V14.04 (№8)
ISSN: 2223-6988

Стеганография - скрывайте ваши файлы внутри изображений в Linux

User And LINUX

Больше чем user

Загрузка виртуальной машины с флешки в ESX

Собираем .deb пакеты

Защита данных на телефонах и планшетах на базе Android

Настройка локального веб-сервера LAMP (Linux-Apache-MySQL-PHP)

Критическая уязвимость в OpenSSL 1.0.1 и 1.0.2-beta

Обновлен Forensic-дистрибутив Ubuntu CyberPack (IRF) 1.1 предназначенный для создания цифрового образа оперативной памяти компьютера
http://ualinux.com/ubuntu-cyberpack

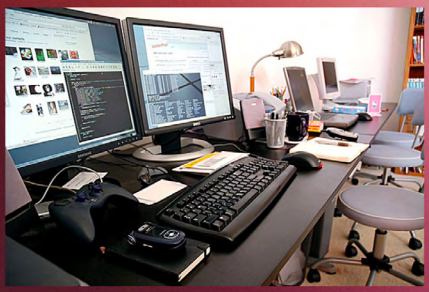
UA Linux
http://ualinux.com

ubuntu BusinessPack

Операционная система, которая идеально подходит для использования на персональных компьютерах и ноутбуках. Она ориентирована на простоту использования и удобство работы.

Включена необходимая подборка программного обеспечения, которая позволяет создать удобное рабочее окружение в корпоративной среде предприятия или на домашнем компьютере.

Ubuntu Business Pack это:



- **простая установка операционной системы не требующая особых знаний;**
- **уверенность в том, что на компьютере установлено только лицензионное программное обеспечение;**
- **это низкая цена по сравнению с аналогами;**
- **создание рабочего места без дополнительных финансовых затрат. Это существенно экономит бюджет организаций;**
- **идеальное решение для перехода на Linux с Windows, если вы все еще используете windows-приложения и игры;**
- **полная поддержка в системе русского, украинского и английского языков;**
- **отсутствие необходимости затрат на антивирусную защиту.**

Программное обеспечение имеет понятный графический интерфейс и полностью совместимо с популярными форматами документов, поэтому переход не вызывает никаких проблем с переносом данных и переквалификацией сотрудников.

поддержка широкого спектра современного оборудования;
дополнительные драйвера для видео-карт, wi-fi адаптеров и принтеров;
возможность использовать Windows-драйвера для WiFi-адаптеров USB;
управление веб-камерами.

безопасность и надежная защита от вирусов;
проверка файлов на вирусы в режиме реального времени (актуально в случае запуска windows-приложений);
защита от вирусных атак системы и электронной почты;
проверка на спам.

поддержка мультимедия (аудио - видео) различных форматов (avi, divX, mp4, mkv, amr, aac, Adobe Flash и многие другие)
просмотр защищенных, зашифрованных лицензионных, двухслойных DVD и Bluray дисков

полный набор офисных компонент (тексты, таблицы, презентации) совместимых с форматами MS Office
включена поддержка импорта файлов MS Visio
поддержка различных типов архивов (RAR, ACE, ARJ и других);

поддержка windows-приложений (гарантированный запуск более 130 приложений и более 600 игр)

OpenJDK

полноценная поддержка Java-приложений;
гарантированная работа онлайн банк-клиентов, таких как Приват24
гарантированная работа онлайн-бухгалтерии, таких как iFin.

Дорогие читатели!

Мы представляем вам новый выпуск журнала «Больше чем USER». Мы рады, что вы остаетесь с нами, продолжаете активно читать журнал.

Мы постоянно стараемся его усовершенствовать, чтобы вы не теряли интерес к нашим материалам.

В этом номере вы найдете инструкцию по загрузке виртуальной машины с USB-флешки в ESXi, научитесь делать резервные копии базы данных Mysql Server, создавать SOHO-сервер на базе Zentyal. В рубрике Workstation вы узнаете, какое будущее ждет Ubuntu One и научитесь самостоятельно собирать .deb пакеты.

Также в этом номере вы найдете подробное описание установки и настройки локального веб-сервера LAMP, узнаете о языке программирования Hack, который представила компания Facebook, познакомитесь с программой Rootkit Hunter, помогающей выявить наиболее коварное вредоносное ПО – руткиты.

Вы узнаете, как защитить свой данные на телефонах и планшетах на базе Android, а также как шифровать файлы в Linux с помощью GPG, Ccrypt, Bcrypt и 7-Zip.

Любителям стеганографии понравится статья, в которой подробно рассказывается, как скрыть ваши файлы внутри изображений.

Оставайтесь с нами, читайте наш журнал и будьте всегда в курсе событий в мире IT. С нами вы – больше, чем простые пользователи. Вы – Больше чем USER

Команда «Больше чем USER»

НАД ВЫПУСКОМ РАБОТАЛИ:

Звенигородская Анастасия
Попов Владимир
Шарай Игорь
Россошанский Андрей
Якимчук Сергей
Кирильчук Виктор
Безруков Марк

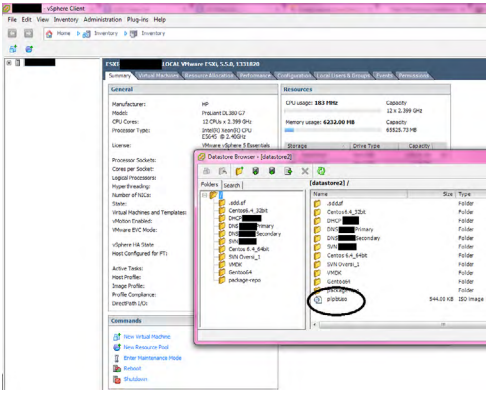
Содержание

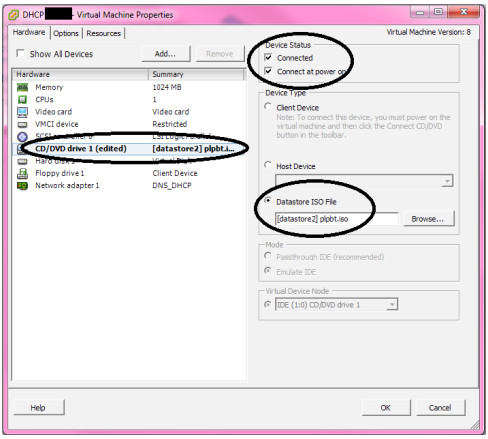
Загрузка виртуальной машины с флешки, USB в ESX

Проблема ESXi в том, что BIOS не позволяет загрузить систему с USB, хоть и позволяет добавлять USB-контроллер и USB-устройства. Это очень и очень неприятно в некоторых случаях, когда целевая система расположена у вас на USB и других вариантов просто нет. На просторах Интернета есть различные решения и одно из них - проект Plop. Всего в три клика удается загрузить только что созданную виртуальную машину с USB.

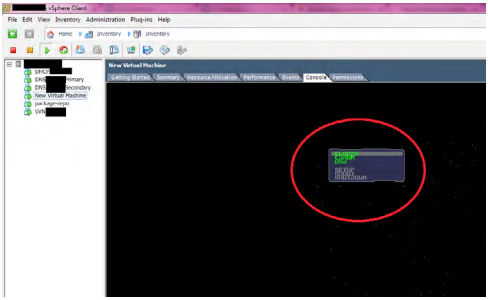
Загрузка VM с USB в ESXi

Загрузите Plop Boot Manager по ссылке http://www.plop.at/en/bootmanager/download.html это должен быть архив вида plpbt-5.0.15-test.zip. Далее распакуйте архив, откройте ваш ESXi хост и загрузите в Datastore образ ISO plpbt-x.x.x.zip





Теперь необходимо загрузить VM с это ISO образа.



В результате вы увидите экран приветствия, где можно будет выбрать три опции: Floppy, CDrom, USB Далее выполняете обычную загрузку с вашей флешки. Все должно работать как часы.

linuxspace.org

Создаем SOHO-сервер на базе Zentyal

Часть 2

В первой части этой статьи мы ознакомились с установкой Zentyal, настройкой сетевых опций, а также немного привели все это в порядок. В этой статье мы рассмотрим опции, которые будут полезны в первую очередь для небольшого офиса

Подключение второго HDD

Как уже говорилось в первой части, на еще одном жестком диске (например, съемном) мы будем хранить общие файлы, а заодно сливать туда резервные копии системы. Диск лучше заранее отформатировать в нужную ФС. Для примера пусть это будет NTFS – в случае чего диск можно подсоединить к Windows-машине и скопировать нужные данные. После подключения HDD к серверу (не важно, по SATA/IDE/USB или как-то еще) нам надо узнать его идентификатор. Запускаем User Console с рабочего стола и выполняем команду:

```
sudo blkid -c /dev/null
```

Команда выводит список блочных устройств. В этом списке надо найти UUID нашего жесткого диска. Сориентироваться можно по метке тома (Label). Затем создаем точку монтирования, откуда, собственно, и будет доступ к нашему диску. Условимся, что она будет совпадать с меткой тома (но вы можете задать имя на ваш выбор):

```
sudo mkdir /media/имя_тома
```

Теперь надо прописать всего лишь одну строчку в fstab…

```
sudo nano /etc/fstab
```

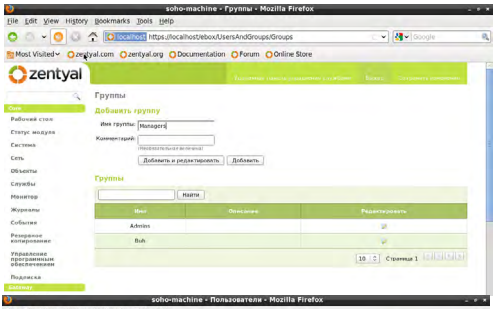
… вида:

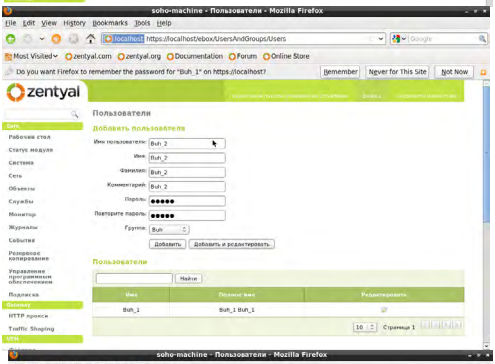
```
UUID=идентификатор_диска /media/
имя_тома ntfs-3g defaults 0 0
```

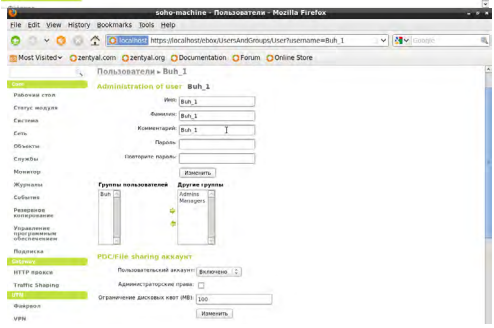
Вместо пробелов в этой строке используем табуляцию (Tab) и в конце жмем Enter. Затем сохраняем файл (F2, Y, Enter) и выходим (Ctrl+X). Все, теперь при каждой загрузке жесткий диск будет автоматически смонтирован.

Настройка домена и файлообмена

Zentyal способен также выступать в роли LDAP-сервера, в том числе в связке с Windows AD. В первую очередь надо создать группы пользователей, например, в соответствии с отделами или территориальным размещением. Для каждой группы можно сразу же задать имя общей папки, куда будут иметь доступ все пользователи данной группы. Затем добавляем новых пользователей и раскидываем их по группам, попутно задавая максимальный объем данных на диске, который может забить своими файлами каждый пользователь. Обязательно надо создать как минимум один аккаунт с правами администратора.







soho-machine - Группы - Mozilla Firefox

https://localhost/ebox/UsersAndGroups/Groups

Группы

Добавить группу

Имя группы: Managers

Комментарий: (Необязательная величина)

Группы

Имя	Описание	Редактировать
Admins		
Buh		

soho-machine - Пользователи - Mozilla Firefox

https://localhost/ebox/UsersAndGroups/Users

Do you want Firefox to remember the password for "Buh_1" on https://localhost?

Пользователи

Добавить пользователя

Имя пользователя: Buh_2

Имя: Buh_2

Фамилия: Buh_2

Комментарий: Buh_2

Пароль: ●●●●●

Повторите пароль: ●●●●●

Группа: Buh

Пользователи

Имя	Полное имя	Редактировать
Buh_1	Buh_1 Buh_1	

soho-machine - Пользователи - Mozilla Firefox

https://localhost/ebox/UsersAndGroups/User?username=Buh_1

Пользователи ▸ Buh_1

Administration of user Buh_1

Имя: Buh_1

Фамилия: Buh_1

Комментарий: Buh_1

Пароль:

Повторите пароль:

Группы пользователей: Buh

Другие группы: Admins, Managers

PDC/File sharing аккаунт

Пользовательский аккаунт: Включено

Административорские права: ☐

Ограничение дисковых квот (MB): 100

soho-machine - Edit group - Mozilla Firefox

https://localhost/ebox/UsersAndGroups/Group?group=Buh

Группы ▸ Buh (показать помощь)

Administration of group Buh

Комментарий:

Пользователи в группе: Buh_1, Buh_2

Пользователи не в группе: suser_1

Каталог совместного доступа для этой группы

Имя каталога: buh_share

Удалить группу

Это действие удалит группу и все связанные с ней данные: общие файлы, и т.д.

Переходим в раздел «Шаринг файлов» и задаем основные настройки SAMBA. Включаем наш маленький домен, указываем его имя и остальные настройки. Если вы решите включить перемещаемые профили пользователей, то дисковые квоты, возможно, лучше будет отключить. На вкладке PDC меняем параметры, касающиеся пользовательских паролей, с. Затем добавляем общие папки (ресурсы). В нашем примере все данные будут храниться на втором жестком диске. У каждого ресурса необходимо прописать права доступа для групп и пользователей. Опционально можно включить корзину для сетевых ресурсов, тогда удаленные файлы будут помещаться в нее, а не удаляться навсегда. Каталоги, которым не требуется такая опция, добавляются в исключения. Наконец, последняя опция — антивирусное сканирование общих папок. Здесь также можно исключить отдельные каталоги. Учтите, что использование антивируса не гарантирует отсутствия вирусов. Впрочем, с наиболее распространенными зловредами он справляется.

soho-machine - Шаринг файлов - Mozilla Firefox

https://localhost/ebox/Samba/Composite/General

Шаринг файлов (показать помощь)

Общие настройки

Включить PDC: ☑

Имя домена: ZENTYAL-DOMAIN

Netbios имя: soho-machine

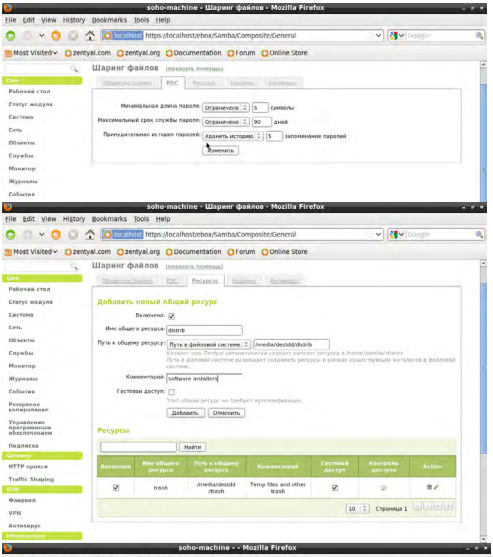
Описание: Zentyal File Server

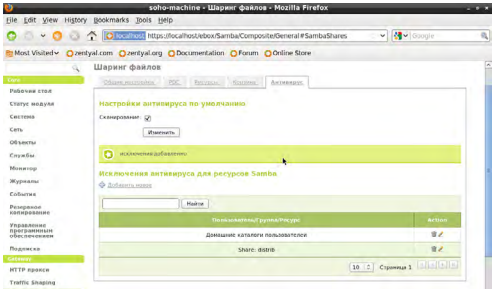
Квота: Отключено

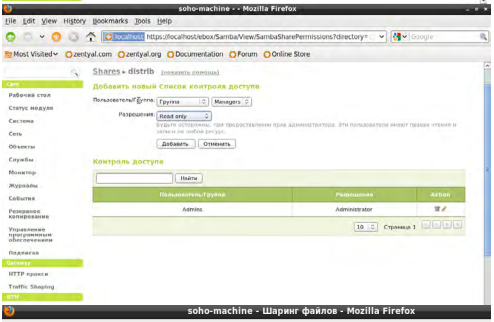
Включить перемещаемые профили: ☐

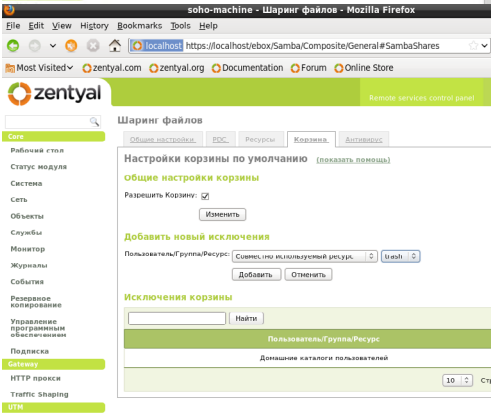
Буква диска: Z:

Группа самбы: All users





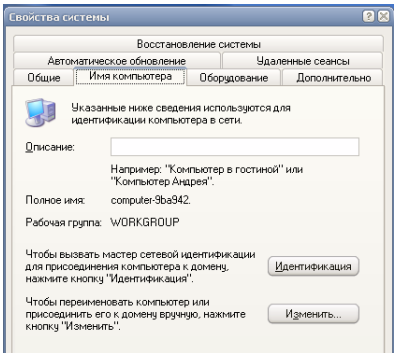


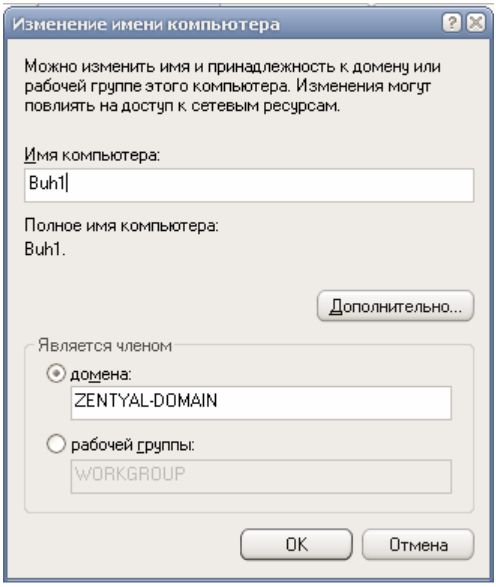


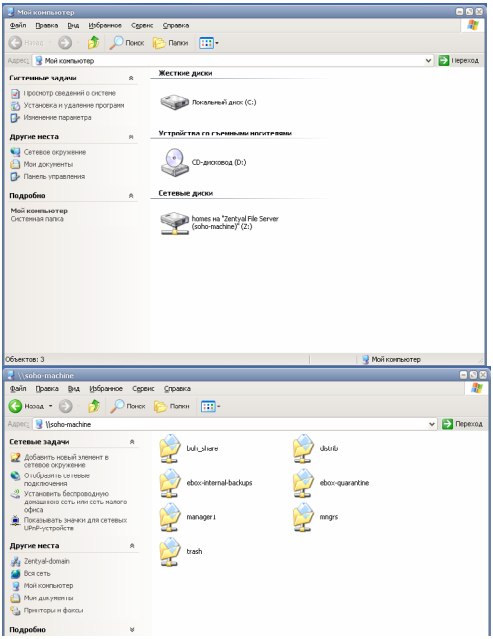
Не забывайте создавать на жестком диске папки, которые привязаны к сетевым ресурсам.

