Руководство сервера Ubuntu

Проект Документации Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Руководство сервера Ubuntu

by Проект Документации Ubuntu <*ubuntu-doc@lists.ubuntu.com*>

Аннотация

Введение в установку и настройку серверных приложений в Ubuntu.

Разработчики и лицензия

В разработке данного документа принимали участие следующие авторы Группы по документированию Ubuntu:

- Bhuvaneswaran Arumugam

Руководство сервера Ubuntu также основано на вкладе:

- Robert Stoffers
- Brian Shumate
- Rocco Stanzione

Заявление об отказе от ответственности

Были приложены все усилия, чтобы информация представленная в данной публикации была точной и правильной. Однако это не гарантирует полную достоверность. Ни Canonical Ltd., ни авторы, ни переводчики не несут ответственности за возможные ошибки или неточности.

Некоторые описания программного и аппаратного обеспечения, используемые в этой публикации, могут быть зарегистрированными торговыми марками и таким образом могут подпадать под ограничения авторского права и законы об ограничении торговли. Авторы никоим образом не утверждают свои права на такие имена.

ЭТА ДОКУМЕНТАЦИЯ ПОСТАВЛЯЕТСЯ АВТОРАМИ "КАК ЕСТЬ" И ЛЮБЫЕ ВЫРАЖЕННЫЕ ИЛИ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ПОДРАЗУМЕВАЕМЫМИ ГАРАНТИЯМИ ПОЛЕЗНОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ, НЕ ПРИНИМАЮТСЯ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ АВТОРЫ НЕ МОГУТ БЫТЬ ПРИВЛЕЧЕНЫ К ОТВЕТСТВЕННОСТИ ЗА ЛЮБОЙ ПРЯМОЙ, НЕПРЯМОЙ, СЛУЧАЙНЫЙ, ОСОБЫЙ, ЕДИНИЧНЫЙ ИЛИ ЯВНЫЙ УЩЕРБ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ПОСТАВКОЙ ЗАМЕЩАЕМЫХ ТОВАРОВ ИЛИ УСЛУГ; ПОТЕРЮ ПРИГОДНОСТИ, ДАННЫХ, ИЛИ ПРИБЫЛИ; ИЛИ ПРЕКРАЩЕНИЯ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ) СТАВШИЙ ПРИЧИНОЙ ЗАДОЛЖЕННОСТИ ПО КОНТРАКТУ, ПРЯМОЙ ОТВЕТСТВЕННОСТИ, ИЛИ ПРАВОНАРУШЕНИЯ (ВКЛЮЧАЯ ХАЛАТНОСТЬ ИЛИ ДРУГОЕ) ПОЯВИВШИЕСЯ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ БЫЛО УВЕДОМЛЕНИЕ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Содержание

Об этом руководстве v
1. Соглашения vi
2. Посильная помощь и обратная связь vii
1. Введение 8
2. Установка 9
1. Подготовка к установке 10
2. Установка с CD 12
3. Управление пакетами 13
1. Введение 14
2. Apt-Get 15
3. Aptitude 17
4. Конфигурация 19
5. Дополнительные репозитории 20
4. Работа в сети 21
1. Настройка сети 22
2. TCP/IP 25
3. Настройка межсетевого экрана (брандмауера) 30
4. Сервер OpenSSH 33
5. FTP Сервер 36
6. Сетевая файловая система (Network File System, NFS) 38
7. Протокол динамической настройки хостов (Dynamic Host Configuration Protocol, DHCP) 40
8. Служба именования доменов (DNS) 43
9. CUPS - сервер печати 45
10. HTTPD - веб сервер Apache2 48
11. Прокси-сервер Squid 58
12. Система контроля версий 60
13. Базы данных 67
14. Сервисы электронной почты 70
5. Работа в сети Windows 82
1. Введение 83
2. Установка SAMBA 84
3. Настройка SAMBA 85
A. Creative Commons by Attribution-ShareAlike 2.0 92
B. GNU Free Documentation License 97

Список таблиц

2.1. Рекомендованные минимальные требования 10
4.1. Методы доступа 61

Об этом руководстве

1. Соглашения

Следующие замечания относятся ко всей документации:

Замечания представляют интересные, иногда технические, куски информации связанные с текущим обсуждением.

Подсказка предлагает совет или более простое решение какой-либо ситуации.

Предостережение предупреждает о возможных проблемах и помогает предотвратить их.

Предупреждение информирует об угрозе, которая может возникнуть вследствие данного действия.

Соглашения о перекрестных ссылках при печати выглядят следующим образом:

- Ссылки на другие документы или веб-сайты выглядят следующим *образом* [http://www.ubuntu.com].

PDF, HTML, и XHTML версии этого документа используют гиперссылки для обработки перекрестных ссылок.

Соглашения о типах выглядят следующим образом:

- Имена файлов или пути директорий будут отображаться `моношинным шрифтом`
- Команды которые вы вводите в командной строке Терминала будут отображаться так:

  ```
  команда для набора
  ```

- Опции которые вы можете кликнуть, выделить или выбрать в интерфейсе отображаются `моношинным шрифтом`.

Выбор меню, действия мышью, и горячие клавиши:

- Порядок выбора меню отображается следующим образом: Файл → Открыть
- Действия мышью предполагают настройку мыши для правой руки. Термины «клик мыши» и «двойной клик мыши» относятся к использованию левой клавиши мыши. Термин «правый клик мыши» относится к использованию правой клавиши мыши. Термин «средний клик мыши» относится к использованию средней клавиши мыши, нажатию вниз колесика прокрутки, или одновременному нажатию левой и правой клавиш, в зависимости от дизайна вашей мыши.
- Комбинации горячих клавиш отображаются следующим образом: **Ctrl**-**N**. Где соглашения для «Control», «Shift,» и «Alternate» клавиш будут **Ctrl**, **Shift**, и **Alt**, соответственно, и означают одновременное нажатие первой и второй клавиш.

2. Посильная помощь и обратная связь

Эта документация создана *Командой Документирования Ubuntu* [https://wiki.ubuntu.com/DocumentationTeam]. *Вы* можете оказать содействие проекту документирования делясь своими идеями и комментариями в листе рассылки Команды Документирования Ubuntu. Информация о команде, листе рассылки, проектах, и т.д, находится по адресу *Команда Документирования Ubuntu* [https://wiki.ubuntu.com/DocumentationTeam].

Если вы увидели ошибку в данном документе, или хотели бы высказать свое мнение, вы можете просто зарегистрировать отчет об ошибке по адресу *Ubuntu Bugtracker* [https://launchpad.net/products/ubuntu-doc/+bugs]. Ваша помощь очень нужна для успеха нашей документации!

Огромная благодарность,

-Ваша Команда Документирования Ubuntu

Глава 1. Введение

Добро пожаловать в *Руководство Сервера Ubuntu*!

В *Руководстве по настройке сервера Ubuntu* содержится информация по установке и настройке различных серверных приложений на Вашу систему Ubuntu в соответствии с Вашими потребностями. Это пошаговое, ориентированное на выполнение конкретных задач руководство по конфигурации и настройке Вашей системы. Это руководство затрагивает и множество промежуточных вопросов, таких как:

- Настройка сети
- Настройка Apache2
- Базы данных
- Работа в сети Windows

Данное руководство поделено на следующие главные категории:

- Установка
- Управление пакетами
- Работа в сети
- Работа в сети Windows

Это руководство предполагает, что вы уже имеете основные навыки работы в системе Ubuntu. Если вам необходимо детальное описание процесса установки Ubuntu, смотрите Руководство по установке Ubuntu.

HTML и PDF версии данного руководства доступны в режиме online на сайте *Документации Ubuntu* [http://help.ubuntu.com].

Вы можете купить данное руководство в бумажном варианте в нашем *Магазине Lulu* [http://www.lulu.com/ubuntu-doc]. Вы заплатите только за стоимость печати и доставки.

Глава 2. Установка

В этой главе представлен быстрый обзор процесса установки Ubuntu 6.06 LTS Server Edition. Для получения более полной информации, пожалуйста, обратитесь к Руководству по установке Ubuntu.

1. Подготовка к установке

В данном разделе объяснены различные аспекты, которые должны быть рассмотрены до начала установки.

1.1. Системные требования

Ubuntu 6.06 LTS Server Edition поддерживает три (3) самые распространенные архитектуры: Intel x86, AMD64, и PowerPC. В таблице, представленной ниже, перечислены рекомендуемые спецификации на аппаратное обеспечение. В зависимости от ваших возможностей, вы можете попробовать обойтись и меньшим. Однако, большинство пользователей рискуют разочароваться, если они пренебрегут данными советами.

Таблица 2.1. Рекомендованные минимальные требования

Тип установки	RAM	Место на жёст
Сервер	64 Мегабайта	500 Мегабайт

Профиль по умолчанию для Ubuntu 6.06 LTS Server Edition показан ниже. Отметим еще раз, что размер установки очень сильно зависит от набора сервисов, которые будут установлены. Для большинства администраторов набор сервисов, выбранный по умолчанию, будет достаточен для обычного использования сервера.

Сервер

Это небольшой серверный профиль, который предоставляет набор общих пакетов для всех серверных приложений. Он минимален и разработан для того, чтобы установить максимально необходимые службы, такие, как службы доступа к файлам, службы печати, веб-хостинга, электронной почты и т.д. Для этих служб достаточно 500 Мегабайт дискового пространства, однако лучше выделить больше места, в зависимости от служб, которые вы захотите разместить на сервере.

Необходимо помнить, что эти размеры не включают все остальные данные, которые обычно хранятся на жёстком диске, такие как пользовательские файлы, электронная почта, файлы событий и т.д. Лучшим выходом будет выделение большего пространства для ваших собственных файлов и данных.

1.2. Создание резервной копии

- Перед началом установки, удостоверьтесь, что вы сделали резервную копию всех файлов, находящихся на вашей текущей системе. Если установка "неродной" операционной системы проводится на ваш компьютер впервые, вполне вероятно, что вам придется провести переразбивку жесткого диска вашей системы, чтобы освободить место для Ubuntu. Каждый раз при переразбивке диска, вы должны быть готовы к полной потере данных на диске, будь то из-за вашей ошибки или из-за проблем во время процесса разбивки диска, например, отключение питания системы. Программы,

используемые в процессе установки, довольно надежны, и большинство из них используется уже многие годы. Однако, они производят в том числе и деструктивные действия, и одна ошибка при их использовании может привести к потере ценных данных.

Если вы создаёте мульти-загрузочную систему, убедитесь, что у вас под рукой есть носители с дистрибутивами всех операционных систем, присутствующих на диске. Особенно если вы переразмечаете загрузочный диск, то можете обнаружить, что затёрли системный загрузчик операционной системы или, в большинстве случаев, всю операционную систему и все файлы на разделах.

2. Установка с CD

Вставьте установочный диск в ваш привод CD-ROM и перезагрузите компьютер. Установочная система запустится сразу же при загрузке с компакт диска.

На данном этапе прочтите текст на экране. Возможно вы захотите прочитать справку, предоставленную системой установки. Чтобы сделать это, нажмите F1.

Для выполнения установки сервера выберите «Установить на жесткий диск» и нажмите **Enter**. Будет запущен процесс установки. Просто следуйте инструкциям на экране и ваша система Ubuntu будет установлена.

В качестве альтернативы, для установки сервера LAMP (Linux, Apache, MySQL, PHP/Perl/Python), выберите «Установить сервер LAMP» и следуйте инструкциям.

Глава 3. Управление пакетами

Ubuntu содержит комплексную систему управления пакетами, используемую для установки, обновления, настройки, а также удаления программного обеспечения. Эта система обеспечивает доступ к систематизированной базе из более чем 17 тысяч программных пакетов для вашей системы Ubuntu, более того, средства манипулирования пакетами имеют возможности для разрешения зависимостей между пакетами и проверки наличия обновлений программ.

Есть несколько программ для работы с системой управления пакетами Ubuntu, начиная с простых консольных утилит, использование которых может быть легко автоматизировано администраторами системы, до простых в использовании программ с графическим интерфейсом, более подходящих для новичков в Ubuntu.

1. Введение

Система управления пакетами создана на основе подобной системы, используемой в дистрибутиве Debian GNU/Linux. Файлы пакетов содержат все необходимые файлы, метаданные и инструкции, чтобы обеспечить использование специфических функций или программного приложения на вашем компьютере под управлением Ubuntu.

Файлы пакетов Debian обычно имеют расширение ".deb" и хранятся в *информационных архивах*, которые являются наборами пакетов, доступных через различные источники, такие как диски CD-ROM, или компьютерные сети. Обычно пакеты предварительно скомпилированы в бинарной форме, таким образом установка проходит быстро и не требует компиляции программ из исходных кодов.

Многие сложные пакеты используют концепцию *зависимостей*. Зависимости - это описание дополнительных пакетов, необходимых для корректной работы основного пакета. Например, пакет программы для синтеза речи Festival зависит от пакета festvox-kalpc16k, который предоставляет один из голосов, используемых данным приложением. Для того, чтобы приложение Festival работало, вместе с основным пакетом Festival должны быть установлены все связанные с ним пакеты. Инструменты Ubuntu для управления программным обеспечением выполнят это автоматически.

2. Apt-Get

Команда apt-get - это мощная консольная утилита, используемая в Ubuntu для работы с *Advanced Packaging Tool* (APT), которая обеспечивает такие функции как установка новых программных пакетов, обновление существующих пакетов, обновление списков доступных пакетов и, более того, даже обновление всей системы Ubuntu целиком.

Несмотря на то, что apt-get это лишь консольная утилита, она имеет множество преимуществ по сравнению с другими средствами управления пакетами, доступными в Ubuntu администраторам серверов. Эти преимущества включают, например, простоту использования через терминальное соединение (SSH) и возможность применения в скриптах администрирования системы, запуск которых, в свою очередь, может быть автоматизирован с помощью утилиты выполнения заданий по расписанию cron.

Несколько примеров использования apt-get:

- **Установка пакета**: Устанавливать пакеты используя apt-get довольно просто. Например, для установки сетевого сканера *nmap*, введите следующую комманду:

```
sudo apt-get install nmap
```

- **Удаление пакета**: Удаление пакета или нескольких такой же прямолинейный и простой процесс. Чтобы удалить пакет nmap, установленый в предыдущем примере, наберите следующее:

```
sudo apt-get remove nmap
```

Несколько пакетов: Вы можете указать сразу несколько пакетов для установки или удаления, разделив их названия пробелами.

- **Обновление индекса пакетов**: Индекс пакетов APT это важная база данных доступных пакетов от источников, указаных в файле `/etc/apt/sources.list`Чтобы обновить локальный индекс пакетов наберите следующее:

```
sudo apt-get update
```

- **Обновление пакетов**: Периодически, становятся доступными обновлённые версии пакетов, установленых в вашей системе (например обновления безопасности). Чтобы обновить систему, сначала обновите индекс пакетов, как было показано выше, а потом наберите:

```
sudo apt-get upgrade
```

Если во время обновления пакета возникнет необходимость добавить или удалить новые зависимости, такой пакет не будет обновлен при использовании комманды

upgrade. Для обновления пакетов в подобной ситуации необходимо использовать комманду *dist-upgrade*.

Вы можете также обновить всю систему Ubuntu целиком от одной версии к другой с помощью dist-upgrade. Например, для обновления Ubuntu с версии 5.10 до версии 6.06 LTS, вам необходимо сначала заменить существующий список репозиториев для версии 5.10 списком для 6.06 LTS в файле `/etc/apt/sources.list`, затем выполнить комманду apt-get update, смотри описание выше, и, в конце концов, непосредственно произвести обновление с помощью:

```
sudo apt-get dist-upgrade
```

По прошествии довольно значительного промежутка времени, ваша система будет обновлена до более новой версии. Обычно, после обновления системы нужно будет выполнить некоторые шаги, следуя инструкции по обновлению, предоставленной в более новой версии системы.

Действия команды apt-get, такие как установка и удаление пакетов, сохраняются в файл /var/log/dpkg.log

За дополнительной информацией об использовании APT обратитесь к *Документации по Debian APT* [http://www.debian.org/doc/user-manuals#apt-howto] или выполните комманду:

```
apt-get help
```

3. Aptitude

Приложение Aptitude предоставляет текстовый интерфейс, управляемый с помощью меню, к функциям системы *Advanced Packaging Tool* (APT). Многие основные функции управления пакетами, такие как установка, удаление и обновление, выполняются в Aptitude с помощью односимвольных комманд, которые обычно представлены прописными буквами.

Наилучший способ использования Aptitude - работа с ним в неграфической терминальной среде для обеспечения правильной работы коммандных клавиш. Вы можете запустить Aptitude как обычный пользователь в коммандной строке терминала с помощью:

```
sudo aptitude
```

После запуска Aptitude, вы увидите строку меню вверху экрана и две панели под ней. Верхняя панель содержит группы пакетов, такие как *Новые пакеты* и *Неустановленные пакеты*. В нижней панели отображается информация, связанная с пакетами и категориями пакетов.

Использование Aptitude для управления пакетами относительно просто, а пользовательский интерфейс облегчает выполнение повседневных задач. Далее следуют примеры, как выполнять основные функции управления пакетами в Aptitude:

- **Установка пакетов**: Чтобы установить пакет, найдите нужный пакет через группу "Неустановленные пакеты", используя, например, курсорные клавиши и клавишу **ENTER**, затем выделите пакет, который вы хотите установить. После выделения нужного пакета, нажмите клавишу **+**, и строка с описанием пакета должна стать *зеленой*, показывая, что пакет отмечен для установки. Теперь нажмите клавишу **g**, вы получите описание опреаций, которые будут произведены над пакетами. Нажмите еще раз клавишу **g**, и программа попросит вас стать администратором для завершения процесса установки. Нажмите **ENTER**, это приведет к появлению строки для ввода пароля. Введите ваш пароль, чтобы стать администратором. В конце концов, нажмите еще раз **g**, вы получите запрос на скачивание пакета. Нажав **ENTER** на элементе *Продолжить*, вы запустите процесс скачивания и установки пакета.
- **Удаление пакетов**: Чтобы удалить пакет, найдите нужный пакет через группу "Установленные пакеты", используя, например, курсорные клавиши и клавишу **ENTER**, затем выделите пакет, который вы хотите удалитьить. После выделения нужного пакета, нажмите клавишу **+**, и строка с описанием пакета должна стать *розовой*, показывая, что пакет отмечен для удаления. Теперь нажмите клавишу **g**, вы получите описание опреаций, которые будут произведены над пакетами. Нажмите еще раз клавишу **g**, и программа попросит вас стать администратором для завершения процесса установки. Нажмите **ENTER**, это приведет к появлению строки для ввода пароля. Введите ваш пароль, чтобы стать администратором. В конце концов, нажмите еще раз **g**, вы получите запрос на ужаление пакета. Нажав **ENTER** на элементе *Продолжить*, вы запустите процесс удаления пакета.

