Александр Соловков

Сетевой колхоз

Рано или поздно у любого пользователя возникает необходимость поделиться своими файлами с другими клиентами локальной сети, обменяться накопленной информацией, организовать совместную работу над проектами. Можно, конечно, осуществить файловый обмен посредством Интернета и протокола FTP (и вы наверняка это уже делали). Но существуют гораздо более удобные способы. Итак, встречайте — NFS!

Сетевая файловая система (NFS — Network File System) обеспечивает совместное использование файлов в ОС Unix. В таких операционных системах как Windows или Mac OS есть собственные механизмы, позволяющие подключенным к сети компьютерам обращаться к файлам на удаленных машинах так, как если бы они находились на их собственном диске. Система NFS обеспечивает те же преимущества, а также ряд других возможностей, отсутствующих в аналогичных протоколах коллективной работы с данными.

Немного теории

ОС Windows использует для совместного доступа к файлам протокол NetBIOS, а Mac OS — протокол AppleTalk. Оба этих протокола двухточечные: каждая система сообщает о своем присутствии в сети широковещательной рассылкой, и все машины могут динамически монтировать ресурсы друг друга, предоставленные для общего доступа. Система NFS отличается от них тем, что использует протокол типа «клиент-сервер», явно выделяя серверы, предоставляющие ресурсы в совместный доступ. Эти ресурсы, в свою очередь, могут быть смонтированы удаленными клиентами NFS. Таким образом, объем передаваемой по сети информации уменьшается за счет отсутствия многочисленных ненужных запросов и ответов на них. Кроме того, сервер явно определяет, какие клиенты могут к нему подключаться, в зависимости от имени хоста или IP-адреса. Еще одно полезное свойство системы NFS заключается в том, что она не зависит от широковещательной рассылки в локальной сети, применяющейся для выявления серверов. Поэтому ее можно использовать в Интернете точно таким же образом, как и в локальной сети. Помимо этого, NFS отслеживает целостность передаваемых данных, уменьшая вероятность их потери.

Для операционной системы Linux NFS — точно такая же файловая система, как и любая другая. Общий ресурс NFS вы

можете смонтировать по сети точно так же, как вы обычно делаете это с дискетой или разделом жесткого диска. Общие ресурсы могут даже автоматически монтироваться в случае обращения к ним, если, конечно, клиентская система настроена соответствующим для этого образом (об этом мы вам расскажем немного позже).

Linux можно сконфигурировать для работы в качестве сервера, клиента NFS или того и другого одновременно.

Конфигурирование сервера NFS

Чтобы настроить Linux для работы в качестве сервера NFS, нужно включить одноименный сервис, например, через утилиту ntsysv или в графическом режиме с помощью меню «Системные параметры → Настройка сервера → Службы». Убедитесь также, что запущен сервер portmap. Он необходим для функционирования системы NFS, поскольку NFS-серверу требуется механизм оповещения клиентов о том, к какому порту им подключаться.

После установки этих опций и перезагрузки Linux предоставит через NFS общие ресурсы, указанные в файле /etc/exports. В нем должны быть перечислены каталоги, которые необходимо выложить в общий доступ через NFS, а также имена пользователей и хосты, которые будут иметь право доступа к ним. Если файл /etc/exports не существует или недоступен для чтения в самом начале работы сети, система NFS просто-напросто не запустится.

Полный формат файла /etc/exports описывается на страницах специального справочного руководства «man exports». Строка экспорта должна включать в себя одно или несколько имен каталогов, которые экспортируются (то есть предоставляются для общего доступа), опций экспорта и необязательного списка хостов (тех, что задаются IP-адресом, именем сети, сетевой группой или по имени), которым разрешается использовать соответствующие каталоги. Например, приведенная ниже строка предоставляет в общий доступ каталог /home и все его внутренние подкаталоги для любого подключившегося хоста:

```
/home -alldirs
```