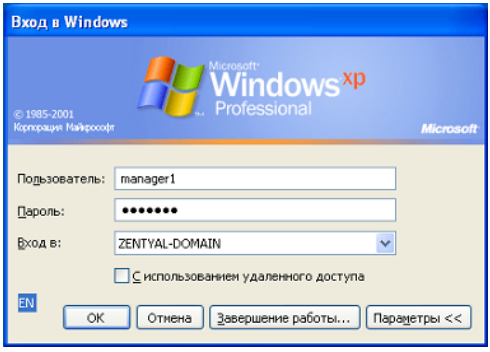
```
mkdir /media/метка_тома/имя_папки
```

Добавим в наш домен машину под управлением Windows XP Professinal. Для этого кликаем правой кнопкой по значку «Мой компьютер», выбираем «Свойства» –>«Имя компьютера» –> «Изменить» –>«Является членом домена» и в поле вводим имя нашего домена, а затем нажимаем ОК. В приглашении вводим логин и пароль аккаунта, который имеет права администратора в домене. Остается только перезагрузиться, а при входе в систему выбрать наш домен и указать логин-пароль пользователя – не локального, а какого-нибудь из тех, что мы завели в Zentyal.





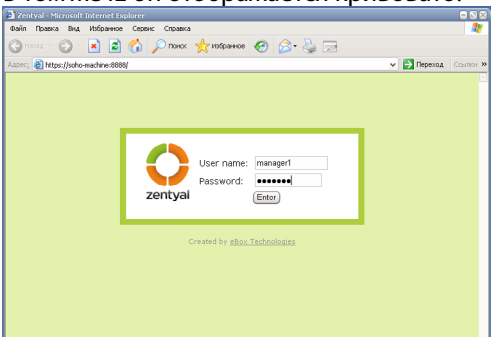


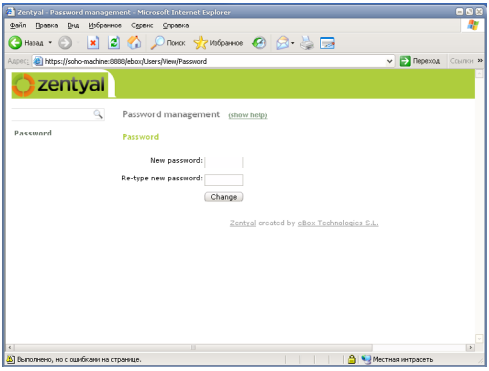


При первом входе придется немного подождать, пока будет создан пользовательский профиль на локальной машине. Все, теперь можно пользоваться ресурсами сети. Личная папка пользователя уже подключена как сетевой диск, а остальные ресурсы на сервере доступны по адресу \\netbios_имя_сервера.

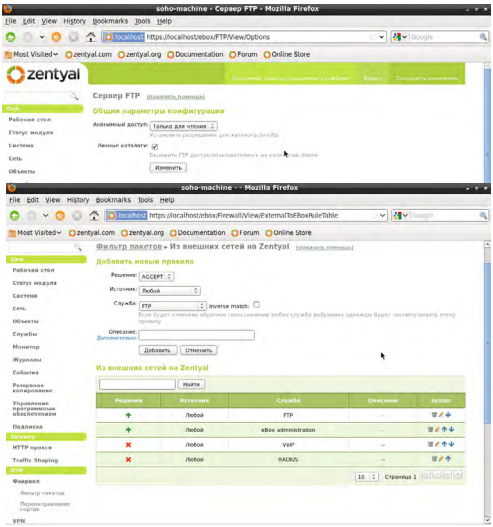
Для входа в так называемый «Уголок пользователя» надо открыть в веб-браузере страничку https://имя_сервера:8888/

В нем можно поменять текущий пароль, но не более того. Кстати, для работы с веб-интерфейсом Zentyal лучше всего использовать Mozilla Firefox или Google Chrome. В том же IE он отображается кривовато.





FTP-сервер мы будем использовать для доступа к файлам на сервере из внешней сети. Устанавливаем компонент FTP, включаем модуль и в настройках сервера разрешаем анонимный доступ к чтению файлов. Можно также включить доступ к личным каталогам пользователей. В этом случае авторизоваться при входе по FTP надо с логином-паролем пользователя домена. Также придется открыть в файерволе доступ к серверу из внешних сетей.



Корневая папка сервера находится в директории /srv/ftp – именно туда надо закидывать файлы и папки, которые вы хотите расшарить. Увы, из-за использования vsftpd, в корне нельзя создавать ссылки на другие папки, находящиеся, к примеру, на втором жестком диске. Однако это ограничение можно обойти. Создадим папки pub в корне FTP и на втором HDD…

```
sudo mkdir /srv/ftp/pub
mkdir /media/метка_тома/pub
```

… а затем просто подмонтируем одну к другой.

```
sudo mount --bind /media/метка_
тома/pub /srv/ftp/pub
```

Чтобы монтирование происходило автоматически, можно добавить последнюю команду в /etc/rc.local или же дописать следующую строчку в /etc/fstab:

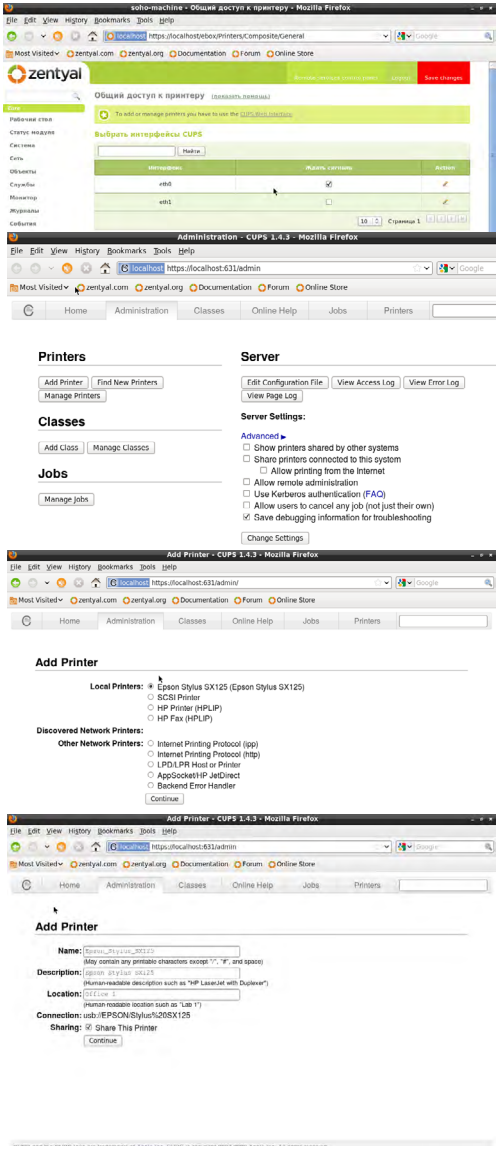
```
/media/метка_тома/pub /srv/ftp/
pub bind defaults,bind 0 0
```

Те, кого не устраивает vsftpd, могут настроить связку proftd+ldap.

Настройка сетевого принтера

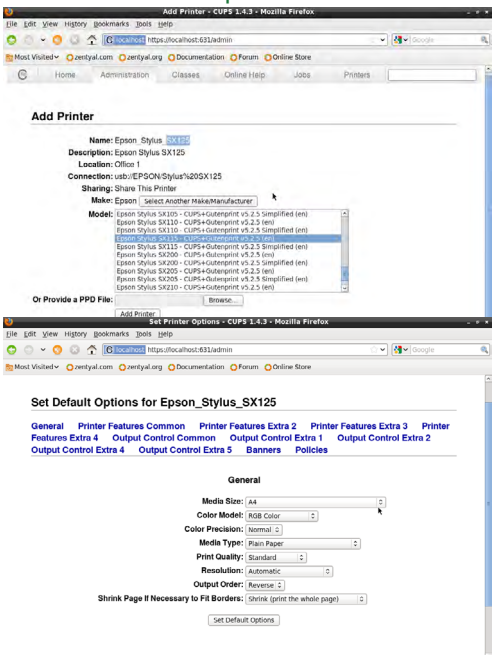
В разделе «Общий доступ к принтеру» надо отметить галочкой сетевой интерфейс, который обслуживает локальную сеть. Там же есть ссылка на веб-интерфейс CUPS, по которой надо перейти. Логин и пароль используем те же, что и для администрирования Zentyal. Нажимаем кнопку Add Printer и выбираем принтер, который подключен к серверу (он должен автоматически определиться), или же вручную указываем нужный тип принтера. Жмем

Continue. В поле Location указываем место, где физически расположен принтер, и ставим галочку Share this printer. Снова нажимаем Continue.

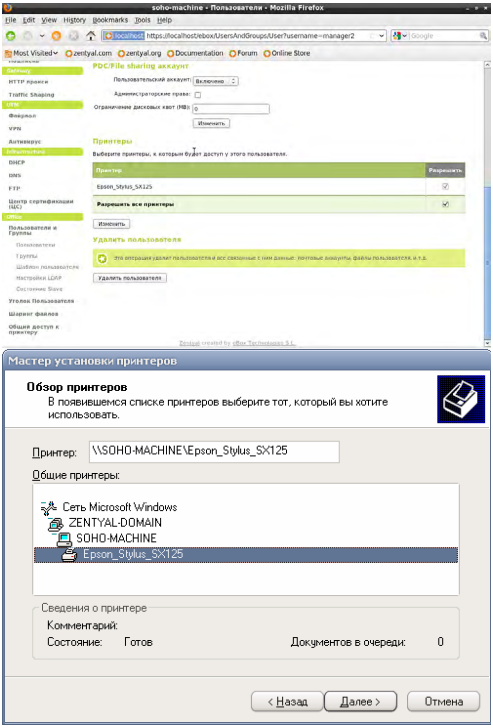


В списке выбираем драйвер нашего принтера, нажимаем Add printer, и в самом конце нам предложат изменить некоторые параметры печати по умолчанию. Учтите, что далеко не для всех устройств есть готовые драйвера под Linux, однако многие из них подходят сразу для нескольких моделей. Если вы все равно не нашли подходящего драйвера или PPD-файла под ваш принтер, то попробуйте выполнить две команды в консоли, которые приведены ниже, и заново добавить принтер. Если и это не помогло, то придется ждать появления нужного драйвера. Обычно такая ситуация возникает с самыми свежими моделями принтеров.

```
sudo apt-get install cups-driver-gutenprint
sudo service cups restart
```

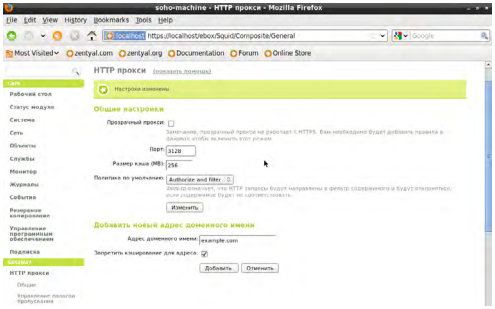


Осталось только разрешить использование принтеров группам и/или отдельным пользователям. Для подключения сетевого принтера на клиентских машинах достаточно зайти на них с аккаунтом администратора домена и добавить с помощью стандартного мастера принтер, который подключен к нашему серверу. После этого станет доступной печать по сети и из-под обычного пользователя.

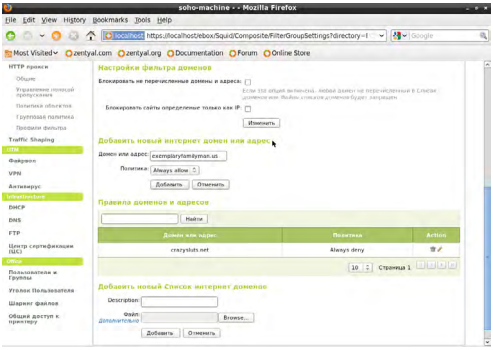


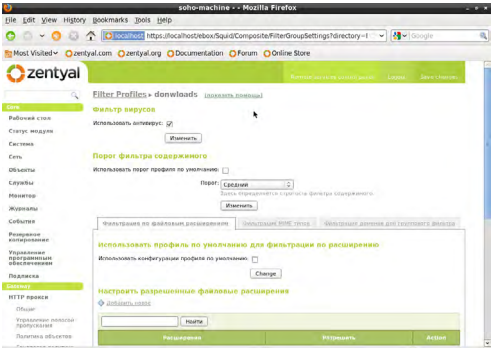
Настройка прокси

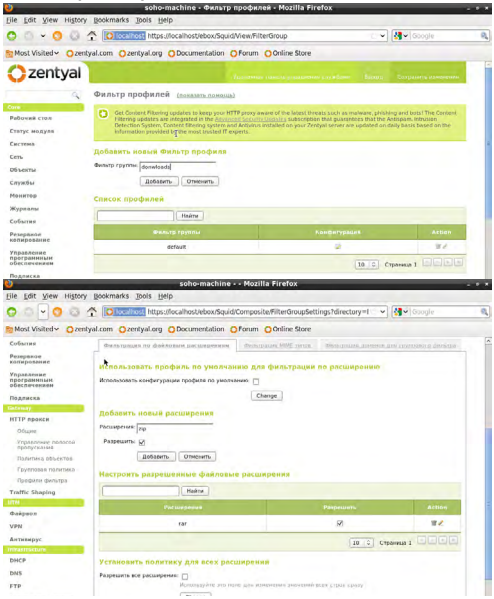
С помощью прокси мы сможем ограничивать пользователей по объему скачиваемых файлов, фильтровать контент, немного сэкономить трафик и ускорить загрузку страниц. Прозрачный прокси в нашем случае лучше не использовать. Во-первых, для HTTPS он не работает. Во-вторых, мы не сможем нормально использовать групповые политики. Размер кеша зависит от числа пользователей и их активности. Здесь придется немного поэкспериментировать. Если размер кеша окажется слишком маленьким, то данные будут чаще загружаться из Сети, а не с локального сервера. Если же он окажется слишком большим, то это тоже может замедлить загрузку. Политика по умолчанию определяет действие прокси-сервера в случае запроса к нему: обработать его, отфильтровать или проигнорировать и требовать ли при этом авторизацию с помощью логина и пароля. Мы рассмотрим вариант с авторизацией пользователей и фильтрацией контента. В список сайтов-исключений, которые не будут кешироваться, модно добавить адреса ресурсов с, например, динамично обновляющимся контентом. Естественно, в настройках браузера и прочих программ, требующих доступа в Интернет, надо указать настройки прокси-сервера. Либо, в случае Windows, прописать параметры прокси в IE для того, чтобы весь трафик шел через него.



Фильтрация контента основывается на так называемых профилях. По умолчанию уже есть один профиль default, в который внесены всевозможные правила. Можно создать собственный профиль на базе того, который выставлен по умолчанию или собственноручно добавить в нужные места свои правила. Первый вариант фильтрации – по расширению файла. Вы добавляете нужные расширения и разрешаете или запрещаете загрузку соответствующих файлов. Аналогичным образом добавляются правила на базе MIME-типов. В фильтр по имени домена можно составить список адресов, которые будут разрешены/запрещены для посещения, или загрузить уже готовые списки в текстовом формате. Наконец, для каждого профиля можно включить антивирусное сканирование на лету и выставить уровень строгости фильтрации.

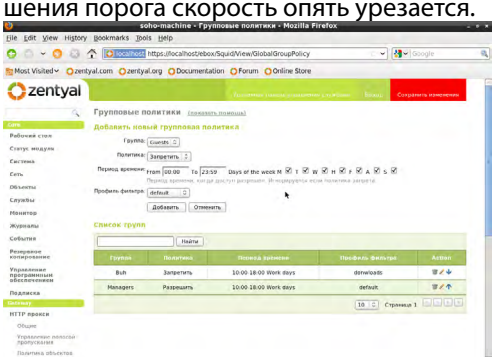


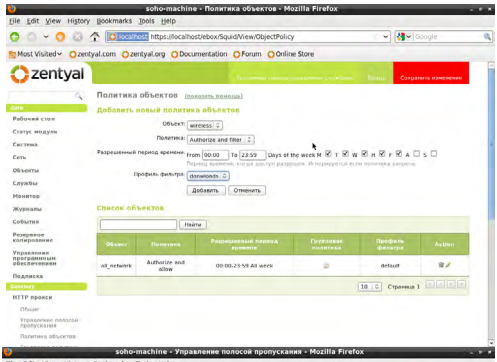


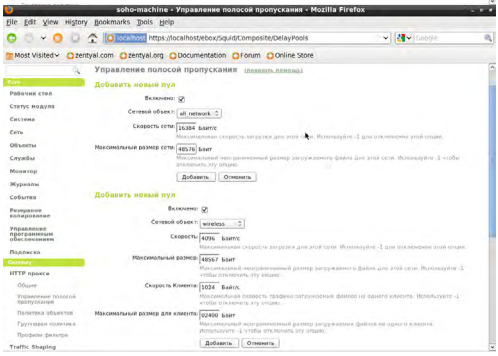


В дальнейшем созданные фильтры используются в групповых политиках и политиках объектов. И с теми, и с другими разобраться очень просто – указываем время, выбираем политику и, если надо, профиль фильтра. Обратите внимание, что для каждого объекта или группы можно задать только одно правило. Наконец, последняя возможность HTTP-прокси в Zentyal – ограничение скорости канала для сетевых объектов. Есть два пула ограничений – первого и второго класса, причем первый имеет более высокий приоритет. В первом пуле задается лимит по объему скачиваемого файла, после

превышения которого скорость будет урезана до указанной. Второй пул похож на первый, но в нем также указываются лимиты на скорость и объем для каждого клиента. При этом общий объем скачанных файлов суммируется и после превышения порога скорость опять урезается.

