

## Настроить резервирование серверов. Подготовить план восстановления.

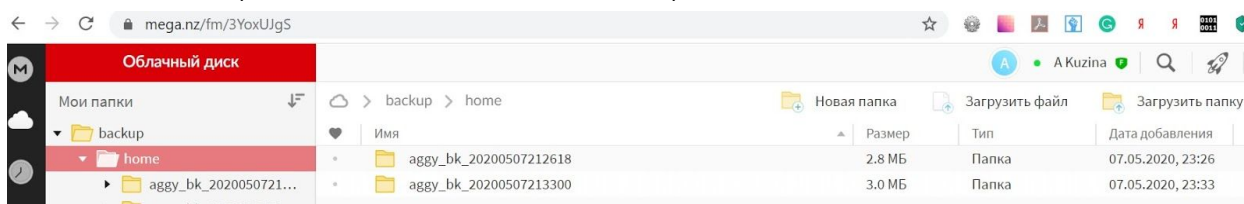
Для организации периодических бэкапов было сделано следующее:

- 1) Принято решение сохранять файлы в облако.
- 2) открыт экаунт в системе облачного резервирования mega.nz
- 3) Скачана из git и скомпилирована утилита MEGAcmd. Для компиляции пришлось вручную скачать множество дополнительных пакетов, согласно инструкции по сборке.

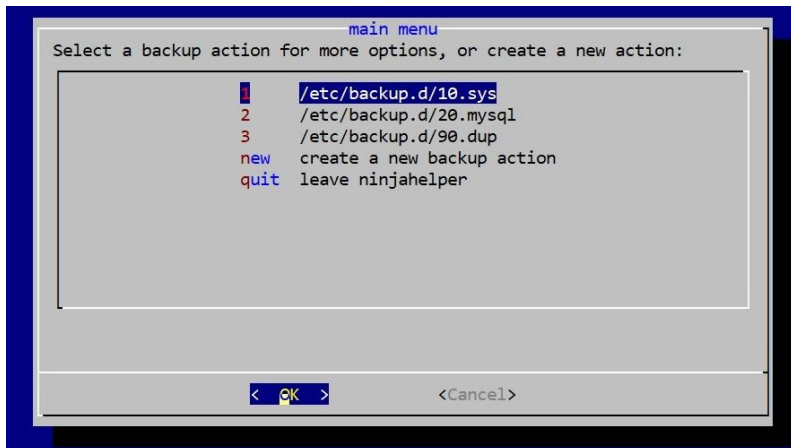
```
aggy@gb: ~$ mega-cmd
=====
                    MEGAcmd
=====
Welcome to MEGAcmd! A Command Line Interactive and Scriptable
Application to interact with your MEGA account.
Please write to support@mega.nz if you find any issue or
have any suggestion concerning its functionalities.
Enter "help --non-interactive" to learn how to use MEGAcmd with scripts.
Enter "help" for basic info and a list of available commands.
=====
[Initiating server in background. Log: /home/aggy/.megaCmd/megacmdserver.log]
aglayaq@gmail.com:/$ backup -l
TAG      LOCALPATH                                     REMOTEPARENTPATH      STATUS
7        /home/aggy                                           /backup/home          ACTIVE
Max Backups: 24
Period: "0 33 * * * *"
Next backup scheduled for: Thu, 07 May 2020 22:33:00 +0000
-- CURRENT/LAST BACKUP --
FILES UP/TOT  FOLDERS CREATED      PROGRESS
0/0           0                      0.00/0.00 B 0.00%
aglayaq@gmail.com:/$
```

- 4) Для тестирования сконфигурирован следующий план бэкапов для домашней директории:

- Раз в день (оставляем последние 31 копию),
- Раз в час (оставляем последние 24 копии)

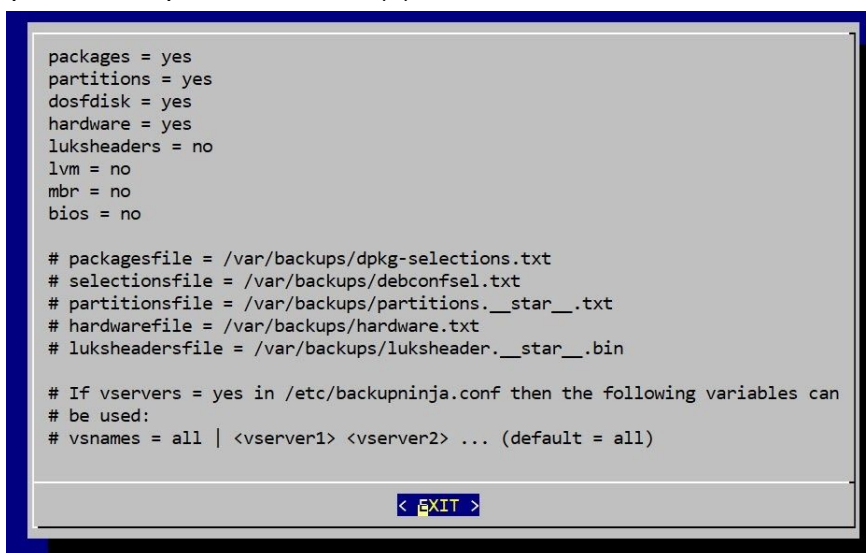


- 5) Выяснилось, что для работы backup необходимо mega-cmd-server, который убивается после выхода из утилиты megacmd, но если запустить mega-backup, то он запускает сервер, который не останавливается при закрытии сессии.
- 6) Из-за нестабильной работы mega-backup (требуется работы дополнительного сервера (который останавливается) принято решение воспользоваться другой системой - backupninja.
- 7) Установлен backupninja и пакеты по зависимостям.
- 8) С помощью утилиты ninjahelper создан backup план.



