в них файлы, обслуживаемые виртуальными серверами в соответствии с настройками, определенными в `/etc/httpd/conf/httpd.conf`, например:

```
[root@test /]# mkdir /var/www/eshop
[root@test /]# mkdir /var/www/eshop/html
[root@test /]# mkdir /var/www/eshop/cgi-bin
[root@test /]# mkdir /var/www/eshop/html/private
[root@test /]# mkdir /var/www/eshopssl
[root@test /]# mkdir /var/www/eshopssl/html
[root@test /]# mkdir /var/www/eshopssl/cgi-bin
[root@test /]# mkdir /var/www/eshopssl/html/private
```

Поместите в каталог `/var/www/eshop/html` файл `index.html`, содержащий следующие строки:

```
<html>
<title>Главная страница e-shop (http-доступ)</title>
<body>
<H1>Главная страница e-shop (http-доступ)</H1>
<a href="private/">Каталог с ограниченным доступом (http-доступ)</a>
</body>
<html>
```

Поместите в каталог `/var/www/eshop/html/private` файл `index.html`, содержащий следующие строки:

```
<html>
<title>Страница e-shop с ограниченным доступом(hhtp-доступ)</title>
<body>
<H1>Страница e-shop с ограниченным доступом(http-доступ)</H1>
</body>
```

```
<html>
```

Поместите в каталог `/var/www/eshopssl/html` файл `index.html`, содержащий следующие строки:

```
<html>
<title>Главная страница e-shop (https-доступ)</title>
<body>
<H1>Главная страница e-shop (https-доступ)</H1>
<a href="private/">Каталог с ограниченным доступом (https-доступ)</a>
</body>
<html>
```

Поместите в каталог `/var/www/eshopssl/html/private` файл `index.html`, содержащий следующие строки:

```
<html>
<title>Страница e-shop с ограниченным доступом (https-доступ)</title>
<body>
<H1>Страница e-shop с ограниченным доступом (https-доступ)</H1>
</body>
<html>
```

Шаг 2

Запустите Apache HTTP Server:

```
[root@test /]# /etc/init.d/httpd start
Запускается httpd:                 [OK]
```

Вполне возможно, что из-за ошибок в конфигурационных файлах вам не удастся запустить Apache HTTP Server, при этом вы получите сообщение вида:

```
[root@test /]# /etc/init.d/httpd start
Запускается Apache: Syntax error on line 252 of
/etc/httpd/conf/httpd.conf:
TransferLog takes one argument, the filename of the access log
                                   [СБОЙ]
```

В этом случае исправьте ошибки в конфигурационном файле `/etc/httpd/conf/httpd.conf`, руководствуясь ссылкой на номер строки и описанием ошибки в полученном сообщении. После устранения ошибки попытайтесь повторно запустить Apache HTTP.

Шаг 3

После удачного запуска сервера проверьте наличие доступа к каталогам и файлам, к которым он должен быть разрешен, а также отсутствие доступа к каталогам и файлам, к которым он должен быть запрещен. В ниже приведенном примере сервер тестировался с использованием текстового браузера. Если вы используете другой браузер, внешнее представление результатов тестирования будет выглядеть, скорее всего, по-другому.

Попытайтесь обратиться к индексному файлу виртуального сервера http://eshop.bruy.info/, поддерживающего соединения по протоколу HTTP:

```
[karlnext@karlnext karlnext]$ lynx http://eshop.bruy.info
```

На экране вы должны увидеть примерно следующее:

```
 Главная страница e-shop (http-доступ)

                    Главная страница e-shop (http-доступ)

   Каталог с ограниченным доступом (http-доступ)
…
Команды: стрелки - перемещение, '?' - помощь, 'q' - выход, '<-' - назад.
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Попробуйте перейти по ссылке

```
Каталог с ограниченным доступом (http-доступ)
```

в закрытый каталог сервера, т. к. это единственная ссылка на странице. Для этого необходимо просто нажать клавишу <Enter>. В результате вы должны увидеть примерно следующее:

```
Главная страница e-shop (http-доступ)

                    Главная страница e-shop (http-доступ)

   Каталог с ограниченным доступом (http-доступ)
…
Имя пользователя для 'Restricted Section' на server
'eshop.bruy.info':shoper
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Введите имя пользователя `shoper`, как показано выше, которому разрешен доступ в закрытый каталог, и нажмите клавишу <Enter>:

```
Главная страница e-shop (http-доступ)

                    Главная страница e-shop (http-доступ)

   Каталог с ограниченным доступом (http-доступ)
…
Пароль: **********
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Введите пароль для пользователя `shoper` и нажмите клавишу <Enter>. В результате вы получите доступ к индексному файлу закрытого каталога и увидите примерно следующее:

```
Страница e-shop с ограниченным доступом(hhtp-доступ)

            Страница e-shop с ограниченным доступом(http-доступ)
…
Команды: стрелки - перемещение, '?' - помощь, 'q' - выход, '<-' - назад.
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Завершите работу с браузером, используя подсказку в нижней части экрана.

Для тестирования доступа к виртуальному серверу, поддерживающего соединения по протоколу HTTPS, наберите:

```
[karlnext@karlnext karlnext]$ lynx https://eshop.bruy.info
```

Вы должны увидеть примерно следующее:

```
Главная страница e-shop (https-доступ)

                    Главная страница e-shop (https-доступ)

   Каталог с ограниченным доступом (https-доступ)
…
Команды: стрелки - перемещение, '?' - помощь, 'q' - выход, '<-' - назад.
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Попробуйте перейти по ссылке

```
Каталог с ограниченным доступом (httpS-доступ)
```

в закрытый каталог сервера, т. к. это единственная ссылка на странице. Для этого необходимо просто нажать клавишу <Enter>, после чего вы должны увидеть следующую информацию:

```
Главная страница e-shop (https-доступ)

                    Главная страница e-shop (https-доступ)
```

```
   Каталог с ограниченным доступом (https-доступ)
…
Имя пользователя для 'Restricted Section' на server
'eshop.bruy.info:443':shoper
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Введите имя пользователя `shoper`, которому разрешен доступ в закрытый каталог, и нажмите клавишу <Enter>:

```
Главная страница e-shop (https-доступ)

                    Главная страница e-shop (https-доступ)

   Каталог с ограниченным доступом (https-доступ)
…
Пароль: **********
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Введите пароль для пользователя `shoper` и нажмите клавишу <Enter>. В результате вы получите доступ к индексному файлу закрытого каталога и увидите примерно следующее:

```
Страница e-shop с ограниченным доступом (https-доступ)

            Страница e-shop с ограниченным доступом (https-доступ)
…
Команды: стрелки - перемещение, '?' - помощь, 'q' - выход, '<-' - назад.
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

Завершите работу с браузером.

Выполнение Apache HTTP Server в среде chroot-jail

Потенциальные уязвимости Apache HTTP Server , как и любого другого программного обеспечения, могут использоваться для реализации атак на вашу систему. Поэтому для повышения безопасности вашей системы Apache HTTP Server можно заставить работать в окружении chroot-jail. Это не простая задача. При этом может потребоваться дополнительные и не всегда заканчивающиеся успехом попытки по адаптации программ (сценариев), обслуживаемых сервером, для работы в среде chroot-jail. Тем не менее, если вы все-таки желаете протестировать работоспособность вашего сервера в относительно безопасном окружении, руководствуйтесь ниже приведенными рекомендациями.

Если вы собираетесь использовать Apache HTTP Server с поддержкой PHP и/или модуля `mod_perl`, пропустите этот раздел и вернитесь к нему после инсталляции и настройки поддержки соответствующих модулей в обычной среде. В этом случае перенос необходимых файлов и каталогов в окружение chroot-jail лучше осуществлять сразу для Apache HTTP Server и всех поддерживаемых им модулей сторонних разработчиков, руководствуясь при этом рекомендациями этой и двух последующих глав.

Шаг 1

Остановите Apache HTTP Server:

```
[root@test /]# /etc/init.d/httpd stop
Останавливается httpd:                          [OK]
```

Шаг 2

Создайте каталоги, необходимые для организации окружения chroot-jail:

```
[root@test /]# mkdir -p /chroot/httpd/dev
[root@test /]# mkdir -p /chroot/httpd/lib
[root@test /]# mkdir -p /chroot/httpd/etc
[root@test /]# mkdir -p /chroot/httpd/var/www/
[root@test /]# mkdir -p /chroot/httpd/tmp/
[root@test /]# chmod 777 /chroot/httpd/tmp/
```

```
[root@test /]# chmod +t /chroot/httpd/tmp/
[root@test /]# mkdir -p /chroot/httpd/usr/lib
[root@test /]# mkdir -p /chroot/httpd/usr/sbin
[root@test /]# mkdir -p /chroot/httpd/var/log
[root@test /]# mkdir -p /chroot/httpd/var/run
[root@test /]# mkdir -p /chroot/httpd/lib/i686
[root@test /]# mkdir -p /chroot/httpd/usr/lib/modules
[root@test /]# mkdir -p /chroot/httpd/var/run/
[root@test /]# mkdir -p /chroot/httpd/usr/lib/modules
[root@test /]# mkdir -p /chroot/httpd/usr/lib/build
```

Шаг 3

Перенесите исполняемые файлы Apache HTTP Server и необходимые для его нормальной работы библиотеки в каталоги окружения chroot-jail:

```
[root@test /]# mv /var/www /chroot/httpd/var/
[root@test /]# mv /etc/httpd /chroot/httpd/etc
[root@test /]# mv /var/log/httpd /chroot/httpd/var/log/
[root@test /]# mv /usr/sbin/ab /chroot/httpd/usr/sbin
[root@test /]# mv /usr/sbin/apxs /chroot/httpd/usr/sbin
[root@test /]# mv /usr/sbin/checkgid /chroot/httpd/usr/sbin/
[root@test /]# mv /usr/sbin/dbmmanage /chroot/httpd/usr/sbin/
[root@test /]# mv /usr/sbin/htdbm /chroot/httpd/usr/sbin/
[root@test /]# mv /usr/sbin/htdigest /chroot/httpd/usr/sbin/
[root@test /]# mv /usr/sbin/htpasswd /chroot/httpd/usr/sbin/
[root@test /]# mv /usr/sbin/httpd /chroot/httpd/usr/sbin/
[root@test /]# mv /usr/sbin/logresolve /chroot/httpd/usr/sbin/
[root@test /]# mv /usr/sbin/rotatelogs /chroot/httpd/usr/sbin/
[root@test /]# mknod /chroot/httpd/dev/null c 1 3
[root@test /]# chmod 666 /chroot/httpd/dev/null
[root@test /]# mknod /chroot/httpd/dev/urandom c 1 9
[root@test /]# chown www.www /chroot/httpd/usr/share/ssl/certs
[root@test /]# chown www.www /chroot/httpd/usr/share/ssl/private
[root@test /]# mv /usr/share/ssl/private/www.key
/chroot/httpd/usr/share/ssl/private/
[root@test /]# mv /usr/share/ssl/certs/www.crt
/chroot/httpd/usr/share/ssl/certs/
[root@test /]# mv /usr/lib/httpd/modules/*
/chroot/httpd/usr/lib/httpd/modules/
[root@test /]# mv /usr/lib/httpd/build/*
/chroot/httpd/usr/lib/httpd/build/
```

ЗАМЕЧАНИЕ Лучше сразу не переносить соответствующие файлы и каталоги, а скопировать их. В этом случае, если ваш сервер будет работоспособен в окружении chroot-jail, вы в дальнейшем всегда сможете уничтожить более не нужные файлы, созданные при инсталляции и конфигурировании сервера в обычной среде. В случае, если сервер окажется не работоспособным, вы сможете вернуться к прежней работоспособной конфигурации.

Шаг 4

Создайте список библиотек, используемых демоном `httpd`, анализируя вывод следующей команды:

```
[root@test /]# ldd /chroot/httpd/usr/sbin/httpd
        libssl.so.0.9.7 => /lib/libssl.so.0.9.7 (0x4753d000)
        libcrypto.so.0.9.7 => /lib/libcrypto.so.0.9.7 (0x4756d000)
        libaprutil-0.so.0 => /usr/lib/libaprutil-0.so.0(0x47673000)
        libgdbm.so.2 => /usr/lib/libgdbm.so.2 (0x47689000)
        libdb-3.3.so => /lib/libdb-3.3.so (0x4768f000)
        libexpat.so.0 => /usr/lib/libexpat.so.0 (0x4771e000)
        libapr-0.so.0 => /usr/lib/libapr-0.so.0 (0x4773d000)
        libpthread.so.0 => /lib/i686/libpthread.so.0 (0x4775d000)
        librt.so.1 => /lib/librt.so.1 (0x47771000)
        libm.so.6 => /lib/i686/libm.so.6 (0x47782000)
        libnsl.so.1 => /lib/libnsl.so.1 (0x477a4000)
        libdl.so.2 => /lib/libdl.so.2 (0x477b9000)
        libc.so.6 => /lib/i686/libc.so.6 (0x477bc000)
        /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x47525000)
```

В результате вы получите список используемых библиотек. Однако, их не всегда бывает достаточно для нормального функционирования демона `httpd`:

- `/lib/libssl.so.0.9.7`;
- `/lib/libcrypto.so.0.9.7`;
- `/usr/lib/libaprutil-0.so.0`;
- `/usr/lib/libgdbm.so.2`;
- `/lib/libdb-3.3.so`;
- `/usr/lib/libexpat.so.0`;
- `/usr/lib/libapr-0.so.0;`
- `/lib/i686/libpthread.so.0`;
- `/lib/librt.so.1`;
- `/lib/i686/libm.so.6`;
- `/lib/libnsl.so.1`;
- `/lib/libdl.so.2`;
- `/lib/i686/libc.so.6`;
- `/lib/ld-linux.so.2`.

Последовательно применяя подобный алгоритм к другим исполняемым файлам и найденным на предыдущем шаге библиотекам (доказательства сходимости этого процесса авторы по соображениям экономии места опускают), было получено следующее дополнение к списку библиотек, необходимых для нормальной работы сервера:

- `/lib/libnss_compat*`;
- `/lib/libnss_dns*`;
- `/lib/libnss_files*`;
- `/lib/libresolv.so.2`.

Шаг 5

Скопируйте необходимые библиотеки в соответствующие каталоги:

```
[root@test /]# cp /lib/libssl.so.0.9.7 /chroot/httpd/lib/
[root@test /]# cp /lib/libcrypto.so.0.9.7 /chroot/httpd/lib/
[root@test /]# cp /usr/lib/libaprutil-0.so.0 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libgdbm.so.2 /chroot/httpd/usr/lib/
[root@test /]# cp /lib/libdb-3.3.so /chroot/httpd/lib/
[root@test /]# cp /usr/lib/libexpat.so.0 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libapr-0.so.0 /chroot/httpd/usr/lib/
[root@test /]# cp /lib/i686/libpthread.so.0 /chroot/httpd/lib/i686/
[root@test /]# cp /lib/librt.so.1 /chroot/httpd/lib/
[root@test /]# cp /lib/i686/libm.so.6 /chroot/httpd/lib/i686/
[root@test /]# cp /lib/libnsl.so.1 /chroot/httpd/lib/
[root@test /]# cp /lib/libdl.so.2 /chroot/httpd/lib/
[root@test /]# cp /lib/ld-linux.so.2 /chroot/httpd/lib/
[root@test /]# cp /lib/i686/libc.so.6 /chroot/httpd/lib/i686/
[root@test /]# cp /lib/libnss_compat* /chroot/httpd/lib/
[root@test /]# cp /lib/libnss_dns* /chroot/httpd/lib/
[root@test /]# cp /lib/libnss_files* /chroot/httpd/lib/
[root@test /]# cp /lib/libresolv.so.2 /chroot/httpd/lib/
```

Шаг 6

Скопируйте в соответствующий каталог файлы `/etc/passwd` и `/etc/group`:

```
[root@test /]# cp /etc/passwd /chroot/httpd/etc/
[root@test /]# cp /etc/group /chroot/httpd/etc/
```

и удалите из них все записи, не имеющие отношения к учетным записям пользователя `WWW` и группы пользователей `WWW`.

