Linux

Создание нового пользователя

- Новый unix-пользователь

```
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
```

- Логин под новым пользователем

```
su new_user
```

Переименование пользователя

Например, инсталятор 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.

- Переменовать 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 конфигурационнфх файлах программ пользователя, но желательно переименовывать только новых пользователей.

Общее локальное хранилище

1. Группа (data) пользователей общего локального ресурса

```
groupadd data
```

2. Каталог локального ресурса

```
mkdir /mnt/data
```

3. Подключение каталога /mnt/data/
4. Установка gid и группы data на каталог

```
chmod 2775 /mnt/data/
chown root:data /mnt/data/
```

5. Добавление пользователей в группу «data»

```
usermod -a -G data user_name
```

6. Настройка прав доступа для вновь создаваемых каталогов

```
setfacl -R -m g::rwx /mnt/data
# show result
getfacl /mnt/data
```

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 **C**ertificate **S**igning **R**equest

```
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 Apahce.

Также инструкция от DigitalOcean ссылка .

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, mc 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

Сслыка.1, ссылка.2

Отправка e-mail'а из оболочки

Один из простых способов отправить электронную почку 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 scritpt"
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.

Отправка online сообщения через Телеграм

1. Создание собственного бота:
    - добавить в список пользователей @BotFather'a;
    - начать с ним разговор и выполнить команду /newbot;
    - установить человеко читаемое имя бота (name);
    - установить уникальное имя бота (username) вида @super_messages_bot;
    - сохранить в надёжном месте полученный TokenID созданного бота.
2. Создание группы и добавление в неё бота
    - Рекомендация. В диалоге с @BotFather'ом в разделе «Bot Settings» запретить добавление приватного бота в сторонние группы настройкой «/setjoingroups»
3. Активирование созданной группы, путём написания «/bla-bla-bla for @super_messages_bot»;
4. Определение ID группы или «chat id»;
    - В браузере необходимо перейти по ссылке вида https://api.telegram.org/botTokenID/getUpdates. Внимание на «bot» перед TokenID.
    - В полученном сообщении находим раздел «chat» и в нём запись «id:» < -1234...>. Отрицательное число и есть искомый «chat id»
5. Отправка сообщения с помощью curl:

```
curl -X POST "https://api.telegram.org/botXXX:YYYY/sendMessage" -d "chat_id=-zzzzzzzzzz&disable_notification=false&text=My sample text"
```

Сообщение с компьютера пришло на телефон в «телегу».

SSH

Запрет логина от root'a

В файле /etc/ssh/sshd_config установить

```
PermitRootLogin no
```

или оставить возможность логина через публичные ключи, запретив логин через пароль

```
PermitRootLogin prohibit-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 откака 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 локальный 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 ~/id_rsa.pub >> ~/.ssh/authorized_keys

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

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

- Проверка работоспособности на локальном компьютере:

```
ssh user@remote
```

- Запрет логина по паролю:

```
PasswordAuthentication no
```

Socks5 proxy через SSH

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

Постоянный туннель через autossh

- Установка autossh:

```
# apt install autossh
```

- Настройка доступа по ключу к <host> для пользователя <user>

```
ssh-copy-id -i ~/.ssh/id_rsa.pub <user>@<host>
```

- systemd unit

```
/etc/systemd/system/autossh-socks5-proxy-<host>-<port>.service
```

```
[Unit]
Description=Auto up socks5 proxy
After=network.target

[Service]
Environment=REMOTE_USER=<remote_user>
Environment=REMOTE_HOST=<host>
User=<local_user>
Restart=on-failure
RestartSec=15
ExecStart=/usr/bin/autossh -M 0 -N -o "ExitOnForwardFailure=yes" \
                                   -o "ServerAliveInterval=30" \
                                   -o "ServerAliveCountMax=3" \
                                   -D 127.0.0.1:8080 \
                                   ${REMOTE_USER}@${REMOTE_HOST}
[Install]
WantedBy=multi-user.target
```

- включение systemd unit'a

```
systemctl enable autossh-socks5-proxy-<host>-<port>.service
```

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]'
```

Отвал SSH при простое

На некоторых каналах связи при отсутствии активности ssh соединение зависает. Решение заключается в посылке внутри ssh канала пустых пакетов между клиентом и сервером.

- SSH-server: `/etc/ssh/sshd_config`

```
TCPKeepAlive yes
ClientAliveInterval 30
ClientAliveCountMax 99999999
```

- SSH-client: `/etc/ssh/ssh_config` или `.ssh/config`