- **Обновление каталога пакетов**: Чтобы обновить каталог пакетов, просто нажмите клавишу **u**, и программа попросит вас стать администратором для завершения процесса установки. Нажмите **ENTER**, это приведет к появлению строки для ввода пароля. Введите ваш пароль, чтобы стать администратором. Начнется процесс обновления каталога пакетов.
- **Обновление пакетов**: Чтобы обновить пакеты, выполните обновление каталога пакетов, как описано выше, затем нажмите клавишу **U** чтобы выбрать все пакеты, для которых имеются обновления. Теперь нажмите клавишу **g**, вы получите описание опреаций, которые будут произведены над пакетами. Нажмите еще раз клавишу **g**, и программа попросит вас стать администратором для завершения процесса установки. Нажмите **ENTER**, это приведет к появлению строки для ввода пароля. Введите ваш пароль, чтобы стать администратором. В конце концов, нажмите еще раз **g**, вы получите запрос на скачивание пакетов. Нажав **ENTER** на элементе *Продолжить*, вы запустите процесс обновления пакетов.

Первая колонка, отображаемая в списке пакетов в верхней панели, при непосредственном просмотре пакетов, отображает текущее состояние пакета и использует следующие символы для индикации этого состояния:

- **i**: Пакет установлен
- **c**: Пакет не установлен, но настройки пакета остались в системе
- **p**: Удален из ситемы
- **v**: Виртуальный пакет
- **B**: Испорченный пакет
- **u**: Файлы распакованы, однако настройка пакета не закончена
- **C**: Полу-настроен - Настройки пакета закончилась неудачей, необходимо исправление проблемы
- **H**: Полу-настроен - Удаление пакета закончилась неудачей, необходимо исправление проблемы

Чтобы выйти из Aptitude просто нажмите клавишу **q** и подтвердите свой выход. Многие другие функции доступны из меню Aptitude, которое доступно по нажатию клавиши **F10**.

4. Конфигурация

Описания репозиториев системы *Advanced Packaging Tool* (APT) хранятся в файле /etc/apt/sources.list. Далее рассмотрен пример подобного файла и дана информация о добавлении в этот файл и удалении из него ссылок на репозитории.

Здесь [../sample/sources.list] вы можете найти простой пример типичного файла `/etc/apt/sources.list`.

Вы можете изменять файл для подключения и отключения репозиториев. Например, для отключения требования вставить диск Ubuntu во время выполнения операций с пакетами просто закомментируйте строки с соответствующим диском, который находится в начале файла:

```
# не надо просить диск Ubuntu
# deb cdrom:[Ubuntu 6.06 _Dapper Drake_ - Release i386 (20060329.1)]/ dapper main restricted
```

5. Дополнительные репозитории

В дополнение к поддерживаемым официально репозиториям доступным в Ubuntu, существуют дополнительные репозитории, поддерживаемые сообществом. В них содержатся тысячи дополнительных пакетов для установки. Два наиболее популярных (из дополнительных) репозитория называются *Universe* и *Multiverse*. Эти репозитории не имеют официальной поддержки Ubuntu, поэтому по умолчанию они отключены. В общем же, использование пакетов их этих репозиториев на вашей Ubuntu системе довольно безопасно.

Пакеты из репозитория Multiverse часто имеют ограничения лицензионного характера, что не позволяет включать данные пакеты в и распространять их вместе со свободной операционной системой, более того использование этих пакетов может быть незаконным в вашей стране.

Обращаем ваше внимание, что указанные репозитории, *Universe* и *Multiverse*, не содержат официально поддерживаемых пакетов. В частности, может не существовать необходимых обновлений безопасности для этих пакетов.

Доступно большое количество других источников пакетов, иногда предоставляющих доступ лишь к одному пакету (например, в случае пакета с исходными кодами, предоставляемого разработчиком отдельного приложения). Вы должны быть очень осторожны и внимательны при использовании нестандартных источников пакетов. Внимательно изучите как источник, так и пакет перед установкой, так как некоторые источники, и пакеты, предоставляемые ими, могут вызвать нестабильную работу вашей системы или даже полную ее неработоспособность.

Чтобы подключить репозитории *Universe* и *Multiverse*, раскомментируйте соответствующие строки в файле `/etc/apt/sources.list`:

```
# Мы очень-очень хотим использовать репозитории Multiverse и Universe! Ну пожалуйста

deb http://archive.ubuntu.com/ubuntu dapper universe multiverse
deb-src http://archive.ubuntu.com/ubuntu dapper universe multiverse
```

5.1. Ссылки

HOWTO: Добавление репозиториев (Ubuntu Wiki)
[https://wiki.ubuntu.com/AddingRepositoriesHowto]

Глава 4. Работа в сети

Компьютерные сети состоят из двух и более устройств, таких как компьютерные системы, принтеры, и сопутствующее оборудование, объединеных кабельными или беспроводными соединениями с целью разделения и распределения информации среди подключенных устройств.

Данный раздел руководства по серверу Ubuntu содержит общие сведения и специфическую информацию относительно работы в сети, включая обзор сетевых концепций и подробное рассмотрение популярных сетевых протоколов и серверных приложений.

1. Настройка сети

Ubuntu поставляется с несолькими графическими инструментами для настройки сетевых устройств. Этот документ рассчитан на продвинутых пользователей и фокусируется на управлении сетью с помощью командной строки.

1.1. Ethernet

Большая часть настроек ethernet сконцентрирована в одном файле: `/etc/network/interfaces`. Если у вас нет сетевых устройств, тогда только loopback-интерфейс будет представлен в этом файле, и файл будет выглядеть примерно вот так:

```
#Этот файл описывает сетевые устройства присутствующие в системе
# и способы их активации. Для более подробной информации см. interfaces(5).

# The loopback interface
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
```

Если в вашей стстеме одно ethernet-устройство, которое получает настроечные данные с сервера DHCP, и оно должно подключаться автоматически при загрузке системы, то для его настройки понадобится всего лишь две строчки дополнительно:

```
auto eth0
iface eth0 inet dhcp boot
```

Первая строка говорит о том, что устройство eth0 должно включатся автоматически при загрузке. Вторая строка определяет, что интерфейс («iface») eth0 должен работать в пространстве адресов IPv4 (замените «inet» на «inet6» для устройств с адресами IPv6) и получает настроечные данные с сервера DHCP. Подразумевая, что ваша сеть и сервер DHCP настроены и работают правильно, настройки сети данного компьютера не требуют дальнейшей настройки для работы в сети. Сервер DHCP предоставит адрес основного шлюза (реализованного с помощью команды route), IP-адрес устройства (реализованного с помощью команды ifconfig) и адреса DNS серверов, используемых в сети (реализовано в файле `/etc/resolv.conf`)

Для настройки вашего устройства ethernet на использование статического IP-адреса и собственных настроек, необходимо иметь больше информации. Допустим, вы хотите присвоить IP-адрес 192.168.0.2 устройству eth1, со стандартной маской сети 255.255.255.0. IP-адрес вашего основного шлюза 192.168.0.1. Тогда ваш файл `/etc/network/interfaces` будет подобен следующему:

```
iface eth1 inet static
 address 192.168.0.2
 netmask 255.255.255.0
 gateway 192.168.0.1
```

В этом случае вам также необходимо определить вручную ваши серверы DNS в файле `/etc/resolv.conf`, который будет выглядеть примерно так: which should look something like this:

```
search mydomain.com
nameserver 192.168.0.1
nameserver 4.2.2.2
```

Директива *search* будет добавлять mydomain.com к запросам имени хоста при попытках разрешить имя в вашей сети. Например, если домен вашей сети mydomain.com и вы попытаетесь послать эхо-запрос хосту «mybox», запрос DNS на разрешение имен будет модифицирован к виду «mybox.mydomain.com». Инструкции *nameserver* определяют серверы DNS, используемые для разрешения имен хостов в IP-адреса. Если вы используете собственный сервер имен, укажите его здесь. В противном случае, запросите у вашего провайдера услуг Интернет (Internet Service Provider, ISP) адреса основного и вспомогательного серверов DNS, и опишите их в файле `/etc/resolv.conf` как показано выше.

Существует большое количество возможных вариантов настроек сети, включая модемные интерфейсы PPP, работу в сети по протоколу IPv6, VPN устройства и т.п. Более полная информация и описание поддерживаемых возможностей дано в руководстве man 5 interfaces. Помните, что файл `/etc/network/interfaces` используется скриптами ifup/ifdown в для предоставления схемы настройек более высокого уровня, чем может использоваться в других дистрибутивах Линукс, а также, что традиционные низкоуровневые утилиты такие как ifconfig, route и dhclient также доступны вам для специально подобранных настроек.

1.2. Управление записями DNS

Данный раздел объясняет как настроить использование существующих серверов имен (name server) при разрешении IP-адресов в имена хостов и обратно. Здесь не объясняется, как настроить систему для работы в качестве сервера имен.

Для управления списком DNS, вы можете добавлять, изменять или удалять имена DNS в файле `/etc/resolv.conf`. Содержимое *файла-примера* [../sample/resolv.conf] представлено ниже:

```
search com
nameserver 204.11.126.131
nameserver 64.125.134.133
nameserver 64.125.134.132
nameserver 208.185.179.218
```

Ключевое слово search определяет строку, которая будет добавляться к неполным именам хостов. В нашем примере это строка com. То есть, если мы выполним комманду: **ping ubuntu**, она будет интерпретирована как **ping ubuntu.com**.

Ключевое слово nameserver определяет IP-адрес сервера имен. Этот адрес будет использован, при разрешении заданного IP-адреса или имени хоста. Данный файл может содержать несколько записей с описанием серверов имен. Серверы имен будут использоваться сетевыми запросами в той же последовательности, как они указаны в файле.

Если сервера имен DNS доставляются автоматически через DHCP или PPPOE (от вашего ISP). не добавляйте записи для серверов имен в этот файл. Он будет обновлен автоматически.

1.3. Управление хостами

Для управления хостами, вы можете добавлять, изменять, удалять хосты в файле `/etc/hosts`. Этот файл содержит IP-адреса и соответствующие им имена хостов. Когда ваша система пытается разрешить название хоста в IP-адрес, сначала происходит обращение к файлу `/etc/hosts` и лишь потом используются серверы имен. Если IP-адрес содержится в файле `/etc/hosts`, серверы имен не используются. Такое поведение может быть изменено настройками в файле `/etc/nsswitch.conf`, на ваш собственный риск.

Если в вашей сети есть компьютеры, чьи IP-адреса не прописаны в DNS, мы рекомендуем вам добавить их в файл `/etc/hosts`.

2. TCP/IP

Протокол контроля передачи данных и Интернет протокол (The Transmission Control Protocol and Internet Protoco - TCP/IP) - это стандартный набор протоколов, разработанных в конце 70-х годов управлением перспективного планирования оборонных научно-исследовательских работ (DARPA) в качестве средства коммуникации между различными типами компьютеров и компьютерных сетей. Так как сеть Интернет построена на стеке протоколов TCP/IP, они представляют самый популярный набор сетевых протоколов на Земле.

2.1. Введение в TCP/IP

Две компоненты протокола TCP/IP имеют дело с различными аспектами компьютерных сетей. *Интернет протокол* (Internet Protocol), "IP" в TCP/IP - это протокол без организации соединения, который обеспечивает лишь пересылку сетевых пакетов, используя *IP датаграммы* в качестве единицы представления сетевой информации. IP датаграмма состоит из заголовка, за которым следует тело сообщения. *Протокол управления передачей*(Transmission Control Protocol), TCP в TCP/IP, обеспечивает хостам сети возможности устанавливать соединения, которые могут быть использованы для обмена потоками данных. TCP обеспечивает гарантированную доставку данных между соединенными системами, а также то, что эти данные доставляются на принимающий хост в том же самом порядке, в котором они были отправлены с другого хоста.

2.2. Настройка TCP/IP

Настройка протокола TCP/IP состоит из нескольких элементов, которые должны быть указаны в соответствующих файлах конфигураций, или получены с помощью дополнительных служб таких как сервер протокола динамической настройки хостов (Dynamic Host Configuration Protocol, DHCP), который, в свою очередь, может быть настроен для автоматического предоставления правильных настроек TCP/IP клиентам сети. Следующим параметрам настройки должны быть указаны правильные значения, чтобы обеспечить нормальную работу вашей системы Ubuntu в сети.

Обычные элементы настроек TCP/IP и их назначение таковы:

- **IP адрес**. IP адрес - это уникальная идентификационная строка, представленная в виде четырёх десятичных чисел в диапазоне от нуля (0) до двухсот пятидесяти пяти (255), разделённых точками, каждое из четырёх чисел представляет восемь (8) бит адреса, полная длина которого тридцать два (32) бита. Этот формат называют *dotted quad notation (четырехкомпонентная система обозначений адресов с точками)*.
- **Маска сети (Netmask)** Маска подсети (или просто, *netmask*) - это локальная битовая маска, или наборы флагов, отделяющая часть IP-адреса, значимую для сети, от битов, значимых для *подсети (subnetwork)*. Например, в сети класса C, стандартная маска сети

определена как 255.255.255.0, она маскирует первые три байта IP адреса и позволяет последнему байту IP адреса оставаться доступным для обозначения хостов в подсети.

- **Адрес сети (Network Address)** Адрес сети представляется байтами, включающими в себя сетевую часть IP адреса. К примеру, хост 12.128.1.2 в сети класса A будет использовать 12.0.0.0 в качестве адреса сети, которая использует двенадцать (12) для представления первого байта IP адреса (сетевая часть), тогда как нули (0) в оставшихся трех байт представляют потенциальные значения для хостов. Хосты сети использующие стандартные закрытые и не маршрутизируемые IP адреса, подобные 192.168.1.100, будут, в свою очередь, использовать в качестве адреса сети 192.168.1.0, которая определяет первые три байта 192.168.1 сети класса C и нуль (0) для всех возможных хостов в сети.
- **Широковещательный адрес (Broadcast Address)** Широковещательный адрес - это такой IP адрес, который позволяет передать сетевые данные одновременно на все хосты заданной подсети, вместо передачи на конкретный хост. Стандартным общим широковещательным адресом для IP сетей является 255.255.255.255, однако этот адрес не может быть использован для передачи широковещательных сообщений всем хостам сети Интернет, так как роутеры блокируют данный адрес. Более приемлем широковещательный адрес соответствующий конкретной подсети. Например, для популярной закрытой сети класса C, 192.168.1.0, широковещательный адрес должен быть настроен как 192.168.1.255. Широковещательные сообщения обычно рассылаются сетевыми протоколами такими, как протокол разрешения адресов (Address Resolution Protocol или ARP) и информационный протокол маршрутизации (Routing Information Protocol, RIP).
- **Адрес шлюза (Gateway Address)** Адрес шлюза - это IP адрес, через который некоторая сеть, или хост в сети, могут быть доступны. Пусть один сетевой хост желает организовать соединение с другим сетевым хостом, но они расположены в разных сетях, в таких случаях должен использоваться *шлюз (gateway)*. Во многих случаях адрес шлюза будет совпадать с адресом маршрутизатора той же сети, который, в свою очередь, будет перенаправлять трафик в другие сети или на другие хосты, такие как хосты Интернет. Адресу шлюза должно быть присвоено правильное значение, в противном случае ваша система не сможет связаться ни с одним хостом, находящимся за пределами вашей сети.
- **Адрес сервера имен (Nameserver Address)** Адреса серверов имен представляют IP адреса систем службы именования доменов (Domain Name Service, DNS), которые разрешают имена хостов сети в IP адреса. Есть три уровня адресов серверов имен, которые могут быть определены в порядке приоритета: *основной (Primary)* сервер имен, *вспомогательный (Secondary)* сервер имен, и *третичный (Tertiary)* сервер имен. Для того, чтобы ваша система могла разрешать сетевые имена хостов в соответствующие IP адреса, вы должны определить допустимые адреса серверов имен, которые вам разрешено использовать в настройках TCP/IP вашей системы. Во многих случаях эти адреса будут предоставлены вашим провайдером сетевых услуг, но также существуют

свободные и открыто доступные сервера имен, которые можно использовать, такие как серверы Level3 (Verizon) с IP адресами от 4.2.2.1 до 4.2.2.6.

IP адрес, маска сети, адрес сети, широковещательный адрес и адрес шлюза обычно определяются с помощью подходящих инструкций в файле `/etc/network/interfaces`. Адреса серверов имен обычно задаются с помощью директивы *nameserver* в файле `/etc/resolv.conf`. Для получения более полной информации, смотрите страницы системного руководства для `interfaces` или `resolv.conf`, соответственно, введя следующие команды в терминале:

Обратитесь к соответствующей странице системного руководства о `interfaces` с помощью комманды:

```
man interfaces
```

Обратитесь к соответствующей странице системного руководства о `resolv.conf` с помощью комманды:

```
man resolv.conf
```

2.3. IP маршрутизация

IP маршрутизация (роутинг) - это способы определения и нахождения путей доставки сетевых данных в сети TCP/IP. Маршрутизация использует набор *таблиц маршрутизации (routing tables)* для управления передачей сетевых пакетов данных от отправителя к получателю, зачастую через множество промежуточных сетевых узлов, именуемых *маршрутизаторы (routers)*. IP маршрутизация - это основной способ определения путей доставки в сети Интернет. Есть две основных формы IP маршрутизации: *статическая маршрутизация (Static Routing)* и *динамическая маршрутизация (Dynamic Routing)*.

Статическая маршрутизация подразумевает ручное добавление IP маршрутов в таблицу маршрутизации системы, обычно это достигается изменением таблиц маршрутизации с помощью команды route. Статическая маршрутизация имеет множество преимуществ над динамической, таких как простота реализации в небольших сетях, предсказуемость (таблицы маршрутизации рассчитываются заранее, следовательно используемые маршруты остаются постоянным от раза к разу), а также малая нагрузка на другие роутеры и сетевые соединения так как не используется протокол динамической маршрутизации. Однако, у статической маршрутизации есть и свои минусы. Например, ее применение ограничено небольшими сетями, к тому же она плохо масштабируется. Более того, из-за фиксированности маршрутов, статическая маршрутизация не может адаптироваться к перебоям в работе сети и ошибкам, возникающим на маршрутах доставки.