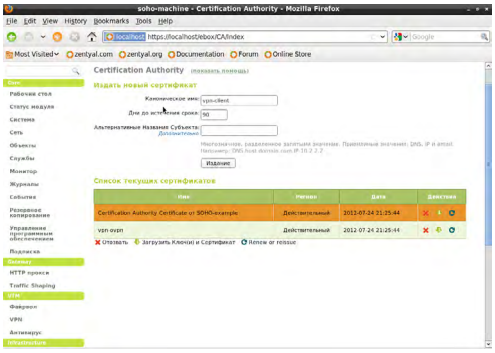


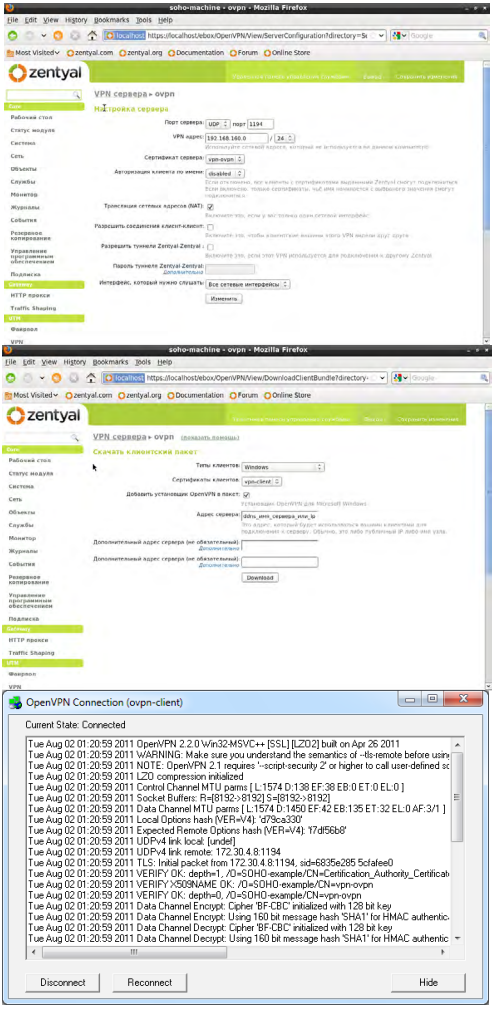




Настройка OpenVPN

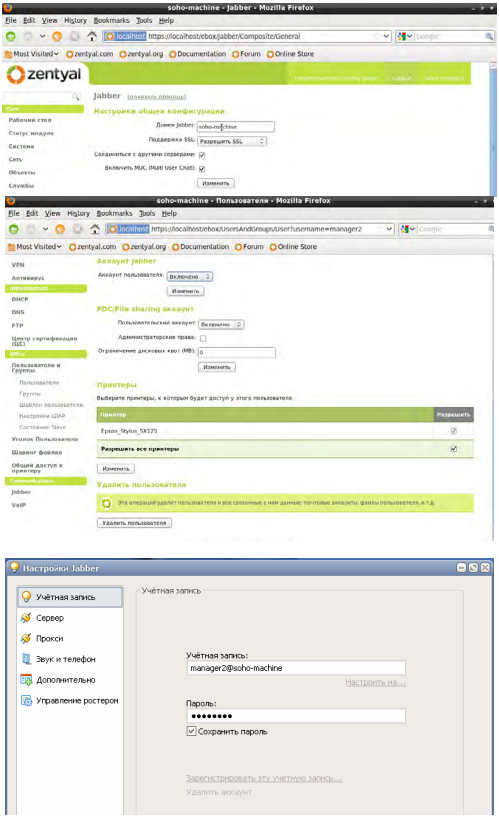
С помощью VPN-соединения мы сможем подключаться к серверу Zentyal извне и работать с ресурсами нашей локальной сети. Для начала нам надо сгенерировать минимум два сертификата – один для сервера, второй для клиента. Затем добавляем VPN-сервер в разделе VPN –> «Сервера». На скриншоте ниже приведена типичная конфигурация сервера. Следите за тем, чтобы адресация в VPN-сети не совпадала с адресацией локальной сети или других интерфейсов. После этого переходим к загрузке клиентского пакета под нужную платформу, где надо указать внешний адрес сервера. В скачанном архиве находятся ключи и файл настроек, которые, в случае Windows-клиента, надо скопировать в каталог C:\Program Files\OpenVPN\config. Для подключения запускаем OpenVPN GUI, кликаем правой кнопкой по появившемуся в трее значку, выбираем наше соединение и кликаем по Connect.





Настройка Jabber

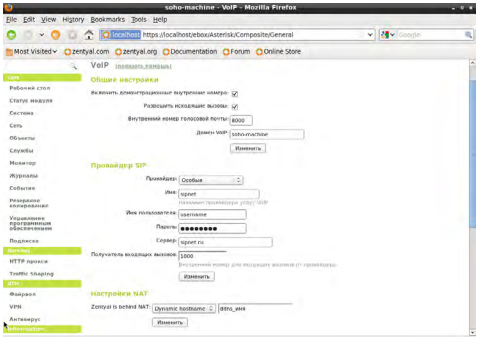
Jabber (XMPP) – это одна из разновидностей протоколов для обмена мгновенными сообщениями. Его можно использовать, например, для быстрого общения между сотрудниками в офисе. Настраивается Jabber-сервер элементарно. Выставляем настройки в соответствии с приведенными на скриншоте ниже и включаем Jabber-аккаунт в настройках пользователей. На компьютеры устанавливаем Jabber-клиенты и настраиваем их. Например, в популярной программе QIP Infium это делается так. Идем в «Настройки» –>«Учетные записи» –> «Добавить учетную запись» –> «XMPP (Jabber)». Используем логин вида имя_пользователя@имя_домена, а в качестве пароля тот, что используется для входа в домен. В ростер (контакт-лист) добавляем логины коллег в том же формате, что и наш логин.

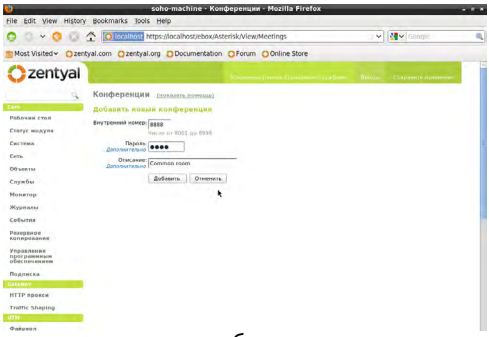


Настройка VoIP

Для использования функции VoIP необходимо иметь аккаунт у какого-нибудь SIP-провайдера. В случае офиса желательно еще и с нормальным городским номером. Недавно мы рассматривали возможность сэкономить на телефонных разговорах, так что можно воспользоваться уже настроенным аккаунтом на pbxes.org. Вообще рекомендуется хотя бы бегло пролистать указанную статью – в ней упрощенно описаны некоторые базовые понятия IP-телефонии. Итак, настраиваем подключение к SIP-провайдеру. Если ваш сервера находится за NAT, то надо указать либо внешний статический IP-адрес (если таковой выдан интернет-провайдером), либо хотя бы DDNS-имя. В противном случае у вас не будут работать входящие звонки. Демонстрационные номера – это 400, 500 и 600. Их можно использовать для проверки работоспособности клиентов. Внизу страницы есть еще одна опция – локальные сети. Сюда можно добавить IP-адреса или подсети, с которых разрешено подключаться к VoIP-серверу. Например, подсеть для OpenVPN-клиентов. Текущую внутреннюю локальную сеть добавлять не надо. Если вы включили поддержку конференций на этапе установки модуля VoIP, то в соответствующем разделе вы можете их добавить и задать пароль (в цифровом виде, конечно). Конференции – это своего рода многопользовательский голосовой чат.

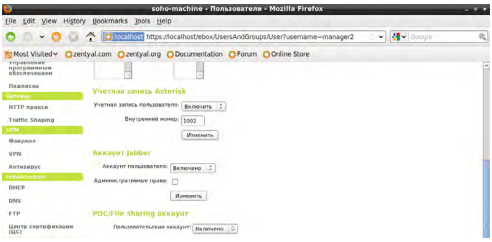
Расширения (экстеншены, или внутренние номера, если хотите) присваиваются пользователям и группам. Для подключения к серверу в SIP-клиенте в качестве логина указывается либо доменное им пользователя, либо номер его расширения, а пароль совпадает с паролем для входа в домен. Если позвонить на расширение, которое присвоено группе пользователей, то у всех них будет отображаться входящий вызов, пока кто-нибудь не снимет трубку. В общих настройках VoIP можно указать расширение, на которое по умолчанию будут переадресовываться все входящие звонки, например экстеншен секретаря или группы сотрудников поддержки. Если внутренний номер оказывается занятым, то звонящему предлагается оставить голосовое сообщение. Прослушать его можно, набрав номер голосовой почты и введя в качестве логина и пароля номер расширения. Пароль для голосо-



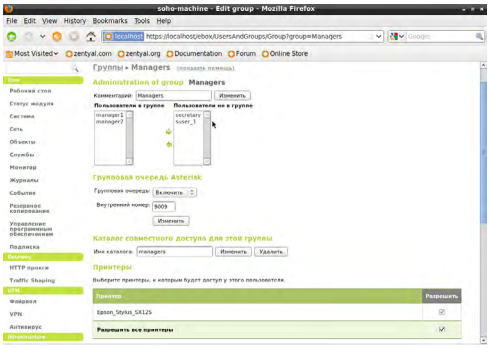


вой почты можно поменять в уголке пользователя (см. первую часть статьи). С помощью голосового меню в почте можно, в том числе, настроить ее параметры. Для перевода звонка на другой экстеншен достаточно набрать # и внутренний номер, куда звонок будет перекинут. Для удержания звонка надо набрать #700, а потом с того же телефона или любого другого еще раз – #700. Для исходящих звонков перед номером надо добавлять 0. Впрочем, с внешними вызовами Zentyal работает не очень корректно, так что при большом желании есть смысл перенастроить Asterisk с использованием FreePBX, например. Да и вообще, раз уж Zentyal построен на свободных компонентах, то никто не мешает вмешиваться в их работу, пусть и с потерей определенного уровня удобства в конфигурировании всего этого серверного хозяйства.

```
sudo apt-get install cups-driver-gutenprint
```




```
sudo service cups restart
```



На этом мы завершаем ту часть материала, которая посвящена возможностям Zentyal, наиболее подходящим для офисного использования. Остались нерассмотренными несколько модулей, которые описывать особого смысла нет. Почту и корпоративный сайт лучше держать у какого-нибудь хостинг-провайдера, IDS и Groupware в маленькой компании не очень-то и нужны, а про настройку RADIUS рассказывать совершенно нечего. В дальнейшем мы рассмотрим некоторые другие возможности сервера, которые могут вам пригодиться и которые непосредственно к Zentyal уже мало относятся.

3dnews.ru

Резервное копирование базы данных Mysql Server. Как создать дамп Mysql в Linux/FreeBSD

Как создать дамп базы данных mysql в Linux/FreeBSD?

```
# mysqldump -u dbuser -ppassword
-B database_name > /home/bakup/
database_makup.sql
```

Как создать дамп базы данных, содержащий только структуру базы?

```
# mysqldump -u dbuser -ppassword
--no-data -B database_name > /
home/bakup/database_makup.sql
```

Как создать дамп определенных таблиц базы данных?

```
# mysqldump -u dbuser -ppassword
-B database_name --tables table1
table2 > /home/bakup/database_
makup.sql
```

Как создать дамп нескольких баз данных mysql?

```
# mysqldump -u dbuser -ppassword
-B database_name1 database_name1
> /home/bakup/database_makup.sql
```

Как создать дамп всех баз данных mysql-server?

```
# mysqldump -u dbuser -ppassword
-A > /home/bakup/database_makup.
sql
```

linux-freebsd.ru

Создание домашнего сетевого хранилища (NAS) на базе Openfiler

В статье представлено пошаговое руководство по настройке домашнего сетевого хранилища данных (NAS) на базе GNU/Linux-дистрибутива Openfiler. Каждый шаг проиллюстрирован скриншотами. Доступ к ресурсам обеспечивается без пароля с любого компьютера из сети.

Учитывая тот факт, что во многих семьях количество компьютеров приближается к количеству членов семьи, возникает необходимость обращаться к одним и тем же данным (фильмы, музыка, фото, документы) с разных компьютеров. Для такой цели нужно завести отдельный постоянно работающий компьютер, который у нас будет выполнять роль хранилища данных – NAS-сервера (Network Attached Storage – сетевая система хранения данных, сетевое хранилище).

Первым делом нужно выбрать железо. Для домашнего использования мощный компьютер не нужен – подойдет любой ПК с поддержкой сети. Второй вопрос – выбор программного обеспечения. Из бесплатных есть два дистрибутива:

1.Openfiler (на основе rPath Linux);

2.FreeNAS (на основе FreeBSD).

Я остановил свое внимание на Openfiler, потому как посчитал его более «дружелюбным», чем FreeNAS. О настройке Openfiler для дома я и расскажу.

Установка дистрибутива не составляет труда. Инсталлятор здесь основан на Anaconda, которую можно встретить во всех совместимых с Red Hat дистрибутивах (RHEL, Fedora, CentOS и т.п.). Рассказывать о процессе установки не буду, отмечу лишь одну деталь. При разбивке жесткого диска нужно создать 2 раздела:

1.Для системы с точкой монтирования «/», файловой системой ext3 и размером около 1 Гб.

2.Swap – я сделал на 1 Гб (у меня 1 Гб RAM).

Оставшееся пустое место так и оставим (не создаем раздела и не форматируем) – в последующем мы именно его будем использовать как хранилище. После установки заходим на сервер через консоль и проверяем сеть:

```
[root@localhost]# ifconfig
```

Если видим такой вывод, как ниже, то сеть не настроена:

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436  Metric:1
```

```
          RX packets:90 errors:0
dropped:0 overruns:0 frame:0
          TX packets:90 errors:0
dropped:0 overruns:0 carrier:0
          collisions:0
txqueuelen:0
          RX bytes:7476 (7.3 Kb)
TX bytes:7476 (7.3 Kb)
```

Если же вывод – такой:

```
eth0      Link encap:Ethernet
HWaddr 00:17:31:52:D0:A7
          inet addr:192.168.1.100
Bcast:192.168.1.255
Mask:255.255.255.0
          inet6 addr:
fe80::217:31ff:fe52:d0a7/64
Scope:Link
          UP BROADCAST RUNNING
MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0
dropped:0 overruns:0 frame:0
          TX packets:7 errors:0
dropped:0 overruns:0 carrier:1
          collisions:0
txqueuelen:1000
          RX bytes:888 (888.0 b)
TX bytes:528 (528.0 b)
lo        Link encap:Local
Loopback
          inet addr:127.0.0.1
Mask:255.0.0.0
          inet6 addr: ::1/128
Scope:Host
          UP LOOPBACK RUNNING
MTU:16436  Metric:1
          RX packets:118 errors:0
dropped:0 overruns:0 frame:0
          TX packets:118 errors:0
dropped:0 overruns:0 carrier:0
          collisions:0
txqueuelen:0
          RX bytes:9372 (9.1 Kb)
TX bytes:9372 (9.1 Kb)
```

– сеть настроена, так что следующий раздел («Настройка сети») можно пропустить и сразу перейти к обновлению системы.

Настройка сети

Создаем файл ifcfg-eth0 с настройками сети:

```
[root@localhost]# nano /etc/
sysconfig/network-scripts/ifcfg-
eth0
```

В случае DHCP он будет выглядеть примерно так:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
```

Чтобы сохранить файл в запущенном текстовом редакторе nano, надо нажать на «Ctrl» + «X», а затем – «Y». Теперь перезапустим сеть:

```
[root@localhost]# /etc/init.d/
network restart
```

После этого вы должны увидеть примерно следующее:

```
eth0      Link encap:Ethernet
HWaddr 00:17:31:52:D0:A7
          inet addr:192.168.1.100
Bcast:192.168.1.255
Mask:255.255.255.0
          inet6 addr:
```

```
fe80::217:31ff:fe52:d0a7/64
Scope:Link
          UP BROADCAST RUNNING
MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0
dropped:0 overruns:0 frame:0
          TX packets:7 errors:0
dropped:0 overruns:0 carrier:1
          collisions:0
txqueuelen:1000
          RX bytes:888 (888.0 b)
TX bytes:528 (528.0 b)
lo        Link encap:Local
Loopback
          inet addr:127.0.0.1
Mask:255.0.0.0
          inet6 addr: ::1/128
Scope:Host
          UP LOOPBACK RUNNING
MTU:16436  Metric:1
          RX packets:118 errors:0
dropped:0 overruns:0 frame:0
          TX packets:118 errors:0
dropped:0 overruns:0 carrier:0
          collisions:0
txqueuelen:0
          RX bytes:9372 (9.1 Kb)
TX bytes:9372 (9.1 Kb)
```

Обновление

Для обновления системы выполняем команду:

```
[root@localhost]# conary
updateall
```

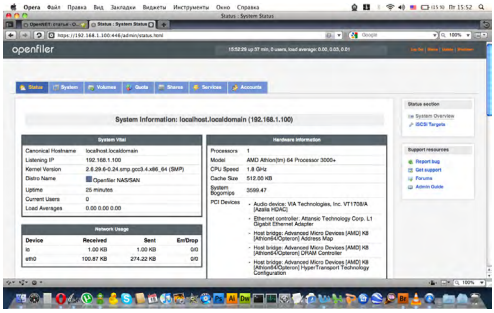
После этого перезагружаемся и приступаем к настройке доступа.

Настройка общего доступа без пароля

Так как мы у себя дома, то и пароли нам ни к чему – доступ к ресурсам будем настраивать по гостевому входу, чтобы любой компьютер в сети без проблем читал расшаренные ресурсы и записывал в них.