```
Host *
   ServerAliveInterval 10
```

Shellinabox

Shellinabox - это программа, реализующая шелл доступ к linux-серверу через браузер

Установка

```
apt install shellinabox
```

Проверка

```
https://192.168.XX.XX:4200
```

Запрет root логина через shellinabox

1. Использовать ssh для логина **/etc/default/shellinabox**

```
SHELLINABOX_ARGS="--no-beep --service=/:SSH"
```

2. Запрет root логина в ssh **/etc/ssh/sshd_config**

```
PermitRootLogin prohibit-password
```

3. Появившиеся предупреждения не критичны, но при желании можно пересобрать пакет с небольшими правками кода ссылка .

WebSSH

Shellinabox всем хорош, но ломает отображение Midnight Commander'a. Выход использовать альтернативу WebSSH написанную на Python'e. Есть определённые различия в философии двух подходов, последний по умолчанию предполагает возможность подключения к любому серверу с поднятого инстанса, это надо иметь в виду, чтобы не сделать общедоступного ssh-proxy от вашего имени.

Применение сертификата Let's Encrypt

Для *shellinabox* требуется специальный комбинированный сертификат с определённым названием

```
cat /etc/letsencrypt/live/*domain.name*/fullchain.pem
/etc/letsencrypt/live/*domain.name*/privkey.pem > /var/lib/shellinabox/certificate-
*domain.name*.pem
```

Проверка работоспособности

```
systemctl stop shellinabox.serivce
shellinaboxd -v
```

Особенность. Для работы shellinabox необходимо существование сертификата с названием файла *certificate.pem*, на который можно делать символические ссылки вида certificate-*domain.name*.pem.

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'a 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.

Nextcloud

Ошибка удаления/переименования файлов из-за блокировки файлов, тыц

Решение.

```
 'filelocking.enabled' => false
```

Отключить ~~кривую~~ блокировку файлов в файле config.php, ссылка

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 монитровать 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 выводы, 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_stereo
master=alsa_output.pci-0000_0a_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_stereo
master=alsa_output.pci-0000_0a_05.0.analog-surround-40 channels=2
master_channel_map=rear-left,rear-right   channel_map=front-left,front-right
remix=no
```

Задать человеческие названия каналам можно следующим образом:

```
update-sink-proplist speakers_stereo   device.description="Speakers [Stereo]"
update-sink-proplist headphones_stereo device.description="Headphones [Stereo]"
```

Изменённый вариант (моно звук) выглядит так:

```
150 load-module module-remap-sink sink_name=speakers_mono
master=alsa_output.pci-0000_0a_05.0.analog-surround-40 channels=2
master_channel_map=front-left,front-right channel_map=front-left,front-left
remix=no
151 load-module module-remap-sink sink_name=headphones_mono
master=alsa_output.pci-0000_0a_05.0.analog-surround-40 channels=2
master_channel_map=rear-left,rear-right   channel_map=front-left,front-left
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'а 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 pactl 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&#8243

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:

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

- Модуль для systemd, если отсутсвует 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

Остановка pulseaudio

```
systemctl --user stop pulseaudio.socket; systemctl --user stop pulseaudio.service
```

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

Образ диска и сжатие

Пример использования: системыне sd-карты на Raspberry Pi.

```
#dd if=/dev/sdX status=progress bs=1M | bzip2 --best > ./$(date
+%Y%m%d_%H%M%S)_sdX-backup.bz2
```

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

- конвертироварть *.m4a to *.flac

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

- именование 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 proxy 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'а:
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.

Частная сеть предприятия

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. После установки данного 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.

Из соображений безопасности и работоспособности коннекта сертификаты должны быть на алгоритме sha256. Проверка сертификата удостоверяющего цента

```
openssl x509 -in ca.crt -noout -text | grep Signature
```

Генерация сертификата и приватного ключа 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]».

Исправление ошибки

- `Error checking x509 extension`

```
./build-key-server server
Ignoring -days without -x509; not generating a certificate
Error checking x509 extension section server
```

- В раздел `X509 Subject Field` файла «vars» добавить

```
export KEY_ALTNAMES="altServerName"
```

- В разделе `[server]` файла openssl.cnf параметр subjectAltName привести к виду

```
subjectAltName="DNS:$ENV::KEY_ALTNAMES"
```

Генерация параметров Diffie Hellman'a

На стороне сервера необходимо создать параметры Diffie Hellman'a:

```
./build-dh
```

Дополнительная проверка пакетов "рукопожатия" TLS (v1)

```
openvpn --genkey secret keys/ta.key
```

Файл ta.key должен быть доступен как на сервере, так и на клиент. При этом в конфигурации необходимо добавить

```
tls-auth ta.key N
```

, где параметр N должен принимать значение «0» на одной стороне и «1» на другой. Например, если на сервере N = «0», то на клиенте N должен быть установлен в «1».

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 CA-сертификат	НЕТ
ca.key	машина для подписи ключей	Корневой CA-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 misson 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.

Запускать[1] OpenVPN[2] 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
```

Смена шифра на AES-256-CBC

https://openvpn.net/vpn-server-resources/change-encryption-cipher-in-access-server/

Обрыв соединения на VPS

- (Возможно) Снижение MTU на внешнем интерфейсе VPS до 1200
- (Возможно) Шейпинг трафика

```
tc qdisc add/change/ dev ens3 root tbf rate 15mbit burst 1214 latency 50ms
```

- Корректировка максимального размера TCP сегмента (источник):

```
iptables -t mangle -I POSTROUTING -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
```

ChatGPT объясняет:

- **-t mangle:** параметр указывает таблицу iptables, с которой мы работаем. В данном случае используется таблица mangle. Таблица mangle используется для изменения пакетов на уровне маршрутизации.
- **-I POSTROUTING:** параметр указывает на цепочку iptables в таблице mangle, в которую будет вставлено правило. В данном случае, правило будет вставлено в цепочку POSTROUTING, которая применяется к пакетам, когда они покидают сетевой интерфейс после прохождения таблицы NAT.
- **-p tcp:** параметр указывает на протокол, которому принадлежат пакеты, к которым применяется правило. В данном случае, это TCP.
- **-tcp-flags SYN,RST SYN:** параметр определяет условие, которое должны соответствовать TCP-пакеты, чтобы быть совпадающими с правилом. Здесь мы говорим, что пакеты должны иметь только установленные флаги SYN и RST.
- **-j TCPMSS –clamp-mss-to-pmtu:** параметр указывает действие, которое необходимо выполнить, если пакеты соответствуют условию. Здесь мы говорим, что пакеты должны пройти обработку

модулем TCPMSS с параметром –clamp-mss-to-pmtu. Это позволяет автоматически настроить максимальный размер TCP сегмента (MSS) таким образом, чтобы он не превышал максимальный размер передаваемого блока данных (PMTU) на маршруте. Это полезно для предотвращения фрагментации пакетов при прохождении через маршрутизаторы с разными MTU.

Получение внешнего IP без DNS запроса

```
curl -s --resolve icanhazip.com:443:104.16.184.241 --max-time 3
https://icanhazip.com
```

Маршрутизация

Дано. На роутере работает vpn-клиент с ip-адресом шлюза 10.73.73.1; доступ в интернет получен через usb-модем со шлюзом 192.168.0.1; локальная сеть роутера представлена подсетью вида 192.168.6.0/24. При установлении vpn-соединения трафик всех клиентов из локальной сети 192.168.6.0/24 по умолчанию заворачивается в vpn.

Задача. Клиенту с ip-адресом 192.168.6.49 предоставлять интернет без использования vpn-соединения.

Решение.

```
# Добавление правила для обработки трафика от 192.168.6.49 таблицей маршрутизации "100"
ip rule add from 192.168.6.49 table 100

# Добавление маршрута по умолчанию через usb-модем (usb0) в таблице 100
ip route add default via 192.168.0.1 dev usb0 table 100
```

Полезные команды

```
# Просмотр основной таблицы маршрутизации
ip route show
```

```
# Просмотр таблицы маршрутизации 100
ip route show table 100
```

```
# Просмотр активных правил маршрутизации
ip rule show
```

Steam

Locale en_US проблема

Решение вопроса

Missing library: libc.so.6

Решение на LOR'е

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 соответсвует 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,wsize=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 установки libvirt-daemon... В общем, очередной Bug #1438612.

