

Linux

Создание нового пользователя

- Создание unix-пользователя `useradd -d /home/new_user -s /bin/bash new_user`
- Домашний каталог для нового пользователя

```
mkdir /home/new_user
```

- Установка владельца для домашнего каталога

```
chown new_user:new_user /home/new_user
```

- Задание пароля пользователя

```
passwd new_user
```

Переименование пользователя

Например, инсталлятор Debian'a не позволяет создавать пользователей, чьи имена содержат нижнее подчёркивание, что может идти в разрез с исторически сложившимися традициями с одной стороны, с другой стороны ручное создание пользователя может противоречить требованию единого id пользователя при работе с файловой системой на кластере.

В общем, разные бывают ситуации, иногда переименовать пользователя необходимо, сохранив его id.

- Переименовать пользователя и группу:

```
groupmod --new-name newuser olduser  
usermod --login newuser --home /home/newhome olduser
```

- Переместить домашний каталог

```
mv /home/oldhome /home/newhome
```

- При необходимости заменить имя пользователя в конфигурационных файлах программ пользователя, но желательно переименовывать только новых пользователей.

SSL-сертификат для сайта

[Создание](#) самоподписанного SSL-сертификата состоит из следующих этапов.

1. Приватный ключ сервера.

```
openssl genrsa -des3 -out jurik-phys.net.key 2048
```

2. Запрос на подпись сертификата **Certificate Signing Request**

```
openssl req -new -key jurik-phys.net.key -out jurik-phys.net.csr
```

В поле «Common Name» ввести доменное имя сайта, несколько имён через запятую, или маску сайта, например, *.jurik-phys.net

3. Удаление пароля секретного ключа. Необходимо, чтобы apache при каждом запуске не спрашивал пароль секретного ключа.

```
mv jurik-phys.net.key jurik-phys.net.key.org  
openssl rsa -in jurik-phys.net.key.org -out jurik-phys.net.key
```

4. Генерация самоподписанного сертификата

```
openssl x509 -req -days 365 -in jurik-phys.net.csr -signkey jurik-phys.net.key  
-out jurik-phys.net.crt
```

Внимание! Использование самоподписанного сертификата будет вызывать в браузере предупреждение безопасности

5. Другой вариант - получить (за соответствующую плату) сертификат от центра сертификации, отправив ему на обработку **csr**-файл.
6. Необходимо скопировать сертификаты в каталог, где их ожидает увидеть Apache, настроить SSL сайта, перезапустить Apache.

VNC

Запуск при старте ситемы

В файле /etc/rc.local добавить:

```
su - user_name -c "vncserver -geometry 1920x1080 -depth 24 -deferupdate 0" &
```

Запуск DE (Xfce4) в VNC

В файле ~/.vnc/xstartup

```
exec /usr/bin/xfce4-session &  
# x-terminal-emulator -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &  
# x-window-manager &
```

Terminal: текстовый редактор

- Просмотр возможных альтернатив текстовых редакторов

```
update-alternatives --list editor
```

- Выбор удобного редактора (vim)

```
update-alternatives --config editor
```

- В случае неуспеха (например, тс по прежнему используетиспользует внутренний редактор)

```
select-editor
```

Руссификация

Квадраты в терминале

Русские буквы в консоли Debian/Ubuntu. После очередного обновления можно столкнуться с «квадратами» вместо букв. Решение:

```
dpkg-reconfigure console-setup
```

Выбрать:

```
UTF-8
Combined - Latin; Slavic and non-Slavic Cyrillic
Fixed
Размер по вкусу.
```

Шрифт Fixed т.к., Terminus может отображаться квадратами.

Закрепить результат:

```
update-initramfs -u
```

Дополнительная информация по [ссылке](#).

Переключение раскладки

[Ссылка.1](#), [ссылка.2](#)

Отправка e-mail'а из оболочки

Один из простых способов отправить электронную почту из шелла - использовать консольный почтовый клиент [mutt](#) в связке с внешним smtp сервером.

- Настройка mutt (на примере mail.ru):

```
vim ~/.muttrc
```

```
set imap_user="mail_login"
set imap_pass="mail_password"
set realname = "Printed info"
set smtp_url="smtps://$imap_user@smtp.mail.ru:465"
```

```
set smtp_pass="$imap_pass"
set ssl_force_tls=yes
```

- Скрипт отправки сообщения:

```
vim mail-send.sh
```

```
#!/bin/bash
```

```
subject="Email from bash"
body="This email send using a bash scrip"
from="mail_login@mail.ru"
to="resieve_email@mail.ru"
```

```
echo "Sending email..."
echo "$body" | mutt -s "$subject" -e "my_hdr From:$from" -b $from "$to"
```

- Отправка скрытой копии на адрес отправителя позволяет сохранять отправленные сообщения на удалённом почтовом сервере.