Шаг 7

Скопируйте в соответствующие каталоги файлы, также необходимые для нормальной работы демона `httpd`:

```
[root@test /]# cp /etc/resolv.conf /chroot/httpd/etc/
[root@test /]# cp /etc/localtime /chroot/httpd/etc/
```

```
[root@test /]# cp /etc/hosts /chroot/httpd/etc/
```

Шаг 8

Сделайте соответствующие файлы «неизменяемыми":

```
[root@test /]# chattr +i /chroot/httpd/etc/passwd
[root@test /]# chattr +i /chroot/httpd/etc/group
[root@test /]# chattr +i /chroot/httpd/etc/resolv.conf
[root@test /]# chattr +i /chroot/httpd/etc/hosts
```

Шаг 9

Отредактируйте файл инициализации `/etc/init.d/httpd` в соответствии с ниже приведенными рекомендациями:

```
#!/bin/bash
# This shell script takes care of starting and stopping Apache.
#
# chkconfig: 345 85 15
# description: Apache is a World Wide Web server. It is used to serve \
#              HTML files and CGI.
#
# processname: httpd
# config: /chroot/httpd/etc/httpd/conf/httpd.conf
# pidfile: /chroot/httpd/var/run/httpd.pid
#
# Source function library.
. /etc/init.d/functions

# Source networking configuration.
. /etc/sysconfig/network

# Source for additional options if we have them.
if [ -f /etc/sysconfig/httpd ] ; then
        . /etc/sysconfig/httpd
fi

# This will prevent initlog from swallowing up a pass-phrase prompt if
# mod_ssl needs a pass-phrase from the user.
INITLOG_ARGS=""

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# If Apache is not available stop now.
[ -f /chroot/httpd/usr/sbin/httpd ] || exit 0

# Path to the Apache apachectl script and server binary.
apachectl=/usr/sbin/apachectl
httpd=/usr/sbin/httpd

RETVAL=0
prog="httpd"

start() {
        echo -n $"Starting $prog: "
        /usr/sbin/chroot /chroot/httpd /usr/sbin/httpd $OPTIONS
        #daemon $httpd $OPTIONS
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && touch /var/lock/subsys/httpd
        return $RETVAL
}

stop() {
        echo -n $"Shutting down $prog: "
        kill -TERM `cat /chroot/httpd/var/run/httpd.pid`
```

```
        #killproc $httpd
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && rm -f /var/lock/subsys/httpd
/var/run/httpd.pid
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        #status $httpd
        status /chroot/httpd/usr/sbin/httpd
        RETVAL=$?
        ;;
  restart)
        stop
        start
        RETVAL=$?
        ;;
*)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 1
esac
exit $RETVAL
```

Шаг 10

Запустите Apache HTTP Server:

```
[root@test /]# /etc/init.d/httpd start
Запускается httpd:                 [OK]
```

Шаг 11

Для того, чтобы проверить, работает ли сервер в окружении chroot-jail, определите идентификационный номер основного и дочерних процессов, используя команду:

```
[root@test /]# ps –axf | grep httpd
10596 ?        S      0:00 /usr/sbin/httpd -DSSL
21501 ?        S      0:00  \_ /usr/sbin/httpd -DSSL
25530 ?        S      0:00  \_ /usr/sbin/httpd -DSSL
 3425 ?        S      0:00  \_ /usr/sbin/httpd -DSSL
17995 ?        S      0:00  \_ /usr/sbin/httpd -DSSL
18381 ?        S      0:00  \_ /usr/sbin/httpd –DSSL
```

Убедитесь, что основной и дочерние процессы работают в окружении chroot-jail:

```
[root@test /]# ls -la /proc/10596/root
lrwxrwxrwx    1 root     root            0 Июл 14 11:12 /proc/10596/root
-> /chroot/httpd
[root@test /]# ls -la /proc/21501/root
lrwxrwxrwx    1 root     root            0 Июл 14 11:13 /proc/21501/root
-> /chroot/httpd
```

Шаг 12

Протестируйте работоспособность сервера с использованием рекомендаций раздела «Тестирование Apache HTTP Server». Результаты тестирования должны быть идентичны результатам, полученным при тестировании работоспособности сервера, запущенного в обычном окружении.

Глава 35

PHP: Hypertext Preprocessor

В этой главе:

Возможно, что сокращение PHP впервые было использовано для обозначения языка сценариев, первая версия которого была разработана в середине девяностых годов Расмусом Лердорфом (Rasmus Lerdorf) и имела название Personal Home Page Tools. В настоящее время разработчики проекта под сокращением PHP подразумевают рекурсивный акроним от словосочетания "PHP: Hypertext Preprocessor". PHP: Hypertext Preprocessor – это широко используемый язык программирования общего назначения с открытым исходным кодом. Он очень удобен при реализации различных Web-проектов и даже может внедряться в HTML-код страниц, динамически изменяя их содержание.

Простейшим примером использования PHP является отображение большого числа страниц с одинаковым HTML-кодом в начале и конце файла. Можно предложить несколько вариантов реализации представленной задачи. Первый метод заключается в том, что:

1) постоянная часть кода, находящаяся в начале страницы, сохраняется в файле `top.php`:

```
<?php?>
 <!-- Начало верхней части HTML-кода -->
 <html>
 <head>
<title> Пример использования PHP </title>
</head>
 <body>
…
 <!-- Конец верхней части HTML-кода -->
```

2) постоянная часть кода, находящаяся в конце страницы, сохраняется в файле `down.php`:

```
<?php?>
 <!—Начало нижней части HTML-кода -->
…
</body>
 </html>
<!-- Конец нижней части HTML-кода -->
```

3) объединения с помощью файла `union12345.php`, содержащего следующие строки:

```
<?php?>
 <?
  Include("top.php");
?>
<p>Смысловое содержание страницы</p>
 <?
   Include("down.php");
 ?>
```

Если эти файлы будут размещены в каталоге, обслуживаемом Web-сервером, поддерживающим PHP, то при обращении к файлу `union12345.php` в клиентском браузере будет отображена страница, содержащая следующий HTML-код:

```
<!-- Начало верхней части HTML-кода -->
<html>
<head>
<title> Пример использования PHP </title>
</head>
<body>
…
 <!-- Конец верхней части HTML-кода -->
<p>Смысловое содержание страницы</p>
<!—Начало нижней части HTML-кода -->
…
</body>
 </html>
<!-- Конец нижней части HTML-кода -->
```

В рассматриваемом примере HTML-код генерируется только при получении запроса от браузера на доступ к файлу `union12345.php`. При этом увеличивается нагрузка на процессор и оперативную память системы, на которой установлен сервер. Но при большом количестве имеющих одинаковую структуру файлов сокращаются требования к объему дискового пространства, так как общие для всех файлов части кода хранятся на сервере в единственном экземпляре. Динамическая генерация кода HTML-страниц с использованием PHP возможна при установке модуля `php4_module` и интеграции его с Apache HTTP Server.

Другим способом решения поставленной задачи является генерация страниц на системе, используемой для администрирования Web-сервера с использованием PHP в режиме командной строки. В этом случае

итоговый код может быть сгенерирован с помощью следующей команды (предполагается, что файлы `top.php`, `down.php` и `union12345.php` находятся в текущем каталоге):

```
[karlnext@test karlnext]$ php union12345.php > union12345.html
```

В результате выполнения команды будет сгенерирован файл `union12345.html`, код которого будет идентичен итоговому коду, приведенному выше. Этот файл может быть размещен в соответствующем каталоге Web-сервера. При таком подходе существенно снижаются требования к производительности процессора и объему оперативной памяти, на которой установлен сервер, но увеличиваются требования к объему жестких дисков. В этом случае нет необходимости интеграции модуля `php4_module` с Apache HTTP Server, а вполне достаточно просто установить PHP.

В любом случае, если вы хотите использовать PHP для решения каких-либо задач, вам необходимо ознакомиться с прекрасно написанной документацией, доступной на сервере разработчиков, существенная часть которой переведена на русский язык. В этой главе рассматриваются лишь вопросы установки PHP и интеграции его с Apache HTTP Server.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

В случае, если вы не используете ядро, входящее в комплект поставки ASPLinux 7.3 версии 2.4.18-5asp или ядро, созданное в соответствии с рекомендациями главы 6, может потребоваться перекомпиляция ядра. Одному из пользователей – тестировавшему установку программного обеспечения в соответствии с инструкциями, приведенными в этой главе, на ядре версии 2.4.20, исходные коды которого были модифицированы патчем Grsecurity – пришлось перекомпилировать ядро для отключения опций `CONFIG_GRKERNSEC_PAX_*`.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта PHP: Hypertext Preprocessor по состоянию на 14.07.2003. Регулярно посещайте домашнюю страницу проекта `http://www.php.net/`и отслеживайте обновления.

Исходные коды PHP: Hypertext Preprocessor содержатся в архиве `php-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `php-4.3.2.tar.gz`).

Для инсталляции и нормальной работы `php4_module` должен быть установлен Apache HTTP Server.

Если вы собираетесь включить в поддержку сервера баз данных MySQL, установите сервер баз данных MySQL в соответствии с рекомендациями главы 31.

Если вы собираетесь использовать PHP с поддержкой протокола SSL, установите OpenSSL в соответствии с рекомендациями главы 12.

Кроме того, для нормальной инсталляции и работы PHP необходимо, чтобы на вашей системе были установлены следующие пакеты:

- `MySQL-devel-4.0.13-0.i386.rpm`;
- `autoconf-2.13-17.noarch.rpm`;
- `automake-1.4p5-4.noarch.rpm`;
- `bzip2-devel-1.0.2-2.i386.rpm`;
- `dmalloc-4.8.1-6.i386.rpm`;
- `file-3.37-5.i386.rpm`;
- `freetype-2.0.9-2.i386.rpm`;
- `freetype-devel-2.0.9-2.i386.rpm`;
- `gd-1.8.4-4.asp.i386.rpm`;
- `gd-devel-1.8.4-4.asp.i386.rpm`;
- `gmp-devel-4.0.1-3.i386.rpm`;
- `libjpeg-6b-19.i386.rpm`;
- `libjpeg-devel-6b-19.i386.rpm`;
- `libpng-1.0.12-2.i386.rpm`;
- `libpng-devel-1.0.12-2.i386.rpm`;
- `pam-devel-0.75-32.2asp.i386.rpm`;

- perl-5.6.1-34.99.6.i386.rpm;
- pspell-0.12.2-8asp.i386.rpm;
- pspell-devel-0.12.2-8asp.i386.rpm;
- zlib-devel-1.1.3-25.7.i386.rpm.

Многие из этих пакетов были установлены на предыдущих этапах инсталляции программного обеспечения.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлены ли пакеты программ из списка, представленного выше. Используйте, например, команду вида:

```
[root@test /]# rpm –iq MySQL-devel
```

Шаг 2

Перейдите в каталог, где находятся пакеты. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог /home/distrib, то выполните команду:

```
[root@test /]# cd /home/distrib
```

Шаг 3

Установите недостающие пакеты. Если вы следовали за установкой, предлагаемой в этой книге, вам останется лишь установить:

```
[root@test distrib]# rpm -ihv MySQL-devel-4.0.13-0.i386.rpm \
bzip2-devel-1.0.2-2.i386.rpm \
dmalloc-4.8.1-6.i386.rpm \
pam-devel-0.75-32.2asp.i386.rpm\
php-4.1.2-7.i386.rpm
```

После установки пакетов перейдите к настройке программы PHP.

Компиляция, оптимизация и инсталляция PHP

Для инсталляции PHP из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами с использованием процедур, описанных в шаге 1, радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами PHP в каталоге /var/tmp:

```
[root@test tmp]# tar xzpf php-4.3.2.tar.gz
```

Шаг 3

Сконфигурируйте исходные коды PHP:

```
[root@test tmp]# cd php-4.3.2
[root@test php-4.3.2]# export CFLAGS="-O2 -march=i686 -funroll-loops –
D_REENTRANT -fPIC"
export LIBS="-lttf -lfreetype -lpng -ljpeg -lz -lnsl"
EXTENSION_DIR=/usr/lib/php4
./configure \
--prefix=/usr \
--exec-prefix=/usr \
--with-layout=GNU \
--with-apxs2=/usr/sbin/apxs \
```

```
--with-config-file-path=/etc/httpd \
--with-exec-dir=/usr/bin \
--with-openssl \
--with-zlib \
--with-bz2 \
--with-gd \
--with-ttf \
--with-png \
--with-jpeg-dir=/usr \
--with-png-dir=/usr \
--with-freetype-dir=/usr \
--with-expat-dir=/usr \
--with-gmp \
--with-xml \
--with-pear=/usr/share/pear \
--with-mysql=shared,/usr \
--with-mysql-sock=/var/lib/mysql/mysql.sock \
--with-pspell \
--disable-debug \
--disable-posix \
--disable-rpath \
--disable-posix \
--enable-discard-path \
--enable-safe-mode \
--enable-magic-quotes \
--enable-dmalloc \
--enable-bcmath \
--enable-dio \
--enable-gd-native-ttf \
--enable-sysvsem \
--enable-sysvshm \
--enable-wddx \
--enable-versioning \
--enable-pic \
--enable-inline-optimization \
--enable-memory-limit
```

Шаг 4

Для изменения заданных по умолчанию путей к каталогам, которые не удалось изменить установкой опций команды `./configure`, внесите следующие изменения в файл `/var/tmp/php-4.3.2/Makefile`.

Строку:

```
prefix = /usr/local
```

замените на:

```
prefix = /usr/
```

Строку:

```
includedir = ${prefix}/include
```

замените на:

```
includedir =/usr/include/php4
```

Строку:

```
libdir = ${exec_prefix}/lib/php
```

замените на:

```
libdir = /usr/lib/php4
```

Строку:

```
mandir = ${prefix}/man
```

замените на:

```
mandir = /usr/share/man
```

Строку:

```
prefix = /usr/local
```

замените на:

```
prefix = /usr/
```

Строку:

```
sysconfdir = ${prefix}/etc
```

замените на:

```
sysconfdir = /etc/sysconfig
```

Шаг 5

Откомпилируйте, проинсталлируйте PHP, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test php-4.3.2]# make
[root@test php-4.3.2]# find /* > /root/php1
[root@test php-4.3.2]# make install
...
libtool: install: warning: remember to run `libtool --finish
/var/tmp/php-4.3.2/libs'
chmod 755 /usr/lib/httpd/modules/libphp4.so
[activating module `php4' in /etc/httpd/conf/httpd.conf]
Installing shared extensions:     /usr/lib/php/20020429/
Installing PEAR environment:      /usr/share/pear/
[PEAR] Archive_Tar    - installed: 0.9
[PEAR] Console_Getopt - installed: 1.0
[PEAR] PEAR           - installed: 1.1
[PEAR] DB             - installed: 1.3
[PEAR] HTTP           - installed: 1.2
[PEAR] Mail           - installed: 1.0.1
[PEAR] Net_SMTP       - installed: 1.0
[PEAR] Net_Socket     - installed: 1.0.1
[PEAR] XML_Parser     - installed: 1.0.1
[PEAR] XML_RPC        - installed: 1.0.4
Installing build environment:     /usr/lib/php/build/
Installing header files:          /usr/include/php/php/
Installing helper programs:       /usr/bin/
  program: phpize
  program: php-config
  program: phpextdist
```

Следуя рекомендациям разработчиков, завершите инсталляцию библиотек PHP, для этого скопируйте библиотеки PHP в каталог `/usr/lib/php/`:

```
[root@test php-4.3.2]# cp /var/tmp/php-4.3.2/libs/* /usr/lib/php4/
```

и выполните команду:

```
[root@test php-4.3.2]# libtool --finish /usr/lib/php4/
PATH="$PATH:/sbin" ldconfig -n /usr/lib/php/
----------------------------------------------------------------------
Libraries have been installed in:
   /usr/lib/php/

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
   - add LIBDIR to the `LD_LIBRARY_PATH' environment variable
     during execution
   - add LIBDIR to the `LD_RUN_PATH' environment variable
     during linking
   - use the `-Wl,--rpath -Wl,LIBDIR' linker flag
   - have your system administrator add LIBDIR to `/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
[root@test php-4.3.2]# install -m0640 php.ini-dist /etc/httpd/php.ini
```

```
[root@test php-4.3.2]# strip --strip-debug -R .comment /usr/lib/php4/*.so
[root@test php-4.3.2]# find /* > /root/php2
[root@test php-4.3.2]# diff /root/php1 /root/php2 > /root/php.installed
[root@test php-4.3.2]# mv /root/php.installed
/very_reliable_place/php.installed.YYYYMMDD
```

Шаг 6

Удалите архив и каталог с исходными кодами:

```
[root@test php-4.3.2]# cd /var/tmp/
[root@test tmp]# rm -rf php-4.3.2/
[root@test tmp]# rm -f php-4.3.2.tar.gz
```

Конфигурирование PHP

Конфигурирование PHP осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/httpd/php.ini`;
- файла `/etc/httpd/conf/httpd.conf` (при интеграции PHP с Apache HTTP Server).

Конфигурационный файл /etc/httpd/ php.ini

Отредактируйте файл `/etc/httpd/php.ini`, руководствуясь вашими потребностями и ниже приведенными рекомендациями:

```
[PHP]

; Language Options
engine                          = On
short_open_tag                  = On
asp_tags                        = Off
precision                       = 14
y2k_compliance                  = Off
output_buffering                = Off
output_handler                  =
unserialize_callback_func       =
zlib.output_compression         = On
implicit_flush                  = Off
allow_call_time_pass_reference  = Off


; Safe Mode
safe_mode                       = On
safe_mode_gid                   = Off
safe_mode_include_dir           = ":./usr/share/pear"
safe_mode_exec_dir              =
;open_basedir                   =
safe_mode_allowed_env_vars      = PHP_
safe_mode_protected_env_vars    = LD_LIBRARY_PATH
disable_functions               =


; Font Colors
highlight.string                = #CC0000
highlight.comment               = #FF9900
highlight.keyword               = #006600
highlight.bg                    = #FFFFFF
highlight.default               = #0000CC
highlight.html                  = #000000


; Misc
expose_php                      = Off


; Resource Limits
```

```
max_execution_time              = 30
memory_limit                    = 8M


; Error handling and logging
error_reporting                 = E_ALL
display_errors                  = Off
display_startup_errors          = Off
log_errors                      = On
track_errors                    = Off
html_errors                     = Off
error_log                       = syslog
warn_plus_overloading           = Off


; Data Handling
;arg_separator.output           = "&" ; Default is "&".
;arg_separator.input            = ";&" ; Default is "&".
variables_order                 = "GPCS"
register_globals                = Off
register_argc_argv              = On
post_max_size                   = 8M


; Magic Quotes
magic_quotes_gpc                = Off
magic_quotes_runtime            = Off
magic_quotes_sybase             = Off
auto_prepend_file               =
auto_append_file                =
default_mimetype                = "text/html"
default_charset                 = "koi8-r"
;always_populate_raw_post_data  = On


; Paths and Directories
;include_path                   = ".:/php/includes"
doc_root                        =
user_dir                        =
extension_dir                   = /usr/lib/php
enable_dl                       = Off
; cgi.force_redirect            = On
; cgi.redirect_status_env       =


; File Uploads
file_uploads                    = Off
;upload_tmp_dir                 =
upload_max_filesize             = 1M


; Fopen wrappers
allow_url_fopen                 = On
;from                           = "user@bruy.info"


; Dynamic Extensions
extension                      = mysql.so

[Syslog]
define_syslog_variables         = Off
;sendmail_path                   =
```

```
[SQL]
sql.safe_mode                   = Off


[ODBC]
odbc.allow_persistent           = Off
odbc.check_persistent           = On
odbc.max_persistent             = -1
odbc.max_links                  = -1
odbc.defaultlrl                 = 4096
odbc.defaultbinmode             = 1


[MySQL]
mysql.allow_persistent          = Off
mysql.max_persistent            = -1
mysql.max_links                 = -1
mysql.default_port              =
mysql.default_socket            = /var/lib/mysql/mysql.sock
mysql.default_host              =
mysql.default_user              =
mysql.default_password          =

[bcmath]
bcmath.scale                    = 0


[browscap]
;browscap                       = extra/browscap.ini


[Session]
session.save_handler            = files
session.save_path               = /tmp
session.use_cookies             = 1
session.name                    = PHPSESSID
session.auto_start              = 0
session.cookie_lifetime         = 0
session.cookie_path             = /
session.cookie_domain           =
session.serialize_handler       = php
session.gc_probability          = 1
session.gc_maxlifetime          = 1440
session.referer_check           =
session.entropy_length          = 0
session.entropy_file            =
;session.entropy_length         = 16
;session.entropy_file           = /dev/urandom
session.cache_limiter           = nocache
session.cache_expire            = 180
session.use_trans_sid           = 0
url_rewriter.tags               =
"a=href,area=href,frame=src,input=src,form=fakeentry"


[Assertion]
;assert.active                  = On
;assert.warning                 = On
;assert.bail                    = Off
;assert.callback                = 0
;assert.quiet_eval              = 0


[Sockets]
```

```
sockets.use_system_read         = On
```

Ниже приведены краткие описания наиболее критичных, с точки зрения обеспечения безопасности и производительности сервера, директив, используемых в приведенном выше конфигурационном файле. С описаниями остальных директив вы можете ознакомиться в документации по PHP.

Директива:

```
engine = On
```

обычно используется для включения и отключения возможности интерпретации файлов, содержащих PHP-код, в некоторых каталогах и виртуальных серверах при интеграции PHP с Apache HTTP Server. В рассматриваемой тривиальной конфигурации мы разрешаем интерпретацию файлов, содержащих PHP-код, во всех каталогах сервера. С примерами более сложных вариантов конфигурации можно ознакомится в документации по PHP и Apache HTTP Server.

Директива:

```
short_open_tag = On
```

используется для включения и отключения обработки тэгов сокращенной формы открывающего PHP-тэга - `<? ?>`, значение которых эквивалентно тэгу `<?php ?>`. Если вы планируете использовать PHP совместно с XML, отключите эту опцию. Отключение этой опции может потребовать внесения изменений в PHP-коды программного обеспечения, используемого на вашем сервере, т. к. использование сокращенных тэгов очень популярно у многих разработчиков.

Директива:

```
asp_tags = Off
```

используется для включения и отключения обработки тэгов вида `<% %>`, в дополнение к обычным тегам `<?php ?>`. Включение это опции имеет смысл, если вы используете программное обеспечение, написанное на ASP (Active Server Page).

Директива:

```
precision = 14
```

используется для определения количества знаков в числах в формате плавающей точки.

Директива:

```
y2k_compliance = Off
```

используется для включения принудительной поддержки в PHP средств предотвращения ошибок 2000 года. Включение этой опции может сделать ваш сервер недоступным для старых браузеров.

Директива

```
output_buffering = Off
```

используется для включения и отключения буферизации вывода. При включенной опции PHP сможет отправлять заголовки, например, `cookies`, даже после передачи основного содержания. Для повышения производительности сервера мы рекомендуем отключить эту опцию, используя значение по умолчанию – "off".

Директива:

```
output_handler =
```

используется для перенаправления вывода сценариев PHP-кода в некоторую функцию. Эта возможность может быть использована, например, для передачи клиентским программам, поддерживающим gzip-перекодировку, содержания документа в сжатом виде. Использование это опции предъявляет достаточно высокие требования к производительности сервера, и поэтому мы рекомендуем не использовать ее, оставив соответствующую строку пустой.

Директива:

```
zlib.output_compression = On
```

используется для включения и выключения сжатия файлов, отправляемых клиентским программам с использованием функций библиотеки zlib. Включение этой опции может существенно повысить время их получения пользователями, подключенных к Интернет через каналы связи с малой пропускной способностью, увеличивая при этом нагрузку на оперативную память и процессор.

Директива:

```
implicit_flush = Off
```

обычно используется при отладке и негативно влияет на производительность сервера. Во всех других случаях рекомендуется ее отключить.

Директива:

```
allow_call_time_pass_reference = Off
```

используется для включения и выключения возможности передачи функциям аргументов не в виде значений, а в виде ссылок на соответствующие значения. По умолчанию для этой опции установлено значение On. Протестируйте работоспособность ваших программ при значении "off", и если программы будут работать нормально, оставьте его. В противном случае установите значение "on".

Директива:

```
safe_mode = On
```

является одной из наиболее важных, с точки зрения обеспечения безопасности вашего сервера, директив. При ее включении PHP осуществляет проверку владельца обрабатываемого сценария и в случае вызова

функций, обращающихся к файлам, разрешает доступ к ним только, если установленные ограничения на доступ к файлу позволяет пользователю, от имени которого выполняется сценарий, получать доступ к файлу. Это может вызывать определенные проблемы при эксплуатации и инсталляции некоторых программ, написанных на PHP.

Директива

```
safe_mode_gid = Off
```

используется для смягчения ограничений, устанавливаемых директивой `safe_mode`. При ее включении (`safe_mode_gid = On`) доступ к файлам осуществляется только по результатам сравнения группы пользователя, от имени которого выполняется сценарий, и группы пользователя владельца файла, к которому сценарий обращается.

Директива:

```
safe_mode_include_dir = /var/lib/mysql
```

используется для отмены ограничений, устанавливаемых директивами `safe_mode` и `safe_mode_gid` для определенного каталога. В рассматриваемом примере – это каталог `/var/lib/mysql`, содержащий файлы баз данных.

Директива:

```
safe_mode_exec_dir =
```

используется для отмены ограничений, накладываемых включением опции `safe_mode` на выполнение функций PHP в определенных каталогах.

Директива:

```
;open_basedir =
```

используется для наложения ограничений при включенной опции `safe_mode` на все операции с файлами в определенных каталогах. Использование этой директивы открывает широкие возможности при конфигурировании отдельных каталогов и виртуальных серверов.

Директива:

```
safe_mode_allowed_env_vars = PHP_
```

используется для определения списка, содержащего префиксы имен переменных, разделенных запятыми, изменение которых разрешено пользователям при включенной опции `safe_mode`.

Директива:

```
safe_mode_protected_env_vars = LD_LIBRARY_PATH
```

используется для определения списка переменных окружения, которые не должны изменяться пользователями при включенной опции `safe_mode`.

Директива:

```
disable_functions =
```

определяет список функций, использование которых запрещено.

Директива:

```
expose_php = Off
```

используется для включения и отключения возможности присутствия в заголовках, выдаваемых Web-сервером, информации о наличии PHP на сервере. Для исключения этой информации из заголовков измените устанавливаемое значение по умолчанию "on" на "off".

Директива:

```
display_errors = Off
```

используется для включения и отключения вывода сообщений пользователям об ошибках. Мы настоятельно рекомендуем установить значение "off", т. к. сообщения об ошибках содержат много конфидециальной информации, например, о путях к различным файлам, находящимся на вашем сервере.

Директива:

```
log_errors = On
```

используется для включения регистрации сообщений об ошибках связанных, с выполнением сценариев PHP. Совместное использование этой и предыдущей директивы позволяет организовать отладку PHP-сценариев без разглашения конфиденциальной информации о структуре каталогов сервера обычным пользователям.

Дирекитива:

```
register_globals = Off
```

используется для предотвращения изменения различных переменных путем импортирования соответствующих выражений в информацию, легитимно принимаемую сервером от внешних пользователей. К сожалению, некоторые написанные на PHP программы не могут нормально работать при отключении этой опции. Попробуйте установить значение `register_globals = Off`, протестируйте работоспособность вашего программного обеспечения. Если все работает нормально, оставьте выбранное значение, в противном случае измените его на "on".

Директива:

```
enable_dl = Off
```

используется для разрешения и запрещения использования функции PHP `dl()`, предназначенной для динамической загрузки расширений PHP. Использование значения "on" опасно, т. к. позволяет легко обойти все ограничения, накладываемые директивами `safe_mode` и `open_basedir`.

Директива:

```
file_uploads = Off
```

используется для разрешения и запрещения загрузки файлов на сервер. Настоятельно рекомендуем запретить использование загрузки файлов на сервер.

Директива вида:

```
extension = mysql.so
```

используется для разрешения использования расширений, обеспечивающих поддержку взаимодействия PHP с внешними приложениями. В рассматриваемом примере мы разрешили использование расширений, реализующих поддержку взаимодействия PHP с сервером баз данных MySQL.

Конфигурационный файл /etc/httpd/conf/httpd.conf

Для интеграции PHP с Apache HTTP Server необходимо выполнить следующие операции.

Шаг 1

Добавьте в конец подраздела `Dynamic Shared Object (DSO) Support` файла `/etc/httpd/conf/httpd.conf` следующую строку:

```
LoadModule php4_module        /usr/lib/httpd/modules/libphp4.so
```

Шаг 2

Проверьте наличие и при необходимости добавьте в файл `/etc/httpd/conf/httpd.conf` следующие строки:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php .php3
AddType application/x-httpd-php .php4
AddType application/x-httpd-php .phtml
AddType application/x-httpd-php .shtml
AddType application/x-httpd-php-source .phps
```

Тестирование PHP

Войдите с систему от имени обычного пользователя, например, `karlnext`.

Шаг 1

Проверьте работоспособность PHP в режиме командной строки, для этого создайте файл `index.php`, содержащий следующие строки:

```
<?php
    echo phpinfo();
?>
```

и выполните команду:

```
[karlnext@test karlnext]$ php index.php
```

Если на экране вы увидите примерно следующее (для экономии места мы приводим только несколько первых строк вывода):

```
phpinfo()
PHP Version => 4.3.2

System => Linux test.bruy.info 2.4.19-grsec #4 Суб Апр 5 17:15:56 MSD
2003 i686
Build Date => Jul 18 2003 10:11:54
Configure Command =>  './configure' '--exec-prefix=/usr' '--with-
layout=GNU' '--with-apxs2=/usr/sbin/apxs' '--with-config-file-
path=/etc/httpd' '--with-exec-dir=/usr/bin' '--with-openssl' '--with-
zlib' '--with-bz2' '--with-gd' '--with-ttf' '--with-png' '--with-jpeg-
dir=/usr' '--with-png-dir=/usr' '--with-freetype-dir=/usr' '--with-expat-
dir=/usr' '--with-gmp' '--with-xml' '--with-pear=/usr/share/pear' '--
with-mysql=shared,/usr' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--
with-pspell' '--disable-debug' '--disable-rpath' '--disable-posix' '--
enable-discard-path' '--enable-safe-mode' '--enable-magic-quotes' '--
```

```
enable-dmalloc' '--enable-bcmath' '--enable-dio' '--enable-gd-native-ttf'
'--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--enable-
versioning' '--enable-pic' '--enable-inline-optimization' '--enable-
memory-limit'
Server API => Command Line Interface
Virtual Directory Support => disabled
Configuration File (php.ini) Path => /etc/httpd/php.ini
PHP API => 20020918
PHP Extension => 20020429
Zend Extension => 20021010
Debug Build => no
Thread Safety => disabled
Registered PHP Streams => php, http, ftp, https, ftps, compress.bzip2,
compress.zlib
This program makes use of the Zend Scripting Language Engine:
Zend Engine v1.3.0, Copyright (c) 1998-2003 Zend Technologies
_____________________________________________________________________
Configuration
PHP Core
Directive => Local Value => Master Value
…
```

то PHP в режиме командной строки работает нормально, и вы можете использовать его для написания различных сценариев, запускаемых из командного интерпретатора. Неплохо проверить все строки вывода на предмет соответствия полученной конфигурации PHP вашим требованиям.

Шаг 2

Проверьте работоспособность совместной работы PHP и Apache HTTP Sever. Для этого запустите (перезапустите) Web-сервер:

```
[karlnext@test karlnext]$ sudo /etc/init.d/httpd start
Password:$ecretnoe_Sl0v0
Запускается httpd:                                [OK]
```

Разместите в каком-нибудь каталоге, обслуживаемом вашим сервером, например, `/var/www/eshop/html/`, файлы `top.php`, `union12345.php` и `down.php`, содержание которых приведено в самом начале этой главы для иллюстрации возможностей PHP. После чего выполните команду:

```
[karlnext@test karlnext]$ lynx http://eshop.bruy.info/union12345.php
```

Если увидите примерно следующее:

```
Пример использования PHP

 Смысловое содержание страницы
…

Команды: стрелки - перемещение, '?' - помощь, 'q' - выход, '<-' - назад.
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево -
возврат. H)elp O)ptions P)rint G)o M)Глав экран Q)uit /=поиск
[delete]=список истории
```

то PHP правильно интегрирован с Web-сервером, и вы можете использовать его для написания сценариев, обслуживаемых Web-сервером.

Шаг 3

Протестируйте работоспособность всего программного обеспечения, содержащего PHP-код, использование которого предполагается на вашем сервере. В случае необходимости внесите соответствующие изменения в конфигурационные файлы `/etc/httpd/php.ini` и `/etc/httpd/conf/httpd.conf`.