Динамическая маршрутизация зависит от больших сетей со множеством возможных IP маршрутов от отправителя к получателю и использует специальные протоколы

маршрутизации, такие как протокол маршрутной информации (Router Information Protocol, RIP), который поддерживает автоматические изменения в таблицах маршрутизации, что делает возможным саму динамическую маршрутизацию. Динамический роутинг имеет несколько преимуществ над статическим, в числе которых отличная масштабируемость и возможность подстройки при возникновении сбоев и ошибок на маршрутах доставки данных. В дополнение к этому, при этом способе необходимо меньше ручных настройек таблиц маршрутизации, так как роутеры обмениваются друг с другом информацией о существовании других роутеров и доступных маршрутах. Это также устраняет возможность внесения ошибочной информации в таблицы маршрутов из-за ошибок операторов. Однако, динамический способ маршрутизации тоже несовершенен. Из недостатков мы отметим повышенную сложность и дополнительную нагрузку на сети, связанную с передачей информации между роутерами, которые не дают мгновенных преимуществ пользователю, но в то же время используют часть пропускной способности сети.

2.4. TCP и UDP

TCP - протокол с установлением соединения, предоставляющий коррекцию ошибок и гарантированную доставку данных через так называемое *управление передачей (flow control)*. Управление передачей определяет когда поток данных необходимо остановить и заново отправить предыдущие пакеты данных вследствие таких проблем как *коллизии (collisions)*. TCP обычно используется при обмене важной информацией, такой как транзакции баз данных.

Протокол пользовательских датаграмм (UDP - User Datagram Protocol), с другой стороны, является протоколом *без установления соединения*, который редко используется для передачи важных данных, поскольку в нем отсутствует управление передачей или другие способы гарантированной доставкой данных. UDP обычно используется в приложениях для передачи потокового аудио или видео, в которых он является быстрее TCP из-за отсутствия коррекции ошибок и управления передачей, и где потеря нескольких пакетов не является катастрофичной.

2.5. ICMP

Протокол управляющих сообщений сети Интернет (Internet Control Messaging Protocol, ICMP) - это расширение Интернет протокола (IP), определенное в документе RFC#792 (Request For Comments), поддерживающее сетевые пакеты, содержащие управляющие и информационные сообщения, а также сообщения об ошибках. ICMP используется сетевыми приложениями, например, утилитой ping, с помощью которой можно определить доступность сетевого хоста или устройства. Например, сообщения об ошибках, возвращаемых ICMP, которые полезны как хостам в сети, так и устройствам типа маршрутизаторов, включают в себя *адресат недоступен (Destination Unreachable)* и *превышено время ожидания (Time Exceeded)*.

2.6. Демоны

Демоны - это специальные системные программы, которые, как правило, выполняются постоянно в фоновом режиме и ожидают запросов на функции, которые они предоставляют для других программ. Многие демоны направлены на работу с сетью; то есть, большое число демонов, выполняющихся в фоновом режиме в системе Ubuntu могут предоставлять сетевую финкциональность. В качестве примера таких сетевых демонов можно привести *Hyper Text Transport Protocol Daemon* (httpd), который предоставляет функции веб-сервера, *Secure SHell Daemon* (sshd), который предоставляет безопасный удаленный доступ к консоли и возможность передачи файлов и *Internet Message Access Protocol Daemon* (imapd), который предоставляет службы электронной почты.

3. Настройка межсетевого экрана (брандмауера)

Ядро Linux включает подсистему *Netfilter*, которая используется для регулирования сетевого траффика, входящего на или проходящего через вашу систему. Все современные средства межсетевой защиты Linux используют эту систему для фильтрации пакетов.

3.1. Введение в брандмауер

Система фильтрации пакетов ядра была бы малопригодной для администраторов без пользовательского интерфейса управления ею. Для этого предназначено приложение iptables. Когда пакет достигает вашего сервера, он передается подсистеме Netfilter для приема, обработки или отклонения, в зависимости от правил, передаваемых ей из рабочего пространства пользователя с помощью iptables. Таким образом, если вы хорошо знакомы с iptables - это все, что вам необходимо для управления межсетевым экраном. Однако, существует множество программ предоставляющих интерфейс для упрощения этой задачи.

3.2. IP маскировка

Назначение IP маскировки в том, чтобы позволить машинам в вашей сети с частными, не маршрутизируемыми IP-адресами, иметь доступ в Интернет через машину, осуществляющую маскировку. Трафик из вашей сети, предназначенный для Интернета, должен быть обработан так, чтобы ответы могли вернуться обратно на машину, которая организовала запрос. Чтобы это сделать, ядро должно изменить IP-адрес *источника* в каждом пакете так, чтобы ответы возвращались на сервер, а не на частный IP-адрес (что невозможно в Интернете), с которого сделан запрос. Linux использует *Connection Tracking* (conntrack) для хранения записи о том, каким машинам принадлежат соединения, и перенаправляет каждый возвращенный пакет соответствующим образом. Таким образом, трафик, покидающий вашу сеть, "замаскирован", как будто исходит от машины, которая выполняет роль шлюза. В документации Microsoft этот процесс упоминается как технология Internet Connection Sharing.

Этого можно достичь с помощью простого правила в iptables, которое может слегка варьироваться в зависимости от настроек вашей сети:

```
sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
```

В команде, приведенной выше, предполагается, что вы используете закрытое адресное пространство 192.168.0.0/16, а подключение к Интернет обеспечено через устройство ppp0. Данный синтаксис может быть объяснен так:

- -t nat -- правило, для обращения к таблице NAT
- -A POSTROUTING -- правило, добавлямое (-A) к цепочке POSTROUTING
- -s 192.168.0.0/16 -- правило применяется для трафика, происходящего из обозначенного адресного пространства

- -o ppp0 -- правило применяется к трафику, который планируется направить через определенное сетевое устройство
- -j MASQUERADE -- трафик попадающий под данное правило должен быть перенаправлен "jump" (-j) с маскировкой (MASQUERADE) для обработки, как описано выше

Любая цепочка правил в таблице фильтрации (это основная таблица, где происходит обработка большинства пакетов) имеет в качестве *политики (policy)* по умолчанию правило ACCEPT (принимать), но если вы создаете межсетевой экран в дополнение к устройству шлюза, вы можете настроить политики на использование правил DROP (пропустить) или REJECT (отклонить), в этом случае (для работы правила, описанного выше) необходимо разрешить прохождение вашего маскированного трафика через цепочку FORWARD (перенаправить):

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.0.0/16 -m state --state ESTABLISHED,RELATED -i ppp0 -j ACCEPT
```

Эти команды разрешают все соединения из вашей локальной сети в Интернет, а также позволяют всему трафику, относящемуся к этим соединениям, возвращаться на машины их инициировавшие.

3.3. Инструменты

Есть большое количество программ, которые помогут вам полностью настроить брандмауэр без необходимости подробного изучения iptables. У тех, кто предпочитает графические оболочки, довольно популярно простое в использовании приложение Firestarter, а также fwbuilder - очень мощный инструмент настройки, который покажется знакомым администраторам, пользовавшимся коммерческими брандмауэрами типа Checkpoint FireWall-1. Для предпочитающих работу в командной строке и простые текстовые файлы настроек, Shorewall - подходящее и мощное решение, которое поможет настроить межсетевой экран любой сложности для любой сети. Если же ваша сеть достаточно простая, или у вас вообще нет локальной сети, утилита ipkungfu предоставит вам работающий "из коробки" (без необходимости настпройки) брандмауэр, а также даст возможность легко настроить более сложный межсетевой экран с помощью редактирования простых и хорошо документированных файлов настроек. Еще одна интересная программа - fireflier, которая разработана как межсетевой экран для настольного ПК. Она состоит из сервера (fireflier-server) и графического клиента на ваш выбор (GTK или QT). Во время работы она ведет себя похоже на многие интерактивные брандмауэры для Windows.

3.4. Журналирование

Сообщения в журнале брандмаура необходимы для определения атак, поиска проблем в правилах, а также для определения необычной активности в вашей сети. Чтобы

активировать журналирование вам необходимо включить соответствующие правила в конфигурацию вашего межсетевого экрана, более того, эти правила должны быть заданы ранее всех применяемых завершающих правил (это правила с целью, которая определяет дальнейшую судьбу пакета, такие как ACCEPT, DROP или REJECT). Например,

```
sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j LOG --log-prefix "NEW_HTTP_CONN: "
```

Тогда запрос на порт 80 с локальной машины будет генерировать сообщение в dmesg подобное следующему:

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.
```

Сообщение выше, будет также записано в файлы `/var/log/messages`, `/var/log/syslog`, и `/var/log/kern.log`. Данное поведение можно изменить соответствующими настройками в файле `/etc/syslog.conf` или с помощью установки и настройки ulogd (при этом нужно использовать цель ULOG вместо LOG). Демон ulogd - это сервер пользовательского рабочего пространства, который ожидает от ядра инструкций для записи в журнал, специфичных для брандмауэров, и может сохранять их в любой файл на ваш вкус, и даже в базу данных PostgreSQL или MySQL. Разобраться в журнале брандмауэра может помочь использование утилит анализа журналов событий, таких как fwanalog, fwlogwatch, или lire.

4. Сервер OpenSSH

4.1. Введение

Данный раздел документации сервера Ubuntu представляет мощный набор инструментов *OpenSSH*, используемый для удаленного управления компьютеров в сети и передачи данных между ними. Вы также узнаете о некоторых возможностях настройки серверного приложения OpenSSH, а также как изменять эти настройки на вашей Ubuntu системе.

OpenSSH - это свободно доступная версия инструментов, поддерживающих протокол Secure Shell (SSH), для удаленного управления компьютером или передачи файлов между компьютерами. Традиционно использовавшиеся для этих целей инструменты, такие как telnet или rcp, не являются безопасными: они передают пароль пользователя простым текстом во время их использования. OpenSSH предоставляет серверного демона и клиентские программы для обеспечения безопасных и зашифрованных операций удаленного управления и передачи файлов, эффективно заменяя при этом устаревшие программы.

Серверная компонента OpenSSH, sshd, постоянно ожидает клиентских соединений от любых клиентских программ. Когда приходит запрос на соединение, sshd устанавливает правильный тип соединения, в зависимости от типа подключаемого клиента. Например, если удаленный компьютер пытается подключится с помощью приложния-клиента ssh, сервер OpenSSH, после авторизации, запустит сеанс удаленного управления. Если же удаленный пользователь подключается с помощью scp, серверный демон OpenSSH, после авторизации, организует безопасное копирование файлов между сервером и клиентом. OpenSSH может использовать множество методов авторизации, включая обычный пароль, использование открытого ключа, и сертификаты Kerberos.

4.2. Установка

Установка клиента и сервера OpenSSH проста. Для установки OpenSSH клиента на вашу систему Ubuntu, используйте следующую команду в строке терминала:

```
sudo apt-get install openssh-client
```

Для установки сервера OpenSSH и всех необходимых файлов выполните эту команду в строке терминала:

```
sudo apt-get install openssh-server
```

4.3. Конфигурация

Вы можете настроить режим работы по умолчанию серверного приложения OpenSSH, sshd, редактируя файл `/etc/ssh/sshd_config`. Для получения информации об инструкциях

настройки, используемых в этом файле, вы можете просмотреть соответствующее руководство с помощью следующей команды, выполненной в командной строке терминала:

```
man sshd_config
```

В конфигурационном файле демона sshd существует множество директив, управляющих такими вещами, как настройки соединения и режимы аутентификации. Ниже перечислены примеры директив, значения которых могут быть изменены в файле `/etc/ssh/ssh_config`.

Перед внесением изменений в файл настроек, вы должны скопировать оригинальный файл и защитить его от записи. Таким образом, вы будите иметь оригинальные настройки для справки или повторного использования, при необходимости.

Создайте копию файла `/etc/ssh/sshd_config` и защитите его от записи, используя следующую команду, введенную в командной строке терминала:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

Ниже даны примеры инструкций настройки, которые вы можете изменять:

- Чтобы настроить демона OpenSSH в режим прослушивания TCP порта 2222, вместо стандартного TCP порта 22, измените директиву Port таким образом:

  Port 2222

- Чтобы sshd позволял возможность процедуры идентификации пользователя с использованием данных, основанных на открытом ключе, просто добавьте или измените следующую строку:

  PubkeyAuthentication yes

  в файле `/etc/ssh/sshd_config`, если такая строка уже присутствует в файле, удостоверьтесь, что она раскомментирована.

- Чтобы ваш сервер OpenSSH отображал содержимое файла `/etc/issue.net` в качестве сообщения перед логином, просто добавьте или измените следующую строку:

  Banner /etc/issue.net

  в файле `/etc/ssh/sshd_config`.

После внесения изменений в файл `/etc/ssh/sshd_config`, сохраните его и, чтобы изменения вступили в силу, перезапустите серверное приложение sshd, выполнив следующую команду в терминале:

```
sudo /etc/init.d/ssh restart
```

Доступно большое количество инструкций для sshd, чтобы настроить поведение серверного приложения под ваши нужды. Однако, мы вас предупреждаем: если единственный для вас метод доступа к серверу - с помощью ssh и вы допустите ошибку при настройке sshd с помощью файла `/etc/ssh/sshd_config`, может случится, что вы заблокируете себе доступ к серверу после его перезапуска или что сервер sshd откажется запуститься из-за неправильной директивы настройки, то есть будьте предельно внимательны при редактировании этого файла на удаленном сервере.

4.4. Ссылки

Сайт OpenSSH [http://www.openssh.org/]

Страница Wiki о расширенных настройках OpenSSH
[https://wiki.ubuntu.com/AdvancedOpenSSH]

5. FTP Сервер

Протокол передачи файлов (FTP) является TCP-протоколом для передачи файлов между компьютерами. FTP работает по модели клиент-сервер. Серверная часть называется *FTP демоном*. Он постоянно прослушивает FTP-запросы от удаленных клиентов. Когда запрос получен, он авторизует клиента и устанавливает соединение. На протяжении всей сессии FTP-сервер выполняет любые команды посланные FTP-клиентом.

Доступ к FTP серверу может быть установлен двумя путями:

- Анонимный
- Авторизованный

В Анонимном режиме, удаленные клиенты могут получить доступ к FTP серверу, используя стандартную учетную запись 'anonymous' или 'ftp' и передававя в качестве пароля свой адрес электронной почты. В Авторизованном режиме пользователь должен иметь учетную запись и пароль. Пользователи получают доступ к файлам и каталогам FTP сервера в соответствии с правами учетной записи, использованной при входе на FTP сервер. Общей нормой является то, что FTP сервер скрывает свою корневую директорию и подставляет вместо нее домашнюю директорию FTP, что позволяет скрыть остальную часть файловой системы от удаленных клиентов.

5.1. vsftpd - Установка FTP сервера

vsftpd - это FTP демон доступный в Ubuntu. Он прост в установке, настройке и использовании. Для установки vsftpd необходимо выполнить следующую команду:

```
sudo apt-get install vsftpd
```

5.2. vsftpd - Настройка FTP сервера

Чтобы сменить настройки сервера, с заданных по умолчанию, вы можете отредактировать файл настроек vsftpd: `/etc/vsftpd.conf`. По умолчанию, позволен только анонимный доступ на FTP. Если вы хотите отключить эту опцию, вам нужно изменить строку

```
anonymous_enable=YES
```

на

```
anonymous_enable=NO
```

По умолчанию, локальным пользователям отключена возможность входа на FTP сервер. Чтобы изменить это, раскомментируйте следующую строку:

```
#local_enable=YES
```

Также настройки по-умолчанию, позволяют пользователям только скачивать файлы с FTP сервера, но не разрешают загружать файлы на сервер. Для изменения этого поведения, раскомментируйте строку

```
#write_enable=YES
```

Точно так же анонимным пользователям запрещена загрузка файлов на FTP сервер. Для изменения этой настройки раскомментируйте эту строку:

```
#anon_upload_enable=YES
```

В конфигурационном файле содержится большое количество параметров настройки. Информация о каждом параметре также дана в файле конфигураци. В качестве альтернативы, для получения более полной информации о каждом параметре, вы можете обратиться к документации: **man 5 vsftpd.conf**.

Как только вы настроили vsftpd, вы можете запустить демона. Для запуска воспользуйтесь следующей командой:

```
sudo /etc/init.d/vsftpd start
```


Примите во внимание, что настройки, прописанные по умолчанию в файле конфигурации, выбраны именно такими из соображений безопасности. Каждое изменение, из описанных выше, делает вашу систему немного более уязвимой. Вносите эти изменения только если вы действительно нуждаетесь в них.

6. Сетевая файловая система (Network File System, NFS)

NFS позволяет системе предоставлять в общий сетевой доступ каталоги и файлы. Посредством NFS, пользователи и программы могут получать доступ к файлам на удаленных машинах так же легко, как будто это файлы на их локальном компьютере.

Некоторые из преимуществ, которые может обеспечить NFS:

- Рабочие станции используют меньше локального дискового пространства, так как общие данные могут содержаться на одной машине и оставаться доступными по сети для всех остальных.
- У пользователей отпадает необходимость в использовании отдельных домашних каталогов на каждой машине, подключенной в сеть. Можно разместить домашние каталоги пользователей на сервере NFS и сделать их доступными с помощью сети.
- Устройства хранения информации такие как флоппи дисководы, приводы компакт дисков и USB приводы могут использоваться другими машинами в сети. Это может уменьшить общее число накопителелей со сменными носителями в сети

6.1. Установка

Введите следующую команду в терминале для установки NFS сервера:

```
sudo apt-get install nfs-kernel-server
```

6.2. Конфигурация

Вы можете настроить директории для экспорта добавляя их в файл `/etc/exports`. Например:

```
/ubuntu *(ro,sync,no_root_squash)
/home *(rw,sync,no_root_squash)
```

Вы можете заменить * одним из форматов записи имени хоста. Сделайте объявление хоста настолько необычными, насколько это возможно, чтобы нежеланные системы не могли получить доступа к монтированию NFS

Для запуска NFS сервера выполните следующую команду в терминале:

```
sudo /etc/init.d/nfs-kernel-server start
```

6.3. Настройка NFS клиента

Используйте команду mount для монтирования NFS директории открытой на другой машине. Наберите в терминале команду, схожую со следующим примером.

```
sudo mount example.hostname.com:/ubuntu /local/ubuntu
```

Точка монтирования `/local/ubuntu` должна существовать. В директории `/local/ubuntu` не должно быть никаких файлов или под-директорий.

Другой способ монтирования NFS ресурса, открытого на другой машине состоит в добавлении соответствующей строчки в файл `/etc/fstab`. Строчка должна содержать имя хоста NFS сервера, название каталога, открытого на сервере, и название директории на локальной машине, куда будет монтироваться NFS каталог.

Общий синтаксис строки файла `/etc/fstab` следующий:

```
example.hostname.com:/ubuntu /local/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr
```

6.4. Ссылки

Линукс NFS FAQ [http://nfs.sourceforge.net/]

7. Протокол динамической настройки хостов (Dynamic Host Configuration Protocol, DHCP)

DHCP (протокол динамической конфигурации узла) это сетевой сервис, позволяющий компьютерам автоматически получать настройки от сервера, в отличие от ручной настройки каждого компьютера в сети. Компьютеры, настроенные в качестве DHCP клиентов не контролируют параметры, которые они получают от DHCP сервера, и настройка прозрачна для пользователя компьютера.