SSH

Запрет логина от root'a

В файле /etc/ssh/sshd_config установить

```
PermitRootLogin no
```

или

```
PermitRootLogin without-password
```

Копирование файлов

На удалённую машину:

```
scp local_file user_name@server_name:/path/to/new/place/
```

С удалённой машины:

Обратно тоже можно:

```
scp user_name@server_name:/path/to/remote_file /local_path/
```

Авторизация по ключу

- Создание открытого и закрытого ключей локальной системы («Enter» для отката от ключевой фразы):

```
ssh-keygen -t rsa
```

- Настройка авторизации ssh по открытому ключу с помощью ssh-copy-id:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@remote
```

- Если ssh-copy-id нет:
 - Копирование открытого ключа на удалённую систему

```
scp ~/.ssh/id_rsa.pub user@remote:id_rsa.pub
```

- Авторизация на удалённом сервере:

```
ssh user@remote
```

- Добавление открытого ключа локальной системы в авторизованные ключи удаленной системы, установка правильных прав, «уборка мусора»:

```
# создаем директорию и даём права
[ -d ~/.ssh ] || (mkdir ~/.ssh; chmod 711 ~/.ssh)

# добавляем открытый ключ
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys

# делаем правильные права
chmod 600 ~/.ssh/authorized_keys

# удаляем не нужное
rm ~/.ssh/id_rsa.pub
```

- Проверка работоспособности на локальном компьютере:

```
ssh user@remote
```

- Запрет логина по паролю:

```
PasswordAuthentication no
```

Эмуляция Socks проху через SSH

```
ssh -D 127.0.0.1:8080 -f -N user.name@remote.domain.name
```

Ошибки подключения

Connection closed by

Образ системы на VPS зачастую идёт с пустыми ключами шифрования, о чём можно судить по ошибкам в /var/log/authorize «No supported key exchange format» и нулевым размерам ключей в /etc/ssh/. Сервис ssh в данном случае не запускается.

Решение заключается в генерации новых ключей:

```
ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key
ssh-keygen -t ecdsa -f /etc/ssh/ssh_host_ecdsa_key
ssh-keygen -t ed25519 -f /etc/ssh/ssh_host_ed25519_key
```

Выполнение команд на удаленном сервере

```
ssh [user]@[server] '[command]'
```

DNSCrypt

Работу DNSCrypt можно оценить через один из сервисов проверки DNS:

- www.perfect-privacy.com/dns-leaktest/
- www.dnsleaktest.com.

Desktop

Net.Storage over Яндекс.Диск

Идея: зарегистрировать N учётных записей [Yandex.Disk](#)'а по 10GB и примонтировать с помощью WebDAV N каталогов, объединить все N каталогов в единое облачное хранилище размером в N*10GB, прикрутить шифрование на стороне клиента и пользоваться сервисом для хранения редко используемых данных.

Особенности регистрации. Похоже, что за один подход лучше не регистрировать более 3-х учётных записей, иначе при переходе в Яндекс.Диск можно словить блокировку (мобильный в помощь):

Доступ временно ограничен

Соответственно, диск через WebDAV не монтируется с ошибкой:

402 Payment Required

Итог. Прежде чем переходить к следующему этапу, необходимо убедиться через Web-интерфейс, что Яндекс.Диск доступен для всех предполагаемых к использованию учётных записей.

Реализация Net.Storage [в статье](#).

Облако Mail.ru

UPDATE: WEBDAV отключён

Подключение

В /etc/fstab, mail_user - имя пользователя

```
https://webdav.cloud.mail.ru/ /mnt/mail.ru davfs
uid=mail_user,file_mode=666,dir_mode=777,user,noauto 0 0
```

В /etc/davfs2/secrets

```
/mnt/mail.ru mail_user@mail.ru "password"
```

Монтирование:

```
mount /mnt/mail.ru
```

Согласно договору, mail.ru получает авторские права на все загружаемые данные, и может использовать их по своему усмотрению. **Данные надо шифровать.**

Шифрование

Например, с помощью EncFS, которая использует директорию для хранения зашифрованных файлов, а не специально подготовленную ФС.

Создадим точку монтирования для расшифрованного каталога:

```
mkdir /mnt/crypt.mail.ru
```

Установка пакета encfs

```
apt-get install encfs
```

Подключение зашифрованного каталога в облаке.

```
encfs /mnt/mail.ru/.encfs /mnt/crypt.mail.ru
```

При первом запуске утилита попросит ввести пароль для шифрования. Если каталог уже зашифрован, то утилита спросит пароль для расшифровки. После этого все операции необходимо производить через /mnt/crypt.mail.ru.

Отключение зашифрованного каталога

```
fusermount -u /mnt/crypt.mail.ru
```

Разное

Разрешить не root пользователям монтировать EncFS.

Файл /etc/fuse.conf:

```
user_allow_other
```

Добавить пользователя в группу fuse

```
usermod -a -G fuse $USER
```

Pulseaudio

Перенаправление звуковых потоков

[Руководство](#) по настройке перенаправления на лету вывода звука приложения между передними выходами звуковой карты (front-left,front-right) и задними выходами (rear-left,rear-right).

Данный способ позволяет подключить к компьютеру акустическую систему на передние выходы, а на задние, например, наушники и при необходимости перенаправлять вывод звука на то или иное устройство.

Однако, как выяснилось, при создании виртуальных sink'ов в /etc/pulse/default.pa, согласно [руководству](#), монофонические файлы не будут слышны при воспроизводстве, увы. Проблема [известная](#) и связанная с тем, что предлагаемый способ требует установки «enable-remixing = no».

Предлагаемое решение состоит в том, чтобы сделать виртуальные sink'и «speakers» и «headphones» не 2-х канальными, а 4-х канальными, с дублированием выходов звуковой карты, но различающимися входами.

Первоначальный вариант при котором монофонические файлы не звучат выглядит так