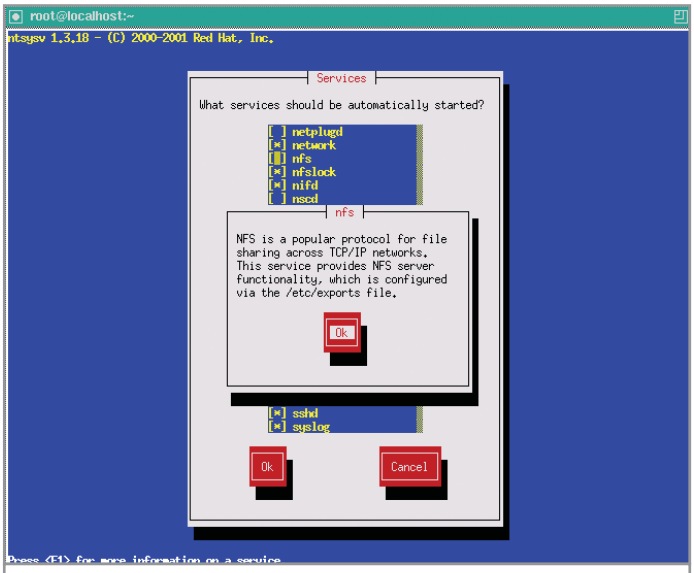
Учтите, что опция -alldirs может быть указана только в том случае, если общий ресурс является точкой монтирования физической файловой системы (например, /usr или /home). Иначе доступ к ресурсу предоставлен не будет.

Общий ресурс, доступ к которому (только для чтения) могут получить три указанных хоста, вы можете задать следующим образом:

```
/usr -ro -alldirs office.domain.ru managers.domain.ru
192.168.0.16
```

После внесения изменений в файл /etc/exports необходимо перезапустить систему NFS. Для этого введите команду:

```
/etc/rc.d/init.d/nfs restart
```



Если вы хотите, чтобы NFS-сервер запускался при старте системы, используйте утилиту ntsysv

Чтобы получить список всех имеющихся общих ресурсов и права доступа к ним, можно использовать команду «showmount». Проверить, правильно ли настроен файл /etc/exports, можно следующим образом:

```
showmount -e
Exports list on localhost:
/usr            Everyone
/home/lena      192.168.0.47
/home/vasya     192.168.0.49
/               192.168.0.1
```

Конфигурирование клиента NFS

Если вы собираетесь монтировать общие ресурсы NFS с других серверов, то для начала необходимо сконфигурировать вашу систему в качестве клиента. С технической точки зрения это совсем необязательно — можно монтировать общий ресурс NFS примитивным способом, не прибегая к каким-либо предварительным настройкам. Однако конфигурирование системы в качестве клиента NFS предоставляет много дополнительных возможностей и гарантирует обеспечение быстрой и надежной работы.

Монтирование удаленных файловых систем

Монтирование общего ресурса NFS выполняется с помощью команды «mount». Как правило, этой команде передаются два аргумента — имя хоста и имя общего ресурса в виде комбинированной строки, а также локальная точка монтирования:

```
mount -t nfs office:/home /home2
```

При успешном монтировании на экран не выдается никаких сообщений. Проверить, успешно ли произошло монтирование, можно командой «df»:

Команда разработчиков пакета Samba

```
df
Filesystem     1K-blocks  Used     Avail    Capacity  Mounted on
/dev/hda1      992239     54353    858597   6%        /
/dev/hda2      26704179   4872963  19694882 20%       /home
procfs         4          4        0        100%      /proc
office:/home   9924475    1642343  7488174  18%       /home2
```

Файловая система будет оставаться смонтированной до тех пор, пока не будет явно демонтирована с помощью команды «umount»:

```
umount /home2
```

Как и в других типах файловых систем, здесь можно добавить описание монтируемых ресурсов NFS в файл /etc/fstab, что впоследствии упростит сам процесс монтирования:

```
Device          Mountpoint  Fstype  Options          Dump  Pass#
office:/home    /home2      nfs     rw,-T,-i,noauto  0     0
```

При наличии такой записи можно смонтировать файловую систему NFS следующей простой командой:

```
mount /home2
```

Более подробную информацию об опциях монтирования вы можете получить в справочной системе с помощью команды «man mount».