В самом общем случае, настройки предоставляемые сервером DHCP его клиентам включают в себя:

- IP адрес и маску сети
- DNS
- WINS

Кроме того, DHCP сервер может дополнительно предоставить параметры настроек такие как:

- Имя хоста
- Имя домена
- Шлюз по умолчанию
- Сервер синхронизации времени
- Сервер печати

Преимущество использования DHCP сервера в сети состоит в том, что изменения настроек сети, например, изменение адреса DNS сервера, должны выполняться только на DHCP сервере. Все остальные компьютеры в сети будут автоматически перенастроены DHCP клиентами во время следующего опроса ими DHCP сервера. Дополнительное преимущество состоит в том, что становится проще подключать в сеть новые компьютеры, так как отпадает необходимость проверять доступность IP адреса. Также сокращается количество конфликтов при назначении IP адресов.

DHCP сервер может предоставлять конфигурацию двумя способами:

MAC-адрес
: Данный метод включает в себя использование DHCP для определения уникальных аппаратных адресов каждой сетевой карты, подключенной в сеть, а затем постоянным предоставлением одной и той же конфигурации каждый раз, когда DHCP клиент делает запрос к серверу, используя данное сетевое устройство.

Пул адресов
: Данный метод подразумевает определение пула (иногда используется термин диапазон) IP адресов, из которых динамически формируются параметры конфигурации для каждого DHCP клиента, обслуживание которых ведется по принципу: первый пришел - первый обслужен. Если DHCP клиент не работает в сети в течение некоторого

определенного периода времени, то присвоенная ему конфигурация утрачивает силу и ее адрес возвращается назад в пул адресов для использования другими DHCP клиентами.

В поставку Ubuntu входят как DHCP сервер, так и клиент. dhcpd (DHCP демон) - это сервер. Клиент, поставляемый с Ubuntu называется dhclient и должен быть установлен на всех компьютерах, которые необходимо настраивать автоматически. Обе программы легко устанавить и настроить. Они автоматически запускаются в процессе загрузки системы.

7.1. Установка

Для установки dhcpd введите следующую команду в терминале:

```
sudo apt-get install dhcpd
```

Вы увидите следующий вывод, объясняющий, что делать далее:

```
↵
Пожулуйста, отметьте, если вы устанавливаете DHCP сервер в первый↵
раз, то его необходимо настроить. Пожалуйста, остановите (/etc/init.d/dhcp↵
stop) DHCP сервер, отредактируйте /etc/dhcpd.conf согласно вашим потребностям↵
в определенной конфигурации, и перезапустите DHCP сервер↵
(/etc/init.d/dhcp start).↵
↵
Необходимо также отредактировать /etc/default/dhcp для указания интерфейсов,↵
которые должен использовать dhcpd. По умолчанию используется eth0.↵
↵
Примечание: сообщения dhcpd's отправляются в syslog. Все диагностические↵
сообщения необходимо смотреть там.↵
↵
Запуск DHCP сервера: Ошибка запуска dhcpd  - для диагностики проверьте syslog.
```

7.2. Конфигурация

Сообщение об ошибке, с которым заканчивается процесс установки может быть немного непонятным, но приведенные ниже шаги помогут вам настроить службу

Наиболее вероятно, вы захотите установить случайную раздачу IP адресов. Это может быть выполнено сдледующим образом:

```
# Sample /etc/dhcpd.conf↵
# (ваши комментарии тут)
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
```

```
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "mydomain.org";

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
}
```

Это приведет к тому, что DHCP сервер присвоит клиенту IP адрес из диапазона 192.168.1.10-192.168.1.100 или 192.168.1.150-192.168.1.200. Ip адрес назначается на 600 секунд, если клиент не запросит конкретных временных рамок. В противном случае максимальное (разрешенное) время аренды IP адреса будет 7200 секунд. Сервер также "посоветует" клиенту использовать 255.255.255.0 в качестве маски подсети, 192.168.1.255 в качестве широковещательного адреса, 192.168.1.254 в качестве маршрутизатора/шлюза, а также 192.168.1.1 и 192.168.1.2 в качестве DNS серверов.

Если вам необходимо задать WINS сервер для вашего Windows клиента, вам нужно включить опцию netbios-name-servers, например

```
option netbios-name-servers 192.168.1.1;
```

Настройки конфигурации Dhcpd берутся из DHCP мини-HOWTO, которое можно найти *здесь* [http://www.tldp.org/HOWTO/DHCP/index.html].

7.3. Ссылки

DHCP FAQ [http://www.dhcp-handbook.com/dhcp_faq.html]

8. Служба именования доменов (DNS)

Служба именования доменов (Domain Name Service, DNS) - это сервис сети Интернет, который устанавливает соответствие между IP адресами и полностью определенными именами доменов (FQDN). DNS частично снимает необходимость в запоминании IP адресов. Компьютеры, которые обслуживают DNS называют *серверы имен (name servers)*. Ubuntu поставляется с приложением BIND (Berkley Internet Naming Daemon - демон именования для Интернет родом из Беркли), самой распространенной программой, используемой для поддержки сервера имен на GNU/Linux.

8.1. Установка

Для установки bind наберите в терминале следующую команду:

```
sudo apt-get install bind
```

8.2. Конфигурация

Конфигурационные файлы DNS храняться в директории `/etc/bind`. Главный файл конфигурации `/etc/bind/named.conf`. Ниже представлено содержимое конфигурационного файла по умолчанию:

```
// Это первоначальный файл конфигурации BIND DNS сервера.
//
// Пожалуйста прочтите /usr/share/doc/bind/README.Debian для получения информации о
// структуре файлов конфигурации BIND в Debian для BIND версий 8.2.1
// и выше, *ДО ТОГО* как вы измените этот файл конфигурации.
//

include "/etc/bind/named.conf.options";

// уменьшение многословности лога при неподконтрольных нам проблемах
logging {
 category lame-servers { null; };
 category cname { null; };
};

// загрузить в сервер знания о корневых серверах
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// быть авторитетным для передней и обратной зон локального хоста, и для
// широковещательных зон как для RFC 1912

zone "localhost" {
```

```
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

// добавьте сюда определения местных зон
include "/etc/bind/named.conf.local";
```

Директива include определяет имя файла, который содержит опции DNS. Директива directory в файле опций говорит DNS где искать эти файлы. Все файлы, которые использует BIND будут относиться к этой директории.

Файл `/etc/bind/db.root` описывает мировые корневые серверы имен. Серверы со временем изменяются и должны поддерживаться сечас и потом.

Раздел zone определяет основной сервер, этот раздел сохранен в файле упомянутом напротив тэга file. Файл каждой зоны содержит 3 ресурсных записи (resource records, RRs): SOA RR, NS RR и PTR RR. SOA - сокращение для Start of Authority. "@" - это специальное обозначение, подразумевающее происхождение. NS - это сервер имен (Name Server RR). PTR - указатель доменного имени (Domain Name Pointer). Для запуска DNS сервера, выполните следующую команду в строке терминала:

```
sudo /etc/init.d/bind start
```

Для получения детальной информации вы можете обратиться к документации, упоминаемой в разделе ссылок.

8.3. Ссылки

DNS HOWTO [http://www.tldp.org/HOWTO/DNS-HOWTO.html]

9. CUPS - сервер печати

Common UNIX Printing System (CUPS) - это основной механизм печати в Ubuntu и представления служб печати. Данная система печати представляет собой свободно распространямый, переносимый уровень управления печатью, который уже стал новым стандартом печати во многих дистрибутивах GNU/Linux.

CUPS управляет заданиями на печать и очередями, а также обеспечивает печать по сети, используя стандартный протокол печати Интернет, (Internet Printing Protocol, IPP). В то же время он поддерживает большое количество принтеров, от матричных до лазерных. CUPS также поддерживает описание принтеров PostScript (PostScript Printer Description, PPD) и авто-определение сетевых принтеров, и имеет простой web-ориентированный инструмент настройки и администрирования.

9.1. Установка

Для установки CUPS на ваш компьютер с Ubuntu, просто воспользуйтесь командой sudo вместе с apt-get, передав названия пакетов в качестве первого аргумента. Полная инсталляция CUPS имеет очень много зависимостей, но все они могут быть указаны в одной команде. Введите следующую команду в строке терминала для установки CUPS:

```
sudo apt-get install cupsys cupsys-client
```

После аутентификации с помощью вашего пароля, пакеты должны бфть скачаны и установлены без ошибок. По завершении установки, сервер CUPS будет автоматически запущен. Для разрешения проблем, вы можете просматривать лог ошибок сервера CUPS в файле журналирования ошибок: `/var/log/cups/error_log`. Если лог-файл не дает достаточной информации для определения источника вашей проблемы, количество информации записываемой в лог CUPS может быть увеличено изменением директивы **LogLevel** в файле настроек (смотри далее) на "debug" или даже "debug2", которая сохраняет все, в отличие от параметра по умолчанию "info". Если вы сделаете эти изменения, не забудьте исправить все обратно, после того, как решите вашу проблему, для предотвращения значительного увеличения размера лог-файла.

9.2. Конфигурация

Поведение сервера CUPS настраивается с помощью инструкций, содержащихся в файле `/etc/cups/cupsd.conf`. Файл настроек CUPS использует такой же синтаксис, как и основной файл настроек HTTP сервера Apache, то есть пользователи знакомые с модификацией файлов настроек Apache должны спокойно ориентироваться при работе с настройками CUPS. Примеры некоторых настроек, которые вы возможно захотите изменить с самого начала, будут представлены здесь.

Перед изменением конфигурационного файла, сделайте копию с оригинала и защитите ее от записи, чтобы использовать файл оригинальных настроек в качестве справки, а также иметь возможность использовать его снова.

Скопируйте файл `/etc/cups/cupsd.conf` и защитите его от записи с помощью следующих команд, выполненных в командной строке терминала:

```
sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.original
sudo chmod a-w /etc/cups/cupsd.conf.original
```

- **ServerAdmin**: Чтобы настроить адрес электронной почты желаемого администратора CUPS сервера, просто отредактируйте файл конфигурации `/etc/cups/cupsd.conf` в вашем текстовом редакторе, и соответственно измените строку *ServerAdmin*. Например, если вы Администратор CUPS сервера, и ваш адрес электронной почты 'bjoy@somebigco.com', тогда измените строку ServerAdmin таким образом:

```
ServerAdmin bjoy@somebigco.com
```

Если вам необходимо большее количество примеров директив файла конфигурации CUPS сервера, обратитесь к соответствующей странице руководства системы введя следующую команду в терминале:

```
man cupsd.conf
```

Если вы внесете изменения в файл конфигурации `/etc/cups/cupsd.conf`, вам будет необходимо перезапустить CUPS сервер, выполнив следующую команду в терминале:

```
sudo /etc/init.d/cupsys restart
```

Некоторые дополнительные настройки CUPS сервера выполняются в файле `/etc/cups/cups.d/ports.conf`:

- **Listen**: в Ubuntu по умолчанию, сервер CUPS прослушивает интерфейс обратной связи по IP адресу *127.0.0.1*. Для настройки сервера CUPS на прослушивание IP адреса конкретного сетевого адаптера, вам нужно указать имя хоста, или IP адрес, или пару IP адрес/порт через дополнение к инструкции Listen. Например, если ваш CUPS сервер находится в вашей локальной сети по IP адресу *192.168.10.250* и вы хотите сделать его доступным для других систем в этой подсети, вам нужно отредактировать файл `/etc/cups/cups.d/ports.conf`, добавив инструкцию Listen следующим образом:

```
Listen 127.0.0.1:631 # существующий Listen интерфейса loopback
Listen /var/run/cups/cups.sock # существующий Listen для сокетов
Listen 192.168.10.250:631 # Listen на интерфейсе LAN, Порт 631 (IPP)
```

В вышеприведенном примере вы можете закомментировать или удалить ссылки на loopback адрес (127.0.0.1), если желаете, чтобы cupsd вместо этого интерфейса, использовал только ethernet интерфейсы локальной сети, Для разрешения использования всех интерфейсов, включая loopback, к которым привязано определенное имя хоста, создав запись Listen для имени хоста *socrates* следующим образом:

```
Listen socrates:631 # Listen на всех интерфейсах хоста по имени 'socrates'
```

или опустив директиву Listen и используя вместо нее *Port* как в

```
Порт 631 # Прослушивание на порту 631 на всех интерфейсах
```

9.3. Ссылки

Сайт CUPS [http://www.cups.org/]

10. HTTPD - веб сервер Apache2

Apache - самый используемый веб-сервер на системах GNU/Linux. Веб-сервера используются для предоставления запрошенных клиентскими компьютерами веб-страниц. Пользователи обычно просматривают вэб-страницы используя веб-браузеры Firefox, Opera, или Mozilla.

Пользователи вводят ссылку (Uniform Resource Locator (URL)), чтобы указать серверу на запрашиваемый ресурс, используя FQDN (Fully Qualified Domain Name (полное доменное имя)). Например, чтобы увидеть домашнюю страницу сайта *Ubuntu* [http://www.ubuntu.com] пользователь должен ввести только FQDN. Для запроса информации о странице *paid support* [http://www.ubuntu.com/support/supportoptions/paidsupport] пользователю надо ввести FQDN и полный путь до страницы.

Самые используемые протоколы для передачи веб страниц - это HTTP (Hyper Text Transfer Protocol). Протокол, подобный HTTP, через Безопасное соединение (HTTPS) и протокол передачи файлов (FTP).

Веб сервер Apache часто используется в связке с движком баз данных MySQL, скриптовым языком PHP и другими популярными скриптовыми языками - Python и Perl. Данная конфигурация обозначена аббривиатурой LAMP (Linux, Apache, MySQL, Perl/Python/PHP) и формирует собой мощный набор инструментов для разработки и использования веб-приложений.

10.1. Установка

Веб сервер Apache2 доступен в Ubuntu Linux. Чтобы установить Apache2:

- Введите в терминале следующие команды:

```
sudo apt-get install apache2
```

10.2. Конфигурация

Apache настроен посредством *директив*, записанных обычным текстом в конфигурационные файлы. Осовной конфигурационный файл назван `apache2.conf`. Кроме того, другие конфигурационные файлы могут добавляться посредством директивы *Include*; в ней могут использоваться обобщающие символы для подключения нескольких файлов. Любая директива может быть расположена в любом и конфигурационных файлов. Изменения в основном конфигурационном файле принимаются сервером Apache2 только после запуска/перезапуска. На работающий сервер изменения не подействуют.

Сервер так же читает файл, содержащий mime-тип документа; имя файла устанавливается директивой *TypesConfig* и по умолчанию оно `mime.types` .

Файл конфигурации Apache2 по умолчанию: `/etc/apache2/apache2.conf` . Вы можете редактировать его для настройки сервера Apache2. Вы можете настроить номер порта, расположение файлов страниц, модули, лог файлы, виртуальные хости и так далее.

10.2.1. Остновные настройки

Данный раздел описывает основные параметры настройки сервера Apache2. За дополнительной информацией обращайтесь по адресу *Apache2 Documentation* [http://httpd.apache.org/docs/2.0/].

- Apache 2 поставляется с удобной для пользователя конфигурацией виртуальных хостов. То есть, сконфигурирован один виртуальный хост по умолчанию (с использованием директивы *VirtualHost*), настройку которого можно модифицировать или использовать как есть или использовать шаблоны для добавления других виртуальных хостов, если у вас несколько сайтов. Если ничего не менять, указанный по умолчанию виртуальный хост будет отображаться как ваш сайт по умолчанию. Так же этот сайт увидят пользователи, запросы которых не совпадут ни с одним значением директивы *ServerName* в конфигурационном файле виртуальных хостов. Для изменения виртуального хоста по умолчанию отредактируйте файл `/etc/apache2/sites-available/default`. Если вы хотите настроить новый виртуальный хост или сайт, скопируйте этот файл в тот же каталог с выбранным вами именем. Например: **sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mynewsite** Отредактируйте новый файл для настройки нового сайта используя директивы, описанные ниже
- Директива *ServerAdmin* определяет почтовый адрес администратора сервера, который будет отображаться пользователям. Значение по умолчанию - webmaster@localhost. Данная переменная должна быть изменена на доступный для вас почтовый адрес (если вы - администратор сервера). Если на вашем сайте возникнут проблемы, Apache2 отобразит ошибку, в которой так же будет отображен указанный почтовый адрес с целью сообщения проблемы. Вы можете найти эту директиву в вашем файле конфигурации сайтов, в каталоге /etc/apache2/sites-available.
- Директива *Listen* определяет порт и, при указании, IP адрес, на котором должен работать Apache2. Если IP адрес не указан, Apache2 работает на всех IP адресах, которые доступны компьютеру, на котором он запущен. Значение директивы по умолчанию - порт 80. Вы можете изменить значение на 127.0.0.1:80 чтобы Apache2 работал только на локальном интерфейсе и не был доступен из вне. Так же можно указать, например, значение 81 для изменения порта сервера или оставить все как есть для работы по умолчанию. Данная директива может быть найдена и изменена в ее собственном файле `/etc/apache2/ports.conf`
- Директива *ServerName* указывает, на какое FQDN (полное доменное имя) должен отвечать ваш сайт. В виртуальном хосте по умолчанию директива ServerName не указана, потому он будет отвечать на любые запросы, несоответствующие директивам ServerName в других виртуальных хостах. Если вы только что приобрели домен

ubunturocks.com и хотите его разместить на своем сервере, вам потребуется установить значение директивы ServerName ubunturocks.com в вашем файле конфигурации виртуального хоста. Добавьте эту директиву к новому виртуальному хосту, файл которого вы создали раньше (`/etc/apache2/sites-available/mynewsite`).

Возможно вы захотите, чтобы ваш сайт отвечал запросу www.ubunturocks.com, потому что многие пользователели привыкли использовать приставку www. Воспользуйтесь директивой *ServerAlias* для реализации этой задачи. Вы так же можете воспользоваться обощающим символом (*). Например, при указании значения директивы вида **ServerAlias *.ubunturocks.com** ваш сайт будет отвечать на любые запросы, оканчивающиеся строкой .ubunturocks.com.

- Директива *DocumentRoot* определяет, где Apache должен искать файлы сайта. Значение по умолчанию /var/www. По этому пути сайта нету, но если вы раскомментируете директиву *RedirectMatch* в файле `/etc/apache2/apache2.conf`, запросы будут перенаправлены по адресу /var/www/apache2-default, где расположен сайт Apache2 по умолчанию. Измените значение этой директивы в вашем файле конфигурации виртуального хоста и не забудьте создать каталог, если он еще не создан.