```
load-module module-remap-sink sink_name=speakers
master=alsa_output.pci-0000_08_05.0.analog-surround-40 channels=2
master_channel_map=front-left,front-right channel_map=front-left,front-right
remix=no
load-module module-remap-sink sink_name=headphones
master=alsa_output.pci-0000_08_05.0.analog-surround-40 channels=2
master_channel_map=rear-left,rear-right channel_map=front-left,front-right
remix=no
```

Изменённый вариант выглядит так:

```
load-module module-remap-sink sink_name=speakers
master=alsa_output.pci-0000_08_05.0.analog-surround-40 channels=4
master_channel_map=front-left,front-right,front-left,front-right channel_map=front-
left,front-right,mono,mono remix=no
load-module module-remap-sink sink_name=headphones
master=alsa_output.pci-0000_08_05.0.analog-surround-40 channels=4
master_channel_map=rear-left,rear-right,rear-left,rear-right channel_map=front-
left,front-right,mono,mono remix=no
```

Замечание первое. sound_card_name для master=<sound_card_name> определяется из вывода команды

```
pacmd list-sinks | grep name
```

Замечание второе. В файле /etc/pulse/daemon.conf необходимо установить enable-remixing = no

Управление потоком Flash'a через PulseAudio

[тыц](#)

Настройка качества звука

Файл /etc/pulse/daemon.conf

```
resample-method = soxr-vhq  
; resample-method = src-sinc-best-quality  
default-sample-format = float32le  
default-sample-rate = 192000  
alternate-sample-rate = 96000
```

Цена улучшения звука - несколько бОльшая загрузка процессора.

Узнать поддерживаемые алгоритмы ресамплинга

```
pulseaudio --dump-resample-methods
```

Проверить текущий формат вывода звука картой

```
cat /proc/asound/card0/pcm0p/sub0/hw_params
```

Звуковой сервер в локальной сети

На звуковом сервере в файле /etc/pulse/default.pa раскомментировать загрузку сетевого модуля и установить авторизацию для локальной сети

```
load-module module-native-protocol-tcp auth-ip-acl=127.0.0.1;192.168.0.0/16
```

На удалённом клиенте запускать приложение в виде

```
PULSE_SERVER=<pulse_servername> <application>
```

Подробности [раз](#), [два](#), [три](#).

Динамическое перенаправление звука на сервер (1)

На клиенте в /etc/pulse/default.pa

```
load-module module-tunnel-sink-new sink_name=edifier server=dirac  
update-sink-proplist edifier device.description="Remote Bum-Bum"
```

Динамическое перенаправление звука на сервер (2)

На сервере /etc/pulse/default.pa

```
load-module module-zeroconf-publish
```

На клиенте /etc/pulse/default.pa

```
load-module module-zeroconf-discover
```

После перезапуска pulseaudio всё работает, но имя принимающего тунеля на сервере будет не очень красивым. Исправление на сервере

```
update-sink-proplist alsa_output.pci-0000_01_01.0.iec958-stereo  
device.description="Edifire R2800"
```

где alsa_output.pci-0000_01_01.0.iec958-stereo device.description определяется из вывода команды `pacctl list`

Микрофон на выход (loopback)

<http://ubuntuforums.org/showthread.php?t=1324135>

<https://s8dragon.wordpress.com/2010/12/26/listen-to-microphone-over-the-speakers-using-pulseaudio/>

<http://ubuntuforums.org/showthread.php?p=8672035″>

Система с несколькими пользователями

Проблема. Звук работает только для первого вошедшего в систему пользователя. У иных пользователей pulseaudio не видит звуковую карту, а следовательно, звука эти пользователи не слышат.

Решение 1. Использовать системный демон pulseaudio

- /etc/pulse/daemon.conf:

```
daemonize = yes  
system-instance=yes  
local-server-type = system
```

- Модуль для systemd, если отсутствует в дистрибутиве /etc/systemd/system/pulseaudio.service

```
[Unit]  
Description=PulseAudio Daemon  
  
[Service]  
Type=forking  
RemainAfterExit=yes  
ExecStart=/usr/bin/pulseaudio -D  
  
[Install]
```

```
WantedBy=multi-user.target
```

```
systemctl enable pulseaudio.service
```

- Добавить пользователя в группу pulse-access:

```
adduser user_name pulse-access
```

Данный способ разработчики рекомендуют избегать, но он самый безглючный в плане звука.

Решение 2. Организовать подключение к пульсе для второго пользователя через unix-сокеты, открываемые первым пользователем. [Источник](#).

/etc/pulse/default.pa:

```
load-module module-native-protocol-unix auth-anonymous=1 socket=/tmp/my-pulse-socket-name
```

У второго пользователя ~/.config/pulse/client.conf:

```
default-server = unix:/tmp/my-pulse-socket-name
```

Минусы. При логине второго пользователя до первого, звука у второго пользователя не будет вовсе т.к, при запуске pulseaudio выдаст ошибку:

```
pulseaudio --start
N: [pulseaudio] main.c: Обнаружен настроенный вручную сервер на %s, отказ от запуска.
```

Pulseaudio не видит USB устройство в списке карт

В файл /etc/pulse/default.pa добавить

```
load-module module-alsa-sink device=hw:X
```

Здесь «X» - индекс звуковой карты, согласно выводу команды

```
aplay -l | grep card
```

[Источник](#)

Kernel

Добавить модуль в initrd

Описание. Системный раздел зашифрован, при загрузке необходимо ввести пароль. Однако usb-клавиатура после начала загрузки ядра и до момента ввода пароля не функционирует.

Решение. Необходимо добавить модули отвечающие за работу подсистемы usb и hid в образ первоначальной загрузки (initrd).

Реализация (debian). Прописать в `/etc/initramfs-tools/modules` необходимые модули.

```
usbcore
usbhid
hid_generic
hid
ehci_pci
ehci_hcd
xhci_hcd
```

Обновить образ начальной загрузки.

```
update-initramfs -u -k all
```

Результат. Добавленные в `initrd` модули инициализируют подсистему USB до монтирования основной ФС, благодаря чему с помощью usb-клавиатуры можно ввести пароль шифрования и продолжить загрузку операционной системы.

Backup

Duplicity:

<https://kamaok.org.ua/?p=1093>;

http://wiki.hetzner.de/index.php/Duplicity_Script/ru;

<http://www.linuxspace.org/archives/5608>.

<https://wiki.debian.org/Duplicity>

<http://blog.geek.km.ua/2012/06/14/shpargalka-po-duplicity/>

<http://serverfault.com/questions/417158/duplicity-recommended-value-for-volsize>

http://wiki.rfremix.ru/index.php/Архивирование_данных_с_помощью_Duplicity

<https://help.ubuntu.com/community/DuplicityBackupHowto>

Xfce

xfce4-appfinder (slow start)

```
xfconf-query -c xfce4-keyboard-shortcuts -p '/commands/custom/<Alt>F2' -s "xfrun4 -  
-disable-server"
```

[Подробнее... v](#)

Проблема системного лотка

Проблема с отображением значков в системном лотке Xfce (Ubuntu). Решение:

- Отключение indicator-application в автозагрузке (снять галочку с Indicator Application).
- Удаление пакета indicator-application.

Автологин в Xfce4 (lightdm)

```
vim /etc/lightdm/lightdm.conf
```

```
[SeatDefaults]
autologin-user=auto_login_user_name
```

Multimedia

Video

- ffmpeg вырезать видео по времени

```
ffmpeg -i ./file.avi -acodec copy -vcodec copy -ss 00:00:00 -t 00:02:13
./new_file.avi
```

Audio

- конвертировать *.m4a to *.flac

```
for file in *.m4a; do avconv -i "$file" -f flac "`basename "$file"
.m4a`.flac"; done
```

- именованье файлов в соответствии с временем создания

```
for file in *.mp3; do id=`stat --format=%Y "${file}"`; mv "${file}"
"${id}}.${file}"; echo $id; done
```

Image

- конвертировать *.png to *.tiff

```
for f in *.png; do convert -colors 2 -colorspace Gray -normalize +dither "$f"
"${f%.*}.tiff"; done
```

Wine|CrossOver

Won't open docx, xlsx

Проблема: Не открываются docx, xlsx документы.

Решение: `update-binfmts -disable jar`

[Подробнее...](#)

Squid and VPS

<http://nikhgupta.com/code/installing-squid-proxy-server-on-centos-5-vps/>

По-умолчанию все внешние соединения с проху запрещены (при необходимости учитывать):

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all
```

Boot Flash Windows 7

Создание загрузочной флешки Windows 7 из-под Linux'a:

<https://romantelychko.com/blog/352/>

<http://blog.mind-x.org/2011/02/live-usb-windows-7-linux.html>

Восстановление загрузчика

Linux [Grub 2]

Способ №1

1. Загрузка с LiveCD (Linux)
2. Монтирование корня восстанавливаемой системы

```
mount /dev/sda1 /mnt
```

3. Монтирование служебных каталогов в базовую систему

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

```
mount --bind /sys /mnt/sys
```

4. Смена корня загруженной системы

```
chroot /mnt
```

5. Восстановление загрузчика

```
update-grub
```

или

```
grub-install /dev/sda
```

```
grub-mkconfig -o /boot/grub/grub.cfg
```

6. Перезагрузка.