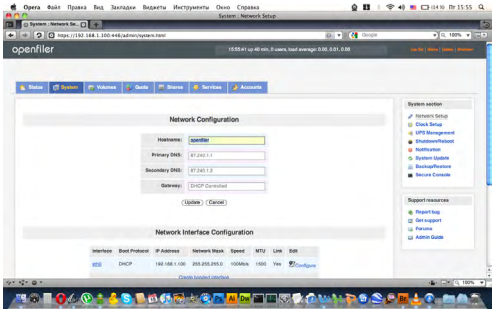
Заходим на сервер с любого компьютера в сети при помощи веб-браузера по адресу https://ip-адрес:446. Для входа используем логин «openfiler» и пароль «password».

Основное окно состоит из 7 основных вкладок. После выбора вкладки справа появляются дополнительные меню, которые открывают доступ к специфическим для данной вкладки настройкам.



Теперь – по порядку.

1. Перейдем на вкладку System, в поле «Hostname:» запишем «openfiler»:



Прокрутив ниже в разделе Network Access Configuration, настраиваем доступ к сети. Если здесь не вбить хоть один компьютер из сети, будущая шара работать не будет.

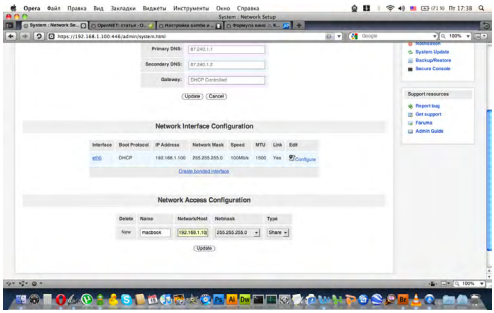
Добавляем компьютер:

Name: имя компьютера

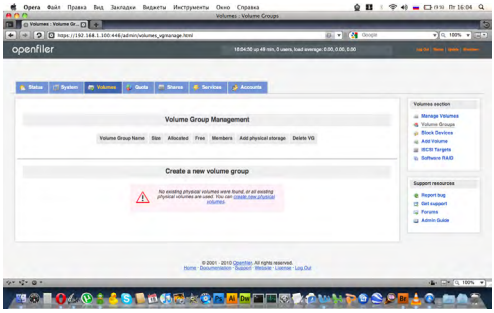
Network/Host: IP-адрес компьютера

Netmask: маска подсети

Нажимаем «Update»:

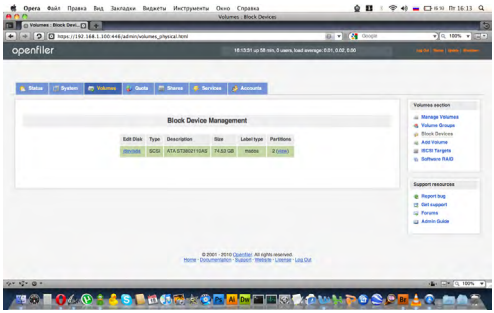


2. Перейдем на вкладку «Volumes». Здесь создадим раздел, на котором будут размещаться наши общие данные:



Нажимаем «create new physical volumes» и попадаем в меню выбора диска:

Выбираем /dev/sda и на следующем экране создаем раздел с такими параметрами:

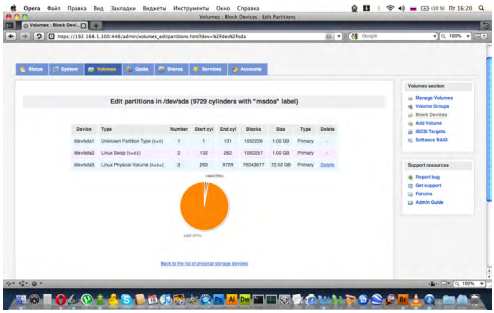


Mode – Primary

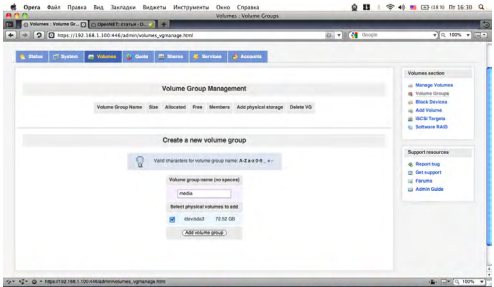
Partition Type – Physical volume

Нажимаем «Create».

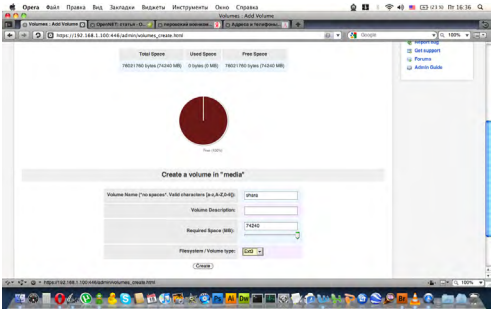
Видим такой экран – раздел создан:



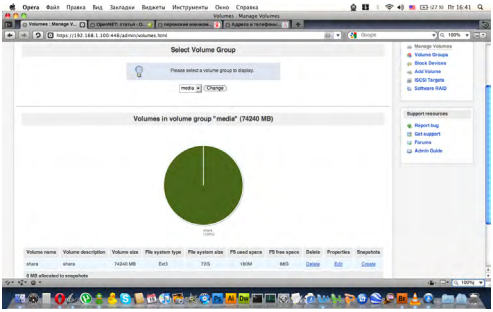
Далее переходим на экран «Volume Groups» в меню справа и создаем группу раздела:



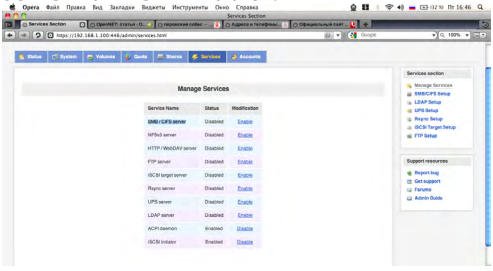
Затем переходим на экран «Add Volume» в меню справа и форматируем диск. Скроллим вниз и видим вот такую картину:



Вводим имя, выбираем размер раздела и файловую систему, нажимаем «Create», ждем пару минут. Раздел создан!



3. Перейдем на вкладку Services, и включим SAMBA, для этого напротив SMB / CIFS server нажмем «Enable».



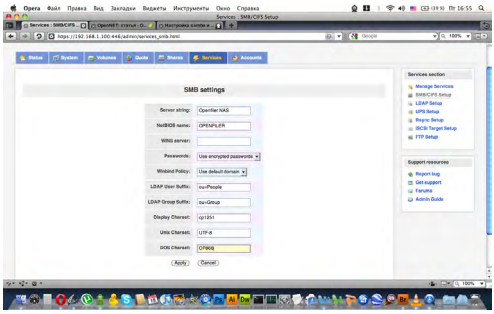
В меню справа переходим на экран SMB/CIFS Setup, и настраиваем там локаль и NetBIOS name:

Display Charset: cp1251

Unix Charset: UTF-8

DOS Charset: CP866

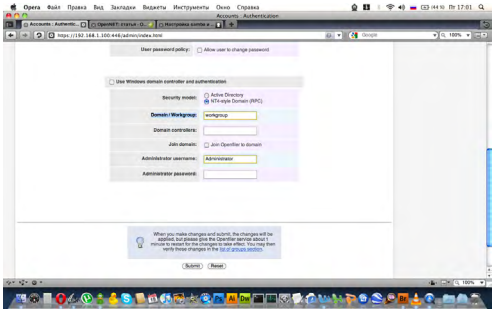
Остальные пункты не трогаем, нажимаем «Apply»:



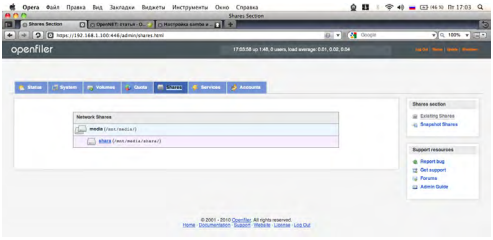
4. Перейдем на вкладку «Accounts», проскроллив чуть ниже. В разделе «Use Windows domain controller and authentication» введем название нашей workgroup:

Domain / Workgroup: workgroup

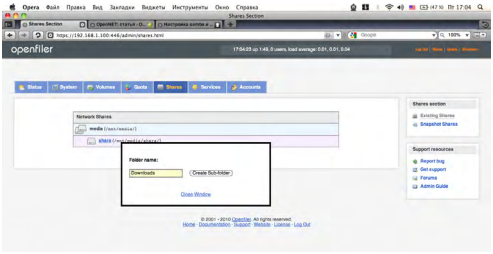
Опускаемся еще чуть ниже и нажимаем «Submit»:



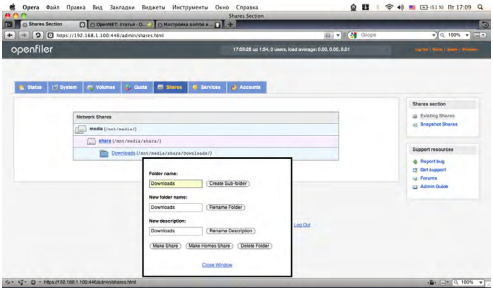
5. Перейдем на вкладку «Shares» – вкладка, на которой настраиваются наши ресурсы и доступ к ним:



Нажимаем на «shara» и создаем папку:



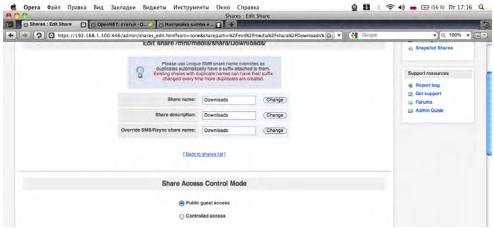
Нажимаем на только что созданную папку и в открывшемся окне нажимаем «Make share»:



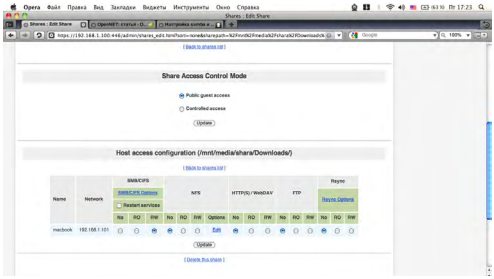
Попадаем на следующий экран, где настраиваем общий доступ:

Override SMB/Rsync share name: Downloads

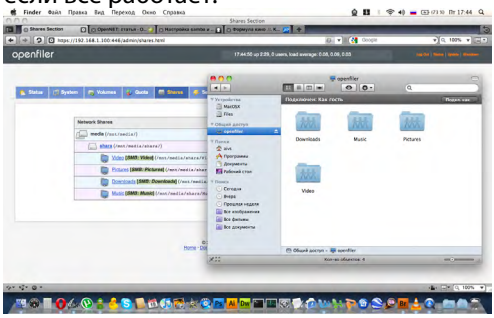
Нажимаем «Change». Напротив «Public guest access» ставим галку и нажимаем «Update»:



Прокручиваем вниз и видим таблицу. Включаем SAMBA для хоста в сети, нажав «RW» в разделе «SMB/CIFS», нажимаем «Update»:



Аналогично с остальными папками. На этом настройка окончена, заходим на сервер, закачиваем ваши файлы и радуемся если все работает:



nixp.ru

Как собрать .deb пакет

В любом дистрибутиве GNU/Linux, имеющем на борту пакетный менеджер, приветствуется установка программного обеспечения строго из пакетов. В какой-то момент может возникнуть ситуация, когда проще собрать пакет, чем компилировать и устанавливать классическим методом «*./configure && make && sudo make install*», например, если некоторая программа необходима нескольким коллегам, среди которых не каждый в состоянии понять почему сборка из репозиториев не удалась.

Если вы намереваетесь создавать пакеты, которые могут/будут входить в официальный репозиторий Debian, то для начала стоит ознакомится со следующими материалами:

the Debian New Maintainers' Guide
Debian Packaging Tutorial
Debian Policy
Developers Reference

Но, если вам просто нужно понять, как собрать .deb пакет, здесь и сейчас - читайте статью далее.

Сборка из исходников

GPG ключ

Первое, что необходимо - сгенерировать gpg ключ, если его еще нет, так как пакет, при создании, будет подписан этим ключом:

```
gpg --gen-key
```

Важно помнить, что на дальнейших этапах необходимо будет использовать те же самые имя и email, что использовались при создании ключа.

Для того, чтобы использовать данный ключ для подписи делаем следующее:

```
gpg -a --output ~/.gnupg/YOUR_
NAME.gpg --export 'YOUR NAME'
```

После чего:

```
gpg --import ~/.gnupg/YOUR_NAME.
gpg
```

Все, ключ готов.

Подготовка окружения

Установим необходимые для сборки пакеты:

```
sudo apt-get install build-
essential autoconf automake \
autotools-dev dh-make debhelper
devscripts fakeroot \
xutils lintian pbuilder
```

Получение и подготовка исходников

Разархивируем исходники и переименуем директорию в формат имя-версия, важно, чтобы название директории было в нижнем регистре. После этого, на одном уровне с этой директорией необходимо разместить архив с исходниками, например, в формате tar.gz (можно просто создать архив с директорией, которую только что создали).

Пример:

```
mkdir -p ~/build/memcached/1.4.17
cd ~/build/memcached/1.4.17
wget -c http://www.memcached.org/
files/memcached-1.4.17.tar.gz
```

```
tar -xzf memcached-1.4.17
```

Подготовка к сборке

Первое что мы сделаем – подготовим структуру и информацию о нашем пакете.

```
cd ~/build/memcached/1.4.17/
memcached-1.4.17
dh_make -e youremail@address -f
../memcached-1.4.17.tar.gz
```

Не забываем, что необходимо использовать тот же email, что использовался при генерации ключа. После выполнения данной команды в терминале появится следующее приглашение:

```
Type of package: single binary,
indep binary, multiple binary,
library, kernel module, kernel
patch?
[s/i/m/l/k/n/b]
```

Выберем пока самый простой вариант – s

В нашей директории появилась новая поддиректория – debian, которая содержит файлы, необходимые для дальнейшей сборки. Теперь отредактируем информацию о нашем пакете.

Файл «control»

```
Source: memcached
Section: unknown
Priority: optional
Maintainer: YOUR NAME <your @
email.org>
Build-Depends: debhelper (>=
8.0.0), autotools-dev
Standards-Version: 3.9.4
Homepage: <insert the upstream
URL, if relevant>

Package: memcached
Architecture: any
Depends: ${shlibs:Depends},
${misc:Depends}
Description: </insert><insert up
to 60 chars description>
  </insert><insert long
description, indented with
spaces>
```

Добавим зависимости и описание пакета

```
# Смотрим зависимости
dpkg-depcheck -d ./configure
```

В терминале видим следующее:

```
Packages needed:
  mime-support
  libsigsegv2:amd64
  gawk
  libevent-dev
```

Теперь изменим файл debian/control, учитывая эти зависимости и добавим необходимую информацию:

```
Source: memcached
Section: web
Priority: optional
Maintainer: YOUR NAME <your @
email.org>
Build-Depends: debhelper (>=
8.0.0), autotools-dev,
 mime-support, libsigsegv2, gawk,
libevent-dev
Standards-Version: 3.9.4
Homepage: http://memcached.org/
Package: memcached
Architecture: any
Depends: ${shlibs:Depends},
${misc:Depends}
Description: High-performance,
distributed memory object caching
system
  Memcached is an in-memory key-
value store for small chunks of
arbitrary data (strings, objects)
```

```
from results of database calls,
API calls, or page rendering.
```

Файл «copyright»

Тут размещаем правовую информацию, в частности, можно разместить текст лицензии, под которой распространяется исходный код программы.

Файл «changelog»

Этот файл автоматически заполняется при вызове dh_make, важно убедиться, что указанный в файле email тот же, что использовался для генерации gpg-ключа.

Сборка

```
dpkg-buildpackage -rfakeroot
```

Если не было допущено ошибок на предыдущих этапах, то в процессе сборки будет получено приглашение ввести пароль от gpg-ключа, после ввода которого в директории на уровень выше появятся файлы:

- memcached_1.4.17-1_amd64.changes
- memcached_1.4.17-1_amd64.deb
- memcached_1.4.17-1.dsc
- memcached_1.4.17-1.debian.tar.xz
- memcached_1.4.17.orig.tar.gz

Как видите, сборка производилась на платформе x86_64. Нужна другая платформа – не проблема.

Сборка под другую платформу

Для сборки, например, под платформу i386 нам понадобится pbuilder – система автоматической сборки, работающая в chroot.

```
sudo pbuilder --create
--architecture i386
sudo pbuilder --update
sudo pbuilder --build ../
memcached_1.4.17-1.dsc
```

Готовый пакет можно будет забрать из директории */var/cache/pbuilder/result*

Пересборка пакета

Если в дальнейшем необходимо будет изменить содержимое пакета, то после внесения изменений необходимо выполнить:

```
dpkg-buildpackage -rfakeroot -b
```

lushpai.org

Canonical закрывает Ubuntu One

Canonical анонсировала закрытие сервиса Ubuntu One. Как это ни прискорбно, но популярный облачный сервис полностью прекратит свою работу 31 июля 2014 года. Основная же функциональность Ubuntu One будет заблокирована уже 1 июня.

Подобное касается как сервиса хранения файлов Ubuntu One, так и музыкального магазина Ubuntu One Music Store. Уже сейчас в музыкальном магазине стало невозможным приобретать музыку, а на облачном хранилище - дополнительное место.

Что касается тех, кто приобрел дополнительное место на Ubuntu One, то Canonical вернет им деньги в течение нескольких недель.

Таким образом, в Ubuntu 14.04 LTS, которая выйдет уже через пару недель, не будет ни клиента Ubuntu One, ни связанных с ним веб-приложений, ни индикатора синхронизации.

Почему упраздняется Ubuntu One?

Конечно же, основная причина заключается в том, что сервис не приносит достаточно прибыли, чтобы окупить себя. Canonical, как коммерческой компании, приходится обеспечивать бесперебойную работу серверов с данными, но выгода от продажи дополнительного места не окупает расходов. Поэтому и появляются тормоза при работе с сервисом, а также периодические сбои, когда невозможно загрузить данные на сервис/с него.

Главный исполнительный директор Canonical Джейн Силбер заявила о том, что сервис не выдерживает конкурентной борьбы:

На данный момент конкурирующие сервисы предоставляют по 25-50 Гб бесплатного пространства... Когда мы что-либо разрабатываем, то хотим быть лучшими в своем классе, и для развития Ubuntu One в этом направлении нам придется потратить слишком много средств, что не входит в наши планы.