Apache2 **не** просматривает каталог /etc/apache2/sites-available. Символические ссылки в /etc/apache2/sites-enabled указывают на доступные сайты. Воспользуйтесь утилитой a2ensite (Apache2 Enable Site) для создания символических ссылок. Например: **sudo a2ensite mynewsite**, где mynewsite - имя файла конфигурации `/etc/apache2/sites-available/mynewsite`. Так же используйте эту утилиту для выключения активных конфигурации.

10.2.2. Настройки по умолчанию

Данный раздел описывает настройку параметров Apache2 по умолчанию. Они необходимы, например, если вы добавляете виртуальный хост, настраиваете нужные директивы, а некоторые не указываете. В этом случае используются значения по умолчанию.

- *DirectoryIndex* указывает на страницу (файл) по умолчанию, которую отдает пользователю сервер при запросе индекса каталога, указывая слеш (/) в конце имени каталога.

  Например, когда пользователь запрашивает страницу http://www.example.com/this_directory/, он получит ее в случае существования указанного в DirectoryIndex файла, иначе будет отображен сгенерированный сервером каталог, если указана опция Indexes или будет отбражена страница "Доступ запрещен". Сервер попытается найти один из файлов, указанных в директиве DirectoryIndex, просматривая ее значения по порядку и вернет первый существующий файл из списка. Если ни один из перечисленных в директиве файлов не будет найден и для этого каталога будет установлена опция Indexes, сервер сгенерирует список файлов и

подкаталогов в html-формате. Значение по умолчанию, которое можно найти в файле `/etc/apache2/apache2.conf` " index.html index.cgi index.pl index.php index.xhtml". Вообщем, если Apache2 найдет в запрошенном каталоге один из файлов, указанных в списке, он его отобразит.

- Директива *ErrorDocument* дает возможность указать файл, который Apache будет возвращать в случае сообщений об ошибке. Например, если пользователь запросит несуществующую страницу, будет вызвана ошибка 404 и Apache вернет файл, указанный в конфигурации по умолчанию - `/usr/share/apache2/error/HTTP_NOT_FOUND.html.var` . Файл не находится внутри каталога, указанного в директиве DocumentRoot, но директива Alias, описанная в файле `/etc/apache2/apache2.conf` перенаправляет запросы к каталогу /error в каталог /usr/share/apache2/error/. Чтобы просмотреть список директив ErrorDocument, воспользуйтесь командой **grep ErrorDocument /etc/apache2/apache2.conf**
- По умолчанию, лог запрашиваемых документов сервер пишет в файл /var/log/apache2/access.log. Вы можете указать для каждого виртуального хоста отдельный файл для логов посредством директивы *CustomLog* или же заменить значение по умолчанию, указанное в файле `/etc/apache2/apache2.conf`. Вы так же можете указать файл для записи ошибок посредством директивы *ErrorLog* (по умолчанию - `/var/log/apache2/error.log`). Он записывается отдельно от логов запрашиваемых документов, что упрощает поиск ошибок при каких либо проблемах с сервером Apache2. Так же вы можете указать директивы *LogLevel* и *LogFormat* (смотрите файл `/etc/apache2/apache2.conf` для определения настроек по умолчанию).
- Некоторые опции указаны для каждого каталога, а не для сервера, опции директив. Строфа Directory заключена в xml-подобные тэги:

```
<Directory /var/www/mynewsite>
    ...
  </Directory>
```

Директива Options внутри строфы Directory может принимать одно или несколько перечисленных далее значений, разделенных пробелом:

- emphasis role="bold">ExecCGI
- **Includes** - Разрешить server-side includes. Server-side includes разрешают подключать к html-файлам другие файлы. Это не общая опция. Для дополнительной информации посетите страницу *the Apache2 SSI Howto* [http://httpd.apache.org/docs/2.0/howto/ssi.html].
- **IncludesNOEXEC** - Разрешить server-side includes, но выключить команды #exec и #include в CGI скриптах.
- **Indexes** - Отображать список содержимого каталога, если ни одного файла из списка DirectoryIndex не обнаружена в запрошенном каталоге.

Из соображений безопасности обычно это не устанавливается и естественно не должно устанавливаться для каталога DocumentRoot. Включайте эту опцию только на отдельные каталоги и только в том случае, если уверены, что хотите, чтобы пользователи могли просматривать все содержимое каталога.

- **Multiview** - Поддержка content-negotiated multiviews; опция выключена по умолчанию в целях безопасности. Посетите *Apache2 документацию по этой опции* [http://httpd.apache.org/docs/2.0/mod/mod_negotiation.html#multiviews].
- **SymLinksIfOwnerMatch** - Переходить по символическим ссылкам только в случае, если у файла/каталога и ссылки один и тот же владелец.

10.2.3. Параметры виртуальных хостов

Виртуальные хосты позволяют вам запускать разные сервера для разных ip-адресов, разные имена хостов или разные порты на одних и тех же компьютерах. Например, вы можете запустить сайты http://www.example.com и http://www.anotherexample.com на одном и том же веб-сервере используя виртуальные хоста. Эта опция соответствует директиве <VirtualHost> для виртуального хоста по умолчанию и виртуального хоста по IP-адресу. Она соответствует директиве <NameVirtualHost> для базированного на имени виртуального хоста.

Директивы, установленные для виртуального хоста применяются только для того виртуального хоста, для которого они установлены. Если директива установлена в основной конфигурации сервера и не установлена для конкретного виртуального хоста, то будет использовано значение по умолчанию. Например, вы можете указать адрес электронной почты вебмастера в основном конфигурационном файле сервера и не указывать его для каждого виртуального хоста.

Установите директиву DocumentRoot для определения каталога, содержащего корневой документ (такой как index.html) для виртуального хоста. Значение директивы DocumentRoot по умолчанию - `/var/www`.

Директива ServerAdmin внутри строфы VirtualHost - это почтовый адрес, отображаемый внизу на страницах ошибок, если вы выбрали отображение подписей страниц с почтовым адресом на страницах ошибок.

10.2.4. Параметры Сервера

Данный раздел объясняет, как настроить основные параметры сервера.

LockFile - Директива LockFile устанавливает путь к lock-файлу сервера, который используется, если сервер собран с параметрами USE_FCNTL_SERIALIZED_ACCEPT или USE_FLOCK_SERIALIZED_ACCEPT. Он должен располагаться на локальном диске. Значение директивы должно быть оставлено по умолчанию за исключением случая, когда каталог логов находится в разделе NFS. Доступ к файлу должен быть только у суперпользователя (root).

PidFile - Директива PidFile устанавливает имя файла, в который сервер записывает свой номер поцесса (process ID (pid)). Файл должен читаться только суперпользователем (root). В большинстве случаев следует оставить значение по умолчанию.

User - Директива User определяет userid, под которым сервер отвечает на запросы. Она определяет возможности в доступе для сервера. Любые файлы, недоступные для этого пользователя не будут доступны и для посетителей сайтов. Значение по умолчанию www-data.

Без полного понимания того, что вы делаете, не устанавливайте директиву User в значение root. Использование суперпользователя (root) как пользователя веб-сервера создаст очень серьезные дыры в безопасности вашего сервера.

Директива Group по значению сходна с директивой User. Она устанавливает группу, от которой работает веб-сервер. Значение по умолчанию - www-data.

10.2.5. Модули Apache

Apache - модульный сервер. Под этим подразумевается, что в основную часть сервера входят только самые базовые функции. Расширеные возможности доступны посредством модулей, которые могут быть загружены в сервер. По умолчанию, базовый набор модулей входит в состав сборки. Если сервер собран с возможностью использования динамически загружаемых модулей, то модули могут собираться отдельно и добавляться в директику LoadModule. Иначе, Apache должен быть пересобран для добавления или удаления каких-либо модулей. В Ubuntu Apache2 собран с поддержкой динамической загрузки модулей. Вы можете устанавливать дополнительные модули Apache2 и использовать их вместе с вашим сервером. Вы можете установить модули Apache2 используя команду apt-get. Например, чтобы установить модуль аутентификации MySQL, вам нужно запустить следующую команду в терминале:

```
sudo apt-get install libapache2-mod-auth-mysql
```

После установки модуля он будет доступен в каталоге `/etc/apache2/mods-available`. Вы можете использовать команду a2enmod для включения модуля. Вы можете использовать команду a2dismod для выключения модуля. После включения модуля он будет доступен в каталоге `/etc/apache2/mods-enabled`.

10.3. Конфигурация HTTPS

Модуль mod_ssl добавляет важную функцию к серверу Apache2 - возможность шифровать передаваемую информацию. Таким образом, когда ваш браузер использует SSL шифрацию, в начале ссылки (Uniform Resource Locator (URL)) используется префикс https:// .

Модуль mod_ssl доступен в пакете apache2-common. Если данный пакет у вас установлен, вы можете запустить в терминале следующую команду для включения модуля mod_ssl:

```
sudo a2enmod ssl
```

10.3.1. Сертификаты и безопасность

Для настройки безопасности вашего сервера используйте криптографию с открытым ключем (public key cryptography), чтобы создать пару публичного/частного ключей (public and private key pair). В большинстве случаев, вы посылаете запрос на сертификат, доказательство идентификации вашей компании и оплату в Certificate Authority (CA). CA проверяет ваш запрос на сертификат, вашу идентификацию и затем высылает сертификат для вашего сервера.

Альтернативный вариант - вы можете создать свой собственный сертификат, подписанный собственоручно. Однако, собственоручно подписанные сертефикаты не могут использоваться на большинстве предприятий. Собственоручно подписанные сертификаты не принимаются браузером автоматически. Пользователям задается вопрос, принимать ли сертификат и создавать ли защищенное соединение.

Как только у вас будет сертификат (не важно, подписанный в CA или собственоручно), вам нужно установить его на ваш сервер.

10.3.2. Типы сертификатов

Вам нужен ключ и сертификат для управления вашим безопасным сервером, то есть вам нужно сгенерировать собственно подписанный сертификат или приобрести сертификат подписанный в CA. Подписанный в CA сертификат предоставляет две важные возможности вашему серверу:

- Браузеры (обычно) автоматически определяют сертификаты и разрешают безопасные соединения без подтверждения пользователя.
- Выданный CA подписанный сертификат является гарантией идентификации организации, предоставляющей веб страницы браузеру.

В большинстве браузеров, поддерживающих SSL, есть список сертификатов CA, который они автоматически принимают. Если у браузера нету в списке сертификата, подписанного CA, браузер задаст вопрос пользователю, устанавливать соединение или нет.

Вы можете сформировать свой самоподписанный сертификат для вашего безопасного сервера, но надо помить, что самоподписанный сертификат не предоставляет ту же функциональность как сертификат подписанный подписью CA. Самоподписанный сертификат не признается автоматически большинством Веб браузеров, и подобный сертификат не предоставляет никакой гарантии относительно компании, обеспечивающей вебсайт. Сертификат подписанный подписью CA гарантирует оба этих важных критерия для безопасного сервера. Процесс получения сертификата подписанного CA достаточно прост. Далее следует краткий обзор:

1. Создайте пару ключей шифрования, открытый и закрытый
2. Создайте запрос сертификата основанный на открытом ключе. Данный запрос содержит в себе информацию о вашем сервере и компании где он размещается.

3. Отправьте запрос сертификата вместе с документами подтверждающую вашу личность в CA.Мы не можем рекомендовать вам, какой тип сертификата выбрать. Ваше решение может основываться на вашем последнем опыте, на опыте ваших друзей и коллег или просто на финансовых факторах

   Если вы остановились на CA, вам необходимо следовать инструкциям, которые они предоставят для получения их сертификата
4. Когда CA установит, что вы являетесь тем, за кого себя выдаете, они пришлют вам цифровой сертификат
5. Установите этот сертификат на свой сервер и начинайте использовать безопасную передачу данных.

Получаете вы сертификат от CA или генерируете его собственоручно, первым шагом должно быть создание ключа.

10.3.3. Генерация Certificate Signing Request (CSR)

Для генерирования Certificate Signing Request (CSR) вам потребуется создать свой собственный ключ. Вы можете запустить описанные далее команды в терминале для создания ключа:

```
openssl genrsa -des3 -out server.key 1024
```

```
Generating RSA private key, 1024 bit long modulus
......................++++++
.................++++++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

Теперь вы можете ввести ваш пароль. Для наилучшей безопасности он должен содержать не менее восьми символов. Минимальная длинна - четыре символа. Пароль должен содержать цифры и/или специальные символы и не являться словом из словаря. Запомните то, что вы введете.

Повторите пароль для достоверности. После правильного повтора пароля сервер сгенерирует ключ и запишет его в файл `server.key`.

Вы так же можете запустить защищенный веб сервер без паспорт-пароля. Это удобно потому, что вам не нужно будет вводить пароль каждый раз при запуске защищенного сервера. Но это очень небезопасно.

В любом случае, вы можете запускать ваш сервер и без паспорт-пароля не указывая параметр -des3 при генерации паспорта или указав следующую команду в терминале:

```
openssl rsa -in server.key -out server.key.insecure
```

Запустив вышеуказанную команду сервер сохранит небезопасный ключ в файле `server.key.insecure`. Вы можете использовать этот файл для генерации CSR без паспорт-пароля.

Для создания CSR, выполните следующую команду в терминале:

```
openssl req -new -key server.key -out server.csr
```

Будет выдано приглашение ввести ключевую фразу. Если вы ввели правильную ключевую фразу, вам будет предложено ввести название компании, название сайта, адрес эл. почты и т.д. После того как вы введете эти параметры, ваш CSR будет создан и сохранен в файле `server.csr`. Вы можете отправить данный CSR в CA для обработки. CAN использует данный CSR для выпуска сертификата. С другой стороны вы можете создать самоподписанный сертификат используя этот CSR

10.3.4. Создание сертификата со своей подписью

Для того, чтобы создать сертификат со своей подписью исполните следующую комманду в терминале:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Вышеприведенная команда предложит ввести ключевую фразу. При вводе правильной ключевой фразы, ваш сертификат будет создан и сохранен в файле `server.crt`.

Если ваш защищенный сервер будет использован в коммерческих целях, вам скорее всего необходим сертификат подписанный CA. В данном случае не рекомендуется использовать самоподписанный сертификат.

10.3.5. Установка сертификата

Вы можете установить файл ключа `server.key` и файл сертификата `server.crt` или сертификат, предоставленный вам CA, следующей командой в терминале:

```
sudo cp server.crt /etc/ssl/certs
sudo cp server.key /etc/ssl/private
```

Вы должны добавить следующие четыре строки в файл `/etc/apache2/sites-available/default` или в конфигурационный файл вашего виртуального хоста. Вы должны расположить их в разделе *VirtualHost*. И они должны идти после строки *DocumentRoot*:

```
SSLEngine on
```

```
SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars +StrictRequire

SSLCertificateFile /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
```

Протокол HTTPS должен быть привязан к порту 443. Вам нужно добавить следующую строку в конфигурационный файл `/etc/apache2/ports.conf` :

```
Listen 443
```

10.3.6. Доступ к Серверу

После установки сертификата вам нужно перезапустить сервер. Вы можете перезапустить сервер следующей командой в терминале:

```
sudo /etc/init.d/apache2 restart
```

Вам нужно запомнить и вводить паспорт-пароль каждый раз при запуске вашего безопасного сервера.

У вас будет запрошен паспор-пароль. После ввода правильного пароля сервер будет запущен. Вы сможете посетить страницы на безопасном сервере указав ссылку https://your_hostname/url/ в адресной строке браузера.

10.4. Ссылки

Документация Apache2 [http://httpd.apache.org/docs/2.0/]

Документация Mod SSL [http://www.modssl.org/docs/]

11. Прокси-сервер Squid

Squid - полноценное приложение веб прокси кеш сервера, предоставляющее прокси и кэширование сервисов для HTTP, FTP и других популярных протоколов. Squid может обеспечить кэширование и посредничество SSL запросов и кэширование DNS обзоров; так же выполнять прозрачное кэширование. Squid поддерживает широкий спектр кэширующих протоколов, такие как Internet Cache Protocol (ICP), Hyper Text Caching Protocol (HTCP), Cache Array Routing Protocol (CARP) и Web Cache Coordination Protocol (WCCP).

Прокси/кеш сервер Squid - великолепное решения для разных задач, в которых требуется использование прокси или кэширования. Его применение варьируется от малых офисов до серьезных многоуровневых сетей, которые предоставляют обширные системы управления доступом и наблюдение за критическими параметрами через Simple Network Management Protocol (SNMP). При выборе компьютера для выделенного сервера под Squid убедитесь, что он оснащен большим количеством оперативной памяти, так как Squid кэширует данные в оперативную память для повышения производительности.

11.1. Установка

В строке терминала введите следующую команду для установки сервера Squid:

```
sudo apt-get install squid squid-common
```

11.2. Конфигурация

Squid настраивается посредством редактирования значений директив в файле `/etc/squid/squid.conf` . Следующие примеры показывают несколько директив, которые могут быть изменены для влияния на поведение Squid сервера. Для более детальной настройки Squid смотрите раздел Справка.

Перед редактированием конфигурационного файла сделайте копию оригинала с целью востановления каких-либо значений, если это потребуется или просто для справки.

Скопируйте файл `/etc/squid/squid.conf` и защитите от записи следующей командой:

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original
sudo chmod a-w /etc/squid/squid.conf.original
```

- Для того, чтобы настроить порт, на котором будет работать сервер Squid, на 8888 (по умолчанию 3128), вам нужно изменить значение директивы http_port следующим образом:

  http_port 8888

- Измените директиву visible_hostname для указания имени серверу Squid. Не обязательно, чтобы имя сервера Squid совпадало с именем компьютера. В данном примере оно установлено как *weezie*

  visible_hostname weezie

- Опять же, используя контроль доступа Squid-а, вы можете настроить доступ к ресурсам интернета только для пользователей с определенными ip-адресами. Например, мы продемонстрируем доступ пользователям только из подсети 192.168.42.0/24 :

  Добавьте следующее в **конец** секции ACL в вашем файле `/etc/squid/squid.conf` :

  acl fortytwo_network src 192.168.42.0/24

  Потом, добавьте следующее в **начало** секции http_access в вашем файле `/etc/squid/squid.conf` :

  http_access allow fortytwo_network

- Используя отличные возможности разграничения доступа в Squid, вы можете разрешить доступ к ресурсам Интернет только в рабочие часы. Напрмер, мы продемонстрируем доступ с 9:00 до 17:00, с понедельника по пятницу, для подсети 10.1.42.0/24:

  Добавьте следующее в **конец** секции ACL в вашем файле `/etc/squid/squid.conf` :

  acl biz_network src 10.1.42.0/24 acl biz_hours time M T W T F 9:00-17:00

  Потом, добавьте следующее в **начало** секции http_access в вашем файле `/etc/squid/squid.conf` :

  http_access allow biz_network biz_hours

После внесения изменений в файл `/etc/squid/squid.conf`, сохраните его и, набрав в терминале следующую команду, перезапустите squid сервер, чтобы изменения вступили в силу.

```
sudo /etc/init.d/squid restart
```

11.3. Ссылки

Squid Интернет-сайт [http://www.squid-cache.org/]

12. Система контроля версий

Контроль версий - это искусство управления изменениями в информации. Данный инструмент издавна был важен для программистов, которые обычно вносят небольшие изменения в программы, а затем, на следующий день, отменяют эти изменения. Однако, польза от систем контроля версий простирается далеко за границы мира разработки программного обеспечения. Место для систем контроля версий есть везде, где люди используют компьютеры для управления часто изменяющейся информацией

12.1. Subversion

Subversion - это система контроля версий с открытым исходным кодом. Используя Subversion вы можете сохранять историю изменений файлов и документов. Дерево файлов и папок хранится в центральном репозитории похожем на обыкновенный файловый архив, за исключением того, что сохраняются любые их модификации.