Способ №2

1. Загрузка с LiveCD (Linux).
2. Монтирование корня или /boot-раздела восстанавливаемой системы:

```
mount /dev/sda1 /mnt/custom
```

3. Восстановление загрузчика:

```
grub2-install /dev/sda
```

4. Перезагрузка.
5. Из меню grub осмотреться командой «ls»;
6. Настроить параметры загрузки и убедиться, что загрузчик видит файлы модулей:
 1. для /boot-раздела:

```
set prefix=(hd0,1)/grub
set root=(hd0,1)
ls /grub
```

2. для /-раздела:

```
set prefix=(hd0,1)/boot/grub
set root=(hd0,1)
ls /boot/grub
```

7. Если файлы модулей видны, то подключаем необходимые:

```
insmod ext2
insmod normal
```

8. Переводим grub в полнофункциональный режим:

```
normal
```

9. Выбрав необходимый пункт появившегося меню, загружаем систему.
10. Окончательно восстанавливаем загрузчик из рабочей системы:

```
grub2-install --root-directory=/ /dev/sda
```

Способ №3

Загрузиться с установочного диска в режим восстановления, согласно [инструкции](#) [дистрибутив Debian].

- To access rescue mode, select rescue from the boot menu, type rescue at the boot: prompt, or boot with the rescue/enable=true boot parameter.

Windows 7

1. Загрузка с установочного диска
2. Вызов командной строки Shift+F10
3. В зависимости от «тяжести» случая выполнить

```
Bootrec.exe /FixMbr
```

```
Bootrec.exe /FixBoot
```

```
Bootrec.exe /RebuildBcd
```

4. Перезагрузка.

Suspend

Windows

Предотвращение отключения usb и переход в настоящий suspend. Мануал [тут](#).

OpenVPN

Создание удостоверяющего центра

Система пользовательских сертификатов, центра сертификации и БД отозванных сертификатов называется PKI - Public Key Infrastructure.

На стороне сервера создается корневой сертификат [ca.crt] и закрытый ключ [ca.key].

- Корневой сертификат [ca.crt] раздается всем клиентам. Служит для проверки подписи сертификатов клиента и сервера центром сертификации.
- Корневой закрытый ключ [ca.key] используется для подписи сертификата сервера и всех клиентских сертификатов.

Для создания корневого сертификата и закрытого используется утилита `easy-rsa` из состава OpenVPN [`/usr/share/doc/openvpn/examples/easy-rsa`]. Начиная с версии 2.3 данную утилиту из пакета удалили, поэтому после установки отдельного пакета примеры лежат в `/usr/share/easy-rsa`. Путь к каталогу с PKI не должен содержать пробелов.

```
source ./vars
./clean-all
./build-ca
```

Последняя команда [`build-ca`] создаст корневой сертификат [`ca.crt`] и приватный ключ центра сертификации [`ca.key`], вызвав интерактивную команду `openssl`.

Большинство запрошенных параметров установлены в значения по умолчанию взятые из файла `vars`, `common name` - единственный параметр, который должен быть явно указан.

Дополнение. Для избежания ошибки вида: *The <someName> field needed to be the same in the CA certificate and the request* необходимо отредактировать поле `<someName>`, изменив его с «match» на «optional» в файле `openssl.cnf`. [Подробнее](#).

Генерация сертификата и приватного ключа OpenVPN сервера

Аналогично, с помощью утилиты `easy-rsa` генерируются сертификат сервера [`server.crt`] и закрытый ключ сервера [`server.key`]:

```
./build-key-server server
```

Большинство параметров могут быть оставлены в значениях по умолчанию, явного ввода требует параметр `Common name`, можно ввести «server». Два других запроса требуют положительных ответов, «Sign the certificate? (Подписать сертификат?) [y/n]» и «1 out of 1 certificate requests certified, commit? (заверен 1 из 1 запросов на сертификацию, фиксировать?) [y/n]».

Генерация параметров Diffie Hellman'a

Для сервера OpenVPN необходимо создать параметры Diffie Hellman'a:

```
./build-dh
```

Создание ключей для клиентов

```
source ./vars
./build-key client_somename
```

Нюансы Android [раз](#), [два](#).

Основные файлы

Созданные ключи и сертификаты расположены в каталоге `keys`.

Имя файла	Где необходим	Назначение	Секретный
ca.crt	сервер + все клиенты	Корневой СА-сертификат	НЕТ
ca.key	машина для подписи ключей	Корневой СА-ключ	ДА
dh{n}.pem	только сервер	Параметры Diffie Hellman'a	НЕТ
server.crt	только сервер	Сертификат сервера	НЕТ
server.key	только сервер	Ключ сервера	ДА
client1.crt	только клиент1	Сертификат клиента1	НЕТ
client1.key	только клиент1	Ключ клиента1	ДА
client2.crt	только клиент2	Сертификат клиента2	НЕТ
client2.key	только клиент2	Ключ клиента2	ДА

При подготовке материала по OpenVPN использовались источники: opennet.ru, habrahabr.ru, wiki.525.su, debian-help.ru

Настройка клиента (tap - интерфейс)

Файл /etc/openvpn/newton.conf

```
client
dev-type tap
dev vpn0
proto udp

remote AA.BB.CC.DD

resolv-retry infinite
persist-key
persist-tun
comp-lzo
ns-cert-type server
mute-replay-warnings

ca /etc/openvpn/key/ca.crt
cert /etc/openvpn/key/newton.crt
key /etc/openvpn/key/newton.key

script-security 3 system

up /etc/openvpn/dhcp.sh
down /etc/openvpn/dhcp.sh

verb 0
```