Демон автоматического монтирования

Демон автоматического монтирования amd дает возможность сделать работу с общими ресурсами NFS еще более простой и удобной. Он позволяет монтировать их (а на самом деле и все типы файловых систем тоже) динамически при переходе в необходимый каталог, не вводя при этом никаких соответствующих команд.

Настроить этот демон можно с помощью утилиты ntsysv или через пункт меню «Системные параметры → Настройка сервера → Службы».

Демон можно также запустить вручную с помощью ниже приведенной команды:

```
amd -a /.amd_mnt -l syslog /host /etc/amd.map /net
/etc/amd.map
```

Теперь при работающем демоне amd нужно перейти с помощью команды «cd» в каталог /host и просмотреть его содержимое. Как видите, система выдает сообщение о том, что данный каталог пуст:

```
cd /host
ls
#
```

Однако можно попытаться найти каталог по имени таким образом, как будто бы там уже имеется директория, имя которой совпадает с именем одного из серверов NFS в сети:

```
ls office
# homes
```

В каталоге /host действительно появился office, а в нем — подкаталог homes, содержащий то же самое, что и office:/homes. Он только что автоматически подмонтировался в каталог /host при первом же обращении к нему.

Для еще большего удобства можно создать символическую ссылку на нужный каталог:

```
ln -s /host/office/homes /home2
```

С этого момента при переходе в каталог /home2 общий ресурс office:/homes будет монтироваться автоматически, и вы получите доступ к нужным файлам. Неиспользуемый общий ресурс будет автоматически демонтирован.

Можно создавать намного более сложные карты монтирования для демона amd, задавая записи в файле /etc/amd.conf. Подробные сведения о его формате и предоставляемых им возможностях можно найти на страницах справочного руководства «man amd.conf».

Взаимодействие с сетью Windows

А что делать, если большинство пользователей вашей локальной сети работают на компьютерах под управлением операционной системы Windows? Система NFS — отличное решение проблемы совместного использования файлов Unix-машинами, однако она мало распространена в большинстве пользовательских операционных систем. Windows поддерживает ее только с помощью приложений сторонних производителей. Поэтому при включении компьютера под управлением Linux в существующую сеть нужно выполнить несколько необходимых настроек, позволяющих операцион-

ной системе поддерживать те же методы совместного использования файлов, что и Windows.

Какие-либо подобные средства изначально не встраиваются в Linux. Однако дополнительный пакет, который называется Samba, предоставит вашей машине под управлением этой ОС возможность работать в качестве файл-сервера Windows и участвовать в совместном использовании файлов с реальными клиентами Windows.

Введение в систему Samba

Система Samba — это некоммерческий проект с открытым исходным кодом, который позволит вашей системе пользоваться всеми преимуществами совместного доступа к файлам Windows. Но SMB представляет собой нечто большее, чем просто протокол для обмена файлами. Например, он позволяет совместно использовать принтеры, последовательные порты и даже такие абстрактные ресурсы как named pipes и слоты для обмена сообщениями (mailslots). SMB использует протокол более низкого уровня — NetBIOS, разработанный IBM в 1985 году, который, в свою очередь, может работать на любом другом протоколе layer 3 — TCP/IP, SPX/IPX, DECnet; или же на специально созданном для транспорта NetBIOS-пакетов в небольших сетях NetBEUI. В NetBIOS/SMB входят не только методы для работы с файлами, но и средства обнаружения (browsing) SMB-серверов, что отличает этот протокол ото всех остальных. Серверы с помощью широковещательных пакетов анонсируют свое присутствие в сети, а также отвечают на запросы, поступающие от клиентов, что позволяет последним получать актуальные списки сетевого окружения.