12.1.1. Установка

Для доступа к репозиторию Subversion, посредством HTTP протокола, вы должны установить и настроить веб сервер. Apache2 гарантированно работает с Subversion. Для установки и настройки сервера Apache2, обратитесь к подразделу HTTP раздела Apache2. Для доступа к репозиторию Subversion, посредством HTTPS протокола, вы должны установить и настроить цифровой сертификат в веб сервере Apache2. Для установки и настройки цифрового сертификата, обратитесь к подразделу HTTPS раздела Apache2.

Для установки Subversion выполните следующую команду в терминале:

```
sudo apt-get install subversion libapache2-svn
```

12.1.2. Конфигурация сервера

Данный шаг подразумевает, что вы установили в систему пакеты, отмеченные выше. Данная секция объясняет как создать репозиторий Subversion и получить доступ к проекту

12.1.2.1. Создания репоизитория Subversion

Репозиторий Subversion может быть создан используя следующую команду:

```
svnadmin create /path/to/repos/project
```

12.1.3. Методы доступа

Репозиторий Subversion может быть доступен разными способами - на локальном диске или через разные сетевые протоколы. В любом случае, расположение репозитория всегда ссылка (URL). Таблица объясняет разные схемы ссылок в доступных методах доступа.

Таблица 4.1. Методы доступа

Схема	Метод доступа
file://	прямой доступ к репозиторию (на локальном диске)
http://	Доступ по протоколу WebDAV к вебсерверу Apache2, умеющему работать с системой Subversion
https://	То же самое, что и http://, но с SSL шифрованием
svn://	Доступ через выборочный протокол к серверу svnserve
svn+ssh://	То же самое, что и svn://, но через SSH тунель

В этой секции объясняется как настроить Subversion для всех этих методов доступа. Здесь мы описываем основы. Для более детального описания, обратитесь к *книге svn* [http://svnbook.red-bean.com/].

12.1.3.1. Прямой доступ к репозиторию (file:///)

Это самый простой из всех методов доступа. Он не требует запуска никакого процесса сервера Subversion. Этот метод доступа используется для доступа к Subversion с той же машины. Синтакс команды, введенной в строке терминала, следующий:

```
svn co file:///path/to/repos/project
```

или

```
svn co file://localhost/path/to/repos/project
```

Если вы не указали имя хоста, используйте три слэша (///) - два для протокола (в данном случае - файл) плюс первый слэш в пути. Если вы указали имя хоста, используйте два слеша (//).

Права доступа к репозиторию зависят от прав доступа к файловой системе. Если пользователь обладает правами на чтение/запись - он может производить отладку и вносить изменения в репозиторий

12.1.3.2. Доступ через протокол WebDAV (http://)

Для доступа к репозиторию Subversion через протокол WebDAV необходимо сконфигурировать сервер Apache 2. Добавьте этот фрагмент в файл `/etc/apache2/apache2.conf`:

```
<Location /svn>
 DAV svn
 SVNPath /путь/к/репозиторию
 AuthType Basic
 AuthName "Название репозитория"
 AuthUserFile /etc/subversion/passwd
 <LimitExcept GET PROPFIND OPTIONS REPORT>
 Require valid-user
 </LimitExcept>
 </Location>
```

Следующим шагом необходимо создать файл `/etc/subversion/passwd`. Этот файл содержит настройки идетнификации. Для добавления записи, например новго пользователя, Вы можете запустить эту команду из окна терминала:

```
htpasswd2 /etc/subversion/passwd имя_пользователя
```

Команда запросит ввести пароль. Как только пароль будет введён - пользователь будет добавлен. Теперь что бы получить доступ к репозиторию Вам необходимо выполнить эту команду:

```
svn co http://имясервера/svn
```

Передача пароля происходит открытым текстом. Если Вы не хотите, что бы пароль был перехвачен используйте шифрование траффика с применением SSL. Дополнительные сведения Вы можете найти в следующей секции.

12.1.3.3. Доступ к протоколу WebDAV с применением SSL (https://)

Доступ к репозиторию Subversion через протокол WebDAV с применением SSL (https://) похож на http://, за исключением того, что в веб сервере Apache 2 необходимо установить и сконфигурировать цифровой сертификат.

Можно установить цифровой сертификат выданный такой организацией, как Verisign или сертификат, подписанный Вами.

Этот шаг подразумевает, что у вас есть установленный и сконфигурированный цифровой сертификат в веб сервере Apache 2. Для доступа к репозиторию Subversion, обязательно ознакомьтесь с предыдущей секцией! Спобобы доступа такие же, за исключением протокола. Необходимо использовать https:// для доступа к репозиторию Subversion.

12.1.3.4. Доступ с использованием своего протокола (svn://)

Как только репозиторий Subversion будет создан, можно будет сконфигурировать контроль доступа. Для изменения контроля доступа измените файл `/путь/к/репозиторию/проект/conf/svnserve.conf`. Например, для включения аутентификации, уберите комментарий на следующих строчках:

```
# [general]
```

```
# password-db = passwd
```

Как только Вы раскомментируете вышеуказанные строки, Вы можете использовать список пользователей из файла passwd. Редактировать необходимо файл `passwd` , находящийся в той же директории и добавьте нового ползователя.

```
username = password
```

Что бы получить больше информации посмотрите файл.

Теперь что бы получить доступ к Subversion через свой протокол svn:// с того же или с другого компьютера, Вы можете запустить сервер Subversion используя комманду svnserve. Синтаксис:

```
$ svnserve -d --foreground -r /путь/к/репозиторию
# -d -- daemon режим сервиса (невидимый)
# --foreground -- запустить на консоль (полезно для отладки)
# -r -- корень репозитория

Для подробного описания использования команды выполните команду:
$ svnserve --help
```

После запуска этой команды Subversion будет запущен на порту 3690. Для того, что бы сменить репозиторий, необходимо выполнить команду:

```
svn co svn://имяхотса/проект проект --username имя_пользователя
```

Если в кониге указано, будет запрошен пароль. После аутентификации, будет проверен код из репозитория Subversion. Для синхронизации локальной копии и репозитория проекта можно выполнить под-команду **update**. Синтакс введённой команды следующий.

```
cd директория_проекта ; svn update
```

Вы можете обратиться к инструкции пользователя, если вас интересует детали использования каждой под-команды Subversion. На пример, что бы узнать больше про комманду "co", запустите эту команду:

```
svn co help
```

12.1.3.5. Доступ используя нестандартный протокол с поддержкой SSL (svn+ssh://)

Конфигурация и процесс сервера такие же как и в случае с svn://. Более подробно описано в предыдущей секции. На этом этапе подразумевается что Вы выполнили предыдущие шаги и запустили сервер Subversion, используя комманду svnserve

Так же подразумевается, что на том же компьютере запущен сервер SSH и на него разрешены входящие соединения. Что бы проверить, попробуйте подключиться к этому компьютеру используя SSH. Если вы зашли в этот компьютер, значит всё замечательно.

Если вы не можете войти в этот компьютер, решите эту проблему перед тем, как приступать к дальнейшим шагам.

Протокол svn+ssh:// используется если необходимо подключиться к репозиторию Subversion используя SSL. В этом случае все передаваемые данные будут зашифрованы. Для доступа к репозиторию проекта необходимо использовать следующую комманду:

```
svn co svn+ssh://hostname/var/svn/репозиторий/проект
```

Что бы получить доступ к репозиторию Subversion используя этот метод, необходимо ввести полный путь (/путь/к/репозиторию/проекту).

Если в указано в настройках будет запрошен пароль. Необходимо ввести пароль, используемый при подключении через SSH. Если пароль верный, будет проверен код из репозитория Subversion.

12.2. Сервер CVS

CVS - система контроля версий. Её можно использовать для записи истории исходных файлов.

12.2.1. Установка

Введите следующую команду в окне термниала для установки cvs:

```
sudo apt-get install cvs
```

После того, как вы установите cvs, необходимо установить xinetd для запуска/останова сервера CVS. При запросе введите следующую команду для установки xinetd:

```
sudo apt-get install xinetd
```

12.2.2. Конфигурация

Репозиторий будет инициализирован автоматически после установки cvs. По умолчанию репозиторий находится в директории /var/lib/cvs. Этот путь можно изменить при помощи команды:

```
cvs -d /ваш/новый/cvs/репозиторий init
```

Для запуска CVS сервера после изменения настроек репозитория Вы можете сконфигурировать xinetd. Можно скопировать приведённые строки в файл `/etc/xinetd/cvspserver`.

```
сервис cvspserver
```

```
{
     порт = 2401
     тип_сокета= stream
     протокол = tcp
     пользователь = root
     ждать = no
     тип = UNLISTED
     сервер = /usr/bin/cvs
     аргументы_сервера = -f --allow-root /var/lib/cvs pserver
     отключить = no
}
```

Если была изменена директория по умолчанию (/var/lib/cvs), то необходимо будет изменить репозиторий.

После конфигурирования xinetd Вы можете запустить CVS сервер используя команду command:

```
sudo /etc/init.d/xinetd start
```

Для проверки запущен ли CVS сервер можно использовать команду:

```
sudo netstat -tap | grep cvs
```

После того, Вы запустите эту команду, Вы должны увидеть нечто похоже:

```
tcp 0 0 *:cvspserver *:* LISTEN
```

После этого можно добавлять новых пользвателей, новые проекты и управлять сервером CVS.

CVS позволяет добавлять новых пользователй независимо от установленной у них ОС. Вероятно самый лёгкий путь использовать Linux Users для CVS

12.2.3. Добавление проектов

Эта секция объясняет как добавить новый проект в репозиторий CVS. Создать директорию, добавить необходимые документы и исходные тексты в эту директорию. Что бы добавить проект в репозиторий CVS запустите эту команду:screen> **cd путь/к проекту cvs import -d :pserver:имяпользователя@имяхоста.com:/var/lib/cvs -m "Импортирование моих проектов в репозиторий CVS". новый_проект начало**

12.3. Ссылки

Домашняя страница Subversion [http://subversion.tigris.org/]

Книга Subversion [http://svnbook.red-bean.com/]

Инструкция по CVS [http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html]

13. Базы данных

Поставка Ubuntu включает два сервера баз данных. Это

- MySQL™
- PostgreSQL

. Они так же доступны в главном репозитории. В этой секции описано как установить и настроить эти сервера баз данных.

13.1. MySQL

MySQL это быстрый, многопоточный, многопользовательский и надёжный SQL сервер. Он предназначен как для критически важных производственных систем с большой загруженностью, так и для встраивания в большую часть приложений.

13.1.1. Установка

Выполните эту команду в окне терминала для устнановки MySQL:

```
sudo apt-get install mysql-server mysql-client
```

Как только установка будет оконченна, сервер MySQL должен будет автоматически запущен. Для того, что бы проверить запущен ли сервер MySQL или нет можно воспользоваться коммандой:

```
sudo netstat -tap | grep mysql
```

После того, Вы запустите эту команду, Вы должны увидеть нечто похоже:

```
tcp 0 0 localhost.localdomain:mysql *:* LISTEN -
```

Если сервер не был запущен, то для запуска можно попробовать эту команду:

```
sudo /etc/init.d/mysql restart
```

13.1.2. Конфигурация

По умолчанию пароль администратора не установлен. Первое, что необходимо сделать сразу же после установки - это установить этот пароль. Воспользуйтесь этой командой:

```
sudo mysqladmin -u root (пароль) (новыйпароль) ( (пароль) - вероятно имеется ввиду текущий - прим.
```

```
sudo mysqladmin -u root -h localhost (пароль) (новыйпароль)
```

Для установки базовых настроек можно отредактировать файл `/etc/mysql/my.cnf` -- лог файл, номер порта и тп. Если хотите узнать больше - посмотрите содержимое файла `/etc/mysql/my.cnf`.

13.2. PostgreSQL

PostgreSQL - это объектно-ориентированная база данных, которая имеет характерные черты классических коммерческих баз данных с расширенными возможностями, которые могут быть найдены в системах DBMS следующего поколения. (DBMS - DataBase Management System - система управления базой данных - прим. переводчика).

13.2.1. Установка

Для того, что бы установить PostgreSQL, необходимо выполнить следующую команду:

```
sudo apt-get install postgresql
```

После окнчания установки вы можете настроить сервер PostgreSQL под свои нужды.

13.2.2. Конфигурация

По умолчанию соединение через протокол TCP/IP отключено. PostgreSQL имеет поддержку нескольких методов аутентификации клиентов. По умолчанию используется метод аутентификации IDENT. Подробную информацию вы найдёте в этой инструкции: : *the PostgreSQL Administrator's Guide* [http://www.postgresql.org/docs/8.1/static/admin.html].

В приведённых ниже инструкциях подразумается, что выбрано подключение с использованием TCP/IP и аутентификацией клиентов по алгоритму MD5. Конфигурационные файлы PostgreSQL находятся в `/etc/postgresql/<version>/main`. Например, если вы установили PostgreSQL 7.4, конфигурационные файлы будут сохранены в `/etc/postgresql/7.4/main`.

Для настройки аутентификации с использованием ident отдредактируйте `/etc/postgresql/7.4/main/pg_ident.conf`.

Для включения TCP/IP соединений отредактируйте файл `/etc/postgresql/7.4/main/postgresql.conf`

Найдите строку *#tcpip_socket = false* и измените ее на *tcpip_socket = true*. Вы так же можете отредактировать все остальные параметры, если вы знаете, что нужно делать! Для подробностей, обратитесь к конфигурационному файлу или документации PostgreSQL.

По умолчанию, пользовательские документы не установлены в *MD5* аутентификацию. Потому, в первую очередь необходимо настроить сервер PostgreSQL для использования *доверительной* аутентификации клиента, соединения с базой данных, настроить пароль и вернуть настройки назад для использования аутентификации *MD5*.

Для включения *доверительной* аутентификации клиента отредактируйте файл `/etc/postgresql/7.4/main/pg_hba.conf`

Закоментируйте все существующие строки, которые используют *ident* и *MD5* аутентификацию и добавьте следующую строку:

```
local all postgres trust sameuser
```

Тогда запустите сервер PostgreSQL следующей командой:

```
sudo /etc/init.d/postgresql start
```

Как только PostgreSQL сервер будет успешно запущен, для подключения к примеру базы данных PostgreSQL в терминале наберите следующую команду

```
psql -U postgres -d template1
```

Вышеуказанная команда соединяет с базой данных PostgreSQL *template1* как пользователя *postgres*. Соединившись с сервером PostgreSQL, вы попадаете в строку ввода SQL запросов. Вы можете выполнить следующую команду SQL в строке psql для настройки пароля пользователя *postgres*.

```
template1=# ИЗМЕНИТЕ ПОЛЬЗОВАТЕЛЯ postgres зашифрованным паролем 'ваш_пароль';
```

После настройки пароля, отредактируйте файл `/etc/postgresql/7.4/main/pg_hba.conf` для использования *MD5* аутентификации:

Закомментируйте недавно добавленную *trust* строку и добавьте:

```
↵
local all postgres md5 sameuser↵
```

Приведенная выше конфигурация ни в коем случае не является законченой. Для настройки дополнительных параметров, пожалуйста, обратитесь к *Руководству администратора PostgreSQL* [http://www.postgresql.org/docs/8.1/static/admin.html].

14. Сервисы электронной почты

Процесс доставки электронных писем от одного человека к другому через локальную сеть или Интернет включает в себя взаимодействие множества систем. Каждая из этих систем должна быть правильно настроена, чтобы выполнять свою работу. Оправитель использует *почтовый агент пользователя* (Mail User Agent, MUA) или клиент электронной почты, чтобы отправлять сообщения через один или несколько *агентов передачи почты* (Mail Transfer Agents, MTA), последний из которых передаст сообщение *агенту доставки почты* (Mail Delivery Agent, MDA) для доставки почты в почтовый ящик получателя, откуда оно может быть доставлено получателю с помощью его почтового клиента, обычно через сервер POP3 или IMAP.

14.1. Postfix

В Ubuntu агент передачи почты (Mail Transfer Agent (MTA)) по умолчанию - Postfix. Он считается безопасным, быстрым и легким в администрировании. Он совместим с MTA sendmail. Данный раздел объяснит, как установить и настроить postfix. Так же будет описано, как настроить SMTP сервер с использованием безопасного соединения (для безопасной передачи почты).

14.1.1. Установка

Для устрановки postfix вместе с SMTP-AUTH и Transport Layer Security (TLS) запустите следующую команду:

```
sudo apt-get install postfix
```

Просто нажимайте enter когда установщик будет задавать вопросы, настройки будут описаны более подробно в следующем шаге.

14.1.2. Базовая конфигурация

Для настройки приложения postfix, выполните следующую команду:

```
sudo dpkg-reconfigure postfix
```

Будет запущен пользовательский интерфейс. На каждом экране выберите следующие значения:

- Ok
- Сайт в интернете
- NONE
- mail.example.com
- mail.example.com, localhost.localdomain, localhost
- No

- 127.0.0.0/8
- Yes
- 0
- +
- все

Замените mail.example.com именем хостав вашего почтового сервера

14.1.3. Аутентификация SMTP

Следующие шаги настраивают postfix для использования SASL для SMTP AUTH. Вместо правки файла настроек напрямую, вы можете использовать команду **postconf** для настройки всех параметров postfix. Параметры настройки будут сохранены в файле `/etc/postfix/main.cf`. Позже если вы пожелаете перенастроить определенный параметр, вы можете либо выполнить команду или вручную изменить файл.