Файл dhcp.sh

```
#!/bin/bash
#

[ -x /sbin/dhclient ] || exit 0

case $script_type in
```

```
up)
    # set mac address for tap interface
    ip link set dev ${dev} address 92:56:cd:85:43:d7
    # echo "Your mission should you choose to accept it:"
    # echo "dhclient -v ${dev}"
    # echo "You have 30 seconds...GO!"
    dhclient -v "${dev}" &
    ;;
down)
    echo "Releasing ${dev} DHCP lease."
    dhclient -r "${dev}"
    ;;
esac
```

Запрет на изменение resolv.conf при старте OpenVPN

Подсмотрено [здесь](#). Создать ловушку для обхода изменения /etc/resolv.conf, путём создания файла /etc/dhcp/dhclient-enter-hooks.d/nodnsupdate следующего содержания:

```
#!/bin/sh
make_resolv_conf(){
:
}
```

Сделать его исполняемым:

```
chmod +x /etc/dhcp/dhclient-enter-hooks.d/nodnsupdate
```

Данный скрипт заменяет функцию replace make_resolv_conf() на изменённую, которая ничего не делает.

Также может понадобиться отключить обновление dns в NetworkManager'e (см. [ссылку](#)).

Wi-Fi и OpenVPN

Особенность. OpenVPN релизован в виде tap интерфейса, сеть openvpn входит в домашнюю подсеть 192.168.93.xxx.

Задача.

1. При подключении к домашнему Wi-Fi не подключать OpenVPN т.к. нет необходимости в поднятии туннеля до домашней локальной сети.
2. При подключении к иной Wi-Fi сети подключать OpenVPN, поднимая тем самым туннель до домашней локальной сети, а следовательно и её сетевым ресурсам.

Решение.

Запускать¹⁾ OpenVPN²⁾ при подключении Wi-Fi, проверяя SSID текущей сети, отключать OpenVPN при закрытии Wi-Fi.

Запуск отключение реализуется через параметры Network Manager'a в файле /etc/NetworkManager/dispatcher.d/01ifupdown:

```

up|vpn-up)
    export MODE="start"
    export PHASE="post-up"
    #####
    /etc/openvpn/vpn_status_test
    #####
    run-parts /etc/network/if-up.d
    ;;
down|vpn-down)
    export MODE="stop"
    export PHASE="post-down"
    #####
    /etc/init.d/openvpn stop &
    #####
    run-parts /etc/network/if-post-down.d
    ;;

```

/etc/openvpn/vpn_status_test:

```

#!/bin/bash

# jurik_phys@jabber.ru - ssid домашней сети
local_wifi=`/sbin/iwconfig wlan0 | /bin/grep -c "jurik_phys@jabber.ru"`
# 192.168.93.5 - домашний ip для ethernet порта ноута
local_wire=`/sbin/ifconfig eth0 | /bin/grep -c "192.168.93.5"`

if [ $local_wifi == "1" ] || [ $local_wire == "1" ]; then
    # echo "Home network. OpenVPN will be stop now"

    # SysV init version
    # /etc/init.d/openvpn stop

    # SystemD version
    systemctl stop openvpn@tesla
else
    # SysV init version
    # vpn_not_run=`/etc/init.d/openvpn status | /bin/grep -c "not running"`

    # SystemD version
    vpn_not_run=`systemctl status openvpn@tesla | grep -c "inactive"`

    if [ $vpn_not_run == "1" ]; then
        # echo "Intranet and OpenVPN not running. OpenVPN will be start"

        # SysV init version
        # /etc/init.d/openvpn restart

        # SystemD version
        systemctl start openvpn@tesla
    fi
fi

```

Steam

Locale en_US проблема

[Решение вопроса](#)

Missing library: libc.so.6

Решение на [LOR'e](#)

Cool Reader 3 (Debian)

Проблема. Версия [cr3-3.0.56](#) с сайта проекта мало того, что не проходит по зависимостям (приходится вытаскивать содержимое deb-пакета), так ещё и не сохраняет настройки пользователя, пытаясь сохранить их в системном каталоге `/usr/share/cr3`.

Решение. Использовать [данную](#) версию из репозитория Alt Linux'a. Содержимое rpm пакета также придётся доставать вручную. Правда в дебиане потребуется собрать библиотеку [libpng15.so](#) и положить ещё в `/usr/lib`.

SystemD

Руководство администратора по [SystemD](#) от RH. Рассуждения справедливы для Debian 8 «Jessie».

Также хороший обзорный материал, [SystemD in Action](#).

OpenVPN and NetworkManager

Запуск OpenVPN после появления connect'a в NetworkManager'e (конфигурация openvpn расположена в `/etc/openvpn/newton.conf`):

1. Создать каталог

```
/etc/systemd/system/openvpn@newton.service.d
```

2. В каталоге создать файл NetworkManager-dependency.conf, следующего содержания

```
[Unit]
After=NetworkManager-wait-online.service wpa_supplicant.service
```

3. Включить сервис NetworkManager-wait-online

```
systemctl enable NetworkManager-wait-online.service
```

P.S. OpenVPN подключение поднимается не средствами NetworkManager из-за того, что при

использовании tap сетевого интерфейса NM не может получить сетевые параметры из openvpn-сети через dhclient ([Bug #297707](#)).