В SMB используются две модели защиты — на уровне ресурса (share level) и на уровне пользователя (user level). В первом случае устанавливается пароль на ресурс (share) в целом, и при успешной аутентификации клиент получает права на доступ ко всем файлам, находящимся внутри. Во втором же случае в процессе установки сессии происходит аутентификация пользователя, и ему выдается UID (универсальный идентификатор пользователя), который впоследствии будет применяться для определения различных прав доступа на файловом уровне.

При работе используются фиксированные «хорошо известные» (well-known) TCP/UDP-порты (135, 137-139, 445), что позволяет легко настроить брандмауэр для защиты от посторонних вторжений. Это особенно актуально, если вспомнить о регулярно обнаруживаемых уязвимостях в сетевых сервисах от Microsoft. Защиты передаваемых данных не предусмотрено, за исключением шифрования пароля при аутентификации.

Для данного протокола характерны небольшие задержки при работе с файловой системой, но при должной настройке сервера будет обеспечена высокая скорость передачи данных. Значительным преимуществом является поддержка различных кодовых страниц, что позволяет клиентам, использующим Linux, понимать русские имена файлов на Windows-сервере, и наоборот.

В Fedora Core 3 присутствует поддержка smbfs, позволяющая монтировать удаленные ресурсы SMB-сервера. В пакет

Конфигурировать настройки Samba можно и через веб-интерфейс с помощью программы SWAT

Samba входит smbclient, предоставляющий помимо пользовательского интерфейса командной строки, схожего с FTP, еще и возможность печати на удаленных принтерах. Samba-сервер позволяет компьютеру с Linux подключаться к NT-домену в качестве клиента или контроллера домена (разумеется, поддерживается и работа без него), предоставлять Windows- и Unix-клиентам доступ к локальному принтеру, а также поддерживать список серверов для своей рабочей группы.

Протокол не стоит использовать при наличии заметных задержек в сети (например, в случае, когда пакетам нужно пройти через несколько маршрутизаторов). В целом SMB делает ограничение доступа к файлам на уровне ресурсов несколько проще, а множество настроек Samba-сервера и SWAT (веб-интерфейс для его конфигурирования, также входящий в пакет Samba) позволяют оптимально настроить сервер даже начинающему администратору.

Установка и конфигурирование Samba

В самом простом случае запуска системы Samba необходимо только отредактировать файл smb.conf, изменив строку рабочей группы в соответствии с именем рабочей группы или домена, в который должна входить машина:

```
workgroup = MY_WORKGROUP
```

Теперь при перезагрузке системы Samba будет запускаться автоматически.

Интернет-SWAT

Основным файлом конфигурации системы Samba является /usr/local/etc/smb.conf, в котором можно устанавливать десятки различных параметров и задавать общие ресурсы. Каждая опция неплохо описана в комментариях в файле примера smb.conf.default, однако с ходу разобраться в его содержимом непросто: опций для установки там очень много (все они детально описаны на страницах справочного руководства man smb.conf), и между ними есть масса тонких различий.

Существует также альтернативный метод формирования и настройки файла smb.conf. Речь идет о системе SWAT (Samba Web Administration Tools), который входит в состав портированного пакета Samba и позволяет конфигурировать его через веб-браузер. В результате существенно упрощается работа с файлом конфигурации, снижается вероятность появления в нем ошибок. Недостаток же этой системы, к сожалению, присущ всем без исключения веб-приложениям — это существенная угроза безопасности. Система SWAT аутентифицирует клиентов с помощью базы данных пользователей системы Linux, хранящейся в каталоге /etc/master.passwd, и посылает эти данные по сети в нешифрованном виде, из-за чего они могут быть легко перехвачены злоумышленником. Риск можно значительно снизить, воспользовавшись следующими рекомендациями.

- Обращайтесь к системе SWAT только с локального хоста (localhost). Это предотвратит пересылку информации по сети.
- Работайте, пользуясь защитой брандмауэра, запрещающего передачу информации извне.
- По умолчанию файл smb.conf принадлежит суперпользователю, поэтому браузер должен регистрироваться в системе SWAT, передавая пароль пользователя root, который посылается по сети в явном виде вместе с каждым HTTP-запросом к SWAT. Никогда не делайте этого в сети, в которой потенциально может находиться злоумышленник.
- Создайте фиктивного пользователя (например, smbowner) и сделайте его владельцем файла smb.conf (с помощью команды «chown»). Работая с системой SWAT, регистрируйтесь под именем smbowner, а не root. Не используйте это имя пользователя для решения других задач на сервере, не давайте ему никаких привилегий, запретите доступ к командному интерпретатору и не создавайте для него домашний каталог.