В самом деле, сервис Ubuntu One находился в последнее время в довольно ужасающем состоянии. Клиент был переписан на Qt ради более простой поддержки Windows- и MacOS-систем, однако это привело к тому, что под Ubuntu он стал выглядеть просто отвратительно. Со временем была упразднена кнопка "Сохранить на Ubuntu One". Ну и, конечно же, эти постоянные перебои с доступом к данным, а также низкая скорость...

Понятно, что без серьезных денежных вложений что-либо кардинально изменить тут не получится.

Что касается исходного кода, то он будет передан сообществу ради того, чтобы все желающие могли создать платформу синхронизации файлов с открытым программным кодом. Закрытие Ubuntu One не коснется прочих сервисов, завязанных на Ubuntu Single Sign On.

По словам Силбер, в конвергентном будущем Ubuntu они делают ставку на активное использование сервисов третьих сторон, и предложение своего конкурирующего сервиса было бы нечестным. Что бы это значило? Уж не интеграцию ли с Dropbox или Google Drive?

ubuntu-news.ru

Open Build Service 2.5 - новая версия автоматизированной системы сборки пакетов

Недавно вышла новая версия популярной автоматизированной сборки Linux-пакетов - Open Build Service (OBS) 2.5.

Система Open Build Service предназначена для сборки и распространения бинарных пакетов для Linux-дистрибутивов (поддерживаются openSUSE и SLES, Fedora и RHEL, Debian и Ubuntu, Arch Linux).

Система OBS создает изолированное окружение для сборки пакетов, пересобирает зависимые пакеты, упрощает работу с разными дистрибутивами и архитектурами - в общем, помогает сборщикам в решении их типовых задач, предоставляя автоматизированную и простую в использовании «сборочную ферму».

В релизе Open Build Service (OBS) 2.5:

API для создания аутентификационных ключей, используемых для подключения внешних источников кода (source services), - например, можно создать токен для GitHub, чтобы автоматически инициировать сбор пакета из исходников при выполнении git push в репозиторий этого сервиса;

пользовательский веб-интерфейс (Web UI) и интерфейс API объединили в одно приложение на Ruby on Rails;

новый API для конфигурации;

новая интегрированная система уведомлений и комментариев;

автоматическое обнаружение и удаление устаревших веток пакетов;

система поиска пакетов (по названию, описанию и дополнительными полям) на базе Sphinx.

Дмитрий Шурупов
по материалам Open Build Service.

Contributions made easy

Магазин "TOTAL"

- персональные компьютеры;
- компьютерные комплектующие;
- ноутбуки, нетбуки, планшеты;
- принтеры, МФУ, расходники;
- сетевое оборудование;
- CD/DVD диски, флеш-накопители;
- и многое другое.

г. Кривой Рог, ул. Адмирала Головко, 40, Терновской р-н
тел. (067)-698-87-79, (097)-692-73-38

Терминал Linux. 2 статья - команда поиска файлов и директорий в терминале

Цикл статей о терминале:

1.Терминал Linux 1 (Больше чем USER № 7) - команды навигации в терминале.

2.Терминал Linux 2 (Больше чем USER № 8) - команда поиска файлов и директорий в терминале

3.Терминал Linux 3 (Больше чем USER № 9) - команды поиска файлов (продолжение)

4.Терминал Linux 4 (Больше чем USER № 10) - создание, удаление, форматирование, монтирование разделов жесткого диска

5.Терминал Linux 5 (Больше чем USER № 11) - создание aliases (псевдонимов) в Ubuntu

При работе с Linux, довольно часто возникает необходимость поиска файлов с определенными характеристиками.

Этими характеристиками могут быть размер или тип файла, время изменения и многое другое.

Для поиска файлов в терминале используется команда "find"

Формат команды find:

find путь -опции

путь – это каталог, в котором произвести поиск.

В обычном случае мы просто указываем путь к нужному каталогу, например:

/usr/share

Но в качестве пути можно указывать следующие значения:

. – поиск в текущем каталоге;

/ – поиск от корневого каталога;

~ – поиск в домашнем каталоге.

Опции

Основные опции команды find:

-name - поиск файлов по имени, используя приведенный шаблон;

-user - поиск файлов, принадлежащих указанному пользователю;

-type - поиск файлов определенного типа.

Вот наиболее используемые типы:

d – каталог;

f – обычный файл;

l – символическая ссылка;

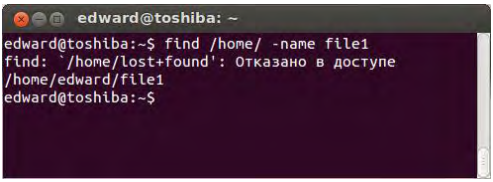
-size -n +n n - поиск файлов с размером n единиц;

-mtime -n +n – поиск файлов, созданных или модифицируемых менее чем (-) или более чем (+) дней назад.

Примеры использования команды "find".

Самый простой поиск, указываем путь и имя файла. Например, найдем файл с именем file1

```
find /home/ -name file1
```

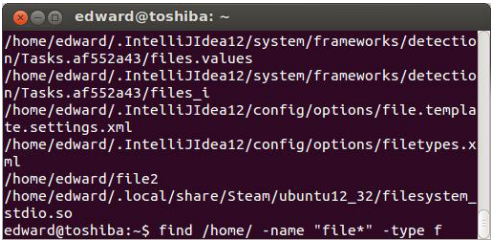


Но если бы мы написали не полностью имя, например "file", то файл "file1" не был найден. Для этого нужно писать имя в кавычках и в конце добавить *, вот таким образом:

```
find /home/ -name "file*"
```

Но нашлись и файлы и директории, где встречается название file, чтобы разграничить это и используется опция -type и параметр f, чтобы искать только файлы (для только директорий d):

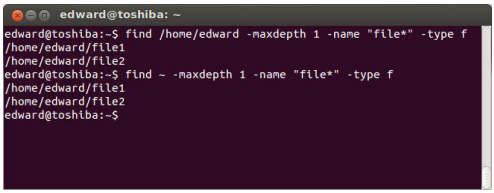
```
find /home/ -name "file*" -type f
```



Но теперь нашлись файлы в фиг знает какой глубины директориях. А что если нам надо найти в текущем каталоге или в папках вложенности 1 или 2?

Для этого используется опция maxdepth (глубина поиска), то есть, если мы хотим найти файл в директории поиска, без рекурсивного просмотрах всех директорий:

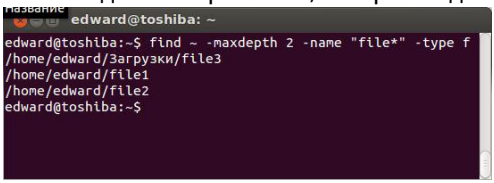
```
find ~ -maxdepth 1 -name "file*"
-type f
```



Как видим, что нашлись файлы только в директории поиска. Если хотим включить первый уровень папок внутри каталога поиска, тогда нужно указать maxdepth 2:

```
find ~ -maxdepth 2 -name "file*"
-type f
```

Как видно на скриншоте, теперь найден файл и в папке "Загрузки". Просто выставляем параметр опции -maxdepth для установки глубины поиска.



Важно! Нужно указывать его перед опцией -name.

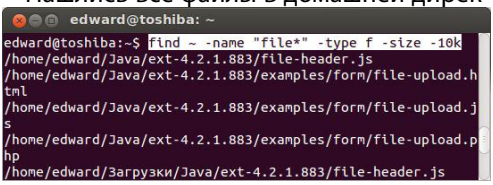
Теперь разберем очень важную опцию поиска файла с размером "-size". Важно, если мы хотим найти файлы раз-

мером в килобайтах, нужно писать в конце k, для мегабайт M, для гигабайт G, для байт b. Важно соблюдать регистр. Разберем пример:

Найдем файлы в домашней директории менее 10 килобайт с именем file*:

```
find ~ -name "file*" -type f -size -10k
```

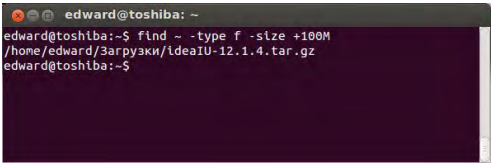
Нашлись все файлы в домашней директории и ее папках, размер которых менее 10 килобайт.



Теперь давайте найдем файлы в домашней директории, которые весят больше 100 мегабайт:

```
find ~ -type f -size +100M
```

Нашелся один файл, который весит более 100 мегабайт.



Также можно искать файлы определенного размера, например которые весят 1G или 1M:

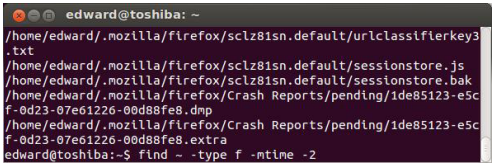
```
find ~ -type f -size 1G
```

И теперь переходим к поиску файлов, которые были созданы или модифицированы n дней назад.

Например, для поиска файлов, которые были изменены или созданы менее 2 дней назад:

```
find ~ -type f -mtime -2
```

Было найдено очень много файлов. Что-



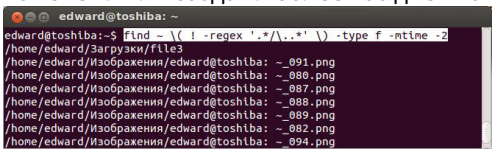
бы найти только файлы определенного пользователя, нужно использовать опцию -user (edward - это мое имя пользователя, вам нужно указывать своё):

```
find ~ -user edward -type f -mtime -2
```

В домашней папке все файлы принадлежат вашему текущему пользователю, поэтому повторится список.

Но, что если Вы хотите исключить из поиска скрытые директории, не меняя при этом глубину поиска? Данная команда может показаться сложной на первый взгляд. find ~ \(! -regex '.*/\..*' \) -type f -mtime-2 Вот эта вот конструкция (! -regex '.*/\..*' \) как раз и уберет из поиска все скрытые файлы и директории:

Ну и для поиска файлов, которые были изменены или созданы более 100 дней назад, к примеру:




```
find ~ -type f -mtime +100
```

Это не все возможности этой команды. Я перечислил основные для поиска файлов и директорий.

linuxrussia.com

Разработчики elementary OS планируют перенести Pantheon в Debian Linux

Один из разработчиков elementary OS Сергей Давидов (Sergey “Shnatsel” Davidoff) рассказал о планах по интеграции кодовой базы рабочего окружения Pantheon (а именно, шелла, набора инструментов для работы GUI, стандартных приложений и GTK-темы) в Debian Linux. Цель проекта - создать установочные пакеты полноценной рабочей среды для официального репозитория Debian.

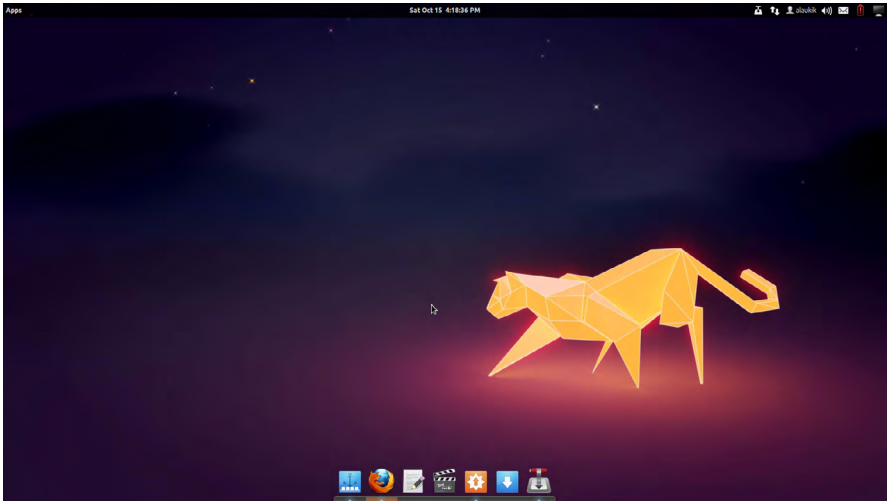
Это поможет нам справиться с некоторыми проблемами, возникшими из-за эксклюзивной поддержки лишь дистрибутивов Ubuntu, хотя Pantheon с успехом портирован на Gentoo и частично на Arch.

Разработчик также отмечает, что портировать удастся не все: например, Wingpanel для работы требует наличия зависимостей, существующих лишь для Ubuntu.

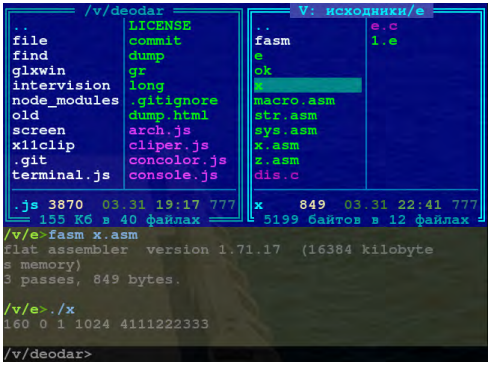
Скорее всего, мы начнем работу по портированию вскоре после выхода нового релиза на основе Ubuntu 14.04 (elementary OS «Isis»), но пока не знаем, на что заменим проблемные пакеты.

Проект заявлен на участие в Google Summer of Code 2014, а его участники заявляют, что планируют в будущем полностью перенести elementaryOS с Ubuntu LTS на Debian.

linux.org.ru



«Деодар» - новая рабочая среда для Linux



«Деодар» - классическая двухпанельная рабочая среда для Linux, автор которой вдохновлялся Norton Commander, Volkov Commander, Dos Navigator, Far Manager.

Распространяется по антилицензии Unlicense.org. Безвозмездно, то есть даром. Основан на Node.js, написан на JavaScript с добавлением C++. Состоит из двух панелей, строки ввода и консоли, совместимой с color-xterm. Все это удобно объединено друг с другом. Есть текстовый редактор и просмотрщик.

Редактор «заточен» под правку исходных кодов. Интерфейс пользователя полностью русскоязычный.

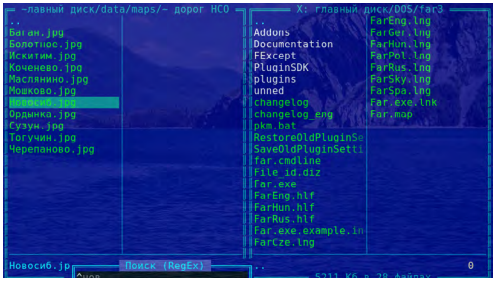
Рабочая среда легко настраиваемая и расширяемая (за счет того, что большая часть кода написана на JavaScript). Возможно подключение расширений npm (существует более 50,000 расширений).

Деодар опирается на библиотеку Intervision, напоминающую TurboVision. Поддерживается пользовательский ввод-вывод как знакового отображения, так и точечного. Не возникает проблем с Юникодом.

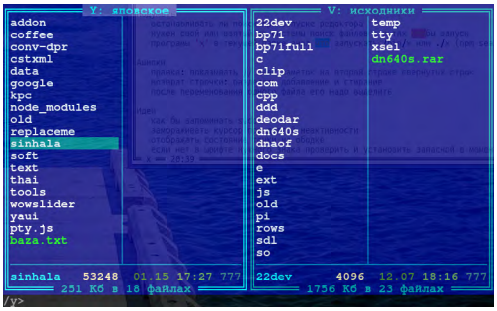
Исходный код и инструкция по сборке размещены на GitHub.

Скриншоты

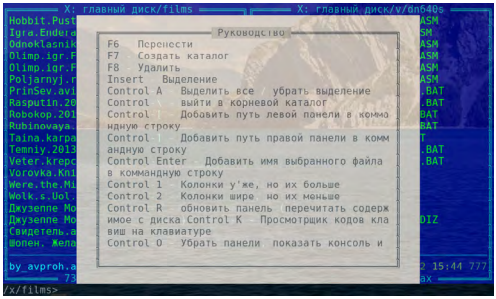
Быстрый поиск;



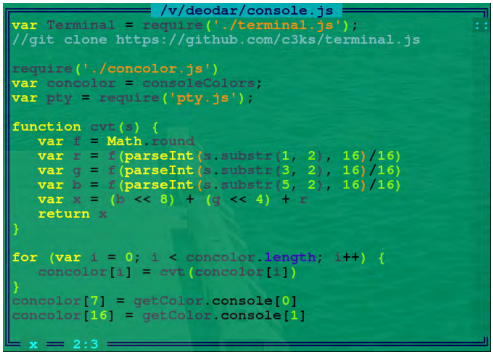
Виртуальный корень. Панели Деодара имеют способность считать некоторые каталоги дисками и не отображать две точки для перехода в родительский каталог, что помогает сосредоточиться на работе в данном каталоге:



Простое руководство. Вы узнаете больше горячих клавиш, заглянув в norton.js и edit.js;



Правка исходного кода на JavaScript;



bash, запущенный в Деодаре. Можно нажатием Control-O переключаться между bash и панелями, а в панелях править какой-нибудь файл;


```
sudo apt-get install npm curl git
clang g++
sudo apt-get install libx11-dev
libxcursor-dev mesa-common-dev
libfreetype6-dev libgl1-mesa-dev
sudo npm install -g n
sudo n 0.10.26
node --version
0.10.26
sudo npm install -g node-gyp
git clone https://github.com/
exebook/deodar
cd deodar
git clone https://github.com/
exebook/glxwin
git clone https://github.com/
exebook/x11clip
git clone https://github.com/
exebook/dnaof
git clone https://github.com/
exebook/intervision
cd x11clip
node-gyp configure build
cd ..
cd glxwin
node-gyp configure build
cd ..
git clone https://github.com/
c3ks/terminal.js
npm install pty.js
если 'npm install pty.js' выдаёт
странную ошибку, то можно устано-
вить pty.js с github:
git clone https://github.com/
chjj/pty.js
cd pty.js
npm install nan extend
node-gyp configure build
```

linux.org.ru

Facebook представила собственный язык программирования Hack

Социальная сеть Facebook представила новый открытый язык программирования под названием Hack. Он схож с PHP и предлагает присущую ему быстроту программирования, но одновременно отличается от него статической типизацией, используемой в C++, Java и других современных языках.

Динамическая типизация, присущая языку PHP (а также, к примеру, JavaScript), сокращает код и позволяет тратить меньше времени на его написание, однако не позволяет исключать ошибки на стадии компиляции.

В свою очередь, статическая типизация позволяет исключать ошибки в коде на стадии компиляции, поэтому она подходит для сложных, больших программ, в написании которых принимает участие множество разработчиков

Для компаний вроде Facebook, в которых работают тысячи программистов, которые обновляют код дважды в день, ошибки в коде являются проблемой значительного масштаба. Именно поэтому был рожден Hack, сочетающий сильные стороны языков программирования того и другого типа, пояснили в компании.