Отключение NFS при выключении системы

Обход бага #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

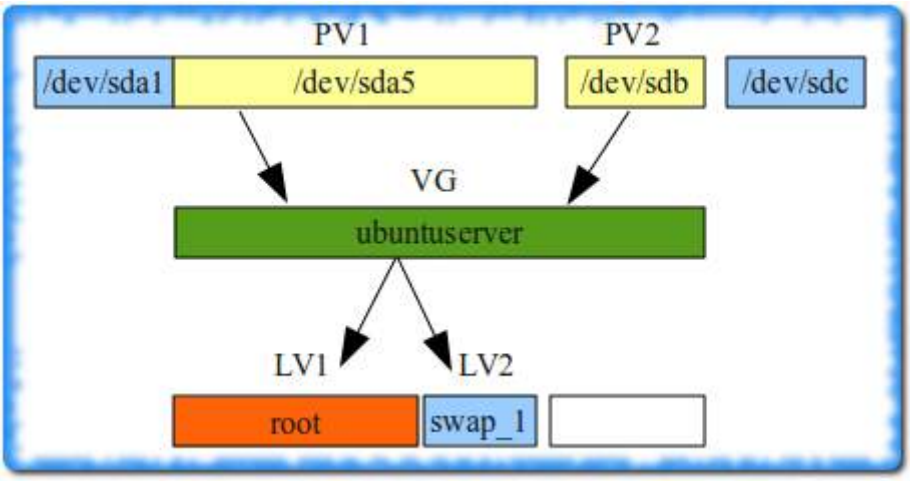
http://debian-help.ru/articles/nastroika-nfs-servera-debian/

Основы mdadm

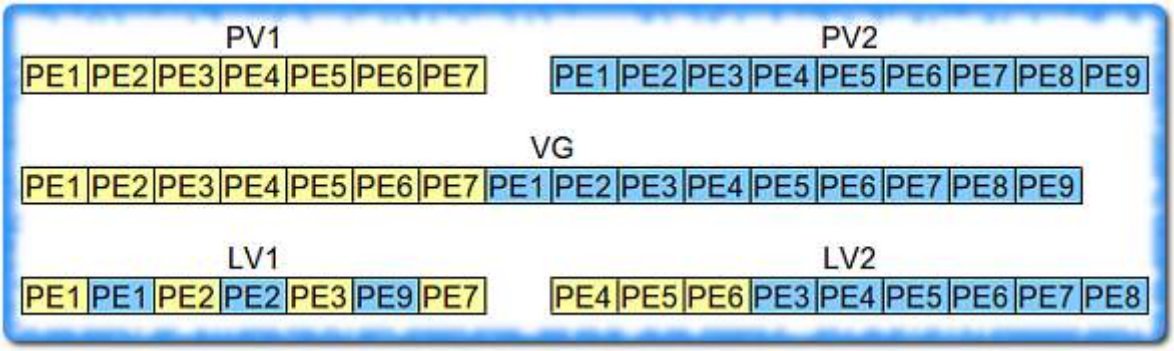
Создание RAID-1 + LVM

Основная терминология LVM

- **PV** (Physical Volume/Физический том) для системы LVM - это реальный физический диск или раздел диска, который инициализирован командой **pvcreate**. Основа для VG - Volume Group.
- **VG** (Volume Group/Группа томов) - это логическая единица которая образуется в результате объединения PV. Можно понимать, как аналог неразмеченного жесткого диска в не-LVM системе.
- **LV** (Logical Volume/Логический том) - раздел на VG, представляющий собой блочное устройство, может содержать файловую систему.



- **PE** (Physical extent) - блок данных в пространстве PV фиксированного размера, по умолчанию PE равен 4 Мб.
- **LE** (Logical extent) - блоки данных, из которых состоит логический том. Размер логических экстентов не меняется в пределах VG и совпадает с размером физических экстентов. Существует возможность указать тип соответствия PE и LE (линейное или чередующееся)



Источники: раз, два, три

Создание RAID-1

Рекомендуется создавать массив на разделах с типом FD (Linux RAID), что позволит ядру автоматически собирать разделы при загрузке системы (см. раз, два, три).

Для этого, например, для диска sda в fdisk'e (fdisk /dev/sda) необходимо:

- **g** создать новую таблицу разделов GPT;
- **n** добавить новый раздел;
- **t** изменить тип раздела на «Linux RAID»;
- **w** записать изменения на диск.

Можно создавать raid-массив:

```
mdadm --create /dev/md<N> --level=1 --raid-device=2 /dev/sd<A><K> /dev/sd<B><K>
```

После создания стартует процесс начальной синхронизации (initial resync), который работает в фоне и не препятствует нормальному использованию raid-массива, но лучше дождаться завершения синхронизации перед активным использованием созданного raid-массива.