1. Настройте Postfix для выполнения SMTP AUTH используя SASL (saslauthd):

```
↵
postconf -e 'smtpd_sasl_local_domain ='↵
postconf -e 'smtpd_sasl_auth_enable = yes'↵
postconf -e 'smtpd_sasl_security_options = noanonymous'↵
postconf -e 'broken_sasl_auth_clients = yes'↵
postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_
postconf -e 'inet_interfaces = all'↵
echo 'pwcheck_method: saslauthd' >> /etc/postfix/sasl/smtpd.conf↵
echo 'mech_list: plain login' >> /etc/postfix/sasl/smtpd.conf↵
```

2. Далее, настройте цифровой сертификат TLS. При ответе на задаваемые вопросы, следуйте инструкциям, и выбирайте подходящие ответы

```
↵
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024↵
chmod 600 smtpd.key↵
openssl req -new -key smtpd.key -out smtpd.csr↵
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt↵
openssl rsa -in smtpd.key -out smtpd.key.unencrypted↵
mv -f smtpd.key.unencrypted smtpd.key↵
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650↵
mv smtpd.key /etc/ssl/private/↵
mv smtpd.crt /etc/ssl/certs/↵
mv cakey.pem /etc/ssl/private/↵
mv cacert.pem /etc/ssl/certs/↵
```

Вы можете получить цифровой сертификат в компании сертификации или создать сертификат самостоятельно. За подробностями обращайтесь к документу *Раздел 10.3.4, «Создание сертификата со своей подписью» [56]*

3. Настройте Postfix для выполнения TLS шифрования, как для входящей, так и для исходящей почты:

```
↵
postconf -e 'smtpd_tls_auth_only = no'↵
postconf -e 'smtp_use_tls = yes'↵
postconf -e 'smtpd_use_tls = yes'↵
postconf -e 'smtp_tls_note_starttls_offer = yes'↵
postconf -e 'smtpd_tls_key_file = /etc/ssl/private/smtpd.key'↵
postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt'↵
postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'↵
postconf -e 'smtpd_tls_loglevel = 1'↵
postconf -e 'smtpd_tls_received_header = yes'↵
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'↵
postconf -e 'tls_random_source = dev:/dev/urandom'↵
postconf -e 'myhostname = mail.example.com'↵
```

SMTP AUTH для with postfix будет настроена после того, как вы запустите все команды. Собственный сертификат создан для TLS и настроен для использования с postfix.

Теперь, файл `/etc/postfix/main.cf` должен выглядеть *подобным* [../sample/postfix_configuration] образом.

Начальная настройка postfix завершена. Вы можете запустить демона postfix с помощью следующей команды:

```
sudo /etc/init.d/postfix start
```

Теперь демон postfix установлен, настроен и удачно запущен. Postfix поддерживает SMTP AUTH как определено в документе *RFC2554* [ftp://ftp.isi.edu/in-notes/rfc2554.txt], который основан на *SASL* [ftp://ftp.isi.edu/in-notes/rfc2222.txt]. Однако, аутентификацию SASL все таки необходимо настроить до того, как вы сможете использовать SMTP.

14.1.4. Настройка SASL

libsasl2, sasl2-bin и libsasl2-modules необходимы для включения SMTP AUTH используя SASL. Вы можете установить эти приложения, если ещё этого не сделали.

```
apt-get install libsasl2 sasl2-bin
```

Некоторые изменения необходимы для корректной работы. Из-за того, тчто Postfix запускается в окружении с измененным корнем (с помощью chroot) в `/var/spool/postfix`, необходимо сконфигурировать SASL для запуска в "поддельном" root-окружении (`/var/run/saslauthd` становится `/var/spool/postfix/var/run/saslauthd`):

```
mkdir -p /var/spool/postfix/var/run/saslauthd
rm -rf /var/run/saslauthd
```

Для активации saslauthd отредактируйте файл `/etc/default/saslauthd`, изменив или добавив в него переменную START. Для настройки запуска saslauthd в "поддельном"

root-окружении, добавьте параметры PWDIR, PIDFILE и PARAMS. Напоследок, измените переменную MECHANISMS на подходящую для вашего случая. Файл должен выглядеть примерно вот так:

```
# This needs to be uncommented before saslauthd will be run
# automatically
START=yes

PWDIR="/var/spool/postfix/var/run/saslauthd"
PARAMS="-m ${PWDIR}"
PIDFILE="${PWDIR}/saslauthd.pid"

# You must specify the authentication mechanisms you wish to use.
# This defaults to "pam" for PAM support, but may also include
# "shadow" or "sasldb", like this:
# MECHANISMS="pam shadow"

MECHANISMS="pam"
```

Если хотите, вы можете использовать **shadow** вместо **pam**. Этот способ будет использовать передачу паролей хешированных с помощью MD5, что является полностью безопасным. Имя пользователя и пароль, необходимые для авторизации, будут такими же, как и у пользователей на системе, которую вы используете под сервер.

Теперь обновите "состояние" dpkg для `/var/spool/portfix/var/run/saslauthd`. Инициализационный скрипт saslauthd воспользуется заданными настройками, чтобы создать недостающие каталоги с соответствующими правами доступа и владения:

```
dpkg-statoverride --force --update --add root sasl 755 /var/spool/postfix/var/run/saslauthd
```

14.1.5. Тестирование

Настройка SMTP AUTH завершена. Теперь самое время для проверочного запуска и тестирования установок. Вы можете запустить демон SASL с помощью следующей команды:

```
sudo /etc/init.d/saslauthd start
```

Чтобы проверить правильно ли работают SMTP-AUTH и TLS, выполните следующую команду:

```
telnet mail.example.com 25
```

После установки соединения с почтовым сервером postfix, введите:

```
ehlo mail.example.com
```

Все работает правильно, если в представленном выводе вы увидите в том числе и строки представленные ниже:

```
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```

Введите команду **quit** для завершения сеанса.

14.2. Exim4

Exim4 - это другой агент передачи сообщений (Message Transfer Agent, MTA), разработанный в Кембриджском университете (University of Cambridge) для использования на Unix-системах, подключенных к сети Интернет. Можно установить Exim как замену sendmail, однако настройка exim довольно сильно отличается от настройки sendmail.

14.2.1. Установка

Для установки exim4, выполните следующую команду:

```
sudo apt-get install exim4 exim4-base exim4-config
```

14.2.2. Конфигурация

Для настройки exim4, выполните следующую команду:

```
sudo dpkg-reconfigure exim4-config
```

Отобразится пользовательский интерфейс. Он позволяет настроить многие параметры. Например, в exim4 файлы настроек разбиты на множество файлов. Если вы желаете иметь настройки в одном файле вы можете настроить это в пользовательском интерфейсе.

Все параметры, котрые вы настраиваете с помощью пользовательского интерфейса, хранятся в файле `/etc/exim4/update-exim4.conf.conf`. Если вы хотите изменить настройки, то вы можете: либо запустить еще раз мастер настройки, либо отредактировать данный файл вручную в вашем любимом текстовом редакторе. После завершения настройки, выполните следуующую команду, чтобы создать основной конфигурационный файл:

```
sudo update-exim4.conf
```

Основной файл конфигурации будет создан и сохранен под именем `/var/lib/exim4/config.autogenerated`.

Вы не должны, ни при каких обстоятельствах, редактировать вручную основной файл настроек `/var/lib/exim4/config.autogenerated`. Он обновляется автоматически каждый раз, когда вы запускаете команду **update-exim4.conf**

Для запуска демона exim4 воспользуйтесь следующей командой:

```
sudo /etc/init.d/exim4 start
```

TODO: This section should cover configuring SMTP AUTH with exim4.

14.3. Dovecot Server

Dovecot - это агент доставки почты, написанный с упором на безопасность. Он поддерживает основные форматы почтовых ящиков: mbox или Maildir. Этот раздел рассказывает о том, как настроить его в качестве сервера imap или pop3.

14.3.1. Установка

Для установки dovecot, выпоните следующую команду в командной строке:

```
sudo apt-get install dovecot-common dovecot-imapd dovecot-pop3d
```

14.3.2. Конфигурация

Для настройки dovecot вы можете отредактировать файл `/etc/dovecot/dovecot.conf`. Вы можете выбрать протокол, который будете использовать. Возможные варианты: pop3, pop3s (pop3 secure), imap и imaps (imap secure). Описание этих протоколов выходит за пределы данного руководства. Для дальнейшей информации посетите статьи в википедиа ulink url="http://en.wikipedia.org/wiki/POP3">POP3

IMAPS и POP3S более безопасны, чем IMAP и POP3, так как они используют шифрование SSL для установки соединения. После того, как вы определились с протоколом, внесите изменения в следующую строку файла `/etc/dovecot/dovecot.conf`:

```
protocols = pop3 pop3s imap imaps
```

Она включает протоколы при старте dovecot. Далее, добавьте следующую строку в раздел pop3 файла `/etc/dovecot/dovecot.conf`:

```
pop3_uidl_format = %08Xu%08Xv
```

Затем выберите используемый почтовый ящик. Dovecot поддерживает форматы **maildir** и **mbox**. Это наиболее часто используемые форматы почтовых ящиков. Каждый из этих форматов имеет свои преимущества, которые обсуждены на *веб-сайте dovecot* [http://dovecot.org/doc/configuration.txt].

Выбрав тип почтового ящика, отредактируйте файл `/etc/dovecot/dovecot.conf` и измените следующую линию:

```
default_mail_env = maildir:~/Maildir # (для maildir)
```

```
или
default_mail_env = mbox:~/mail:INBOX=/var/spool/mail/%u # (для mbox)
```

Вам следует настроить ваш Mail Trasport Agent (MTA) для передачи входящей почты этому типу почтового ящика если он отличается от того, которого вы настроили.

По окончании настройки dovecot, запустите демона dovecot, чтобы проверить работу ваших установок:

```
sudo /etc/init.d/dovecot start
```

Если вы активировали imap или pop3, вы можете также попробовать войти на сервер при помощи команд **telnet localhost pop3** или **telnet localhost imap2** Установка выполнена успешно, если вы видите вывод, подобный следующему:

```
bhuvan@rainbow:~$ telnet localhost pop3
Пытаемся 127.0.0.1...
Соединился с localhost.localdomain.
Клавиша возврата '^]'.
+OK Dovecot готов.
```

14.3.3. Dovecot: Настройка SSL

Для настройки использования SSL в dovecot, вы можете отредактировать файл`/etc/dovecot/dovecot.conf`, изменив следующие строки:

```
ssl_cert_file = /etc/ssl/certs/dovecot.pem
ssl_key_file = /etc/ssl/private/dovecot.pem
ssl_disable = no
disable_plaintext_auth = no
```

Файлы **cert** и **key** создаются автоматически при установке dovecot. Пожалуйста, обратите внимание, что данные ключи не подписаны и их использование будет давать ошибки вида "bad signature" (плохая подпись) при подключении клиентов. Чтобы избежать этого, вы можете воспользоваться коммерческими сертификатами, или, что еще лучше, вы можете использовать свои собственные сертификаты SSL.

14.3.4. Настройка брандмауэра для почтового сервера

Для доступа к вашему почтовому серверу с другого компьютера вы должны настроить брандмауер на разрешение соединений по необходимым портам.

- IMAP - 143
- IMAPS - 993
- POP3 - 110
- POP3S - 995

14.4. Mailman

Mailman - это программа с открытыми кодами для управления дискуссиями, ведущимися через электронную почту, и рассылками электронных новостных сообщений. Многие открытые списки рассылок (включая все на *Ubuntu mailing lists* [http://lists.ubuntu.com]) используют Mailman, в качестве программы управления почтовыми списками. Это мощное приложение, при этом его легко установить и поддерживать.

14.4.1. Установка

Mailman предоставляет веб-интерфейс для администраторов и пользователей. То есть, ему необходим сервер Апач (apache) с поддержкой mod_perl. Mailman использует внешний почтовый сервер для отправки и получения электронной почты. Он отлично взаимодействует со следующими почтовыми серверами:

- Postfix
- Exim
- Sendmail
- Qmail

Мы рассмотрим как установить mailman, веб-сервер apache и почтовый сервер Exim. Если вы хотите установить mailman для другого почтового сервера, пожалуйста, обратитесь к разделу ссылки.

14.4.1.1. Apache2

Для описания установки apache2 смотрите *Раздел 10.1, «Установка» [48].*

14.4.1.2. Exim4

Для установки Exim4 выполните следующие команды в строке терминала:

```
sudo apt-get install exim4
sudo apt-get install exim4-base
sudo apt-get install exim4-config
```

После установки exim4, файлы настроек сохраняются в каталоге `/etc/exim4`. В Ubuntu, по умолчанию, настройки exim4 распределены среди различных файлов. Вы можете изменить это поведение изменив следующую переменную в файле `/etc/exim4/update-exim4.conf`:

- dc_use_split_config='true'

14.4.1.3. Mailman

Для инсталляции Mailman выполните следующую команду в строке терминала:

```
sudo apt-get install mailman
```

Она копирует файлы, необходимые для установки, в каталог /var/lib/mailman. Плюс, устанавливает скрипты CGI в каталог /usr/lib/cgi-bin/mailman. А также создает линукс пользователя *list* и линукс группу *list*. Этот пользователь будет владельцем процесса mailman.

14.4.2. Конфигурация

Данный раздел подразумевает, что у вас уже установлены: mailman, apache2 и exim4. Теперь вам нужно только настроить их.

14.4.2.1. Apache2

После установки apache2, добавьте следующие строки в файл `/etc/apache2/apache2.conf`:

```
Alias /images/mailman/ "/usr/share/images/mailman/"
Alias /pipermail/ "/var/lib/mailman/archives/public/"
```

Mailman использует apache2 для исполнения своих CGI-скриптов. CGI скрипты mailman-а установлены в каталоге /usr/lib/cgi-bin/mailman. То есть его url-адрес будет http://hostname/cgi-bin/mailman/. Чтобы изменить это, вы можете отредактировать файл `/etc/apache2/apache2.conf`.

14.4.2.2. Exim4

После установки Exim4, сервер Exim может быть запущен из командной строки терминала при помощи:

```
sudo /etc/init.d/exim4 start
```

Для того, чтобы mailman работал с exim4, вам необходимо настроить exim4. Как замечено ранее, по умолчанию exim4 использует множество конфигурационных файлов различных типов. Для получения более подробной информации, обратитесь к *веб-странице Exim* [http://www.exim.org]. Для запуска mailman, нам нужно добавить новый файл настроек к следующим типам конфигураций:

- Основное
- Передача почты
- Маршрутизатор

Exim создает основной файл настроек, разбирая все эти настроечные мини-файлы. То есть порядок, в котором идут эти файлы настроек, очень важен.

14.4.2.3. Основное

Все настроечные файлы основного типа хранятся в каталоге `/etc/exim4/conf.d/main/`. Создайте новый файл `04_exim4-config_mailman` и добавьте в него следующее:

```
# start
```

```
# Home dir for your Mailman installation -- aka Mailman's prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman"
# This is normally the same as ~mailman
MM_HOME=/var/lib/mailman
#
# User and group for Mailman, should match your --with-mail-gid
# switch to Mailman's configure script. Value is normally "mailman"
MM_UID=list
MM_GID=list
#
# Domains that your lists are in - colon separated list
# you may wish to add these into local_domains as well
domainlist mm_domains=hostname.com
#
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
#
# These values are derived from the ones above and should not need
# editing unless you have munged your mailman installation
#
# The path of the Mailman mail wrapper script
MM_WRAP=MM_HOME/mail/mailman
#
# The path of the list config file (used as a required file when
# verifying list addresses)
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck
# end
```

14.4.2.4. Передача почты

Все настроечные файлы, принадлежащие к типу транспортировка, хранятся в каталоге `/etc/exim4/conf.d/transport/`. Создайте новый файл `40_exim4-config_mailman` и добавьте в него следующее:

```
  mailman_transport:
   driver = pipe
   command = MM_WRAP \
               '${if def:local_part_suffix \
                     {${sg{$local_part_suffix}{-(\\w+)(\\+.*)?}{\$1}}} \
                     {post}}' \
               $local_part
    current_directory = MM_HOME
    home_directory = MM_HOME
    user = MM_UID
    group = MM_GID
```

14.4.2.5. Маршрутизатор

Все настроечные файлы, принадлежащие к типу роутер, хранятся в каталоге `/etc/exim4/conf.d/router/`. Создайте новый файл `101_exim4-config_mailman` и добавьте в него следующее:

```
mailman_router
 driver = accept
 require_files = MM_HOME/lists/$local_part/config.pck
 local_part_suffix_optional
 local_part_suffix = -bounces : -bounces+* : \
                     -confirm+* : -join : -leave : \
                     -owner : -request : -admin
 transport = mailman_transport
```

Порядок основных и транспортных файлов настроек не важен. Однако, порядок файлов настроек роутера должен быть сохранен. Конкретно этот файл по порядку должен быть до файла 200_exim4-config_primary. Оба этих файла содержат одинаковый тип информации. Первый из них будет определен как предшественник. Для получкения более полной информации, обратитесь к секции ссылки.

14.4.2.6. Mailman

После установки mailman, для его запуска воспользуйтесь командой:

```
sudo /etc/init.d/mailman start
```

Теперь вам нужно создать основной список рассылки. Воспользуйтесь для этого следующей командой:

```
sudo /usr/sbin/newlist mailman
```

```
Enter the email address of the person running the list: bhuvan at ubuntu.com
Initial mailman password:
To finish creating your mailing list, you must edit your /etc/aliases (or
equivalent) file by adding the following lines, and possibly running the
`newaliases' program:
mailman: "|/var/lib/mailman/mail/mailman post mailman"
mailman-admin: "|/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces: "|/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm: "|/var/lib/mailman/mail/mailman confirm mailman"
mailman-join: "|/var/lib/mailman/mail/mailman join mailman"
mailman-leave: "|/var/lib/mailman/mail/mailman leave mailman"
mailman-owner: "|/var/lib/mailman/mail/mailman owner mailman"
mailman-request: "|/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe: "|/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe: "|/var/lib/mailman/mail/mailman unsubscribe mailman"

Hit enter to notify mailman owner...