Для запуска приложений, написанных на Hack, необходимо установить виртуальную машину HHVM (HipHop Virtual Machine). Она поддерживает одновременно и Hack, и PHP. Поэтому разработчикам не придется разом переделывать весь код из PHP в Hack, они могут делать это постепенно, по необходимости. Виртуальная машина поддерживает смешанный код, поэтому разработчики могут продолжить писать на PHP, но уже использовать функции нового языка программирования.

Hack похож на PHP, но отличается статической типизацией (вверху: фрагмент кода PHP, внизу: тот же код на языке Hack)

```php
<?php

function dbfetch() {
  $r = mysql_query('SELECT ...');
  if ($r === false || mysql_num_rows($r) == 0) {
    return null;
  }

  return new DBData(mysql_fetch_array($r));
}

function test() {
  $data = dbfetch();
  $data->doFunStuff();
}
```

```hack
<?hh

function dbfetch(): ?DBData {
  $r = mysql_query('SELECT ...');
  if ($r === false || mysql_num_rows($r) == 0) {
    return null;
  }

  return new DBData(mysql_fetch_array($r));
}

function test(): void {
  $data = dbfetch();
  $data->doFunStuff();
}
```

Для загрузки Hack и HHVM требуется Ubuntu 12.04 LTS, Ubuntu 13.10 или Debian 7. Пользователи также при желании могут скачать код Hack и скомпилировать его самостоятельно.

Facebook – не единственная ИТ-компания, которая создала собственный язык программирования. В июле прошлого года собственный вариант PHP - KittenPHP - представила крупнейшая рос-

сийская соцсеть "ВКонтакте". Переход на новый язык, на разработку которого ушло более года, и который вдвое увеличивает производительность, соцсеть завершила в мае 2013 года. В марте 2014 года компания предоставила открытый доступ к языку.

Собственные разработки в области средств программирования имеет и поисковый гигант Google. В ноябре Google выпустила высокопроизводительную замену языку JavaScript под названием Dart, разработка которого велась более 2 лет. Еще один собственный язык программирования Go корпорация предлагает разработчикам приложений для настольных операционных систем, включая Windows и OS X.

it.tut.by

LAMP

LAMP – акроним, обозначающий набор (комплекс) серверного программного обеспечения, широко используемый во Всемирной паутине. LAMP назван по первым буквам входящих в его состав компонентов: Linux – операционная система Linux; Apache – веб-сервер; MySQL – СУБД; PHP – язык программирования, используемый для создания веб-приложений (помимо PHP могут подразумеваться другие языки, такие как Perl и Python).

Попробуем установить и настроить свой локальный веб-сервер. Он может пригодится для веб-разработки, тестирования веб-приложений и прочего.

Для начала установки обновим список репозиториев

```
sudo aptitude update
```

(Рекомендуем использовать именно aptitude, хотя во многих инструкциях вы можете встретить установку через apt-get, потому что он при установке решает многие зависимости пакетов, а также имеет более гибкий поиск и логичный синтаксис).

Установка Apache

```
sudo aptitude install apache2
apache2-doc apache2-mpm-prefork
apache2-utils apache2-suexec
```

Вводим в адресной строке браузера http://localhost/

И если видим сообщение It works!, значит установка удалась и сервер запущен.

Установка PHP

Копируем и устанавливаем одним движением все необходимые пакеты

```
sudo aptitude install php5 php-
doc php-pear libapache2-mod-php5
```

```
libapache2-mod-ruby libapache2-
mod-auth-mysql php5-mysql
libapache2-mod-python php5-dev
php5-cgi php5-mcrypt php5-gd
php5-cli php5-common php5-curl
php5-idn php5-imagick php5-imap
php5-memcache php5-ming php5-ps
php5-pspell php5-recode php5-snmp
php5-sqlite php5-tidy php5-xmlrpc
php5-xsl libapache2-mod-evasive
```

Установка дополнительных пакетов для gd

```
sudo aptitude install libpng12-
dev libjpeg62-dev libxpm-dev
libfreetype6-dev
```

Подключение модулей

```
sudo a2enmod php5 mod-evasive ssl
rewrite suexec include
```

Редактируем конфиг хостов:

```
sudo nano /etc/apache2/sites-
available/default
```

Изменяем параметр: AllowOverride None на AllowOverride All

Проверим функциональность php

Создадим каталог, и тестовый файл index.php

```
sudo mkdir /var/www/php
sudo nano /var/www/php/index.php
```

Со следующим содержимым:

```
<?php
phpinfo();
?>
```

Сохраняем файл, и проверяем в браузере:

http://localhost/php/

Должна вывестись служебная информация по PHP

Настоятельно рекомендуем либо удалить этот файл с сервера, либо защитить его паролем.

Установка MySQL сервера

```
sudo aptitude install mysql-
server
```

В процессе установки, будет запрошен ввод пароля для root MySql сервера.

Установка phpMyAdmin

Во время установки выберем apache2

```
sudo aptitude install phpmyadmin
```

В процессе установки, будет запрошен ввод пароля root MySQL Следующим шагом, задаем пароль для phpMyAdmin

Создание виртуального хоста для нашего сайта

Создадим структуру каталогов под наш будущий сайт

```
sudo mkdir /var/www/sitename.ru
sudo mkdir /var/www/sitename.ru/
www
sudo mkdir /var/www/sitename.ru/
log
sudo mkdir /var/www/sitename.ru/
sess
sudo mkdir /var/www/sitename.ru/
tmp
```

Создание конфигурационного файла виртуального хоста нашего сайта

```
sudo nano /etc/apache2/sites-
available/sitename.ru
```

Со следующим содержимым:

```
<VirtualHost *:80>
```

```
ServerName sitename.ru
ServerAlias www.sitename.ru
DocumentRoot /var/www/sitename.
ru/www
ServerAdmin
ErrorLog /var/www/sitename.ru/
log/apache_error.log
CustomLog /var/www/sitename.ru/
log/apache_access.log combined
<Directory /var/www/sitename.ru/
www>
Options FollowSymLinks
Options +Indexes
AllowOverride All
Order allow,deny
Allow from all
</Directory>
php_admin_value upload_tmp_dir /
var/www/sitename.ru/tmp
php_admin_value error_log /var/
www/sitename.ru/log/php.log
php_admin_value session.save_path
/var/www/sitename.ru/sess
</VirtualHost>
```

Активируем сайт на сервере

```
sudo a2ensite sitename.ru
```

Внесем имя сайта в список хостов сервера

```
sudo nano /etc/hosts
```

Найдем строчку

```
127.0.0.1 localhost
```

И допишем в нее через пробел

```
sitename.ru www.sitename.ru
```

Чтобы Apache не ругался, внесем строчку в один из конфигурационных файлов Apache (начиная с версии 11.04 не требуется)

```
sudo nano /etc/apache2/httpd.conf
```

Добавим следующее содержимое:

```
ServerName localhost
```

Закрываем и сохраняем.

Перезапускаем Apache

```
sudo service apache2 restart
```

Теперь по выбранному вами адресу вы имеете полноценный локальный веб-сервер.

ubuntomania.ru

Dropbox анонсировал выпуск открытой реализации Python

Dropbox, поставщик облачных систем хранения данных, анонсировал Pyston – JIT-компилятор для Python собственной разработки с открытым исходным кодом. Большой упор в разработке Pyston делается на увеличение производительности.

Dropbox признают PyPy, Jython и другие проекты на базе Python, но они надеются на улучшение производительности по сравнению с ними, а также сохранение совместимости с вышестоящими реализациями Python.

feolug.vpz.org.ua

ED.ua Школьный Электронный Дневник

Школа | Учительская | Профиль | Оплата | Обучение

Социальный проект компании "ВИТ" – Школьный электронный дневник

- Электронная база данных
- Персональный сайт школы
- Новости, события, праздники
- Связь с учителями и родителями
- Домашнее задание, оценки, замечания и поощрения
- Мобильная версия сайта
- Электронная очередь детских садов
- Отчеты, статистика, рейтинг школ

а также:

различные акции, скидки, праздники для наших пользователей!

Функции постоянно добавляются и модернизируются!

с ED.ua сбудется моя мечта!

ПОТОМУ ЧТО НА САЙТЕ ED.UA ЕСТЬ ПОЛНОЕ ДОМАШНЕЕ ЗАДАНИЕ!

ФЕОДОСИЯ
ФЛП Касьянова О. В. :
тел: +380991605920
+380950244989
http://ed.ua

ЛУГАНСК
ФЛП Турецкая З. В. :
тел: +380500311340
+380990631993
http://m.ed.ua

98112, Украина, АР Крым, г.Феодосия, ул. Крымская, 21-А Тел.: (06562) 7-44-79

Защита данных на телефонах и планшетах на базе Android

На сегодняшний день практически все смартфоны стали носителями важных персональных либо корпоративных данных. Также посредством телефона можно легко получить доступ к учетным записям таким как Gmail, DropBox, FaceBook и даже корпоративным сервисам. Поэтому в той или иной степени стоит побеспокоиться о конфиденциальности этих данных и использовать специальные средства для защиты телефона от несанкционированного доступа в случае его кражи или утери.

Что и от кого защищаем?

Смартфон или планшет часто выполняют функции мобильного секретаря, освобождая голову владельца от хранения большого количества важной информации. В телефонной книге есть номера друзей, сотрудников, членов семьи. В записной книжке часто пишут номера кредитных карточек, коды доступа к ним, пароли к соцсетям, электронной почте и платежным системам.

Список последних звонков также очень важен.

Утеря телефона может обернуться настоящей бедой. Иногда их крадут специально, чтобы проникнуть в личную жизнь или разделить прибыль с хозяином.

Иногда их вовсе не крадут, а пользуются ими недолго, незаметно, но нескольких минут бывает вполне достаточно для опытного пользователя-злоумышленника, чтобы узнать все подробности.

Потеря конфиденциальной информации может обернуться финансовым крахом, крушением личной жизни, распадом семьи.

Итак? что надо защищать в телефоне :

1. Учетные записи. Сюда входит, например, доступ к вашему почтовому ящику gmail. Если вы настроили синхронизацию с facebook, dropbox, twitter. Логины и пароли для этих систем хранятся в открытом виде в папке профиля телефона /data/system/accounts.db.

2. История SMS-переписки и телефонная книжка иногда содержат конфиденциальные данные.

3. Web-браузер. Весь профайл браузера должен быть защищен. Известно, что Web-браузер (встроенный либо сторонний) запоминает для вас все пароли и логины. Это все храниться в открытом виде в папке профиля программы в памяти телефона. Мало того, обычно сами сайты (с помощью cookies) помнят вас и оставляют доступ к аккуанту открытым, даже если вы не указывали запоминать пароль.

Если вы используете синхронизацию мобильного браузера (Chrome, FireFox, Maxthon и др.) с настольной версией бра-

узера для передачи закладок и паролей между устройствами, тогда можно считать что с вашего телефона можно получить доступ ко всем паролям от других сайтов.

4. Карта Памяти. Если вы храните на карте памяти конфиденциальные файлы либо загружаете документы из Интернета. Обычно на карте памяти хранятся фотоснимки и снятые видео.

От чего следует защищать телефон

1. От случайного человека, который найдет потерянный вами телефон либо от "случайной" кражи телефона.

Маловероятно, что данные в телефоне будут иметь ценность для нового владельца в этом случае. Поэтому даже простая защита обеспечит сохранность данных. Скорее всего, телефон будет просто-напросто переформатирован для повторного использования.

2. От любопытных глаз (как правило - это сослуживцы либо ваши дети/близкие), которые могут получить доступ к телефону без вашего ведома, воспользовавшись вашим отсутствием. Даже простая защита обеспечит сохранность данных.

3. От целенаправленной кражи вашего телефона.

Например, кто-то очень сильно хотел узнать, что у вас в телефоне и приложил усилия, чтобы заполучить его.

В этом случае помогает только полное шифрование телефона и SD-карты.

Способы защиты персональных данных на устройствах Android

Существуют встроенные программы защиты, а также средства, предоставленные сторонними разработчиками.

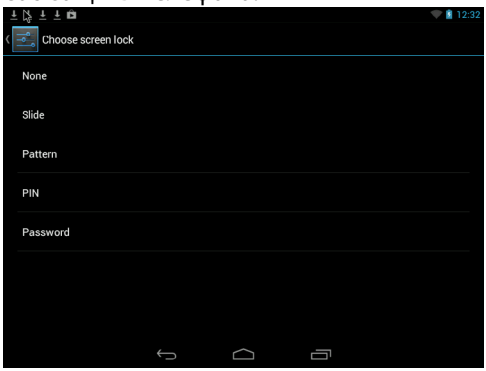
Встроенные средства защиты

Экран блокировки с Графическим Ключом

Данный способ очень эффективный в первом и втором случаях (защита от случайной утери телефона и защита от любопытных глаз). Если Вы случайно потеряете телефон или забудете его на работе, то никто не сможет им воспользоваться. Но если за Ваш телефон попал в чужие руки целенаправленно, тогда это вряд-ли спасет. Взлом может происходить даже на аппаратном уровне.

Экран можно заблокировать паролем, PIN-кодом и Графическим Ключом. Выбрать способ блокировки можно, запустив настройки и выбрав раздел Security -> Screen lock.

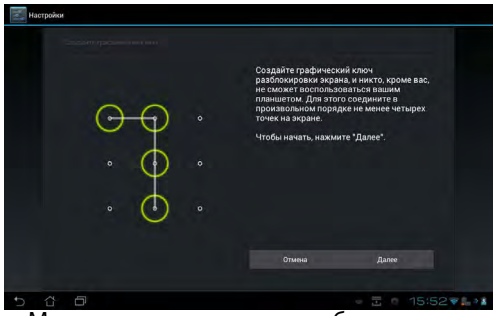
Графический Ключ (Pattern) – самый удобный и одновременно надежный способ защиты телефона.



None – отсутствие защиты,

Slide - для разблокировки необходимо провести пальцем по экрану в определенном направлении.

Pattern - это Графический Ключ, выглядит это примерно так:



Можно повысить уровень безопасности двумя способами.

1. Увеличить поле ввода Графического ключа. Оно может варьировать от 3x3 точки на экране до 6x6 (Android 4.2 встречается в некоторых моделях, зависит от сборки, версии телефона).2. Скрыть отображение точек и "пути" графического ключа на экране смартфона.

Внимание!!! Что случится, если Вы забыли графический ключ:

1. Количество неверных попыток рисования Графического Ключа ограниченно до 5 раз (в различных моделях телефона количество попыток может доходить до 10 раз).

2. После того как вы использовали все попытки, но так и не нарисовали правильно Графический Ключ телефон блокируется на 30 секунд.

3. Телефон запрашивает логин и пароль вашего Gmail-аккаунта.

4. Этот метод сработает только в том случае, если телефон или планшет подключен к Интернету. В противном случае тупик или перезагрузка к настройкам производителя.

PIN - это пароль состоящий из нескольких цифр.

И наконец, Password – самая надежная защита, с возможностью использования букв и цифр. Если вы решили использовать пароль – тогда можно включить опцию Шифрование телефона.

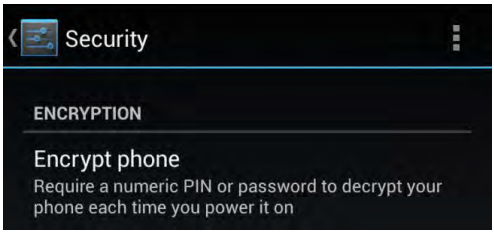
Шифрование памяти телефона

Функция входит в пакет Android версии 4.0* и выше. для планшетов. Но эта функция может отсутствовать во многих бюджетных телефонах.

Позволяет зашифровать внутреннюю память телефона так, чтобы доступ к ней осуществлялся только по паролю или PIN-коду. Шифрование помогает защитить информацию в вашем телефоне в третьем случае (целенаправленная кража). Злоумышленники никак не смогут получить доступ к вашим данным с телефона.

Обязательное условие для использования шифрования – установка блокировки экрана с помощью пароля.

Этим способом достигается сохранение данных пользователя, расположенных в памяти телефона, например телефонной книги, настроек браузеров, паролей, используемых в Интернете, фотографий и видео, которые пользователь получил с помощью камеры и не переписал на SD-карту.



Программа не шифрует при этом SD-карту. Шифрование может занять до часа времени в зависимости от объема памяти устройства.

Возврат к исходному состоянию не предусмотрен. Можно сделать телефону или планшету полный RESET, т.е. переустановить Android, но пользовательские данные из памяти телефона или планшета будут стерты. Таким образом, если злоумышленник не знает пароля для разблокировки телефона, он не сможет им воспользоваться. Невозможно будет также увидеть данные из памяти телефона с помощью других программ, подключив телефон к компьютеру, ведь вся внутренняя память зашифрована. Единственный способ вновь заставить телефон работать – переформатировать его.

Недостатком этой функции:

1. Присутствует, только начиная с Android OS 4.0 – 4.1 и то не на всех моделях телефонах.

Чаще всего встречается в телефонах от Samsung, HTC, Philips. Некоторые китайские модели также имеют функцию шифрования. У Телефонов от HTC эта функция расположена в разделе "Память". У Lenovo – в разделе Безопасность.

2. Требование постоянно вводить довольно сложный пароль (6-10 символов), даже если вы хотите просто позвонить.

3. Невозможно отключить эту функцию, если вы хотите снять защиту. Шифрование отключается только ресетом и возвратом заводских настроек телефона.

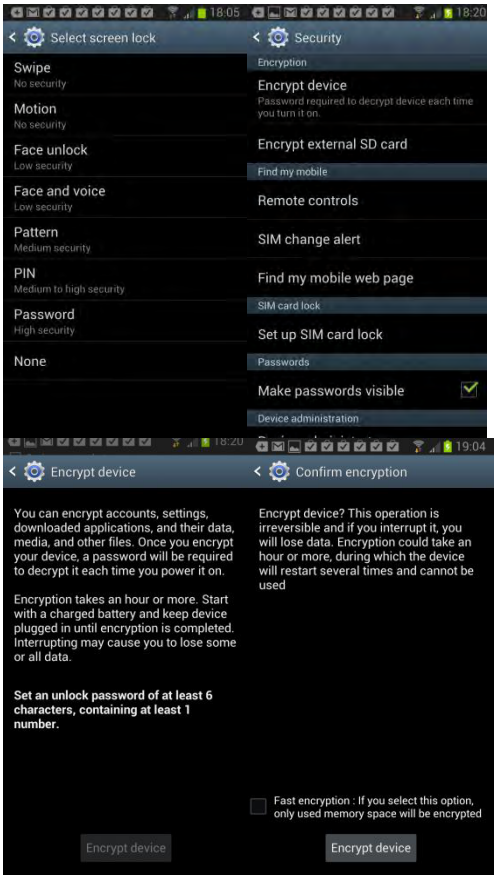
Шифрование внешней SD-карты

Функция входит в стандартный пакет Android 4.1.1 для планшетов. Отсутствует во многих бюджетных сборках.