Сохранение информации о созданном массиве

```
mdadm --examine --scan
...
ARRAY /dev/md/<N>  metadata=1.2 UUID=071e1eec:c0224deb:edbe49f1:e7620e05
name=maxwell:2
```

Отсутствующую строку с /dev/md/<N> необходимо добавить в /etc/mdadm/mdadm.conf и выполнить обновление initramfs

```
update-initramfs -u
```

Инициализация физических разделов под LVM. В данном случае - это созданный ранее raid-1.

```
pvcreate /dev/md<N>
# Просмотреть результат
pvscan
```

Создание группы разделов (VG) LVM.

```
vgcreate -v storage /dev/md<N>
# Просмотреть результат
vgdisplay
```

Создана группа томов с именем «storage»

Создание логического тома под файловую систему. При этом, если планируется использование LVM снапшотов, размер логического тома (LV) необходимо выбирать исходя из необходимости наличия свободного места в группе томов (VG) для функционирования снапшотов.

```
lvcreate --size <XXX>G --name vol1 storage
```

```
# Просмотреть результат
lvdisplay
vgdisplay
```

Источник: раз.

Создание файловой системы на логическом томе. Если файловая система не будет использоваться под системные нужды, то резервирование места для файлов пользователя «root» можно отключить, также при дальнейшем использовании снапшотов рекомендуется монтировать файловую систему с параметром **noatime** для избежания избыточных изменений основной фс и их записи в снимок.

```
mkfs.ext4 -m 0 -L storage /dev/storage/vol1
```

Изменение размера LV. Ниже производится увеличение (+) размера логического тома на 5ГБ

```
lvresize --resizefs --size +5G /dev/storage/vol1
```

Создание снимка логического тома (LV)

Как работают снапшоты LVM и какие данные записываются на диск при работе со снапшотами можно прочитать по ссылке. Кратко, новые блоки пишутся в оригинальный раздел, а те данные, что должны остаться неизменными, но изменились, копируются в изначальном виде в снапшот, поэтому в группе логических томов (VG) должно быть свободное место под созданный снапшот.

Создание снапшота с выделением под него всего свободного места на VG

```
lvcreate -l 100%FREE --snapshot --name vol1.snap /dev/storage/vol1
# Просмотреть результат
lvs
lvdisplay
```

Полученный снимок может быть примонтирован, как обычное блочное устройство

```
mount -o noatime /dev/storage/vol1.snap /mnt/storage.snap/
```

Удаление снимка. После резервного копирования или иных процедур, снапшот должен быть удалён т.к., его наличие отрицательно сказывается на скорости основной файловой системы.

```
lvremove -y /dev/storage/vol1.snap
```

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 загруузчик 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 замер 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/

/dev/mdX -> /dev/mdY

Переименовать raid-массив
https://delightlylinux.wordpress.com/2019/07/27/md127-how-to-rename-a-raid-array-with-mdadm/

Проверка диска на плохие сектора

При размере диска более 2TB можно столкнуться с ошибкой «Value too large for defined data type invalid end block»

```
badblocks -svw /dev/sda
badblocks: Значение слишком велико для такого типа данных invalid end block
(13672382464): must be 32-bit value
```

Быстрое решение - использовать иной размер блока, например, «badblock -b 4096» вместо значения по умолчанию «1024», где значение 4096 можно получить из вывода команды «blockdev –getbsz /dev/sda», ссылка .

```
badblocks -svw -b 4096 /dev/sda
```

Bash

Перенаправление потоков

0 - stdin
1 - stdout
2 - stderr

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

```
#stderr в stdout:
2>&1
```

Алиасы

С точки зрения администрирования удобно все используемые алиасы располагать в отдельном файле, обычно это файл ~/.bash_aliases

Необходимо помнить, что данный файл должен быть загружен через ~/.bashrc

```
if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi
```

Для ручной загрузки алиасов можно использовать команду source ~/.bash_aliases

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 OpenGLIsUnsafe=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.

Benchmark

Память

Скорость записи

```
sysbench memory --memory-block-size=1G --memory-total-size=50G --memory-oper=write
--threads=1 run | grep transferred
```

Скорость чтения

```
sysbench memory --memory-block-size=1G --memory-total-size=50G --memory-oper=read -
-threads=1 run | grep transferred
```

1)
Предполагается, что сервис OpenVPN не стартует при запуске системы.
2)
Файл конфигурации /etc/openvpn/tesla.conf