Поддержку SWAT можно включить добавлением в файл /etc/services следующей строки:

```
swat 901/tcp
```

Затем впишите в файл /etc/xinetd.conf следующее:

```
swat stream tcp nowait root /usr/local/sbin/swat swat
```

И, наконец, перезапустите демон inetd:

```
/etc/rc.d/init.d/xinitd restart
```

Теперь вы можете обращаться к системе SWAT по адресу http://localhost:901. Она запросит имя пользователя и пароль. SWAT позволяет изменять настройки предоставляемых для общего доступа ресурсов и принтеров, а также глобальные настройки Samba. Вы можете также узнавать текущее состояние сервера и управлять пользователями системы.

Если же вы предпочитаете делать все собственными руками, можете внести изменения в файл конфигурации Samba посредством прямого редактирования smb.conf.

История развития и разновидности NFS

Сеть из мира Unix

В 1985 году компания Sun Microsystems выпустила первую версию сетевой файловой системы NFS (Network File System). Изначально предназначенная для экспортирования частей файловой системы с одного сервера на другой, она активно использовала протокол RPC для взаимодействия компонентов между собой, поддерживала совместный доступ к файлам, а также все их атрибуты, использующиеся в системах Unix, и являлась совершенно прозрачной для пользователя. Применение UDP-протокола вместо TCP уменьшило влияние сетевых задержек и требовательность к ресурсам слабых по нынешним меркам компьютеров того времени. В некоторых реализациях NFS приобрела различные полезные дополнения, например поддержку кеширования файлов NFS-сервера на диске клиента.

Время шло, требования возрастали. Первое значительное изменение протокола NFS в основном было связано с необходимостью поддержки файлов размером свыше 2 Гбайт. В состав изменений вошли:

- **увеличение максимального размера блока данных при операциях чтения/записи до 32 кбайт (large block file transfers);**
- **поддержка отложенной записи (прежние стандарты требовали от сервера сбросить данные на диск или в NVRAM, прежде чем отвечать на клиентский запрос о записи);**
- **readdirplus — возврат атрибутов файлов вместе с листингом каталога за одну операцию (в старых версиях для получения атрибутов всех файлов в каталоге с файлами в количестве N потребовалось бы число операций, равное N+1);**
- **поддержка TCP-протокола, что положительно сказалось на загрузке маршрутизаторов и брандмауэров.**

Все это привело к созданию сетевой файловой системы, которая стала настоящим чемпионом по производительности практически в любых операциях внутри локальной сети. Основным недостатком системы осталась слабая защищенность. Ведь NFS создавалась для экспорта файловой системы с Unix-хоста на Unix-хост внутри корпоративной сети. Сами пользователи работали с ней как с частью файловой системы, и никаких клиентских программ, как для FTP, не требовалось, поэтому и защита была реализована достаточно примитивно. Она работала только при том условии, что и сеть, и клиент, и сервер были защищены от хакерских действий. NFS-запросы должны были приходить с привилегированных портов 1–1024, которые не могли быть использованы пользовательскими приложениями в Unix. Права доступа к файлам определялись с помощью UID пользователя, переданного клиентом серверу.