Выполнение PHP в окружении chroot-jail

Потенциальные уязвимости PHP, как и любого другого программного обеспечения, могут использоваться для реализации атак на вашу систему. Поэтому для повышения безопасности вашей системы PHP можно заставить работать в окружении chroot-jail. Это не простая задача, при этом может потребоваться дополнительные и не всегда заканчивающиеся успехом попытки по адаптации программ (сценариев), содер-

жащих PHP-код, для работы в окружении chroot-jail. Тем не менее, если вы все-таки желаете протестировать работоспособность вашего сервера в относительно безопасном окружении, руководствуйтесь ниже приведенными рекомендациями. Если вы собираетесь использовать Apache HTTP Server с поддержкой PHP и модуля `mod_perl`, пропустите этот раздел и вернитесь к нему после инсталляции и настройки поддержки `mod_perl` в обычной среде. В этом случае перенос необходимых файлов в окружение chroot jail лучше осуществлять сразу для Apache HTTP Server и всех поддерживаемых им модулей сторонних разработчиков, руководствуясь при этом рекомендациями этой, предыдущей и последующей глав.

Шаг 1

Выполните все рекомендации предыдущей главы по переносу и тестированию Apache HTTP Server в окружение chroot-jail. Только после удачного тестирования перейдите к следующему шагу.

Шаг 2

Остановите Apache HTTP Server:

```
[karlnext@test karlnext]$ sudo /etc/init.d/httpd start
Password:$ecretnoe_Sl0v0
Останавливается httpd:                          [OK]
```

Шаг 3

Перенесите файлы, необходимые для работы PHP, в окружение chroot-jail:

```
[root@test /]# mv /usr/lib/httpd/modules/libphp4.so
/chroot/httpd/usr/lib/httpd/modules/
[root@test /]# mv /usr/lib/php /chroot/httpd/usr/lib
[root@test /]# mv /usr/share/pear/ /chroot/httpd/usr/share/
[root@test /]# mv /etc/httpd/php.ini /chroot/httpd/etc/httpd/
```

ЗАМЕЧАНИЕ Лучше сразу не переносить соответствующие файлы и каталоги, а скопировать их. В этом случае, если PHP и использующее его программное обеспечение будет работоспособно в окружении chroot-jail, вы в дальнейшем всегда сможете уничтожить более не нужные файлы, созданные при инсталляции и конфигурировании PHP в обычной среде. В случае, если PHP или использующее его программное обеспечение окажется не работоспособным, вы всегда сможете вернуться к прежней работоспособной конфигурации.

Если вы собираетесь также использовать PHP в режиме командной строки, то вы должны **СКОПИРОВАТЬ, А НЕ ПЕРЕНЕСТИ** указанные выше файлы и каталоги.

Шаг 4

Составьте список библиотек, используемых `libphp4.so`, анализируя вывод следующей команды:

```
[root@test /]# ldd /chroot/httpd/usr/lib/httpd/modules/libphp4.so
        libexpat.so.0 => /usr/lib/libexpat.so.0 (0x4c786000)
        libpspell.so.4 => /usr/lib/libpspell.so.4 (0x4c7a6000)
        libgmp.so.3 => /usr/lib/libgmp.so.3 (0x4c7c1000)
        libpng.so.2 => /usr/lib/libpng.so.2 (0x4c7e9000)
        libz.so.1 => /usr/lib/libz.so.1 (0x4c80a000)
        libbz2.so.1 => /usr/lib/libbz2.so.1 (0x4c818000)
        libssl.so.0.9.7 => /lib/libssl.so.0.9.7 (0x4c827000)
        libcrypto.so.0.9.7 => /lib/libcrypto.so.0.9.7 (0x4c857000)
        libdmalloc.so => /usr/lib/libdmalloc.so (0x4c95d000)
        libresolv.so.2 => /lib/libresolv.so.2 (0x4c9a4000)
        libm.so.6 => /lib/i686/libm.so.6 (0x4c9b7000)
        libdl.so.2 => /lib/libdl.so.2 (0x4c9d9000)
        libttf.so.2 => /usr/lib/libttf.so.2 (0x4c9dc000)
        libfreetype.so.6 => /usr/lib/libfreetype.so.6 (0x4ca07000)
        libjpeg.so.62 => /usr/lib/libjpeg.so.62 (0x4ca46000)
        libnsl.so.1 => /lib/libnsl.so.1 (0x4ca64000)
        libc.so.6 => /lib/i686/libc.so.6 (0x4ca79000)
        libltdl.so.3 => /usr/lib/libltdl.so.3 (0x4cbb0000)
        libpspell-modules.so.1 => /usr/lib/libpspell-modules.so.1
(0x4cbb7000)
        libstdc++-libc6.2-2.so.3 => /usr/lib/libstdc++-libc6.2-2.so.3
(0x4cbba000)
        /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x0957e000)
```

В результате вы получите список библиотек, используемых модулем `libphp4.so`. Однако их не всегда бывает достаточно для его нормального функционирования:

- `/usr/lib/libexpat.so.0`;
- `/usr/lib/libpspell.so.4`;
- `/usr/lib/libpng.so.2`;
- `/usr/lib/libz.so.1`;
- `/usr/lib/libbz2.so.1`;
- `/lib/libssl.so.0.9.7`;
- `/lib/libcrypto.so.0.9.7`;
- `/usr/lib/libdmalloc.so`;
- `/lib/libresolv.so.2`;
- `/lib/i686/libm.so.6`;
- `/lib/libdl.so.2`;
- `/usr/lib/libttf.so.2`;
- `/usr/lib/libfreetype.so.6`;
- `/usr/lib/libjpeg.so.62`;
- `/lib/libnsl.so.1`;
- `/lib/i686/libc.so.6`;
- `/usr/lib/libltdl.so.3`;
- `/usr/lib/libpspell-modules.so.1`;
- `/usr/lib/libstdc++-libc6.2-2.so.3`.

Шаг 5

Скопируйте библиотеки в соответствующие каталоги окружения chroot-jail:

```
[root@test /]# cp /usr/lib/libexpat.so.0 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libpspell.so.4 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libpng.so.2 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libz.so.1 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libbz2.so.1 /chroot/httpd/usr/lib/
[root@test /]# cp /lib/libssl.so.0.9.7 /chroot/httpd/lib/
[root@test /]# cp /lib/libcrypto.so.0.9.7 /chroot/httpd/lib/
[root@test /]# cp /usr/lib/libdmalloc.so /chroot/httpd/usr/lib/
[root@test /]# cp /lib/libresolv.so.2 /chroot/httpd/lib/
[root@test /]# cp /lib/i686/libm.so.6 /chroot/httpd/lib/i686/
[root@test /]# cp /lib/libdl.so.2 /chroot/httpd/lib/
[root@test /]# cp /usr/lib/libttf.so.2 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libfreetype.so.6  /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libjpeg.so.62 /chroot/httpd/usr/lib/
[root@test /]# cp /lib/libnsl.so.1 /chroot/httpd/lib/
[root@test /]# cp /lib/i686/libc.so.6 /chroot/httpd/lib/i686/
[root@test /]# cp /usr/lib/libltdl.so.3 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libpspell-modules.so.1 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/lib/libstdc++-libc6.2-2.so.3
/chroot/httpd/usr/lib/
```

Шаг 6

Протестируйте работоспособность модуля `libphp4.so`, запустив Web-сервер:

```
[karlnext@test karlnext]$ sudo /etc/init.d/httpd start
Password:$ecretnoe_Sl0v0
```

При этом вы можете получить сообщение об ошибке:

```
Запускается httpd: Syntax error on line 57 of /etc/httpd/conf/httpd.conf:
Cannot load /usr/lib/php/libphp4.so into server: libgmp.so.3: cannot open
shared object file: No such file or directory
                                                    [СБОЙ]
```

содержащее информацию об отсутствии какой-нибудь библиотеки, в рассматриваемом примере – `libgmp.so.3`.

В этом случае (если вы забыли, где находится требуемая библиотека) определите путь к ней с использованием команды:

```
[root@test /]# whereis libgmp.so.3
libgmp.so: /usr/lib/libgmp.so.3 /usr/lib/libgmp.so
```

и скопируйте необходимые файлы в соответствующие каталоги окружения chroot-jail:

```
[root@test /]# cp /usr/lib/libgmp.so.3 /usr/lib/libgmp.so
/chroot/httpd/usr/lib/
```

Выясните, какие еще библиотеки используются `libgmp.so.3` в соответствие с алгоритмом, используемым в шаге 4. Нам повезло, т. к. выяснилось, что никакие библиотеки, кроме уже скопированных в окружение chroot-jail ранее, не требуются. В результате сервер запустился без проблем в окружении chroot-jail с поддержкой модуля `libphp4.so`:

```
[karlnext@test karlnext]$ sudo /etc/init.d/httpd start
Password:$ecretnoe_Sl0v0
Запускается httpd:                [OK]
```

Шаг 7

Протестируйте работоспособность сервера в окружении chroot-jail с `php4_module`, воспользовавшись рекомендациями раздела «Тестирование PHP». Результаты тестирования должны быть идентичны результатам, полученным при тестировании работоспособности сервера, запущенного в обычном окружении.

Глава 36

mod_perl– модуль, позволяющий включить интерпретатор языка Perl непосредственно в Apache HTTP Server

В этой главе:

В этой глава рассматривается еще один модуль сторонних разработчиков, ориентированный на совместное использование с Apache HTTP Server – mod_perl. Модуль mod_perl позволяет включить интерпретатор языка Perl непосредственно в Apache HTTP Server, после чего Web-сервер может существенно быстрее (на сервере разработчиков представлен пример, демонстрирующий увеличение быстродействия простого сценария в 30 раз) выполнять код написанных на Perl сценариев. Использование модуля целесообразно только в том случае, если на своем сервере вы активно используете сценарии, написанные на языке Perl.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Перекомпиляция ядра не требуется.

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы этого не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта mod_perl по состоянию на 14.07.2003. Регулярно посещайте домашнюю страницу проекта `http://perl.apache.org/`и отслеживайте обновления.

Исходные коды mod_perl содержатся в архиве `mod_perl-2.0-current.tar.gz` (последняя доступная на момент написания главы стабильная версия `mod_perl-1.99_09`).

Для инсталляции и нормальной работы mod_perl должен быть установлен Apache HTTP Server версии 2.0.xx.

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить следующие операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Шаг 1

Проверьте, установлен ли пакет программы mod_perl с помощью следующей команды:

```
[root@test /]# rpm –iq mod_perl
```

Шаг 2

Перейдите в каталог, где находится пакет `mod_perl-1.26-5.i386.rpm`. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@test /]# cd /home/distrib
```

и установите:

```
[root@test distrib]# rpm -ihv mod_perl-1.26-5.i386.rpm
```

или обновите пакет:

```
[root@test distrib]# rpm –Uhv mod_perl-1.26-5.i386.rpm
```

Компиляция, оптимизация и инсталляция mod_perl

Для инсталляции mod_perl из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами. Для этого можно воспользоваться процедурой, описанной в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами `mod_perl` в каталоге `/var/tmp`:

```
[root@test tmp]# tar xzpf mod_perl-2.0-current.tar.gz
```

Шаг 3

Сконфигурируйте, откомпилируйте, проинсталлируйте mod_perl, создайте и сохраните в надежном месте список установленных файлов:

```
[root@test tmp]# cd mod_perl-1.99_09
[root@test mod_perl-1.99_09]# perl Makefile.PL MP_APXS=/usr/sbin/apxs
[root@test mod_perl-1.99_09]# make
[root@test mod_perl-1.99_09]# find /* > /root/mod_perl1
[root@test mod_perl-1.99_09]# make install
[root@test mod_perl-1.99_09]# find /* > /root/mod_perl2
[root@test mod_perl-1.99_09]# diff /root/mod_perl1 /root/mod_perl2 >
/root/mod_perl.installed
[root@test mod_perl-1.99_09]# mv /root/mod_perl.installed
/very_reliable_place/mod_perl.installed.YYYYMMDD
```

Шаг 4

Удалите архив и каталог с исходными кодами:

```
[root@test mod_perl-1.99_09]# cd /var/tmp/
[root@test tmp]# rm -rf mod_perl-1.99_09/
[root@test tmp]# rm -f mod_perl-2.0-current.tar.gz
```

Конфигурирование mod_perl

Для включения поддержки mod_perl в Apache HTTP Server в файле `/etc/httpd/conf/httpd.conf` добавьте (проверьте наличие) строки:

```
LoadModule perl_module          modules/mod_perl.so
```

Тестирование mod_perl

Для тестирования mod_perl выполните следующие операции.

Шаг 1

Перезапустите Apache HTTP Server:

```
[root@test /]# /etc/init.d/httpd restart
Запускается httpd:                         [OK]
Останавливается httpd:                     [OK]
```

Шаг 2

Разместите в каком-нибудь каталоге вашего сервера, предназначенного для хранения файлов-сценариев, например, `/var/www/eshop/cgi-bin/`, файл `printenv`, содержащий следующие строки:

```
#!/usr/bin/perl
##
##  printenv -- demo CGI program which just prints its environment
##

print "Content-type: text/plain\n\n";
foreach $var (sort(keys(%ENV))) {
    $val = $ENV{$var};
    $val =~ s|\n|\\n|g;
    $val =~ s|"|\\"|g;
    print "${var}=\"${val}\"\n";
}
```

Шаг 3

Сделайте файл исполняемым и определите его владельцем пользователя `www`:

```
[root@test /]# chmod 500 /var/www/eshop/cgi-bin/printenv
[root@test /]# chown www.www /var/www/eshop/cgi-bin/printenv
```

Шаг 4

Проверьте работоспособность сценария:

```
[karlnext@test karlnext]$ lynx eshop.bruy.info/cgi-bin/printenv
```

Если вы увидите вывод, подобный этому:

```
DOCUMENT_ROOT="/var/www/eshop/html/"
GATEWAY_INTERFACE="CGI/1.1"
```

```
HTTP_ACCEPT="text/html, text/plain, text/sgml, */*;q=0.01"
HTTP_ACCEPT_CHARSET="koi8-r, iso-8859-1;q=0.01, us-ascii;q=0.01"
HTTP_ACCEPT_ENCODING="gzip, compress"
HTTP_ACCEPT_LANGUAGE="en,ru"
HTTP_HOST="eshop.bruy.info"
HTTP_USER_AGENT="Lynx/2.8.4rel.1 libwww-FM/2.14 SSL-MM/1.4.1
OpenSSL/0.9.6b"
PATH="/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin"
QUERY_STRING=""
REMOTE_ADDR="212.111.80.127"
REMOTE_PORT="40359"
REQUEST_METHOD="GET"
REQUEST_URI="/cgi-bin/printenv"
SCRIPT_FILENAME="/var/www/eshop/cgi-bin/printenv"
SCRIPT_NAME="/cgi-bin/printenv"
SERVER_ADDR="212.111.80.127"
SERVER_ADMIN="sales@test.bruy.info"
SERVER_NAME="eshop.bruy.info"
SERVER_PORT="80"
SERVER_PROTOCOL="HTTP/1.0"
SERVER_SIGNATURE=""
SERVER_SOFTWARE="Apache"
```

то модуль mod_perl правильно установлен и интегрирован с Apache HTTP Server.

Выполнение mod_perl в окружении chroot-jail

Потенциальные уязвимости mod_perl, как и любого другого программного обеспечения, могут использоваться для реализации атак на вашу систему. Поэтому для повышения безопасности вашей системы mod_perl можно заставить работать в окружении chroot-jail. Это не простая задача, при этом может потребоваться дополнительные и не всегда заканчивающиеся успехом попытки по адаптации программ (сценариев), содержащих Perl-код, для работы в окружении chroot-jail. Тем не менее, если вы все-таки желаете протестировать работоспособность вашего сервера в относительно безопасном окружении, руководствуйтесь ниже приведенными рекомендациями. Перенос в окружение chroot jail лучше осуществлять сразу для Apache HTTP Server и всех поддерживаемых им модулей сторонних разработчиков, руководствуясь при этом рекомендациями этой и двух предыдущих глав.

Шаг 1

Выполните все рекомендации раздела «Выполнение Apache HTTP Server в среде chroot jail» главы 34 по переносу и тестированию Apache HTTP Server в окружение chroot-jail. Только после удачного тестирования переходите к следующему шагу.

Шаг 2

Если вы используете PHP, выполните все рекомендации раздела «Выполнение PHP в окружении chroot-jail» главы 35 по переносу и тестированию в окружение chroot-jail. Только после удачного тестирования переходите к следующему шагу.

Шаг 3

Остановите:

```
[root@test /]# /etc/init.d/httpd stop
Останавливается httpd:                     [OK]
```

Шаг 4

Создайте в окружении chroot jail необходимые каталоги и скопируйте в них файлы, требующиеся для работы mod_perl:

```
[root@test /]# mkdir -p /chroot/httpd/usr/bin/
[root@test /]# cp /usr/lib/httpd/modules/mod_perl.so
/chroot/httpd/usr/lib/httpd/modules/
[root@test /]# cp -a /usr/lib/perl5 /chroot/httpd/usr/lib/
[root@test /]# cp /usr/bin/perl /chroot/httpd/usr/bin/
[root@test /]# cp /lib/libutil.so.1 /chroot/httpd/lib
[root@test /]# cp -a /etc/locale /chroot/httpd/etc/
[root@test /]# cp -a /usr/lib/locale /chroot/httpd/usr/lib/
```

```
[root@test /]# cp -a /usr/share/locale /chroot/httpd/usr/share/
[root@test /]# cp /usr/bin/locale /chroot/httpd/usr/bin
```

Шаг 5

Запустите Apache HTTP Server:

```
[root@test /]# /etc/init.d/httpd start
Запускается httpd:                         [OK]
```

Шаг 6

Протестируйте работоспособность сервера в окружении chroot-jail с поддержкой с использованием рекомендаций раздела «Тестирование mod_perl». Результаты тестирования должны быть идентичны результатам, полученным при тестировании работоспособности сервера запущенного в обычном окружении.

Часть 11

Программное обеспечение для организации совместного использования общих сетевых ресурсов

Глава 37

Сервер Samba

В этой главе:

Для организации совместного доступа к сетевым ресурсам рабочих станций и серверов, использующих различные операционные системы, необходимо соответствующее программное обеспечение. Таковым является сервер Samba, одной из функций которого является предоставление совместного доступа пользователям, работающим в различных операционных системах (Linux, Microsoft Windows, OS/2 и др.) к общим сетевым ресурсам – файлам и принтерам. Кроме того, в комплект поставки программного обеспечения Samba входят клиентские программы – например, smbclient, позволяющая устанавливать соединение с другими системами по протоколу SMB и работать с размещенными на них файлами по аналогии, как это делается с FTP-клиентом, smbmount, предназначенная для монтирования файловых систем, обслуживаемых сервером Samba – и средства администрирования.

В настоящее время готовится к выходу новая версия Samba 3.0. К сожалению, на момент написания этой главы была доступна только версия, предназначенная для тестирования Samba-3.0.0beta3. Использование версий программ, предназначенных для тестирования, недопустимо на серверах и рабочих станциях, используемых для решения практических задач. Тем не менее, мы протестировали новую версию Samba в надежде, что когда эта книга дойдет до своего читателя, разработчики устранят основные недостатки новой версии программного обеспечения и стабильной версией станет версия Samba 3.0.xx. По этой же причине (т. к. разработчики могут изменить порядок настройки Samba) в этой главе мы ограничимся рассмотрением простейшего случая инсталляции, компиляции и настройки Samba в качестве отдельно стоящего файл-сервера с организацией доступа пользователей с PAM-аутентификацией. Другие возможности этого программного продукта, который, скорее всего, станет в ближайшее время адекватной заменой программных продуктов от Microsoft, вы сможете освоить самостоятельно. Проект прекрасно документирован и применение его на практике часто и достаточно подробно обсуждается в различных статьях, списках рассылки и форумах, в том числе, и на русском языке. Схема организации совместного доступа к сетевым ресурсам представлена на рис. 37.1.

Ограничения и допущения

Исходные коды находятся в каталоге `/var/tmp`.

Все операции по инсталляции и настройке выполняются пользователем с учетной записью `root`.

Используется дистрибутив ASPLinux 7.3 (Vostok).

Процедуры, описанные в этой главе, могут оказаться применимыми для других версий ядра и дистрибутивов Linux, но авторы это не проверяли.

Пакеты

Последующие рекомендации основаны на информации, полученной с домашней страницы проекта Samba по состоянию на 25.07.2003. Регулярно посещайте домашнюю страницу проекта `http://www.samba.org/` и отслеживайте обновления.

Исходные коды Samba содержатся в архиве `samba-version.tar.gz` (последняя доступная на момент написания главы стабильная версия `samba-3.0.0beta3.tar.gz`).

Для нормальной инсталляции и работы Samba необходима установка OpenSSL. В случае, если на вашем сервере установлено программное обеспечение OpenSSL или ядро, собранное из исходных кодов, инсталляция Samba из rpm-пакетов, входящих в комплект поставки дистрибутива, скорее всего, будет невозможной.

Инсталляция с помощью rpm-пакетов

Если вы предпочитаете использование системы со стандартным ядром и программным обеспечением, установленным из rpm-пакетов, для установки или обновления пакета необходимо выполнить некоторые операции.

ЗАМЕЧАНИЕ Авторы настоятельно рекомендуют устанавливать программное обеспечение из исходных кодов.

Если вы следовали за установкой, описанной в этой книге, для инсталляции Samba вам понадобятся следующие пакеты, входящие в дистрибутив ASPLinux 7.3:

- `tcsh-6.10-6.src.rpm`;
- `samba-2.2.3a-6.asp.i386.rpm`;
- `samba-client-2.2.3a-6.asp.i386.rpm`;
- `samba-common-2.2.3a-6.asp.i386.rpm`.

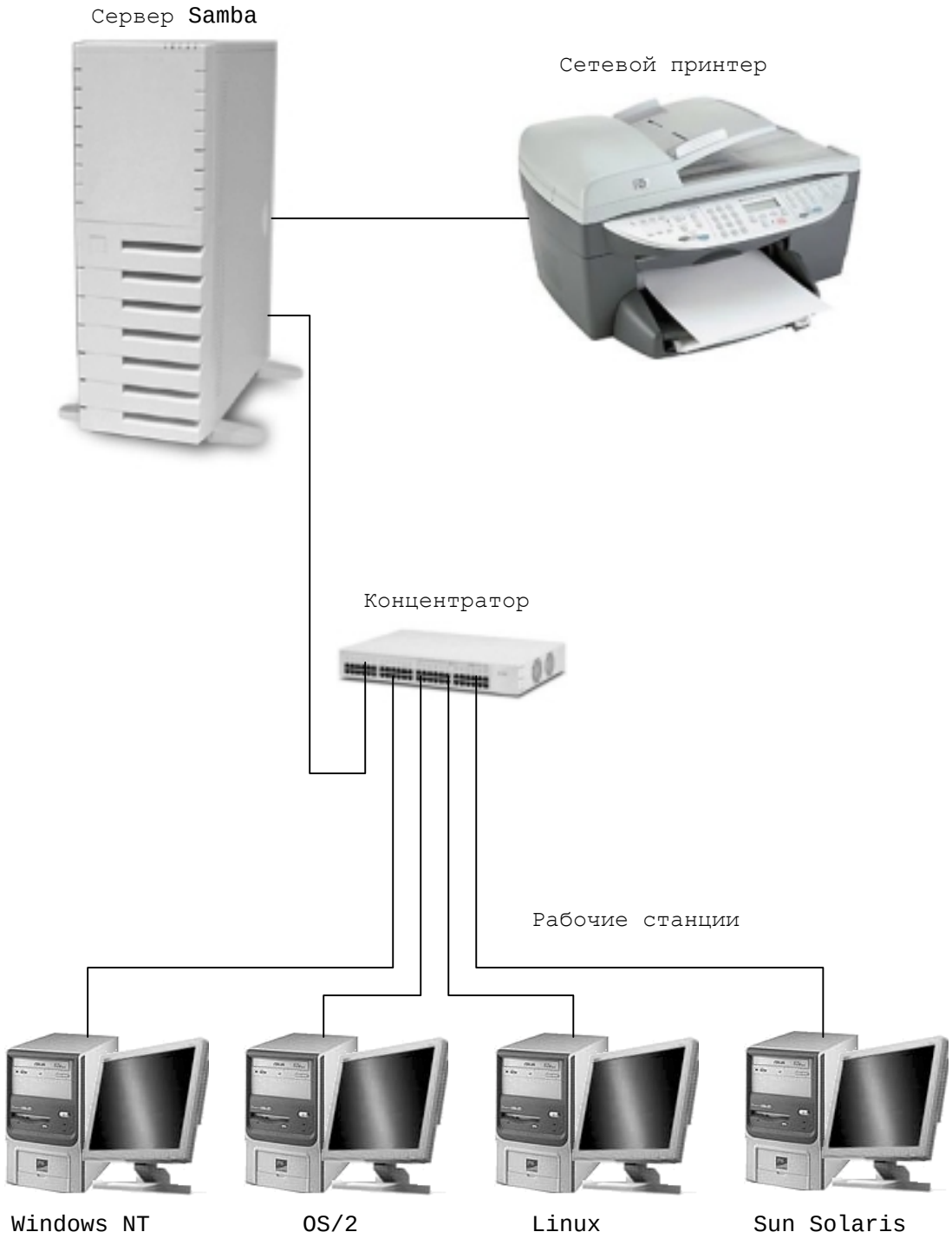


Рис. 37.1. Схема организации совместного доступа к сетевым ресурсам.

ЗАМЕЧАНИЕ Программа OpenSSL должна быть установлена обязательно из пакета. Для данной версии дистрибутива – `openssl-0.9.6b-24asp.i686.rpm`.

Шаг 1

Проверьте, установлены ли пакеты программ из списка, приведенного выше. Используйте, например, команду вида:

```
[root@drwalbr /]# rpm –iq samba
```

Шаг 2

Перейдите в каталог, где находятся rpm-пакеты. Если вы в соответствии с рекомендациями главы 2 скопировали все пакеты, входящие в дистрибутив, в каталог `/home/distrib`, то выполните команду:

```
[root@drwalbr /]# cd /home/distrib
```

Шаг 3

Установите необходимые пакеты:

```
root@drwalbr distrib]# rpm -ihv tcsh-6.10-6.src.rpm \
samba-2.2.3a-6.asp.i386.rpm \
samba-client-2.2.3a-6.asp.i386.rpm \
samba-common-2.2.3a-6.asp.i386.rpm
```

После установки пакетов перейдите к настройке программы Samba.

Компиляция, оптимизация и инсталляция Samba

Для инсталляции Samba из исходных кодов необходимо выполнить следующие операции.

Шаг 1

Осуществите проверку подлинности имеющегося в вашем распоряжении архива с исходными кодами, воспользовавшись, например, процедурой, описанной в шаге 1 радела «Компиляция, оптимизация и инсталляция OpenSSL» главы 12.

Шаг 2

Распакуйте архивы с исходными кодами Samba в каталоге `/var/tmp`:

```
[root@drwalbr tmp]# tar xzpf samba-3.0.0beta3.tar.gz
```

Шаг 3

Сконфигурируйте исходные коды Samba:

```
[root@drwalbr tmp]# cd samba-3.0.0beta3/source
[root@drwalbr source]# CFLAGS="-O2 -march=i686 -funroll-loops -
D_GNU_SOURCE"; export CFLAGS
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--localstatedir=/var \
--libdir=/etc/samba \
--mandir=/usr/share/man \
--with-privatedir=/etc/samba \
--with-lockdir=/var/lock/samba \
--with-piddir=/var/run/samba \
--with-swatdir=/usr/share/swat \
--with-codepagedir=/usr/share/samba/codepages \
--with-sslinc=/usr/include \
--with-ssllib=/usr/lib \
--with-ssl \
--with-fhs \
--with-pam \
--with-syslog \
--with-quotas \
```

В рассматриваемом примере изменены каталоги, используемые для установки Samba по умолчанию, и оставлен минимальный набор опций, необходимый для работы сервера.

Шаг 4

Откомпилируйте, проинсталлируйте Samba, создайте и сохраните в надежном месте список установленных файлов:

```
[root@drwalbr source]# make
[root@drwalbr source]# find /* > /root/samba1
...
==========================================================================
The modules are installed.  You may uninstall the modules using the
command "make uninstallmodules" or "make uninstall" to uninstall
binaries, man pages, shell scripts and modules.
==========================================================================
[root@drwalbr source]# install -m0511 script/mksmbpasswd.sh /usr/bin/
[root@drwalbr source]# rm -rf /usr/private/
[root@drwalbr source]# rm -rf /usr/share/swat/
[root@drwalbr source]# rm -f /usr/sbin/swat
[root@drwalbr source]# rm -f  /usr/share/man/man8/swat.8
[root@drwalbr source]# mkdir -m1777 /var/spool/samba/
[root@drwalbr source]# mkdir -m0700 /var/log/samba/
[root@drwalbr source]# strip /usr/sbin/smbd
[root@drwalbr source]# strip /usr/sbin/nmbd
[root@drwalbr source]# find /* > /root/samba2
[root@drwalbr source]# diff /root/samba1 /root/samba2 >
/root/samba.installed
[root@drwalbr source]# mv /root/samba.installed
/very_reliable_place/samba.installed.YYYYMMDD
```

Шаг 5

Удалите архив и каталог с исходными кодами:

```
[root@drwalbr source]# cd /var/tmp/
[root@drwalbr tmp]# rm -rf samba-3.0.0beta3 /
[root@drwalbr tmp]# rm -f samba-3.0.0beta3.tar.gz
```

Конфигурирование Samba

Конфигурирование Samba осуществляется с использованием следующих файлов:

- главного конфигурационного файла `/etc/samba/smb.conf`;
- файла `/etc/samba/lmhost`, используемого для установления соответствий между именами и IP-адресами систем в сети, обслуживаемых Samba;
- системного конфигурационного файла`/etc/sysconfig/samba`;
- файла `/etc/pam.d/samba`, используемого для поддержки аутентификации пользователей с использованием модулей PAM;
- файла инициализации `/etc/init.d/smb`.
- файла `/etc/samba/smbpasswd`, содержащего аутентификационную информацию пользователей.

Конфигурационный файл /etc/samba/smb.conf

В этом файле определяются общие сетевые ресурсы (каталоги, файлы и принтеры) и параметры доступа к ним (пользователи, IP-адреса и т. п.). Файл состоит из трех разделов:

- `[global]` – содержит глобальные директивы конфигурации, применимые ко всем ресурсам, которые также используются по умолчанию для разделов, если эти значения не переопределены явно;
- `[homes]` – содержит директивы, определяющие доступ к различным каталогам;
- `[printers]` – содержит директивы, определяющие доступ к принтерам.

Приведенный ниже пример конфигурационного файла `/etc/smb.conf` содержит пример конфигурации, обеспечивающей доступ в пользовательские каталоги с использованием PAM-аутентификации и зашифрованных паролей.

Шаг 1

Создайте файл `/etc/smb.conf`, руководствуясь приведенными ниже рекомендациями и вашими потребностями:

```
[global]

        workgroup = UND
```

```
        server string = UNDEGROUND SAMBA SERVER
        encrypt passwords = Yes
        security = user
        smb passwd file = /etc/samba/smbpasswd
        log file = /var/log/samba/log.%m
        max log size = 0
        socket options = IPTOS_LOWDELAY TCP_NODELAY
        deadtime = 15
        getwd cache = Yes
        lpq cache time = 45
        name resolve order = wins lmhosts host bcast
        bind interfaces only = True
        interfaces = eth0 172.16.181.0/24 127.0.0.1
        hosts deny = ALL
        hosts allow = 172.16.181. 127.0.0.1
        debug level = 1
        create mask = 0644
        directory mask = 0755
        unix charset = koi8-r
        display charset = koi8-r
        dos charset = cp866
[homes]
        comment = Home Directories
        browseable = No
        read only = No
        invalid users = root bin daemon sync nobody sys tty disk mem kmem

[printers]
        comment = Remote Printers
        path = /var/spool/samba
        browseable = No
        printable = Yes
        invalid users = root bin daemon sync nobody sys tty disk mem kmem
```

В данном файле директива:

```
workgroup = UND
```

определяет имя рабочей группы.

Директива:

```
server string = UNDEGROUND SAMBA SERVER
```

содержит произвольную текстовую строку, содержащую описание сервера и отображаемую пользователям, например, при просмотре из Microsoft Windows папки "Сетевое окружение".

Директива:

```
encrypt passwords = Yes
```

предписывает использование зашифрованных паролей.

Директива:

```
security = user
```

предписывает разрешать доступ только пользователям, удачно прошедшим аутентификацию с использованием учетных записей, сохраненных в файле `smbpasswd`.

Директива:

```
smb passwd file = /etc/samba/smbpasswd
```

определяет местоположение файла, содержащего пароли пользователей сервера Samba.

Директива:

```
log file = /var/log/samba/log.%m
```

предписывает вести отдельные файлы регистрации для каждой системы (Samba-сервера и рабочих станций), участвующих в доступе к общим ресурсам, и сохранять их в файлах с именами вида: `log.xx.xx.xx.xx`.

Директива:

```
max log size = 0
```

снимает ограничения на размер файлов регистрации.

Директива:

```
socket options = IPTOS_LOWDELAY TCP_NODELAY
```

устанавливает параметры сетевых соединений, максимально повышающие производительность вашего сервера.

Директива:

```
deadtime = 15
```

определяет величину интервала времени, измеряемого в минутах, в течение которого осуществляется автоматическое рассоединение с клиентом при отсутствии активности со стороны последнего. Увеличение этого интервала позволяет повысить производительность сервера.

Директивы:

```
getwd cache = Yes
lpq cache time = 45
```

также позволяют повысить производительность сервера за счет организации кэширования данных.

Директива:

```
name resolve order = wins lmhosts host bcast
```

определяет порядок обращения к различным ресурсам для определения соответствия IP-адресов именам систем.

Директивы:

```
bind interfaces only = True
interfaces = eth0 172.16.181.103/24 127.0.0.1
```

ограничивают обслуживаемые сервером сетевые интерфейсы.

Директивы:

```
hosts deny = ALL
hosts allow = 172.16.181. 127.0.0.1
```

ограничивают IP-адреса, с которых разрешен доступ к серверу.

Директива:

```
debug level = 1
```

определяет объем информации, выводимой в файлы регистрации. Вы можете увеличить этот параметр до 2 при настройке сервера и поиске различных неполадок. В режиме штатной эксплуатации увеличение этого параметра приводит к снижению производительности сервера.

Директива:

```
create mask = 0644
```

определяет и устанавливает права доступа к файлам, создаваемым или копируемым в общие каталоги, обслуживаемые сервером.

Директива:

```
directory mask = 0755
```

определяет и устанавливает права доступа к каталогам, создаваемым или копируемым в общие каталоги, обслуживаемые сервером.

Директивы

```
unix charset = koi8-r
display charset = koi8-r
dos charset = cp866
```

предназначены для корректного отображения русских кодировок.

Следующий блок директив определяет доступ к домашним каталогам пользователей:

```
[homes]
        comment = Alexander Yesin share catalog
        path = /home/yesin
        browseable = No
        read only = No
        valid users yesin
        invalid users = root bin daemon sync nobody sys tty disk mem kmem
```

здесь разрешается доступ к домашнему каталогу `/home/yesin` пользователя `yesin` после прохождения удачной аутентификации (что задано выше директивой `security = user` для всех пользователей сервера) и запрещает доступ к этому каталогу всех специальных пользователей системы.

Блок директив:

```
[printers]
        comment = Remote Printers
        path = /var/spool/samba
        browseable = No
        printable = Yes
        valid users = drwalbr karlnext international yesin
        invalid users = root bin daemon sync nobody sys tty disk mem kmem
```

разрешает доступ к принтеру пользователям `drwalbr`, `karlnext`, `international` и `yesin`.

Шаг 2

Установите права доступа к файлу и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 600 /etc/samba/smb.conf
[root@drwalbr /]# chown 0.0 /etc/samba/smb.conf
```

Конфигурационный файл /etc/samba/lmhosts

Шаг 1

Создайте файл `/etc/samba/lmhosts` и внесите в него все имена систем вашей сети и соответствующие им IP-адреса. В нашем примере это выглядит так:

```
# Sample Samba lmhosts file.
#
127.0.0.1        localhost
172.16.181.1     ntsrv
…
172.16.181.15    arm3
172.16.181.13    graf
…
172.16.181.103   drwalbr
```

Шаг 2

Установите права доступа к файлу и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 640 /etc/samba/lmhosts
[root@drwalbr /]# chown 0.0 /etc/samba/lmhosts
```

Конфигурационный файл /etc/sysconfig/samba

Шаг 1

Создайте файл `/etc/sysconfig/samba`, содержащий следующие строки:

```
# Options to smbd
SMBDOPTIONS="-D"
# Options to nmbd
NMBDOPTIONS="-D -H /etc/samba/lmhost"
```

Шаг 2

Установите права доступа к файлу и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 640 /etc/sysconfig/samba
[root@drwalbr /]# chown 0.0 /etc/sysconfig/samba
```

Конфигурационный файл /etc/pam.d/samba

Этот файл используется для поддержки аутентификации пользователей с помощью модулей PAM.

Шаг 1

Создайте файл `/etc/pam.d/samba`, содержащий следующие строки:

```
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_access.so
account    required     /lib/security/pam_time.so
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_limits.so
session    optional     /lib/security/pam_console.so
```

Шаг 2

Установите права доступа к файлу `/etc/pam.d/samba` и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 640 /etc/pam.d/samba
[root@drwalbr /]# chown 0.0 /etc/pam.d/samba
```

Конфигурационный файл /etc/logrotate.d/samba

Этот файл используется для настройки чередования файлов регистрации. В рассматриваемом примере файлы регистрации будут чередоваться еженедельно.

Шаг 1

Создайте файл `/etc/logrotate.d/samba`, содержащий следующие строки:

```
/var/log/samba/log.* {
    notifempty
    missingok
    sharedscripts
    copytruncate
    postrotate
        /bin/kill -HUP `cat /var/lock/samba/*.pid 2> /dev/null` 2>
/dev/null || true
    endscript
}
```

Шаг 2

Установите права доступа к файлу `/etc/logrotate.d/samba` и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 640 /etc/logrotate.d/samba
[root@drwalbr /]# chown 0.0 /etc/logrotate.d/samba
```

Файл инициализации /etc/lnit.d/smb

Шаг 1

Для запуска и остановки сервера Samba создайте файл `/etc/init.d/smb`, содержащий следующие строки:

```
#!/bin/sh
#
# chkconfig: - 91 35
# description: Starts and stops the Samba smbd and nmbd daemons \
#              used to provide SMB network services.

# Source function library.
if [ -f /etc/init.d/functions ] ; then
  . /etc/init.d/functions
elif [ -f /etc/rc.d/init.d/functions ] ; then
  . /etc/rc.d/init.d/functions
else
  exit 0
fi

# Source networking configuration.
. /etc/sysconfig/network

if [ -f /etc/sysconfig/samba ]; then
   . /etc/sysconfig/samba
fi

# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0

# Check that smb.conf exists.
[ -f /etc/samba/smb.conf ] || exit 0

RETVAL=0


start() {
        KIND="SMB"
        echo -n $"Starting $KIND services: "
        daemon smbd $SMBDOPTIONS
        RETVAL=$?
        echo
        KIND="NMB"
        echo -n $"Starting $KIND services: "
        daemon nmbd $NMBDOPTIONS
        RETVAL2=$?
```

```
        echo
        [ $RETVAL -eq 0 -a $RETVAL2 -eq 0 ] && touch /var/lock/subsys/smb
|| \
           RETVAL=1
        return $RETVAL
}

stop() {
        KIND="SMB"
        echo -n $"Shutting down $KIND services: "
        killproc smbd
        RETVAL=$?
        echo
        KIND="NMB"
        echo -n $"Shutting down $KIND services: "
        killproc nmbd
        RETVAL2=$?
        killproc nmbd
        RETVAL2=$?
        [ $RETVAL -eq 0 -a $RETVAL2 -eq 0 ] && rm -f /var/lock/subsys/smb
        echo ""
        return $RETVAL
}

restart() {
        stop
        start
}

reload() {
        echo -n $"Reloading smb.conf file: "
        killproc smbd -HUP
        RETVAL=$?
        echo
        return $RETVAL
}

status() {
        status smbd
        status nmbd
}

case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart)
        restart
        ;;
  reload)
        reload
        ;;
  status)
        status
        ;;
  condrestart)
        [ -f /var/lock/subsys/smb ] && restart || :
        ;;
  *)
        echo $"Usage: $0 {start|stop|restart|status|condrestart}"
        exit 1
```

```
esac

exit $?
```

Шаг 2

Установите права доступа к файлу и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 700 /etc/init.d/smb
[root@drwalbr /]# chown 0.0 /etc/init.d/smb
```

Шаг 3

Если вы хотите, чтобы сервер `samba` запускался автоматически при загрузке системы, создайте соответствующие ссылки:

```
[root@drwalbr /]# chkconfig --add smb
[root@drwalbr /]# chkconfig --level 345 smb on
```

Добавление новых пользователей (конфигурационный файл /etc/samba/smbpasswd)

Для создания новой учетной записи пользователя, имеющего доступ к общим сетевым ресурсам, обслуживаемым Samba-сервером, необходимо выполнить следующие операции.

Шаг 1

Создайте пользователя `yesin` с использованием следующей команды:

```
[root@drwalbr /]# useradd –s /bin/false yesin
```

Проверьте наличие, а при необходимости добавьте в файл `/etc/shells` строку:

```
/bin/false/
```

Определите пароль нового пользователя для доступа к системе:

```
[root@drwalbr /]# passwd yesin
Changing password for user yesin
New UNIX password: secretn()e_sL0v()
Retype new UNIX password: secretn()e_sL0v()
passwd: all authentication tokens updated successfully
```

Шаг 2

Далее вы можете добавить нового пользователя в систему, используя команду:

```
[root@drwalbr /]# smbpasswd -a yesin
New SMB password: secretn()e_sL0v()
Retype new SMB password: secretn()e_sL0v()
```

или экспортировать аутентификационную информацию из файла `/etc/passwd` в файл `/etc/samba/smbpasswd` с использованием утилиты `mksmbpasswd.sh`:

```
[root@drwalbr /]# cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
```

Шаг 3

Установите права доступа к файлу `/etc/samba/smbpasswd` и назначьте его владельцем пользователя `root`:

```
[root@drwalbr /]# chmod 600 /etc/samba/smbpasswd
[root@drwalbr /]# chown 0.0 /etc/samba/smbpasswd
```

Тестирование Samba

Шаг 1

Проверьте отсутствие ошибок в конфигурационном файле `/etc/samba/smb.conf`:

```
[root@drwalbr /]# testparm –v
```

Шаг 2

Запустите Samba:

```
[root@drwalbr /]# /etc/init.d/smb start
Запускаются сервисы SMB:                                   [OK]
Запускаются сервисы NMB:                                   [OK]
```

Шаг 3

Зарегистрируйтесь в системе в качестве обычного пользователя и попробуйте установить соединение с использованием утилиты `smbclient`:

```
[yesin@drwalbr yesin]$ smbclient //localhost/yesin -U yesin -I
172.16.181.103
Password: secretn()e_sL0v()
OS=[Unix] Server=[Samba 3.0.0beta3]
smb: \> ls -l *.html
NT_STATUS_NO_SUCH_FILE listing \-l

                39373 blocks of size 262144. 34839 blocks available
smb: \> exit
```

Шаг 4

Проверьте доступ к общим ресурсам с другой системы, работающей на операционной системе Microsoft Windows.

Шаг 5

Проверьте работоспособность вашего сервера с использованием утилиты `smbstatus`:

```
[root@drwalbr /]# smbstatus

Samba version 3.0.0beta3
PID     Username      Group         Machine
-------------------------------------------------------------------
 3097   yesin         users         arm3         (172.16.181.15)

Service      pid     machine       Connected at
-------------------------------------------------------
yesin         3097   arm3          Fri Jul 25 16:45:38 2003
Locked files:
Pid    DenyMode   Access      R/W        Oplock           Name
--------------------------------------------------------------
3097   DENY_NONE  0x1         RDONLY     EXCLUSIVE+BATCH
/home/yesin/photo1.jpg   Fri Jul 25 16:45:51 2003
3097   DENY_NONE  0x1         RDONLY     EXCLUSIVE+BATCH
/home/yesin/photo2.jpg   Fri Jul 25 16:45:56 2003
```

Часть 12

Организация резервного копирования

Глава 38

Резервное копирование

В этой главе:

1. Резервное копирование файлов программного обеспечения с использованием программы tar
2. Автоматическое резервное копирование периодически изменяемых файлов
3. Полное резервное копирование
4. Инкрементное резервирование копирование

Безопасный и надежный сервер предполагает выполнение регулярного резервного копирования. Это необходимо для того, чтобы вы могли восстановить сервер в случае возникновения аппаратных сбоев, например, из-за выхода из строя жестких дисков, человеческого фактора, скачков напряжения и т. д. Файлы, содержащие резервные копии лучше размещать на съемных внешних носителях информации (компакт-дисках, лентах, дискетах и т. п.) или специальных серверах, предназначенных для резервного копирования. В любом случае резервные копии файлов следует хранить за пределами системы, для восстановления которой они создаются. Перенос файлов с системы на систему следует осуществлять с использованием безопасной технологии OpenSSH, рассмотренной нами в главе 13.

Схема организации службы резервного копирования представлена на рис. 38.1.

Существует множество программ для осуществления резервного копирования, использование которых возможно на Linux-системах. К их числу относятся:

- программы для создания резервных копий файлов и каталогов tar (`http://www.gnu.org/software/tar/tar.html`), cpio (`http://www.gnu.org/software/cpio/cpio.html`), работающие в режиме командной строки;
- имеющая текстовый интерактивный интерфейс программа Amanda (`http://sourceforge.net/projects/amanda/`), также предназначенная для создания резервных копий файлов и каталогов;
- программа dump для создания резервных копий файловых систем;
- утилита mysqldump, предназначенная для резервного копирования баз данных, обслуживаемых сервером MySQL.

Существует также коммерческое программное обеспечение, реализующее функции резервного копирования, например, программа BRU-Pro™ (`http://www.bru.com/`).

В этой главе мы рассмотрим использование только программы tar, т. к. ее функциональных возможностей в сочетании с простыми сценариями, выполняемыми в оболочке командного интерпретатора, достаточно для решения практически любых задач, связанных с резервным копированием критически важной информации.

Обратите внимание, что на вашей системе имеются файлы, которые не должны изменяться вообще, и которые изменяются периодически.

К первому типу относятся файлы установленного программного обеспечения и конфигурационные файлы.

Ко второму типу относятся:

- файлы, создаваемые реальными пользователями системы, например, файлы сохраняемые пользователями вашей локальной сети на файл-сервере Samba;
- файлы, динамически изменяемые программным обеспечением сервера, например, файлы баз данных;
- файлы, используемые при администрировании системы. Например, файл `/etc/passwd/` изменяется каждый раз, когда вы добавляете новую учетную запись пользователя в систему.

В случае утраты хранимых на диске данных программное обеспечение может быть относительно легко восстановлено в случае, если вы сразу же после инсталляции сохранили свои конфигурационные файлы, и воспользуетесь сценариями конфигурирования исходных кодов, прилагаемых к этой книге, и рекомендациями соответствующих глав. Вы также можете сохранить все исполняемые файлы установленного программного обеспечения с целью исключения – в случае возникновения нештатной ситуации – выполнения операций, связанных с повторным конфигурированием, компиляцией и настройкой программного обеспечения.

Резервное копирование программного обеспечения будет рассмотрено на примере программного обеспечения Apache HTTP Server, поддерживающего mod_php и mod_perl и функционирующего в окружении chroot-jail.

Периодически изменяемые файлы следует регулярно архивировать. Для того, чтобы определить, как часто следует архивировать периодически изменяемые файлы, задайте себе и пользователям вашей сети вопрос: «За какой период времени потеря информации, внесенной вами и пользователями сети в периодически изменяемые файлы, не причинит существенных потерь?». Проанализируйте ответы, отсейте необоснованные и некомпетентные. Оцените ресурсы, потребные для реализации требуемой периодичности резервного копирования, например, объем дискового пространства на серверах резервного копирования или съемных носителях информации, пропускную способность сети и т. п. Оцените затраты на реализацию резервного копирования и соответствующие убытки от потери информации.

В этой главе также рассматривается пример организации ежедневного резервного копирования периодически изменяемых файлов.

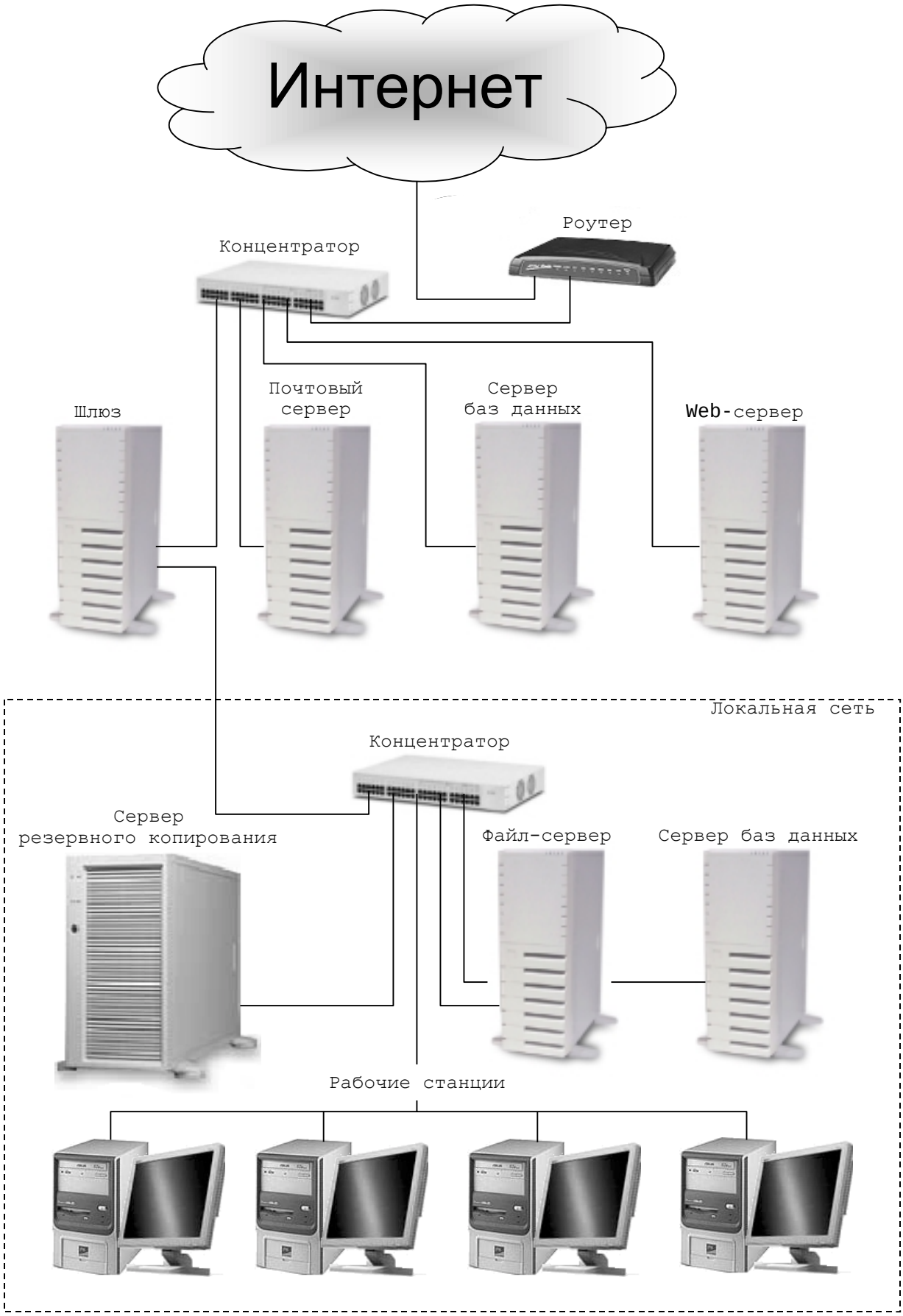


Рис. 38.1. Схема организации службы резервного копирования.

Резервное копирование файлов программного обеспечения с использованием программы tar

Если вы устанавливали Apache HTTP Server, PHP, mod_perl и переносили его в окружение chroot-jail в соответствии с рекомендациями глав 34,35 и 36, то все исполняемые файлы установленного программного обеспечения находятся в каталоге `/chroot/httpd`. Единственным исключением является инициализационный файл `/etc/init.d/httpd`. Следует отметить, что доступ даже на чтение к этому файлу разрешен только пользователю `root`. Поэтому резервное копирование и восстановление файлов необходимо осуществлять от имени пользователя `root`, используя программу Sudo или команду `su`. Для большей безопасности мы используем Sudo, а использование `su` запрещено на нашей системе в соответствии с рекомендациями главы 14.

Для резервного копирования файлов инсталляции Apache HTTP Server, PHP, mod_perl необходимо выполнить следующие операции.

Шаг 1

Для создания архива, содержащего все файлы, необходимые для запуска Apache HTTP Server в окружении chroot jail с поддержкой PHP и mod_perl, необходимо выполнить команду:

```
[karlnext@test karl_next]$ sudo tar cpf
> /home/karl_next/apache-php-perl-chroot.20030719.tar \
> /chroot/httpd /etc/rc.d/init.d/httpd
Password: Secretnoe_$loV0
tar: Removing leading `/' from member names
tar: Removing leading `/' from member names
```

В рассматриваемом примере опция `c` указывает на необходимость создания архива, `p` – сохранения в архиве прав доступа к файлам и каталогам, `f` – на то, что после нее идет только перечисление имен файлов и каталогов, первый из которых является именем создаваемого архива.

ЗАМЕЧАНИЕ Программа tar выдала два предупреждения о том, что из путей к каталогу `/chroot/httpd` и файлу `/etc/rc.d/init.d/httpd` удалены первые символы `/`. Эту особенность программы tar следует учитывать при распаковке архива, осуществляя ее в корневом каталоге сервера. В противном случае пути к файлам и каталогам, создаваемым при распаковке архива, будут неверными, т. к. будут определяться от текущего каталога.

Например, если вы распаковываете архив `apache-php-perl-chroot.20030719.tar` в каталоге `/var/tmp`, то главный конфигурационный файл Apache HTTP Server окажется в каталоге `/var/tmp/etc/rc.d/init.d/httpd`.

Шаг 2

При использовании архива для восстановления файлов вам необходимо будет убедиться в их целостности. Для этого определите контрольную сумму архива с использованием утилиты `md5sum` и сохраните контрольную сумму в файле, имеющем то же имя, но с добавлением расширения `md5`, например:

```
[karlnext@test karl_next]$ md5sum apache-php-perl-chroot.20030719.tar  >
\
> apache-php-perl-chroot.20030719.tar.md5
```

В результате выполнения указанных выше операций у вас появятся два файла. В первом из них – `apache-php-perl-chroot.20030719.tar` – содержатся все файлы, необходимые для восстановления вашей инсталляции, а во втором – `apache-php-perl-chroot.20030719.tar.md5` – содержится контрольная сумма, с помощью которой вы можете проверить целостность архива.

В случае необходимости восстановление вашей инсталляции Apache HTTP Server может быть выполнена с использованием следующих операций.

Шаг 1

Для моделирования нештатной ситуации удалите все файлы инсталляции Apache HTTP Server с использованием команд:

```
[karlnext@test karl_next/]$ sudo rm –f /etc/rc.d/init.d/httpd
[karlnext@test karl_next/]$ sudo rm –rf /chroot/httpd/
```

Шаг 2

Определите текущее время:

```
[karlnext@test karl_next]$ date
```

```
Суб Июл 19 17:41:19 MSD 2003
```

Шаг 3

Скопируйте архив и файл, содержащий его контрольную сумму, в корневой каталог вашего сервера:

```
[karlnext@test karl_next]$ cd /
[karlnext@test /]$ sudo cp \
> home/rootarh/apache-php-perl-chroot.20030719.tar \
> home/rootarh/apache-php-perl-chroot.20030719.tar.md5sum /
Password: Secretnoe_$loV0
```

ЗАМЕЧАНИЕ Обратите внимание, что в рассматриваемом примере Sudo запрашивает пароль не при каждом выполнении команд от имени пользователя `root`. Это объясняется тем, что в настройках, используемых Sudo по умолчанию, пароль при выполнении команд должен вводиться не каждый раз, а по истечении пятиминутного интервала.

Шаг 4

Проверьте совпадение контрольных сумм архива и контрольной суммы, определенной нами при создании архива:

```
[karlnext@test /]$ sudo cat /apache-php-perl-chroot.20030719.tar.md5sum
c1977535648f0840db3893b3c2d36730  apache-php-perl-chroot.20030719.tar

[karlnext@test /]$ sudo md5sum /apache-php-perl-chroot.20030719.tar
c1977535648f0840db3893b3c2d36730  /apache-php-perl-chroot.20030719.tar
```

Шаг 5

Восстановите инсталляцию Apache HTTP Server:

```
[karlnext@test /]$ sudo tar xpf /apache-php-perl-chroot.20030719.tar
```

Шаг 6

Запустите Apache HTTP Server:

```
[karlnext@test /]$ sudo /etc/init.d/httpd start
Запускается httpd:                    [OK]
```

Шаг 7

Удалите в корневом каталоге архив и файл, содержащий контрольную сумму:

```
[karlnext@test /]$ sudo rm -f apache-php-perl-chroot.20030719.tar \
> apache-php-perl-chroot.20030719.tar.md5sum
```

Шаг 8

Определите текущее время:

```
[karlnext@test /]$ date
Суб Июл 19 17:44:55 MSD 2003
```

Неплохой результат – всего лишь за несколько минут программа tar восстановила инсталляцию. При хорошем стечении обстоятельств повторная инсталляция Apache HTTP Server, PHP, mod_perl в окружении chroot-jail заняла бы не менее часа. На самом деле времени на восстановление инсталляции с использованием программы tar уйдет несколько больше, т. к. при этом возможно несанкционированное изменение прав доступа к файлам. Права доступа к файлам придется проверить вручную, при этом списки проинсталлированных файлов, которые мы рекомендовали создавать для каждого программного обеспечения, устанавливаемого на сервере, могут оказаться очень полезными. А где же взять исходные права доступа к файлам? Их нужно запомнить и сохранить в надежном месте сразу же после инсталляции программного обеспечения. Например, если вы установили программу LogSentry в соответствии с рекомендациям главы 16, после удаления из файла `logsentry.installed` файлов псевдофайловой системы `/proc`, непрерывно модифицируемых во время нормальной работы системы, в частности, при инсталляции программного обеспечения, в нем останется следующий список проинсталлированных файлов:

```
/etc/logsentry
/etc/logsentry/violations
/etc/logsentry/violations.ignore
/etc/logsentry/ignore
/etc/logsentry/hacking
/usr/bin/logtail
/usr/sbin/logcheck.sh
/var/logsentry
```

Для сохранения прав доступа к этим файлам выполните команду:

```
[karlnext@test /]$ sudo ls -l `cat logsentry.installed` \
> > logsentry.installed.perm
Password: Secretnoe_$loV0
```

В результате выполнения команды в файле `logsentry.installed.perm` сохранятся права доступа файлов, установленные при инсталляции программы LogSentry:

```
-rw-------    1 root     root         1037 Апр 24 14:11
/etc/logsentry/hacking
-rw-------    1 root     root         1172 Апр 24 14:11
/etc/logsentry/ignore
-rw-------    1 root     root          407 Апр 24 14:11
/etc/logsentry/violations
-rw-------    1 root     root           14 Апр 24 14:11
/etc/logsentry/violations.ignore
-rwx------    1 root     root         6500 Апр 24 14:12 /usr/bin/logtail
-rwx------    1 root     root        10915 Апр 24 14:11
/usr/sbin/logcheck.sh

/etc/logsentry:
итого 6
-rw-------    1 root     root         1037 Апр 24 14:11 hacking
-rw-------    1 root     root         1172 Апр 24 14:11 ignore
-rw-------    1 root     root          407 Апр 24 14:11 violations
-rw-------    1 root     root           14 Апр 24 14:11 violations.ignore

/var/logsentry:
итого 0
```

Сохранив файл `logsentry.installed.perm` в надежном месте, вы всегда сможете использовать его при восстановлении программы LogSentry из архива с помощью программы tar.

Автоматическое резервное копирование периодически изменяемых файлов

Ниже предлагается алгоритм организации автоматического резервирования периодически изменяемых файлов. В рассматриваемом примере автоматизация резервирования осуществляется с использованием файлов сценариев, исполняемых командным интерпретатором, и регулярно запускаемых с помощью `cron`.

Как было отмечено выше, для архивации некоторых файлов в каталоге `/etc/` требуются права суперпользователя `root`. Запуск сценария, осуществляющего архивацию от имени пользователя `root`, да еще в автоматическом режиме, представляет существенную угрозу для безопасности сервера. Использование для запуска сценария учетных записей пользователей `drwalbr` и `karlnext`, которым в соответствии с рекомендациями главы 14 в настройках программы Sudo по существу делегированы полномочия пользователя `root`, также не является приемлемым вариантом. Кроме того, указанные пользователи при выполнении команд от имени суперпользователя `root` должны вводить пароли, что исключает запуск сценария архивации в автоматическом режиме. Поэтому в дальнейшем мы создадим пользователя `rootarh`, полномочия которого с использованием настроек Sudo будут существенно ограничены, т. е. ему будет разрешено запускать от имени пользователя `root` только сценарий архивации без ввода пароля.

Полное резервное копирование

Схема полного копирования подразумевает периодическое, например, ежедневное, создание и перенос на съемный носитель или сервер резервного копирования архива, содержащего копии всех подлежащих архивации файлов и каталогов. Для реализации такой схемы необходимо выполнить следующие операции.

Шаг 1

Создайте пользователя `rootarh`, которому в дальнейшем будет разрешен доступ для архивации файлов, доступных только для пользователя `root`:

```
[karlnext@test karl_next]$ sudo /usr/sbin/useradd -d /home/rootarh -g us-
ers -s /bin/bash rootarh
[karlnext@test karl_next]$ sudo /usr/bin/passwd rootarh
Enter new password: ()(hen_$ecretnoe_S!0vo
```

```
Re-type new password: ()(hen_$ecretnoe_S!0vo
passwd: all authentication tokens updated successfully.
```

Шаг 2

Создайте файл `/root/tar_etc`, содержащий следующие строки:

```
#!/bin/bash
#########################################################################
#                 Исходные данные                                       #
#########################################################################
COMPUTER =test.bruy.info  #Имя системы.
LABELARH=etc-configs      #Осмысленное название архива.
DIRECTORIES="/etc/"       #Архивируемый каталог.
BACKUPDIR=/home/rootarh   #Каталог в который архивируется.
TAR=/bin/tar              #Путь к программе tar.
MD5SUM=/usr/bin/md5sum    #Путь к программе md5sum.
RESSERV=reserv.bruy.info  #Сервер резервного копирования.
RESSERVUSER=rootarh       #Пользователь для доступа к серверу
                          #резервного копирования.
RESDIR=/home/test.bruy.info
                          #Каталог на сервере резервного копирования.
MAIL=/bin/mail            #Путь к программе mail.
ADMINMAIL=ahradmin@bruy.info
                          #Почтовый адрес администратора
                          #резервного копирования.
SCP=/usr/bin/scp          #Путь к программе scp.
PATH=/usr/local/bin:usr/bin:/bin
#########################################################################
#########################################################################

#Текущая дата в,включаемая в имена файлов.
DATA=`date +%Y%m%d-%H.%M` #YYYYMMDD-HH.MM
#########################################################################
#                       Полное резервное копирование                    #
#########################################################################
#Создаем имя архива, включая путь.
#Имя файла имеет вид:
#etc-configs-test.bruy.info-YYYYMMDD-HH.MM.tar.
ARHIVNAME=$BACKUPDIR/$LABELARH-$COMPUTER-$DATA.tar
#Создаем архив.
$TAR -cpf $ARHIVNAME $DIRECTORIES
#Рассчитываем контрольную сумму архива и сохраняем ее в файле вида:
#etc-configs-test.bruy.info-YYYYMMDD-HH.MM.tar.md5
$MD5SUM $ARHIVNAME > $ARHIVNAME.md5
#Копируем архив и его контрольную сумму
#на сервер резервного копирования, используя команду scp.
$SCP -p $ARHIVNAME $ARHIVNAME.md5 $RESSERVUSER@$RESSERV:$RESDIR
RETVAL=$?
if [ $RETVAL = 0 ]; then
   #Если копирование прошло удачно
   #удаляем архив и файл с контрольной суммой на системе $COMPUTER.
   rm -f $ARHIVNAME
   rm -f $ARHIVNAME.md5
else
#Если копирование прошло неудачно,
#создаем тело сообщения о неудачном копировании.
   BODY=$LABELARH-$COMPUTER-$DATA.body
   echo Не могу скопировать $ARHIVNAME и $ARHIVNAME.md5 на $RESSERV ! \
      > $BODY
   #Отправляем сообщение о неудачном копировании
   #администратору, оставляя архив и контрольную сумму
   #на системе $COMPUTER.
   $MAIL $ADMINMAIL \
      -s "$COMPUTER:$BACKUPDIR проблемы с резервным копированием !" \
      < $BODY
```