Функция обеспечивает надежную защиту данных на внешней SD-карте. Здесь могут храниться личные фотографии, текстовые файлы с информацией коммерческого и личного характера.

Позволяет зашифровать файлы на SD-карте, не изменяя их названий, файловой структуры, с сохранением предварительного просмотра графических файлов(иконки). Функция требует установки блокировочного пароля на дисплей длиной не менее 6 символов.

Имеется возможность отмены шифрования. При смене пароля происходит автоматическая перешифровка.



Если пользователь потерял карту памяти, зашифрованные файлы не могут быть прочтены через card-reader. Если ее поставить на другой планшет, где стоит другой пароль, то зашифрованные данные также не могут быть прочтены.

Другие Свойства Шифрования:

Прозрачное шифрование. Если карта вставлена в планшет и пользователь разблокировал экран при помощи пароля, любое приложение видит файлы в расшифрованном виде.

Если подключить планшет через USB-кабель к компьютеру, зашифрованные файлы также можно прочесть на компьютере, предварительно разблокировав карту с экрана мобильного устройства.

Если через card-reader на карту записать какие-то другие незашифрованные файлы, они тоже будут зашифрованы после вставки карты в планшет.

При наличии зашифрованной карты отменить пароль блокировки нельзя.

Данные шифруются на уровне файлов (при этом видны названия файлов, но содержимое файла зашифрованно).

Недостаток программы: отсутствие в большинстве сборок Android.

Следует подчеркнуть, что лучшая сохранность данных – это полная их копия на ПК.

Смартфон достаточно хрупкое устройство небольших размеров, а значит всегда есть вероятность его поломки или потери.

Итак, подведем итоги

Встроенные средства защиты Android являются весьма надежными и удобными инструментами защиты данных на мобильных телефонах и планшетах.

Они способны защитить от посторонних глаз контакты пользователя, его переписку и звонки, аккуанты в различных программах и сетях, а также файлы и папки, расположенные как в памяти телефона, так и на съемной SD-карте.

К недостаткам защиты данных этими программами следует отнести отсутствие их самих в некоторых версиях Android, необходимость использования сложного

PIN-кода или пароля на экране блокировки (Графический Ключ не подходит).

Следует указать также на необратимость шифровки внутренней памяти телефона, т.е. единственный способ отказаться от шифрования – это полный сброс настроек телефона.

Важно! Убедитесь что в случае, если Вы забыли пароль либо Графический Ключ, Вы сможете восстановить доступ к телефону либо сможете легко восстановить настройки телефона и информацию в случае если придется сделать hard reset (сброс телефона в заводские настройки с потерей всех данных).

rohos.ru

Как шифровать файлы в Linux с помощью GPG, Ccrypt, Bcrypt и 7-Zip

В системе Linux есть несколько различных утилит командной строки, которые могут зашифровывать и расшифровывать файлы с использованием пароля, задаваемого пользователем. Такие средства шифрования можно применять во многих случаях, в том числе для шифрования файлов, подготавливаемых для безопасной отправки через интернет, с тем, чтобы не беспокоиться о том, что кто-то третий получит доступ к файлам в случае, если передача данных будет перехвачена.

Прежде чем рассматривать отдельные инструментальные средства, вам нужно убедиться в том, что установлены все соответствующие пакеты. В Ubuntu для установки программ вы должны использовать следующую команду:

```
sudo apt-get install gnupg bcrypt
ccrypt p7zip-full
```

GPG

Пакет GNU Privacy Guard (GPG) является инструментальным средством, предназначенным в первую очередь для шифрования и подписи данных с использованием криптографии с открытым ключом. Тем не менее в нем также есть также возможность выполнять шифрования данных просто с использованием пароля, введенного пользователем, и в нем поддерживаются различные криптографические алгоритмы.

Чтобы с помощью gpg зашифровать файл, в данном случае файл big.txt, введите следующую команду:

```
gpg -c big.txt
```

Вам будет предложено ввести пароль (дважды). В процессе шифрования создается новый файл, который называется

big.txt.gpg. Исходный файл также останется, так что вам потребуется его удалить в случае, если вы намереваетесь сохранить только зашифрованную копию. Если сравнивать размеры исходного и зашифрованный файлов, то вы увидите, что зашифрованный файл будет по размеру меньше. Это происходит потому, что команда gpg сжимает файл во время шифрования. Если файл уже сжат (например, файл .zip или файл .tgz), то зашифрованный файл может, на самом деле, оказаться несколько большим.

Чтобы расшифровать файл, используйте команду:

```
gpg big.txt.gpg
```

По умолчанию файлы, зашифрованные с помощью gpg, будут использовать алгоритм шифрования cast5, который одобрен национальным криптологическим агентством правительства Канады. Однако в утилите gpg также поддерживает ряд других встроенных алгоритмов шифрования, в том числе Triple DES (3DES), который используется в индустрии электронных платежей; Advanced Encryption Standard (AES) – технология шифрования, одобренная Американским национальным институтом стандартов и технологии (NIST); и Camellia - шифр совместно разработанный фирмами Mitsubishi и NTT, который одобрен Европейским союзом и Японией.

Чтобы увидеть список доступных алгоритмов, наберите:

```
gpg --version
```

Список доступных алгоритмов приведен в выданных данных в разделе «Supported algorithms» («Поддерживаемые алгоритмы») ниже тега «Cipher» («Шифр»). Чтобы использовать другой алгоритм, добавьте параметр -crypto-algo, за которым укажите алгоритм, который вы хотите использовать, например, -crypto-algo=3DES

Тогда полная команда будет иметь следующий вид:

```
gpg -c -crypto-algo=3DES big.txt
```

bcrypt и ccrypt

Пакет gpg – это не единственный инструмент шифрования, доступный в системе Linux. В оригинальных системах Unix, была команда под названием crypt, однако уровень безопасности, который она обеспечивала, был очень низким. По аналогии с ней были созданы некоторые другие команды, которыми ее можно заменить, в том числе bcrypt и ccryrpt.

В команде bcrypt используется алгоритм blowfish, в то время как команда ccrypt базируется на шифре Rijndael, который является алгоритмом, используемый для AES. Многие криптоаналитики не рекомендуют далее использовать алгоритм blowfish, т. к. опубликованы некоторые теоретические описания атак, которые его ослабляют, однако для повседневного шифрования, для которого не требуется обеспечить шифрование уровня государственной безопасности (NSA, MI5, FSA), он все еще полезен.

Для шифрования с использованием команды bcrypt:

```
bcrypt big.txt
```

В отличие от команды gpg, команда bcrypt заменит оригинальный файл зашифрованным файлом и добавит в кон-

це имени файла .bfe. Точно также, как и в случае с командой gpg, полученный файл также сжимается и поэтому для несжатых файлов размер файла должен быть значительно меньше. Сжатие может быть отключено с помощью параметра -c.

Для расшифровки файла используйте:

```
bcrypt big.txt.bfe
```

Файл .bfe будет заменен исходным незашифрованным файлом.

Есть два возможных способа вызова команды ccrypt:

непосредственный вызов команды ccrypt с параметрами -e или -d

использовать для шифрования и дешифровки команды ccencrypt и ccdecrypt, соответственно.

Чтобы зашифровать файл введите:

```
ccencrypt big.txt
```

Исходный файл будет заменен файлом big.txt.cpt. В отличие от gpg и bcrypt, выходной файл сжат не будет. Если сжатие необходимо, то можно использовать такие инструменты, как gzip. Предлагаемые расширения для сжатых и зашифрованных файлов - .gz.cpt или .gzc.

Для расшифровки файла используйте:

```
ccdecrypt big.txt.cpt
```

7-Zip

В архиваторе 7-Zip также есть шифрование AES. Чтобы создать зашифрованный архив используйте в команде 7z параметр -p:

```
7z a -p big.txt.7z big.txt
```

Вам будет предложено ввести пароль (дважды). Затем файл будет сжат и зашифрован. Исходный файл останется, точно также, как и с командой gpg, поэтому вам нужно удалить его в случае, если вы хотите сохранить только зашифрованную копию. Преимуществом использования пакета 7-Zip является то, что в одном архиве можно сохранять и зашифровывать несколько файлов и папок.

Заключение

С помощью этих методов сжатия можно зашифровать конфиденциальные данные с достаточной стойкостью с тем, чтобы даже агентства, спонсируемые правительствами, не смогли получить доступ к файлам. Как и во всех случаях использования паролей (используемых в сети или вне сети), применение более длинных паролей обеспечивает лучшую безопасность, чем при использовании коротких паролей.

rus-linux.net

Rootkit Hunter в Ubuntu

Общеизвестный факт – операционные системы, базирующиеся на GNU/Linux, сами вирусами не заражаются. В том числе и Ubuntu. Однако пользователь, особенно неопытный, может установить что-нибудь нехорошее собственноручно, подключив неофициальный источник софта. Тем более что, анонимных PPA («Personal Package Archive») развелось немало.

Также не исключена некоторая вероятность, что в официальных источниках (репозиториях Ubuntu) далеко не все проверено достаточно тщательно. Там ведь десятки тысяч «пакетов». В общем, на всякий случай познакомимся с программой Rootkit Hunter, помогающей выявить наиболее коварное вредоносное ПО – руткиты.

Установка

Условия эксперимента примерно следующие:

1. компьютер с Linux Mint 13 LTS MATE (это Ubuntu 12.04 LTS, немного переделанная ирландскими парнями);

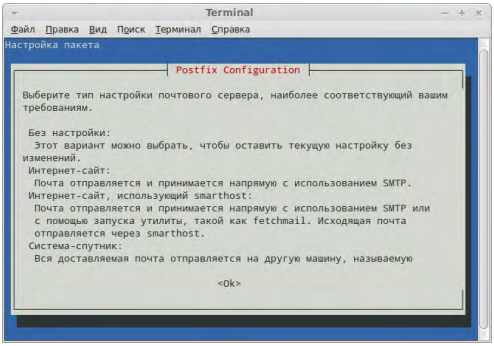
2. софт берем принципиально лишь из упомянутых в преамбуле официальных источников, то есть из репозиториев Canonical и больше ниоткуда;

3. испытываем программы на практике, чтобы все изложенное базировалось на личном опыте.

Программно-техническая база, обозначенная в первом пункте, уже есть, поэтому начинаем сразу со второго. Не ходим по страницам предполагаемых разработчиков Rootkit Hunter, не качаем какие-то архивы со скриптами-установщиками. Вместо этого сразу выясняем, есть ли требующаяся программа в репозиториях Canonical. Оказывается, есть, и получаем ее вот так:

```
sudo apt-get install rkhunter
```

Скачать нужно лишь полдюжины пакетов общим весом около трех с половиной мегабайт. В процессе их установки эмулятор терминала покажет запрос настройки почтового сервера, системы-спутника, интернет-сайта или еще чего-то там. Наша задача – просто произвести сканирование бинарных файлов в Linux Mint, поэтому даже не подумаем что-либо настраивать. Реагируем так:



1. жмем Tab до тех пор, пока кнопка «OK» внизу не станет красной;

2. жмем Enter;

3. выбираем «Без настройки» в следующем списке.

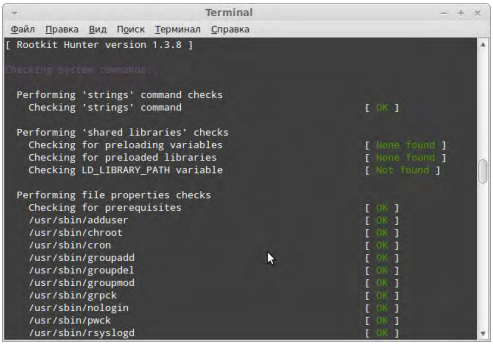
После чего установка продолжится. А когда закончится, сразу можно приступать к проверке.

Запуск Rootkit Hunter

Еще один факт, который полезно иметь ввиду новичкам, – краткую инструкцию по эксплуатации незнакомых программ часто можно получить командой «man имя_программы» в эмуляторе терминала. В нашем случае: man rkhunter (чтобы потом убрать инструкцию, нажимаем клавишу Q). Правда, справка, пожалуй, слишком уж лаконичная для неопытных. Поэтому сразу укажем, как быстро запустить проверку:

```
sudo rkhunter --check
```

Сначала Rootkit Hunter просматривает системные библиотеки, затем берется за содержимое папок usr/sbin и usr/bin. Если все в порядке, ставит зелеными буквами пометки «None found», «Nothing found» и «OK». Если же находит что-то подозрительное, тогда пишет красным «Warning». Ожидаем завершения сканирования и выключаем программу комбинацией клавиш Ctrl+C.



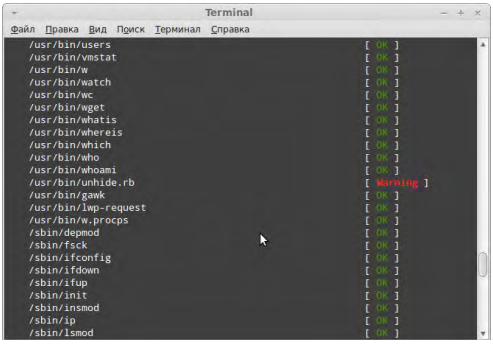
Результаты

Красная пометка «Warning» зажглась напротив файла usr/bin/unhide.rb. Вследствие обращения к поисковой системе Google выяснилось следующее:

1. программа unhide.rb есть в репозиториях Canonical и служит для выявления скрытых процессов;

2. еще в начале 2012-го на англоязычном форуме Ubuntu народ беспокоился о том, что Rootkit Hunter почему-то считает файл unhide.rb опасным (но, как обычно, ничего толкового в ходе обсуждения не выяснили);

3. люди уже загружали сей файл на сервис Virustotal.com, и три человека пометили эту программу как опасную, хотя сканеры ничего не находят.



Как быть? Данная программа в Linux Mint не очень-то нужна, поэтому можно поступить следующим образом:

sudo apt-get purge unhide.rb

То есть удалить ее подчистую.

Rootkit Hunter тоже с легкостью ликвидируется штатными средствами. Например, не закрывая все тот же эмулятор терминала, вот так:

sudo apt-get purge rkhunter && sudo apt-get autoremove

Rootkit Hunter – это не антивирус, это утилита для анализа обстановки. Сканирование запускается с повышенными привилегиями, однако с системой ничего не делает, просто указывает на сомнительные компоненты. Разбираться со всеми тревожными сигналами придется вручную.

Как именно разбираться, если опыта пока мало? Нашлось нечто подозрительное – идем в поисковые системы и выясняем, что это за программа, известна ли людям, существует ли для Ubuntu, так сказать, легально. И нужна ли вообще вам или ОС.

xbb.uz

Yahoo «сломала» почти все списки рассылки в мире

Инженерный совет Интернета обсуждает проблему, что делать с компанией Yahoo. которая на этих выходных изменила запись DMARC на своих серверах и установила новое правило: отказывать в обработке любого письма с адреса @yahoo.com, если оно не проходит проверку DMARC.

DMARC – стандарт для идентификации электронных сообщений принимающими узлами с использованием механизмов Sender Policy Framework (структуры политики отправителя, SPF) и DomainKeys Identified Mail (почты, идентифицируемой при помощи доменных ключей, DKIM). Для большинства случаев система работает отлично, отсекая спамеров и фишеров, которые осуществляют рассылки с поддельными обратными адресами.

Проблема в том, что почтовые списки рассылки никак не могут удовлетворять требованиям DMARC, потому что они всячески модифицируют каждое письмо. Сервер списка рассылки изменяет тему сообщения, удаляет вложенные файлы, изменяет адрес для возвращенных писем и производит другие полезные манипуляции, которые делают невозможным прохождение проверки SPF и DKIM. Значит, по новым правилам DMARC от Yahoo, почтовый сервер обязан вернуть письмо с адресом @yahoo.com.

Почтовый сервер списка рассылки, конечно же, не выполняет требования DMARC, ибо тогда не сможет работать. Он добросовестно пересылает письмо с адреса @yahoo.com всем подписчикам, установив новый адрес для возвращаемых писем. Но письмо не доходит до большинства адресатов, потому что почтовые провайдеры, которые поддерживают DMARC, блокируют его, высылая в ответ техническое сообщение с отказом. Сервер списка рассылки, в свою очередь, если не может доставить письмо и получает отказ от сервера, то исключает адресата из списка рассылки. То есть многие невинные пользователи Gmail, Hotmail и прочих сервисов, сами того не зная, автоматически исключаются из списка рассылки, потому что их сервер заворачивает назад письма из-за новых правил Yahoo.

Таким образом, Yahoo своими действиями нарушила работу всех списков рассылки, в которые пришло хотя бы одно письмо с адреса @yahoo.com. Поскольку Yahoo Mail – вторая по популярности почтовая служба в мире, пострадали почти все списки рассылки.

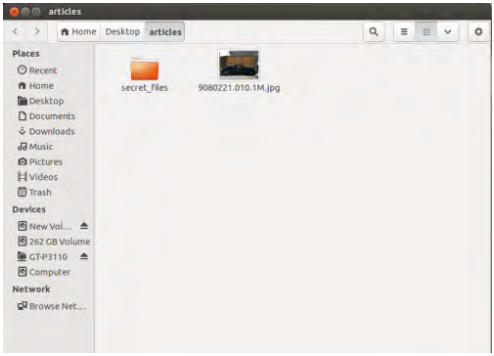
Специалисты из Инженерного совета Интернета рекомендуют изменить настройки серверов списков рассылки, прекратив прием писем с адресов @yahoo.com, а пользователям Yahoo Mail – сменить адрес. Кроме того, имеющих знакомство в компании Yahoo просят разузнать там, может, изменение DMARC было не слишком хорошей идеей?