Кириллица в именах юнитов

<http://forum.russianfedora.pro/viewtopic.php?f=15&t=6686>

Монтирование NFS при старте системы

Случай управления сетью через systemd-networkd

1. Проверка статуса сервиса контроля доступности сети:

```
systemctl is-enabled systemd-networkd-wait-online.service
```

2. Включение сервиса в случае его неактивности:

```
systemctl enable systemd-networkd-wait-online.service
```

Случай доступа к файловому серверу через OpenVPN

1. Создание mount-юнита. Имя юнита соответствует пути к точке монтирования, например, /mnt/openvpn/public соответствует:

```
/etc/systemd/system/mnt-openvpn-public.mount
```

2. Содержание mount-юнита

```
[Unit]
Description=Mount NFS over OpenVPN (public)
After=openvpn@newton.service

[Mount]
What=192.168.XX.YY://storage/public
Where=/mnt/openvpn/public
Type=nfs4
Options=rsize=8192,wsizе=8192,timeo=5

[Install]
WantedBy=multi-user.target
```

Следует отметить, что в данном случае nfs монтируется из OpenVPN сети после установления связи.

В категории Options важным параметром является timeo=5, без него монтирование не происходит, а в логах systemd упоминается об истекшем timeout при монтировании ресурса.

3. Включение mount-юнита в systemd:

```
systemctl enable mnt-openvpn-public.mount
```

Готово, при загрузке системы и удачном подключении openvpn в каталог /mnt/openvpn/public будет автоматически примонтирован удалённый ресурс 192.168.XX.YY:/storage/public.

Однако на этом настройка не закончена, ибо, система при выключении будет вставать в ступор на несколько минут, пытаясь отключить удалённый ресурс... Такой же ступор будет наблюдаться и при установке libvirt-daemon... В общем, очередной [Bug #1438612](#).

Отключение NFS при выключении системы

Обход [бара #1438612](#) связанного с ранним отключением dbus.service реализуется дополнением зависимостей к сервису NetworkManager, для чего:

1. Необходимо создать каталог

```
/etc/systemd/system/NetworkManager.service.d
```

2. Внутри каталога создать conf-файл

```
nfs-shutdown-unmount.conf
```

следующего содержания:

```
[Unit]
After=dbus.service
```

В итоге выключение системы должно нормализоваться.

Управление сетью

[systemd-networkd](#).

SecuringNFS

<https://wiki.debian.org/SecuringNFS>

Networkd Wait Online

1. Перейти на управление сетью через systemd-networkd.
2. [Включить](#) systemd-networkd-wait-online

```
systemctl enable systemd-networkd-wait-online
```

Использование screen

<http://s.arboreus.com/2008/01/screen.html>

Opera Browser

Flash don't start automatically

Флеш не стартует автоматически при включённом Opera Turbo. Решение - отключить Opera Turbo.

Настройка NFS

<http://debian-help.ru/articles/nastroika-nfs-servera-debian/>

Основы mdadm

Установка ОС на LVM поверх Raid-1

1. Удаление с помощью fdisk'a существующих разделов на /dev/sd{a,b} и создание одного большого типа «fd».
2. Создание массивов:

```
mdadm --create /dev/md0 --level=1 --raid-device=2 --metadata=0.90 /dev/sda1  
/dev/sdb1
```

3. Создание LVM:

```
pvcreate /dev/md0  
vgcreate hdd /dev/md0  
lvcreate -n root -L 34G hdd  
lvcreate -n swap -L 3.26 hdd
```

4. Ожидание окончания синхронизации массивов:

```
watch -n 1 cat /proc/mdstat
```

5. В дальнейшем установка Debian'a проходит в штатном режиме. К /dev/hdd/root подключить точку монтирования »/«, к /dev/hdd/swap - раздел подкачки. (Если установщик автоматически не соберёт raid+lvm, то его не сложно собрать через разметку диска установщика).
6. После установки ОС необходимо установить загрузчик и на второй диск:

```
grub-install /dev/sdb
```

Уменьшение размера Raid-1

Дано:

1. `df -h`


```
/dev/md5 424G          11G 414G    3% /home
```

2. **cat** /proc/mdstat

```
md5 : active raid1 sdb2[0] sda2[1]
      451684216 blocks super 1.2 [2/2] [UU]
```

Рейд1 /dev/md5 смонтирован в каталог /home и содержит данные пользователей, размер 414ГБ;

Задача: Уменьшить размер домашнего каталога до 14 ГБ и на оставшихся 400ГБ поднять raid-1 для хранения данных.