Со временем серверы обзавелись дополнительными возможностями:

- **root_squash и all_squash указывают серверу, что операции, заявленные клиентом как проводящиеся с UID = 0 (root_squash) или вообще с любым UID (all_squash), должны исполняться с при-**

Предоставление каталогов для общего доступа

Немало примеров конфигурирования каталогов общего доступа можно найти в файле smb.conf.default. Чтобы задействовать их, вы должны внести соответствующие изменения (сняв комментарии на нужных строках) в файл smb.conf, а затем перезапустить сервер Samba:

```
/etc/rc.d/init.d/smb restart
```

Чтобы предоставить какой-либо каталог в общее пользование, нужно определить его как общий ресурс:

```
[public]
  comment = общие файлы
  path = /usr/local/share/samba-public
  public = yes
  writeable = yes
  printable = no
  write list = @users
```

При наличии таких строк клиент будет видеть в сетевом окружении ресурс public вашего компьютера. Однако, пока пользователь не будет аутентифицирован сервером и не станет членом Unix-группы «users», файлы ресурса будут доступны ему только для чтения.

По умолчанию определяется и включается [homes] — специальный общий встроенный ресурс, обеспечивающий доступ к домашнему каталогу для каждого пользователя, определенного на сервере Samba:

```
[homes]
  comment = домашние каталоги
  browseable = no
  writeable = yes
```

Данный ресурс установлен как «непросматриваемый» (browseable = no), но если клиент подключается от имени действительного пользователя, имеющего домашний каталог на сервере Samba, то [homes] появится в числе общедоступных ресурсов. При этом домашние каталоги других пользователей видны не будут.

Совместная печать

Как и [home], [printers] — это специальный общий ресурс, немного отличающийся от остальных. В Linux все принтеры, определенные в файле /etc/printcap, доступны каждому пользователю. По умолчанию ресурс [printers] настроен следующим образом:

```
[printers]
  comment = samba-принтер
  path = /var/spool/samba
  browseable = no
# Установите public = yes, чтобы разрешить печать
пользователю guest
```

вилегиями пользователя nobody. Это позволяет легко организовывать анонимный readonly-доступ к несекретной информации (например, видеофайлам, музыке, документации, дистрибутивам, /usr/share и т. д.);

- uid mapping позволяет организовать трансляцию клиентских UID в соответствующие им UID на стороне сервера, что полезно, например, когда пользователи с одинаковыми именами имеют различные UID на сервере и клиенте;
- insecure mounting и возможность привязки RPC-сервисов к определенным портам отменяют обязательное условие использования клиентом портов 1–1024. Это избавляет многих администраторов, настраивающих брандмауэры, от лишней головной боли.

Для привязки сервисов NFS к определенным портам, чтобы облегчить процесс настройки брандмауэра, стоит взглянуть на следующие страницы документации: rpc.statd (ключ -o), rpc.mountd (ключ -p), rpc.rquotad (ключ -p), rpc.nfsd (ключ -p).
Существует несколько реализаций NFS-серверов, поддерживающих шифрование трафика. Это, например, sNFS (www.crufty.net/ftp/pub/sjg/help/sNFS.html). Кроме того, при работе с NFS через TCP, как и практически в любой другой сетевой файловой системе, трафик можно перенаправить в предварительно установленный между хостами SSL-туннель (созданный, например, с помощью openssl, SSH или stunnel (http://www.stunnel.org). В NFSv4 (http://nfsv4.org) поддерживаются Kerberos-аутентификация и шифрование трафика.
Есть несколько NFS-клиентов для Windows, большинство из которых распространяются на коммерческой основе (http://hummingbird.com/products/nc/nfs/index.html?cks=y). Однако компания Microsoft не так давно сделала бесплатным свой Services For Unix v3.5 (www.microsoft.com/windows/sfu), в состав которого были включены и NFS-клиент, и NFS-сервер.
На сегодня область применения NFS не изменилась, и эта файловая система по-прежнему является самым универсальным методом обмена частями файловой системы между логически связанными серверами. С ее помощью можно раздавать дистрибутивы и обновления для серверов (используя параметр all_squash в каталоге /etc/exports). При возможности создания изолированного сегмента сети для серверов можно получить общий каталог /home. Можно создать также бездисковые рабочие станции (www.linux-center.ru/lib/networking/nfs_root_minihowto.phtml; www.remoteboot.ru/ru/remoteboot/dskless.html).
Немалый интерес представляет возможность примонтировать часть файловой системы сервера в chroot-окружение какого-либо демона, работающего на том же самом сервере в readonly-режиме: в случае взлома это гарантирует отсутствие троянов, например, в /usr. «Легкость» NFS в этом случае позволяет вам свести к минимуму издержки монтирования удаленной файловой системы.