#
```

Мы настроили exim на распознавание всех сообщений от mailman. Таким образом, не обязательно создавать новые записи в файле `/etc/aliases`. Если вы внесли какие-либо

изменения в конфигурационные файлы, пожалуйста, удостоверьтесь, что вы перезапустили соответствующие службы до того, как перейдете к следующему разделу.

14.4.3. Администрирование

Поразумевается, что у вас установка по умолчанию. CGI-скрипты mailman все еще находятся в каталоге /usr/lib/cgi-bin/mailman/. Mailman предоставляет легких веб-интерфейс для администрирования. Для доступа к его страницам укажите следующую ссылку в вашем браузере:

http://hostname/cgi-bin/mailman/admin

Список по умолчанию, *mailman*, появится на экране. Если вы щелкните по имени списка рассылки, появится запрос для аутентификации с помощью пароля. После ввода правильного пароля, вы получите возможность изменять административные настройки для данного списка. Для создания нового списка вы можете воспользоваться утилитой командной строки (**/usr/sbin/newlist**). В качестве альтернативы, вы можете использовать для создания нового списка веб-интерфейс.

14.4.4. Пользователи

Mailman предоставляет пользователю веб-интерфейс. Для доступа к этой странице, перейдите в браузере на следующий url:

http://hostname/cgi-bin/mailman/listinfo

На этом экране появится созданный при установке список рассылки "*mailman*". Если щёлкнуть на на названии списка рассылки, появится форма регистрации. Для подписки на этот список можно ввести Ваш почтовый адрес, имя (не обязательно) и пароль. После этого Вам будет отправленно электронной почтой приглашение. Чтобы подписаться на список рассылки, следуйте инструкциям, содержащимся в этом приглашении.

14.4.5. Ссылки

GNU Mailman - руководство по установке [http://www.list.org/mailman-install/index.html]

HOWTO - Совместное использование Exim 4 и Mailman 2.1
[http://www.exim.org/howto/mailman21.html]

Глава 5. Работа в сети Windows

Компьютерные сети часто включают различные системы, и хотя управление сетью, целиком состоящей из рабочих станций и серверов Ubuntu, является простой задачей, некоторые сети должны быть постороены как из Ubuntu-систем, так и из систем Microsoft®Windows®, согласованно работающих вместе. Эта часть Руководства сервера Ubuntu рассматривает принципы и инструменты, используемые для настройки вашего сервера Ubuntu для совместного использования сетевых ресурсов вместе с компьютерами Windows.

1. Введение

Успешное сетевое взаимодействие вашей системы Ubuntu с Windows-клиентами включает в себя обеспечение и интеграцию со службами, общими для окружения Windows. Такие службы поддерживают совместное использование данных и информации о компьтерах и пользователях сети, и могут относиться к трём основным функциональным категориям:

- **Службы доступа к файлам и принтерам**. Использование протокола блока серверных сообщений (SMB) для обеспечения совместного использования файлов, папок, томов, а также общего доступа к принтерам через сеть.
- **Службы каталога**. Распределение важной информации о компьютерах и пользователях сети с использованием таких технологий, как облегченный протокол доступа к каталогам (LDAP) и Microsoft Active Directory®.
- **Аутентификация и доступ**. Установление подлинности компьютера или пользователя сети и определение информации, к которой компьютеру или пользователю разрешается иметь доступ, используя такие принципы и технологии, как права доступа к файлу, групповые политики и службу аутентификации Kerberos.

К счастью, ваша система Ubuntu может обеспечивать все эти возможности для клиентов Windows и распределять сетевые ресурсы между ними. Одной из основных частей програмного обеспечения, которое включает ваша система Ubuntu для сети Windows, является SAMBA - набор приложений и инструментов сервера SMB. Этот раздел Руководства по серверу Ubuntu кратко ознакомит с установкой и базовой конфигурацией набора серверных приложений и утилит из набора SAMBA. Дополнительная, подробная документация и информация о SAMBA выходит за рамки этого руководства и находится на *сайте SAMBA* [http://www.samba.org].

2. Установка SAMBA

В командной строке введите следующую команду для установки серверного приложения SAMBA:

```
sudo apt-get install samba
```

3. Настройка SAMBA

Вы можете настроить сервер SAMBA путем внесения изменений в файл `/etc/samba/smb.conf`, изменив значения по умолчанию и добавив новые. Дополнительная информация о каждом параметре доступна из комментариев в файле `/etc/samba/smb.conf` или из страницы руководства `/etc/samba/smb.conf`, которую можно увидеть, набрав следующую команду в терминальной строке:

```
man smb.conf
```

Прежде чем вносить изменения в конфигурационный файл, вам следует сделать копию исходного файла и защитить ее от записи. Таким образом, первоначальные установки могут использоваться как для справочного руководства, так и для повторного использования.

Сделайте резервную копию файла `/etc/samba/smb.conf`:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.original
```

Теперь откройте файл `/etc/samba/smb.conf` и вносите ваши изменения.

3.1. Сервер

В дополнение к пакету серверных приложений SAMBA для организации совместного доступа к файлам и принтерам, Ubuntu также включает другие мощные серверные приложения, предоставляющие дополнительную функциональность сетевому серверу для Windows-клиентов, аналогичную обеспечиваемой реальными Windows-серверами. Например, Ubuntu предоставляет централизованное управление сетевыми ресурсами, такими как компьютеры и пользователи через службы каталогов, и обеспечивает идентификации и авторизации компьютеров и пользователей через службы аутентификации.

Следующие параграфы рассматривают SAMBA и вспомогательные технологии, такие как сервер облегченного протокола службы каталогов (LDAP) и сервер аутентификации Kerberos более детально. Вы также получите представление о некоторых директивах доступных в конфигурационном файле SAMBA, которые облегчают интеграцию с Windows клиентами и серверами.

3.1.1. Active Directory

Active Directory - это запатентованная реализация службы каталогов от Microsoft, используемая для обеспечения средств распределения информации о сетевых ресурсах и пользователях. Кроме цетрализованного источника информации такого рода, Active Directory также действует как централизованная защищенная база данных для проверки

подлинности в сети. Active Directory сочетает возможности традиционно расположенные в различных, специализированных системах каталогов для упрощения интеграции, управления и обеспечения безопасности сетевых ресурсов. Пакет SAMBA может быть настроен на использование сервисов Active Directory контроллера домена Windows.

3.1.1.1. LDAP

Серверное приложение LDAP обеспечивает функциональность Службы Каталогов для компьютеров Windows на манер, очень схожий со службами Microsoft Active Directory. Такие службы включают управление атрибутами и взаимоотношениями между компьютерами, пользователями, и группами компьютеров или пользователей, которые работают в сети; и обеспечивают адекватные средства для описания, нахождения и управления этими ресурсами. Свободно доступная реализация LDAP, имеющаяся для вашей системы Ubuntu, называется *OpenLDAP*. Серверные демоны, отвечающие за обслуживание запросов к каталогу OpenLDAP и передачу данных каталога от одного LDAP сервера к другому в Ubuntu – это slapd и slurpd. OpenLDAP может использоваться в сочетании с SAMBA, для обеспечения доступа к файлам, печати и службам каталогов так же, как это делает контроллер домена Windows, если пакет SAMBA скомпилирован с поддержкой LDAP.

3.1.1.2. Kerberos

Система обеспечения безопасности аутентификации Kerberos - это стандартизированная служба для предоставления аутентификации компьютерам и пользователям посредством централизованного сервера, который предоставляет зашифрованные билеты установления полномочий, принимаемые в качестве подтверждения авторизации любыми другими компьютерами, использующими Kerberos. Преимущества аутентификации с помощью Kerberos включают обоюдную идентификацию, делегирование, возможность взаимодействия и упрощенное управление доверительными отношениями. Основными демонами сервера для обслуживания аутентификации Kerberos и администрирования базы данных Kerberos в Ubuntu являются krb5kdc и kadmin. SAMBA может использовать Kerberos, как механизм для аутентификации компьютеров и пользователей вместо контроллера домена Windows. Чтобы это сделать, система Ubuntu должна иметь установленную службу Kerberos, и файл `/etc/samba/smb.conf` должен быть модифицирован для выбора верной *области* и *режима безопасности*. Например, отредактируйте файл `/etc/samba/smb.conf`, добавив значения:

realm = ИМЯ_ДОМЕНА

security = ADS

к файлу и сохраните его.

Не забудьте заменить токен ИМЯ_ДОМЕНА в примере выше на фактическое имя вашего домена Windows.

Вам понадобится перезапустить демон SAMBA для того, чтобы изменения вступили в силу. Перезапустите демон SAMBA с помощью следующей команды введенной в терминальной строке:

```
sudo /etc/init.d/samba restart
```

3.1.2. Учетные записи компьютеров

Учетные записи компьютеров используются в Службах Каталога для уникальной идентификации компьютерных систем, находящихся в сети, и обрабатываются таким же образом, в плане безопасности, как и учетные записи пользователей. Учетные записи компьютеров могут иметь пароли так же, как и учетные записи пользователей, и проходят авторизацию для доступа к сетевым ресурсам аналогично учетным записям пользователей. Например, если пользователь, имеющий верную учетную запись именно этой сети пытается аутентифицироваться с сетевым ресурсом с компьютера, который не имеет верной учетной записи, то в зависиммости от применяемых к сети политик, пользователю, возможно, будет отказано в доступе к ресурсу, если компьютер, с которого он пытается это сделать, является посторонним.

Учетная запись компьютера может быть добавлена в файл паролей SAMBA, при условии, что имя добавляемого компьютера существует в качестве допустимой учетной записи пользователя в локальной базе паролей. Синтаксис для добавления учетной записи компьютера заключается в использовании команды smbpasswd в терминальной строке следующим образом:

```
sudo smbpasswd -a -m ИМЯ_КОМПЬЮТЕРА
```

Не забудьте заменить токен ИМЯ_КОПЬЮТЕРА в приведенном выше примере на фактическое имя того компьютера, для которого хотите создать учетную запись.

3.1.3. Права доступа к файлам

Права доступа к файлу определяют точные привилегии, которые имеет компьютер или пользователь по отношению к отдельной директории, файлу или группе файлов. Такие права могут определяться с помощью редактирования файла `/etc/samba/smb.conf` и установки точных разрешений, определяющих доступ к общему каталогу. Например, если вы определили общий ресурс SAMBA, называемый *sourcedocs*, и желаете дать права доступа *только чтение* группе пользователей, известной как *planning*, а так же хотите разрешить запись в общий ресурс группе, называемой *authors*, и пользователю под именем *richard*, тогда вам необходимо отредактировать файл `/etc/samba/smb.conf` и добавить следующие данные под записью *[sourcedocs]*:

read list = @planning

write list = @authors, richard

Сохраните файл `/etc/samba/smb.conf` для того чтобы изменения вступили в силу.

Другое возможное решение - определить *административные* права доступа для конкретного разделяемого ресурса. Пользователи, имеющие административные полномочия, могут производить чтение, запись, изменение любой информации, доступной на ресурсе, для которого этим пользователям были явно заданы административные права доступа. Например, если вы хотите определить пользователю *melissa* административные права доступа к ресурсу *sourcedocs*, вам необходимо изменить файл `/etc/samba/smb.conf`, добавив следующую строку в раздел *[sourcedocs]*:

admin users = melissa

Сохраните файл `/etc/samba/smb.conf` для того чтобы изменения вступили в силу.

3.2. Клиенты

Ubuntu включает клиентские приложения и средства для доступа к сетевым ресурсам, разделяемым по протоколу SMB. Например, утилита smbclient разрешает доступ к удаленной файловой системе, наподобие FTP клиента. Для доступа к общей папке, известной под именем *documents*, предоставляемой удаленным Windows компьютером под названием *bill*, используя, к примеру, smbclient, вы можете ввести в коммандной строке команду подобную следующей:

```
smbclient //bill/documents -U <username>
```

Затем вам будет предложено ввести пароль для пользователя, указанного после опции -U. После удачной аутентификации, будет предоставлена командная строка, где вы сможете вводить команды для обработки и передачи файлов, синтаксически схожие с командами, используемыми неграфическими FTP-клиентами. Для получения более подробной информации об утилите smbclient, ознакомьтесь с руководством для данной утилиты, воспользовавшись командой:

```
man smbclient
```

Используя команду mount, вы можете присоединить удаленный сетевой ресурс, доступный по протоколу SMB, локально. Например, для присоединения к вашей системе Ubuntu в каталог /mnt/pcode совместно используемой папки с названием *project-code*, находящейся на сервере Windows под именем *development*, используя имя пользователя *dlightman*, вам следует ввести такую команду:

```
mount -t smbfs -o username=dlightman //development/project-code /mnt/pcode
```

Затем вам будет предложено ввести пароль и, после успешной аутентификации, содержимое совместно используемого ресурса будет доступно локально через точку монтирования, указанную в качестве последнего параметра в команде mount. Для отключения разделяемого ресурса просто используйте команду umount, как вы это делали с другими присоединенными файловыми системами. Например:

```
umount /mnt/pcode
```

3.2.1. Учетные записи пользователей

Учетные записи пользователей определяют лиц с некоторым набором прав для использования определенных ресурсов компьютера и сетевых ресурсов. Обычно, в сетевой среде, учетная запись пользователя предоставляется каждому лицу имеющему доступ к компьютеру или сети, где политики и разрешения определяют затем точные права доступа, которыми обладает учетная запись. Для определения сетевых пользователей SAMBA вашей системы Ubuntu вы можете использовать команду smbpasswd. Например для того, чтобы добавить пользователя SAMBA с именем *jseinfeld* в вашу систему Ubuntu, вам необходимо ввести следующую команду:

```
smbpasswd -a jseinfeld
```

Затем приложение smbpasswd запросит у вас пароль для этого пользователя:

```
Новый пароль SMB:
```

Введите пароль, который вы хотите установить для пользователя, и приложение smbpasswd предложит поторить ввод пароля:

```
Введите пароль SMB еще раз:
```

Подтвердите пароль и приложение smbpasswd добавит запись для пользователя в файл паролей SAMBA.

3.2.2. Группы

Группы определяют набор компьютеров или пользователей, имеющих одинаковый уровень доступа к определенным сетевым ресурсам, и предоставляют средство для структурирования контроля доступа к ресурсам. Например, если группа *qa* определена и в нее входят пользователи *freda*, *danika* и *rob*, а в другую существующую группу *support* входят *danika*, *jeremy* и *vincent* тогда определенный сетевой ресурс, настроенный для разрешения доступа группе *qa*, будет доступен для пользователей freda, danika, и rob, но не для jeremy или vincent-a. Так как пользователь *danika* входит в обе группы, *qa* и *support*, она будет иметь доступ к ресурсам, настроенным для доступа обеих групп, в то же время все другие пользователи будут иметь доступ только к тем ресурсам, которые непосредственно доступны для группы, в которую они входят.

Для обозначения групп в файле конфигурации SAMBA, `/etc/samba/smb.conf`, используется следующий синтаксис: перед названием группы пишется символ "@". Например, если вы хотите определить группу с именем *sysadmin* в определенной секции файла `/etc/samba/smb.conf`, вам нужно ввести имя группы как **@sysadmin**.

3.2.3. Групповые политики

Групповая политика обозначает некоторые параметры конфигурации SAMBA, относящиеся к учетным записям, принадлежащим домену или рабочей группе, а так же другие глобальные параметры сервера SAMBA. Например, если сервер SAMBA принадлежит рабочей группе компьютеров Windows, называемой *LEVELONE*, можно отредактировать файл `/etc/samba/smb.conf`, изменив соответствующим образом следующий параметр:

workgroup = LEVELONE

Сохраните файл и перезапустите демон SAMBA для того, чтобы изменения вступили в силу.

К другим важным параметрам глобальной политики относится параметр *netbios name*, который определяет имя NETBIOS сервера, сообщаемое Вашей системой Ubuntu другим машиным сети Windows. Это имя будет распознано всеми Windows-клиентами, а так же другими компьютерами, способными к обозру сети по протоколу SMB. Кроме того, можно указать имя и местоположение файла журнала сервера SAMBA, используя параметр *log file* в файле `/etc/samba/smb.conf`.

Несколько дополнительных директив, контролирующих глобальную групповую политику, включают определения глобального характера для всех разделяемых ресурсов. Например, установка определенных параметров в секции *[global]* файла `/etc/samba/smb.conf` будет влиять на все разделяемые ресурсы, если переопределяющая директива не будет помещена в секцию конкретного разделяемого ресурса. Можно определить все общие катагоги как просматриваемые всеми клиентами в сети, поместив параметр *browseable*, который принимает логическое значение, в секцию *[global]* файла `/etc/samba/smb.conf`. Такии образом, если вы добавляете строку:

browseable = true

в секцию *[global]* файла `/etc/samba/smb.conf`, все совместно используемые через SAMBA ресурсы вашей системы Ubuntu смогут просматриваться всеми авторизованными клиентами, если только секция конкретного разделяемого каталога не содержит строку *browseable = false*, которая переопределит глобальный параметр.

Другим примером, работающим подобным образом, являются директивы *public* и *writeable*. Директива *public* принимает логическое значение и определяет является ли конкретный разделяемый ресурс видимым всем клиентам, авторизованным или

неавторизованным. Директива *writeable* также принимает логическое значение и определяет доступен ли конкретный разделяемый ресурс на запись для всех без исключения сетевых клиентов.

Приложение A. Creative Commons by Attribution-ShareAlike 2.0

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE.

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. **Definitions.**
   a. **"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.
   b. **"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.
   c. **"Licensor"** means the individual or entity that offers the Work under the terms of this License.
   d. **"Original Author"** means the individual or entity who created the Work.
   e. **"Work"** means the copyrightable work of authorship offered under the terms of this License.
   f. **"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received

express permission from the Licensor to exercise rights under this License despite a previous violation.

g. **"License Elements"** means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

2. **Fair Use Rights.** Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. **License Grant.** Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

   a. to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

   b. to create and reproduce Derivative Works;

   c. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

   d. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission Derivative Works.

   e. For the avoidance of doubt, where the work is a musical composition:

      i. **"Performance Royalties Under Blanket Licenses."** Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

      ii. **"Mechanical Rights and Statutory Royalties."** Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

   f. **"Webcasting Rights and Statutory Royalties."** For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

   The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4. **Restrictions.** The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested. If You create a Derivative Work, upon notice from any Licensor You must, to the extent practicable, remove from the Derivative Work any reference to such Licensor or the Original Author, as requested.

b. You may distribute, publicly display, publicly perform, or publicly digitally perform a Derivative Work only under the terms of this License, a later version of this License with the same License Elements as this License, or a Creative Commons iCommons license that contains the same License Elements as this License (e.g. Attribution-ShareAlike 2.0 Japan). You must include a copy of, or the Uniform Resource Identifier for, this License or other license specified in the previous sentence with every copy or phonorecord of each Derivative Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Derivative Works that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder, and You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Derivative Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Derivative Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Derivative Work itself to be made subject to the terms of this License.

c. If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Derivative Works or Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied; to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and in the case of a Derivative Work, a credit identifying the use of the Work in the Derivative Work (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). Such credit may be implemented in any reasonable manner; provided, however, that in the case

of a Derivative Work or Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. **Representations, Warranties and Disclaimer**

   UNLESS OTHERWISE AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. **Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Termination**

   a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Derivative Works or Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

   b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. **Miscellaneous**

   a. Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

   b. Each time You distribute or publicly digitally perform a Derivative Work, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

   c. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without

further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

d. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

e. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, neither party will use the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time.

Creative Commons may be contacted at *http://creativecommons.org/*.

Приложение B. GNU Free Documentation License

Version 1.2, November 2002

Free Software Foundation, Inc.
51 Franklin St, Fifth Floor,
Boston,
MA
02110-1301
USA

Version 1.2, November 2002

PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent

copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

GNU FDL Modification Conditions

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the *Addendum [1Ø3* below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network

location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in *section 4 [1Ø0* above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in

parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> ## Sample Invariant Sections list
>
> Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> ## Sample Invariant Sections list
>
> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.