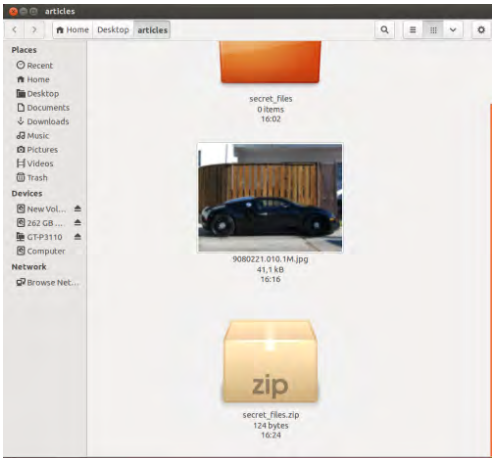
xakep.ru

Стеганография - скрывайте ваши файлы внутри изображений в Linux

В наше время персональный компьютер стал не только рабочим инструментом, но и приватным пространством, где мы храним наши маленькие секреты. Защита наших персональных данных от чьих-то любопытных глаз должна быть одним из приоритетов. Люди используют для этого шифрование, но они забывают, что шифрование не скрывает данные, а позволяет сделать их нечитаемыми для посторонних. Это большая ошибка и она происходит потому, что большинство пользователей никогда не слышали о стеганографии - науки о сокрытии информации. В данной статье мы рассмотрим, как скрывать ваши файлы внутри изображений. Этот метод позволит вам повысить безопасность пересылки данных и не позволит человеку, перехватывающему ваш траффик, понять, что же на самом деле вы передаете. Итак, что требуется для того, чтобы спрятать ваши файлы внутри изображения?

Во-первых, вам нужно изображение в формате JPG, разумеется файлы, которые вы хотите спрятать, и терминал (или эмулятор терминала). Файлы, которые мы будем использовать в качестве примера, показаны ниже. Перед тем, как перейти к основной части, упакуйте ваши файлы в zip-архив и откройте новое окно терминала.



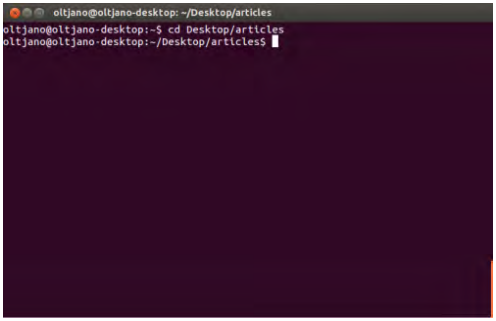


Итак мы будем скрывать архив secret_files.zip внутри изображения 9080221.010.1M.jpg. Мы будем использовать команду cat, которая обычно применяется для таких целей, как вывод файлов, создание новых файлов и так далее. Команда cat прочитает оба наших файла,

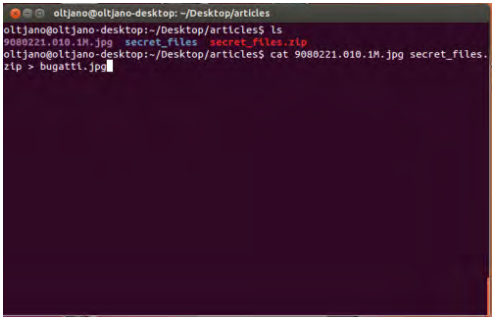
а затем склеит их в один. Открыв терминал, перейдите в директорию, в которой хранится созданный вами архив. У меня это Desktop/articles, поэтому я ввел в терминале

```
cd Desktop/articles
```

и нажал Enter.



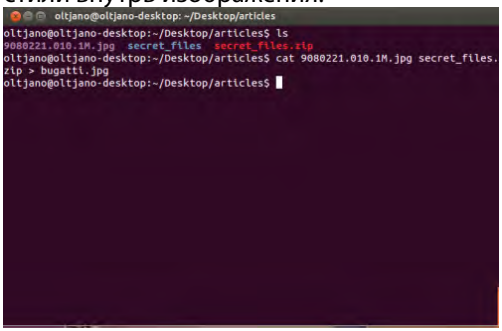
Просмотрите список файлов, находящихся в директории, с помощью команды ls и сохраните имена файлов в каком-нибудь текстовом документе. Позже они нам понадобятся. Теперь спрячем наш архив в изображение.



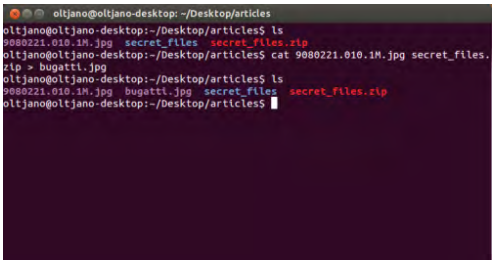
Простое объяснение того, как работает команда на приведенном выше скриншоте:

1. cat читает файл изображения.
2. cat читает zip-архив.
3. cat склеивает изображение и архив вместе в новый файл bugatti.jpg (вы можете поставить любое имя).

Теперь нажмите Enter и будет создан новый файл, который выглядит как обычное изображение, но если мы попробуем открыть его с помощью команды unzip, то можем извлечь архив, который мы поместили внутрь изображения.



Просмотрев содержимое директории с помощью команды ls, мы видим новый файл bugatti.jpg.



Теперь мы спокойно можем удалить исходные файлы. Теперь, чтобы извлечь свои данные из этого изображения, нужно просто воспользоваться командой unzip.

rus-linux.net

Критическая уязвимость в OpenSSL 1.0.1 и 1.0.2-beta

Сотрудники The OpenSSL Project 8 апреля выпустили бюллетень безопасности, в котором сообщается о критической уязвимости CVE-2014-0160 в популярной криптографической библиотеке OpenSSL.

Уязвимость связана с отсутствием необходимой проверки границ в одной из процедур расширения Heartbeat (RFC6520) для протокола TLS/DTLS. Из-за этой маленькой ошибки одного программиста кто угодно получает прямой доступ к оперативной памяти компьютеров, чьи коммуникации «защищены» уязвимой версией OpenSSL. В том числе, злоумышленник получает доступ к секретным ключам, именам и паролям пользователей и всему контенту, который должен передаваться в зашифрованном виде. При этом не остается никаких следов проникновения в систему.

Некто, знавший об уязвимости, мог прослушивать «зашифрованный» трафик почти во всем интернете с марта 2012 года, когда вышла версия OpenSSL 1.0.1. В то время была продемонстрирована успешная атака на TLS (BEAST), и многие перешли на защищенную версию TLS 1.2, появление которой совпало с выходом OpenSSL 1.0.1.

Уязвимая версия OpenSSL используется в популярных веб-серверах Nginx и Apache, на почтовых серверах, IM-серверах, VPN, а также во множестве других программ. Ущерб от этого бага исключительно велик.

Некоторые дистрибутивы операционных систем с уязвимой версией OpenSSL:

- Debian Wheezy (стабильная), OpenSSL 1.0.1e-2+deb7u4)
- Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11)
- CentOS 6.5, OpenSSL 1.0.1e-15)
- Fedora 18, OpenSSL 1.0.1e-4
- OpenBSD 5.3 (OpenSSL 1.0.1c) и 5.4 (OpenSSL 1.0.1c)
- FreeBSD 8.4 (OpenSSL 1.0.1e) и 9.1 (OpenSSL 1.0.1c)
- NetBSD 5.0.2 (OpenSSL 1.0.1e)
- OpenSUSE 12.2 (OpenSSL 1.0.1c)

Дистрибутивы с более ранними версиями OpenSSL: Debian Squeeze (oldstable), OpenSSL 0.9.8o-4squeeze14, SUSE Linux Enterprise Server.

Баг присутствует во всех версиях веток OpenSSL 1.0.1 и 1.0.2-beta, включая 1.0.1f и 1.0.2-beta1. Исправленная версия – 1.0.1g, которую всем пострадавшим необходимо установить немедленно, после чего сгенерировать новые ключи и сертификаты и предпринять прочие меры безопасности. Пользователей следует предупредить о возможной утечке их паролей. В случае невозможности немедленного апдейта на исправленную версию следует перекомпилировать OpenSSL с флагом

-DOPENSSL_NO_HEARTBEATS.

Уязвимость обнаружили специалисты по информационной безопасности из компании Codenomicon, а также, независимо от них, Нил Мехта (Neel Mehta) из подразделения Google Security. Именно последний сообщил разработчикам The OpenSSL Project, что нужно срочно исправить код. Ребята из компании Codenomicon подготовили и даже открыли для него отдельный сайт Heartbleed.com с изображением кровоточащего сердца.

habrahabr.ru

Операция Windigo заразила более 25 тысяч серверов на Linux/UNIX

Исследователи из антивирусной компании ESET со своими коллегами из нескольких европейских агентств зафиксировали в сети крупную атаку «Операция Windigo», которая привела к заражению более 25 тысяч серверов, работающих под управлением ОС GNU/Linux и других UNIX-подобных систем.

По данным отчета, операция Windigo началась еще в конце 2011 года и с тех пор успела найти свое «применение» в инфраструктуре многих организаций (в том числе – cPanel и Linux Foundation) и на широком спектре ОС: Linux (около 60 %), FreeBSD, OpenBSD, Mac OS X и даже Windows через Cygwin. В рамках этой операции ESET рассматривает три основных зловредных компонента, заражающих серверные системы:

Ebury – бэкдор к OpenSSH для управления сервером и получения учетных данных системных пользователей;

Cdorked – бэкдор к веб-серверам (Apache, nginx, lighttpd) для перенаправления веб-трафика;

Calfbot – Perl-скрипт для рассылки спама (он «виноват» в ежедневной отправке более 35 миллионов спам-сообщений по всему миру).

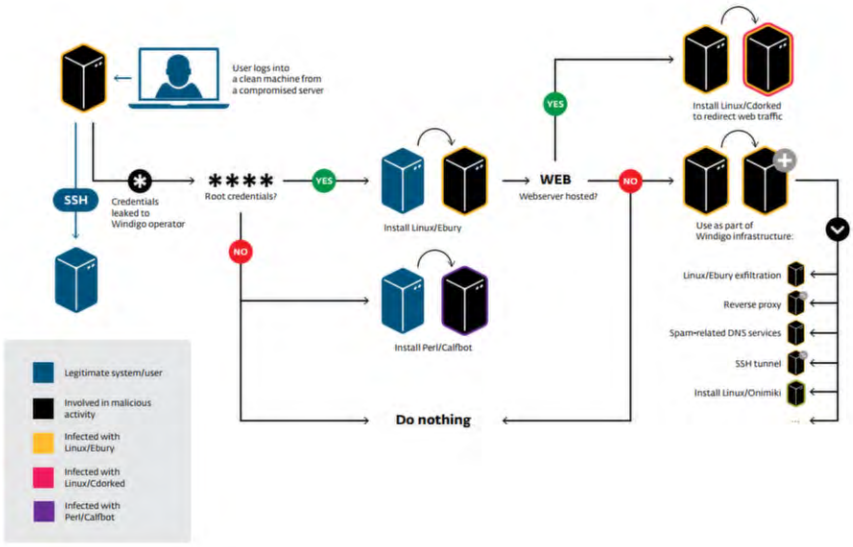
Примечательно, что для достижения своих целей злоумышленники не эксплуатируют уязвимости в безопасности программного обеспечения – для этого использовались лишь различные способы получения паролей для SSH-доступа. В связи с этим, авторы исследования высказывают мнение, что аутентификация на серверах по паролю – архаизм, от которого пора отказаться.

Подробное исследование операции Windigo с хронологией событий и техническими деталями обнаруженных проблем опубликованы в этом отчете ССЫЛКА http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf (PDF; 3,5 Мб).

В связи с этим, а также учитывая тот факт, что более 60 % веб-сайтов во всем мире работают на серверах Linux, специалисты ESET настоятельно рекомендуют веб-разработчикам и системным администраторам проверить системы на наличие угроз для предотвращения дальнейшего распространения «Вендиго». Для этого ИТ-специалистам необходимо запустить следующую команду:

```
$ ssh -G 2>&1 | grep -e illegal
-e unknown > /dev/null && echo
«System clean» || echo «System
infected»
```

nixp.ru



Червь Darlloz поразил около 32 тысяч систем на базе Linux

Компания Symantec провела анализ степени поражения систем червем Linux.Darlloz. Червь был выявлен в ноябре прошлого года и воспринимался как малоопасный прототип, так как для его распространения использовалась база из около десятка типовых паролей и эксплоит для уязвимости в CGI-режиме PHP, исправленной два года назад. Тем не менее, сканирование всего диапазона IP-адресов(!!! Делаем вывод что нас регулярно сканируют все, кому не лень), показало, что червем Linux.Darlloz уже поражено почти 32 тысяч систем.

Присутствие червя удалось идентифицировать благодаря тому, что после проникновения в систему червь запускает http-сервер на порту 58455 и отдает исполняемый файл со своей копией по фиксированному пути. Червь изначально рассчитан на поражение устройств, постоянно подключенных к сети и остающихся без внимания пользователей, которые часто оставляют неизменными заводские параметры входа. В частности, червь поражает домашние маршрутизаторы, точки доступа, телеприставки, web-камеры и сетевые принтеры на базе архитектур x86, ARM, MIPS и PowerPC. Тем не менее, 43% пораженных систем составили работающие под управлением Linux компьютеры и серверы на базе архитектуры x86, и только 38% - специализированные устройства.

Интересно, что в качестве одной из функций червя является майнинг криптовалюты Mincoins и Dogecoins, который выполняется только на Linux-системах с архитектурой x86 и не затрагивает специализированные устройства. При этом злоумышленникам удалось заработать на майнинге всего около 200 долларов.

Дополнительно, можно отметить сообщение в блоге компании Cisco об увеличении интенсивности атак, направленных на поражение давно не обновляемых web-серверов на базе Linux, использующих устаревшие версии ПО. За последние дни выявлено 2700 пораженных систем, при этом 17 и 18 марта фиксировалось поражение около 400 новых хостов в день. После получения контроля над системой, вредоносное ПО осуществляет подстановку платной рекламы и кода для поражения клиентских систем на страницы сайтов, размещенные на пораженной системе. Предполагается для для распространения вредоносного ПО используется какая-то удаленная уязвимость, исправленная в свежих версиях серверного ПО, но проявляющаяся на устаревших системах.

Также выявлены новые варианты вредоносного ПО, поражающего устаревшие системы, подверженные уязвимости в CGI-режиме PHP. Анализ показал, что около 16% всех сайтов используют устаревшие версии PHP (5.3.12- и 5.4.2-), в которых не исправлена уязвимость (не сообщается сколько из этих сайтов использует PHP в режиме CGI и подвержены применению эксплоита).

opennet.ru

Хотите стать частью команды UserAndLINUX?

Если вы давно используете Linux, либо только начали интересоваться продуктами OpenSoure, либо же просто интересуетесь компьютерными и техническими новинками, то мы с радостью примем вас в нашу дружную команду!

Каждый из нас именно так и попал в команду журнала UserAndLINUX – мы просто любим Linux и считаем, что обязаны нести эту любовь в массы. И мы знаем, как отплатить нашей любимой операционной системе – создать сообщество людей с общими интересами, поддерживать друг друга и помогать новичкам в этом интересном деле.

И не имеет значения, опытный ли вы программист, или одаренный школьник, или дизайнер, инженер, секретарь... Ваши идеи в совокупности с нашими могут помочь другим людям узнать, что такое Linux и с чем его едят!

Чем же вы можете нам помочь?

У вас есть творческие способности, креативное чувство стиля? Обладаете вкусом? Создавайте красивые темы и фоны (людям нравятся красивые картинки!) с командой наших дизайнеров!

Владеете иностранным языком? Переводите статьи с англоязычных ресурсов, чтобы наши читателя всегда имели удовольствие читать свежие интервью и новости со всего мира!

Любые навыки, которыми вы владеете, могут помочь команде UserAndLINUX – присоединяйтесь!
Предлагайте свои идеи. Учитесь вместе с нами. Развивайте новые умения, способности.

Спрашивайте. Задавайте вопросы, не стесняйтесь! Нам всегда нужны люди. Не думайте, что вы не сможете помочь, потому что вы не умеете программировать, администрировать или только начинаете работать в Linux как в системе, которая установлена у вас на компьютере.

Существует миллион способов внести свой вклад.
Присоединяйтесь к работе над журналом UserAndLINUX и приложением «Больше чем USER»!

Оставляйте свои вопросы, координаты и описание того, чем бы вы хотели помочь:
magazine@ualinux.com
на форуме ***http://ualinux.com/forum/userandlinux***
в нашей группе Вконтакте - ***https://vk.com/userandlinux***
или группе на Facebook - ***https://www.facebook.com/groups/userandlinux/***

С уважением,
коллектив журнала UserAndLINUX

User And LINUX

UA Linux
open source ■ open future

Адрес журнала в Интернете:
http://ualinux.com/journal

Обсуждение журнала
на форуме:
http://ualinux.com/forum

По вопросам
приобретения журнала:
http://ualinux.com/pay

Адрес редакции:
Украина, 03040,
г. Киев, а/я 56
Email: magazine@ualinux.com

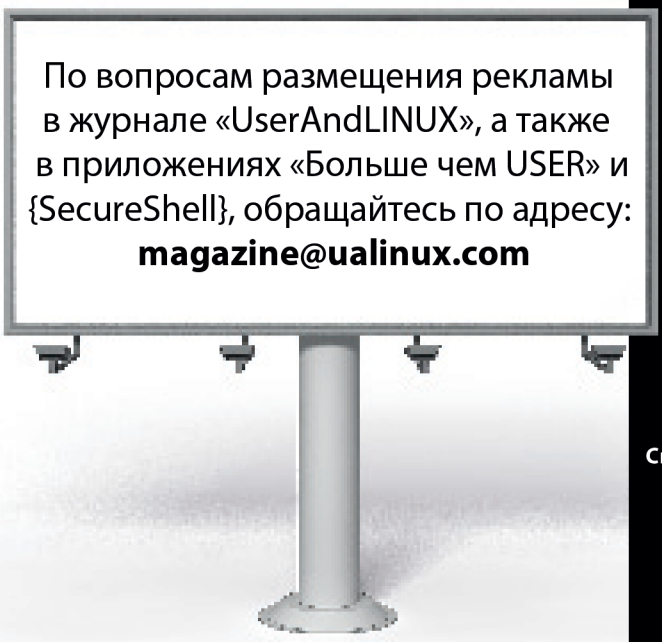
Тип издания:
электронный

Регулярность: ежемесячный
Дата выпуска: 25.04.2014 г.
Тираж: свыше 60 000 загрузок*

*указано среднестатическое ежемесячное суммарное значение, сформированное из полученной статистики загрузок журнала с официального сайта и других известных источников распространения (ftp, http и torrent)

Государственный реестр СМИ
Свид-во: КВ 18270-7070Р от 24.10.2011

Международный стандартный
серийный номер
ISSN: 2223-6988




User
And
LINUX
Больше чем user