Решение:

1. Размонтировать /home:

```
umount /home
```

2. Пометить один из дисков сбойным:

```
mdadm /dev/md5 --fail /dev/sdb2
```

```
cat /proc/mdstat
```

```
Personalities : [raid1]
md5 : active raid1 sdb2[0](F) sda2[1]
      451684216 blocks super 1.2 [2/1] [_U]
```

3. Удалить сбойный диск из массива:

```
mdadm /dev/md5 --remove /dev/sdb2
```

```
cat /proc/mdstat
```

```
Personalities : [raid1]
md5 : active raid1 sda2[1]
      451684216 blocks super 1.2 [2/1] [_U]
```

4. Удалить раздел /dev/sdb2, создать два раздела (тип FD) на 4ГБ и 420 ГБ с помощью [fdisk'a](#):

```
fdisk /dev/sdb
```

```
fdisk -l /dev/sdb
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1	*	2048	73402367	36700160	fd	Linux raid autodetect
/dev/sdb2		73402368	81790975	4194304	fd	Linux raid autodetect
/dev/sdb3		81790976	976773167	447491096	fd	Linux raid autodetect

5. Возможно необходимо перечитать таблицу разделов:

```
partprobe
```

6. Создать массив под /home и /mnt/srv.misc:

```
mdadm --create /dev/md12 --level=1 --raid-devices=2 missing /dev/sdb2
mdadm --create /dev/md13 --level=1 --raid-devices=2 missing /dev/sdb3
```

```
cat /proc/mdstat
```

```
Personalities : [raid1]
md13 : active (auto-read-only) raid1 sdb3[1]
      447359872 blocks super 1.2 [2/1] [_U]
md12 : active (auto-read-only) raid1 sdb2[1]
      4192192 blocks super 1.2 [2/1] [_U]
```

7. Форматировать блочные устройства в требуемую ФС, настроит её параметры:

```
mkfs.ext4 /dev/md12
mkfs.ext4 /dev/md13
```

```
tune2fs -m 0 /dev/md12
tune2fs -m 0 /dev/md13
```

8. Остановить массива:

```
umount /home
mdadm --stop /dev/md5
```

9. Удалить раздел /dev/sda2, создать два раздела (тип FD) на 4ГБ и 420 ГБ, перечитать таблицу разделов (см. выше).

10. Добавляем к деградированным raid-1 массивам созданные разделы:

```
mdadm /dev/md12 --add /dev/sda2
mdadm /dev/md13 --add /dev/sda3
```

```
cat /proc/mdstat
```

```
Personalities : [raid1]
md13 : active raid1 sda3[2] sdb3[1]
      447359872 blocks super 1.2 [2/1] [_U]
      [>.....] recovery = 4.5% (20240576/447359872)
      finish=85.7min speed=83028K/sec
md12 : active raid1 sda2[2] sdb2[1]
      4192192 blocks super 1.2 [2/1] [_U]
      resync=DELAYED
```

Видно, что разделы подхватились массивами и запустился поочерёдный процесс синхронизации raid-массивов. На данном этапе уже можно работать с массивами, но желательно дождаться завершения синхронизации.

Замена диска в RAID-1

Подробности в статье по ссылке <https://anikin.pw/all/zamena-dika-v-programnom-raid1-v-linux/>

Bash перенаправление потоков

0 - stdin
1 - stdout
2 - stderr

```
prog 1>log 2>err
```

```
#stderr в stdout:  
2>&1
```

Дисковые квоты

<https://www.ibm.com/developerworks/ru/library/l-lpic1-v3-104-4/>

USB Flash I/O

Запись на flash-накопители (ограничение буфера) [ссылка](#).

Настройка KDE

Пропадают эффекты Kde4

```
KWin has detected that your OpenGL library is unsafe to use, falling back to  
XRender.  
kwin(5744): Failed to initialize compositing, compositing disabled
```

Решение. В ~/.kde/share/config/kwinrc OpenGLUnsafe=true изменить на false (см. [ссылку](#)).

Обновление дистрибутива

Импортирование нового открытого ключа:

```
apt-key adv --recv-keys --keyserver keys.gnupg.net KEY-ID
```

Прикладное ПО

- [Hugin](#).

FB2 в Firefox

По умолчанию, firefox не позволяет сразу открыть файл FictionBook (fb2) в сторонней программе, предлагая сохранить его на диск. Решение в добавлении типа файлов «fb2» в настройки браузера.

Для этого необходимо добавить в файл `mimeTypes.rdf`, находящийся в профиле пользователя, следующие строки:

```
<RDF:Description RDF:about="urn:mimetype:application/x-fictionbook+xml"
                  NC:fileExtensions="fb2"
                  NC:description="документ FictionBook"
                  NC:value="application/x-fictionbook+xml"
                  NC:editable="true">
  <NC:handlerProp RDF:resource="urn:mimetype:handler:application/x-fictionbook+xml"/>
</RDF:Description>
```

Основой приведённого описания файлов FictionBook является описание zip архива.

1)

Предполагается, что сервис OpenVPN не стартует при запуске системы.

2)

Файл конфигурации `/etc/openvpn/tesla.conf`

From:

<https://jurik-phys.net/> - **Jurik-Phys.Net**

Permanent link:

<https://jurik-phys.net/itechnology:linux?rev=1602055559>

Last update: **2020/10/07 10:25**