Файловый менеджер Nautilus делает навигацию по сети Windows простой и удобной

guest ok = no
writeable = no
printable = yes

Управление доступом

В системе Samba есть два популярных способа управления доступом — на уровне пользователей и на уровне общих ресурсов. Стандартное управление доступом происходит на уровне пользователей и задается командой «security» в файле smb.conf:

security = user

При таком управлении доступом клиент в начале соединения предоставляет серверу имя пользователя и пароль. Если сервер успешно идентифицирует клиента, ему открываются для доступа все общие ресурсы.

При управлении доступом на уровне общих ресурсов клиент может подключаться к серверу Samba безо всякой аутентификации. Клиенту может быть отказано в доступе, только если его IP-адрес не указан в файле smb.conf (в строке «hosts allow»). При таком способе управления доступом клиент свободно может получить только те общие ресурсы, которые помечены параметром «public = yes», но домашние каталоги пользователей попрежнему будут защищены именем пользователя и паролем.

Подробнее об организации защиты ресурсов общего использования вы можете прочесть в файлах раздела документации /usr/share/doc/samba.

Гостевой пользователь

Доступ к некоторым службам Samba, в частности к службе печати, имеет смысл предоставить любому пользователю, независимо от аутентификации. Для этого нужно использовать так называемую гостевую учетную запись для пользователя, которому необходим доступ только к одной конкретной службе. Назначение гостевых пользователей рекомендуется в основном для серверов Samba, работающих с защитой на уровне ресурсов, поскольку доступ гостя к каждому ресурсу предоставляется или запрещается отдельно. Чтобы разрешить работу такому пользователю, раскомментируйте строку «guest account» в файле smb.conf следующим образом:

guest account = pcguest

Теперь необходимо добавить в систему учетную запись pcguest с помощью команды «adduser».

Файловая система smbfs

Совместное использование файлов по протоколу SMB может быть двусторонним. Удаленные общие ресурсы SMB можно монтировать так же, как и любую другую файловую систему. Речь идет о файловой системе smbfs, доступной в портированных приложениях каталога /usr/ports/net/smbfs.

Чтобы смонтировать SMB с помощью smbfs, используйте команду «mount_smbfs» вместе с несколькими простыми опциями. Например, -I задает имя хоста или IP-адрес, а два других аргумента – имя удаленного общего ресурса (в формате //пользователь@<имя NETBIOS>/<имя ресурса>) и локальную точку монтирования. Например, для монтирования общего ресурса public с Windows-машины office в локальный каталог /mnt/public используется следующая команда:

mount -t smbfs -o username = somename, password = somepass //office/public /mnt/public

По аналогии с предыдущими примерами можно добавить общий ресурс SMB для гостевого доступа в файл /etc/fstab с помощью следующей строки:

//guest@office/public /smb/public smbfs rw,noauto 0 0

Ресурс будет примонтирован при старте системы.

Окна в сеть

Есть еще более простой способ получить доступ к ресурсам Windows-сети — использование возможностей оболочек GNOME или KDE. Эти графические среды уже имеют встроенный samba-клиент. Все, что остается сделать, — это набрать в адресной строке файлового менеджера следующее:

smb://имя_ресурса

В появившемся окне нужно будет ввести имя пользователя и пароль. Если никаких ограничений на доступ к ресурсу нет, имя пользователя должно быть guest. Файловый менеджер Nautilus прекрасно отображает русские названия файлов и папок. Однако у такого способа есть и один недостаток, заключающийся в том, что ресурс не монтируется непосредственно в файловую систему Linux.

Как видите, работать в Linux с сетевыми ресурсами очень легко. Простой метод настройки и наличие большого объема различной справочной информации помогут вам сделать систему еще более удобной в использовании. |