```
        #Удаляем тело сообщения о неудачном копировании.
        rm -f $BODY
    fi
```

ЗАМЕЧАНИЕ Раздел сценария, содержащий исходные данные, вы можете модифицировать в соответствии с вашими потребностями, определив при этом, что архивировать, куда копировать полученные архивы и отправлять сообщения об ошибках.

В рассматриваемом примере сценарий выполняет следующие операции:

- создает на системе `test.bruy.info` архив `etc-configs-test.bruy.info-YYYYMMDD-HH.MM.tar`;
- определяет контрольную сумму архива и сохраняет ее в файле `etc-configs-test.bruy.info-YYYYMMDD-HH.MM.tar.md5`;
- копирует файлы, содержащие архив и контрольную сумму, на сервер резервного копирования `reserv.bruy.info` в каталог `/home/test.bruy.info`, используя на удаленном сервере учетную запись пользователя `rootarh`;
- в случае удачного копирования удаляет файлы с архивом и его контрольной суммой с системы `test.bruy.info`, в противном случае оставляет файлы на системе `test.bruy.info` и отправляет администратору резервного копирования на почтовый адрес `ahradmin@bruy.info` сообщение следующего содержания:

```
Subject: test.bruy.info:/home/rootarh проблемы с резервным копированием

Не могу скопировать /home/rootarh/etc-configs-test.bruy.info-YYYYMMDD-
HH.MM.tar и /home/rootarh/etc-configs-test.bruy.info-YYYYMMDD-
HH.MM.tar.md5 на reserv.bruy.info !
```

Шаг 3

Установите права доступа к файлу `/root/tar_etc` и назначьте его владельцем пользователя `root`:

```
[karlnext@test karl_next]$ sudo chmod 500 /root/tar_etc
Password: Secretnoe_$loV0
[karlnext@test karl_next]$ sudo chown 0.0 /root/tar_etc
```

Шаг 4

Разрешите пользователю `rootarh` выполнение сценария `/root/tar_etc` от имени пользователя `root` без ввода пароля. Для этого с использованием специализированного текстового редактора visudo (использование других редакторов недопустимо):

```
[karlnext@test karl_next]$ sudo visudo
```

отредактируйте файл `/etc/sudoers`, руководствуясь вашими потребностями и ниже приведенными рекомендациями:

```
#Описание пользователей, которым разрешено использовать SUDO
User_Alias FULLTIME_USERS = drwalbr, karlnext

#Описание команд
Cmnd_Alias  ETC=/root/tar_etc

#drwalbr, karlnext при обращении к Sudo
#должны вводить не свой, а пароль root
Defaults:FULLTIME_USERS rootpw
Defaults:FULLTIME_USERS !lecture

#Пользователю root разрешено выполнение команд
#от имени других пользователей
root ALL = (ALL) ALL

#drwalbr, karlnext могут выполнять любые команды
# но после ввода пароля
FULLTIME_USERS ALL =  ALL

#rootarh от имени root
#без ввода пароля
#может выполнять только команды
```

```
#определенные алиасом ETC
rootarh test = NOPASSWD: ETC
```

Строка:

```
rootarh test = NOPASSWD: ETC
```

разрешает пользователю `rootarh` выполнять команду, указанную в строке:

```
Cmnd_Alias  ETC=/root/tar_etc
```

на системе `test` без ввода пароля.

Шаг 5

Для организации копирования с использованием команды `scp` необходимо выполнить следующие операции.

Сгенерируйте на системе `test.bruy.info` открытый и закрытый ключи OpenSSH для пользователя `rootarh` в соответствии с рекомендациями главы 13:

```
[karlnext@test karl_next]$ ssh karlnext@resserv.bruy.info
Enter passphrase for key '/home/karlnext/.ssh/id_dsa':
Estcho_()dn0_(ecretn0e_$lovo
```

Создайте на сервере резервного копирования пользователя `rootarh` с домашним каталогом `/home/rootarh`:

```
[karlnext@resserv karl_next]$ sudo /usr/sbin/useradd -d /home/rootarh -g
users -s /bin/bash rootarh
Password: Secretnoe_$loV0
[karlnext@resserv karl_next]$ sudo /usr/bin/passwd rootarh
Enter new password: ()(hen_$ecretnoe_S!0vo
Re-type new password: ()(hen_$ecretnoe_S!0vo
passwd: all authentication tokens updated successfully.
```

и каталог для хранения архивных файлов системы `test.bruy.info`:

```
[karlnext@resserv karl_next]$ sudo mkdir /home/rootarh/test.bruy.info
[karlnext@resserv karl_next]$ sudo chmod 0600 –R /home/rootarh/
```

Сгенерируйте открытый и закрытый ключи OpenSSH для пользователя `rootarh` в соответствии с рекомендациями главы 13.

Осуществите обмен ключами пользователя `rootarh` между системами `test.bruy.info` и `resserv.bruy.info` в соответствии с рекомендациями главы 13.

Для обеспечения доступа пользователя `rootarh` с системы `test.bruy.info` на систему `resserv.bruy.info` внесите изменения в файл `/etc/ssh/ssh_config`, находящийся на сервере резервного копирования, добавив в конец файла строки, разрешающие соединение с IP-адреса, используемого системой `test.bruy.info`, например, 212.111.80.42:

```
Host 212.111.80.42
ForwardAgent no
ForwardX11 no
RhostsAuthentication no
RhostsRSAAuthentication no
RSAAuthentication no
PasswordAuthentication no
FallBackToRsh no
UseRsh no
BatchMode yes
CheckHostIP no
StrictHostKeyChecking yes
IdentityFile ~/.ssh/identity
IdentityFile ~/.ssh/id_dsa
IdentityFiie ~/.ssh/id_rsal
IdentityFile ~/.ssh/id_rsa2
Port 22
Protocol 2,1
Cipher blowfish
EscapeChar ~
```

При этом строка:

```
Host 212.111.80.42
```

указывает на то, что все следующие ниже директивы относятся только к IP-адресу 212.111.80.42.

Строка:

```
BatchMode yes
```

разрешает доступ пользователей без ввода пароля.

В файле /etc/ssh/sshd_config отредактируй строку:

```
AllowUsers drwalbr karlnext
```

в которой определен список пользователей, которым разрешен доступ к системе resserv.bruy.info, добавив в нее пользователя rootarh:

```
AllowUsers drwalbr karlnext rootarh
```

Для вступления изменений в силу перезагрузите sshd на системе resserv.bruy.info:

```
[karlnext@resserv karl_next]$ sudo /etc/init.d/sshd restart
Password: Secretnoe_$loV0
Останавливается sshd:                [OK]
Запускается sshd:                    [OK]
```

Завершите работу с системой resserv.bruy.info:

```
[karlnext@resserv karl_next]$ exit
```

Шаг 6

Для проверки работоспособности сценария и сделанных вами настроек зарегистрируйтесь на системе test.bruy.info в качестве пользователя rootarh и запустите сценарий /root/tar_etc:

```
[rootarh@test rootarh]$ sudo /root/tar_etc
```

Шаг 7

Если сценарий работает нормально, и вы хотите, чтобы он выполнялся ежедневно, например, в 19.25 – добавьте в таблицу заданий crontab пользователя rootarh, используя команду:

```
[rootarh@test rootarh]$ crontab -e
```

и используя функции редактирования текстового редактора vi – следующую строку:

```
25 19 * * * sudo /root/tar_etc
```

Шаг 8

Подождите, пока сценарий запустится автоматически. По окончании его выполнения на почтовый адрес rootarh@test.bruy.info должно поступить сообщение, автоматически сгенерированное демоном crond обо всех ошибках, имевших место при выполнении сценария.

Инкрементное резервирование копирование

Рассмотренная выше схема полного резервного копирования предъявляет достаточно жесткие требования к объему носителей, используемых для хранения резервируемой информации, и пропускной способности сети, т. к. регулярно создает и копирует по сети архив, содержащий копии всех файлов и каталогов. Для сокращения объема хранимой и передаваемой по сети информации обычно используют схему инкрементного резервного копирования. При этом копирование полного архива, содержащего копии всех файлов и каталогов, происходит относительно редко и более часто – архивов, содержащих файлы и каталоги, измененные после последнего полного резервного копирования. Ниже приведен пример сценария, еженедельно осуществляющего полное резервное копирование и инкрементное ежедневное резервное копирование:

```
!/bin/bash
#############################################################################
#                 Исходные данные                                           #
#############################################################################
$COMPUTER=test.bruy.info  #Имя системы
LABELARH=etc-configs      #Осмысленное название архива.
DIRECTORIES="/etc/"       #Архивируемый каталог.
BACKUPDIR=/home/rootarh   #Каталог в который архивируется.
TAR=/bin/tar              #Путь к программе tar.
MD5SUM=/usr/bin/md5sum    #Путь к программе md5sum.
FULLDAY=5                 #Номер дня недели (0,1,2,...6 начиная с Вск.)
                          #в который осуществляется
                          #полная еженедельная
```

```
                          #архивация.
RESSERV=reserv.bruy.info  #Сервер резервного копирования
RESSERVUSER=rootarh       #Пользователь для доступа к серверу
                          #резервного копирования
RESDIR=/home/test.bruy.info
                          #Каталог на сервере резервного копирования
MAIL=/bin/mail            #Путь к программе mail.
ADMINMAIL=ahradmin@bruy.info
                          #Почтовый адрес администратора
                          #резервного копирования.
SCP=/usr/bin/scp          #Путь к программе scp
#############################################################################
#############################################################################

PATH=/usr/local/bin:usr/bin:/bin
#Текущая дата в разных форматах
#включаемая в имена файлов архивов.
DATA=`date +%Y%m%d-%H.%M` #YYYYMMDD-HH.MM
DOW=`date +%w`            #0,1,2,...6 (начиная с Вск.)
DOM=`date +%d`            #01,02,03,...31
NOW=`date +%D`            #MM/DD/YY
TIMEFILE=$LABELARH-$COMPUTER-last-full-date
#############################################################################
#             Еженедельное полное резервное копирование                     #
#############################################################################
if [ $DOW = $FULLDAY ]; then
   #Создаем файл, содержащий дату последнего полного архивирования.
   echo $NOW > $TIMEFILE
   #Создаем имя архива, включая путь.
   #Имя файла имеет вид:
   #etc-configs-test.bruy.info-full_week-YYYYMMDD-HH.MM.tar.
   ARHIVNAME=$BACKUPDIR/$LABELARH-$COMPUTER-full_week-$DATA.tar.
   #Создаем архив.
   $TAR -cpf $ARHIVNAME $DIRECTORIES
   #Рассчитываем контрольную сумму архива и сохраняем ее в файле вида:
   #etc-configs-test.bruy.info-full_week-YYYYMMDD-HH.MM.tar.md5
   $MD5SUM $ARHIVNAME > $ARHIVNAME.md5
   #Копируем архив и его контрольную сумму
   #на сервер резервного копирования, используя команду scp.
   $SCP -p $ARHIVNAME $ARHIVNAME.md5 $RESSERVUSER@$RESSERV:$RESDIR
   RETVAL=$?
   if [ $RETVAL = 0 ]; then
      #Если копирование прошло удачно
      #удаляем архив и файл с контрольной суммой на системе $COMPUTER.
      rm -f $ARHIVNAME
      rm -f $ARHIVNAME.md5
   else
     #Если копирование прошло неудачно,
     #создаем тело сообщения о неудачном копировании.
     BODY=$LABELARH-$COMPUTER-$DATA.body
     echo Не могу скопировать $ARHIVNAME и $ARHIVNAME.md5 на $RESSERV !\
     > BODY
     #Отправляем сообщение о неудачном копировании
     #администратору, оставляя архив и контрольную сумму
     #на системе $COMPUTER.

     $MAIL $ADMINMAIL \
     -s "$COMPUTER:$BACKUPDIR проблемы с резервным копированием !" \
     < $BODY
     #Удаляем тело сообщения о неудачном копировании.
     rm -f $BODY
   fi
else
```

```
#########################################################################
#            Ежедневное инкрементное резервное копирование              #
#########################################################################

   #Генерируем строку, содержащую опцию tar --newer,
   #предписывающую добавлять в архив только файлы
   #с датой модификации после последней полной архивации.
   #Дату последней полной архивации мы берем из файла $TIMEFILE
   OPTIONS="--newer `cat $TIMEFILE`"
   ARHIVNAME=$BACKUPDIR/$LABELARH-$COMPUTER-$DOW-$DATA.tar
   #Создаем архив, куда включаются только файлы с датой модификации
   #большей, чем дата последней полной архивации.
   #Имя файла имеет вид:
   #etc-configs-test.bruy.info-W-YYYYMMDD-HH.MM.tar.
   $TAR $OPTIONS -cpf $ARHIVNAME $DIRECTORIES
   #Рассчитываем контрольную сумму архива и сохраняем ее в файле вида:
   #etc-configs-test.bruy.info-W-YYYYMMDD-HH.MM.tar.md5
   $MD5SUM $ARHIVNAME > $ARHIVNAME.md5
   #Копируем архив и его контрольную сумму
   #на сервер резервного копирования, используя команду scp.
   #В случае неудачного копирования отправляем письмо администратору.
   $SCP -p $ARHIVNAME $ARHIVNAME.md5 $RESSERVUSER@$RESSERV:$RESDIR
   RETVAL=$?
   if [ $RETVAL = 0 ]; then
      rm -f $ARHIVNAME
   else
     BODY=$LABELARH-$COMPUTER-$DATA.body
     echo Не могу скопировать $ARHIVNAME или $ARHIVNAME.md5 на $RESSERV
!\
 > \ $BODY
     $MAIL $ADMINMAIL \
     -s "$COMPUTER:$BACKUPDIR проблемы с резервным копированием !" \
     < $BODY
     rm -f $BODY
   fi
fi
```

В рассматриваемом примере сценарий каждую пятницу осуществляет полное резервное копирование, выполняя следующие операции:

- создает на системе `test.bruy.info` архив `etc-configs-test.bruy.info-full_week-YYYYMMDD-HH.MM.tar`;
- определяет контрольную сумму архива и сохраняет в файле `etc-configs-test.bruy.info-full_week-YYYYMMDD-HH.MM.tar.md5`;
- запоминает дату последнего полного резервного копирования в файле `etc-configs-test.bruy-last-full-date`;
- копирует файлы, содержащие архив и контрольную сумму на сервер резервного копирования `reserv.bruy.info` в каталог `/home/test.bruy.info`, используя на удаленном сервере учетную запись пользователя `rootarh`;
- в случае удачного копирования удаляет файл с архивом и его контрольной суммой на системе `test.bruy.info`, в противном случае оставляет файлы на системе `test.bruy.info` и отправляет администратору резервного копирования на почтовый адрес `ahradmin@bruy.info` сообщение вида:

  `Не могу скопировать $ARHIVNAME и $ARHIVNAME.md5 на $RESSERV !\.`

В остальные дни недели:

- создает с использованием опции `--newer` программы tar на системе `test.bruy.info` архив `etc-configs-test.bruy.info-W-YYYYMMDD-HH.MM.tar`, содержащий все файлы, измененные со времени последнего полного резервного копирования;
- определяет его контрольную сумму архива и сохраняет в файле `etc-configs-test.bruy.info-W-YYYYMMDD-HH.MM.tar.md5`;
- копирует файлы, содержащие архив и контрольную сумму на сервер резервного копирования `reserv.bruy.info` в каталог `/home/test.bruy.info`, используя на удаленном сервере учетную запись пользователя `rootarh`;

- в случае удачного копирования удаляет файл с архивом и его контрольной суммой на системе `test.bruy.info`, в противном случае оставляет файлы на системе `test.bruy.info` и отправляет администратору резервного копирования на почтовый адрес `ahradmin@bruy.info` сообщение.

Научное издание

Валентин Валентинович **Бруй**,
Сергей Владимирович **Карлов**

LINUX-СЕРВЕР:
ПОШАГОВЫЕ ИНСТРУКЦИИ
НАСТРОЙКИ И ИНСТАЛЛЯЦИИ

Изд. лиц. ИД №04975 от 04.06.2001.
Бум. офс. Формат 60x90 1/8.
Гарнитура Таймс. Печать офс.
Усл. печ. л. 35,7. Тираж 1000 экз.
Подписано в печать 03.10.03. Заказ 120/03.
Издательско-полиграфический центр
автономной некоммерческой организации
«Секция «Инженерные проблемы стабильности
и конверсии» Российской инженерной академии» (СИП РИА),
103918, Москва, Газетный пер., д. 9, стр. 4, тел. 745-96-87
http://www.sipria.ru ; e-mail : pva@sipria.msk.ru
Типография СИП РИА. 141092, Московская обл., г. Юбилейный-2,
ул. Тихонравова, 29, тел. 515-35-93