Вначале сохраняются

файлы настройки системы (1),



потом делается дамп всем базам данных mysql (2),

```
### backupninja MySQL config file ###

# hotcopy = < yes | no > (default = no)
# make a backup of the actual database binary files using mysqlhotcopy.
hotcopy = no

# sqldump = < yes | no > (default = no)
# make a backup using mysqldump. this creates text files with sql commands
# sufficient to reconstruct the database.
#
sqldump = yes

# sqldumptions = <options>
# (default = --lock-tables --complete-insert --add-drop-table --quick --
# arguments to pass to mysqldump
# sqldumptions = --add-drop-table --quick --quote-names

# compress = < yes | no > (default = yes)
# if yes, compress the sqldump output.
compress = no

# dbhost      = <host> (default = localhost)

# backupdir = <dir> (default: /var/backups/mysql)
# where to dump the backups. hotcopy backups will be in a subdirectory
# 'hotcopy' and sqldump backups will be in a subdirectory 'sqldump'
backupdir = /var/backups/mysql

# databases = <all | db1 db2 db3 > (default = all)
# which databases to backup. should either be the word 'all' or a
# space separated list of database names.
databases = all

dbusername = root
```

и в завершение делается инкрементный бэкап файлов,

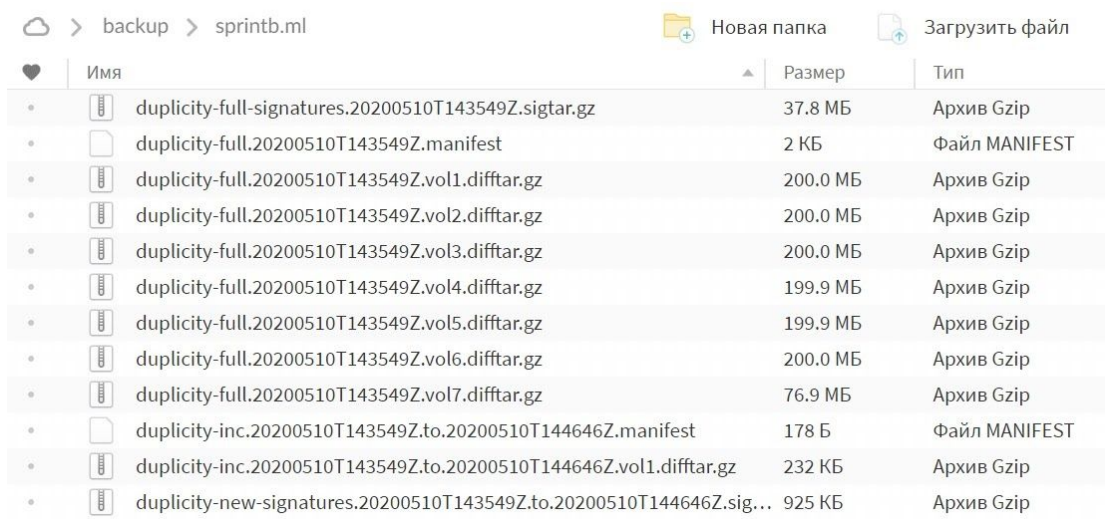
```
# files to include in the backup
#include = /var/spool/cron/crontabs
#include = /var/backups
include = /boot
include = /etc
include = /home
include = /root
include = /lib
include = /lib64
include = /opt
include = /sbin
#include = /usr/local/bin
#include = /var/lib/dpkg/status*
include = /var
include = /var
```

```
# files to exclude from the backup
exclude = /home/*/.gnupg
exclude = /home/*/.local/share/Trash
exclude = /home/*/.Trash
exclude = /home/*/.thumbnails
exclude = /home/*/.beagle
exclude = /home/*/.aMule
exclude = /home/*/.gtk-gnutella-downloads
exclude = /var/cache/backupninja/duplicity
exclude = /var/lock/backupninja

exclude = /cdrom
exclude = /dev
exclude = /media
exclude = /mnt
exclude = /proc
exclude = /run
exclude = /sys
exclude = /tmp
exclude = /usr/tmp
exclude = /var/tmp
exclude = /var/lib/lxcfs
```

включая дампы mysql. Для корректной работы файлового бэкапа необходимо правильно указать каталоги подлежащие сохранению и те папки, которые необходимо исключить, например такие, как: /proc, /sys и другие. Инкрементный файловый бэкап выполняется утилитой duplicity, которую запускает менеджер backupninja.

- 9) В процессе настройки выяснилось, что облачное хранилище mega недавно изменило протокол и стандартная версия сторонней утилиты megatools, доступная в виде пакета ubuntu, не работает. По этой причине была скачана и установлена последняя тестовая версия megatools.
- 10) В результате тестового запуска все задачи бэкап-плана были выполнены успешно и файлы были закачаны в облачное хранилище. Повторный запуск подтвердил корректную работу инкрементного бэкапа (судя по размерам дополнительных файлов).



Имя	Размер	Тип
duplicity-full-signatures.20200510T143549Z.sigtar.gz	37.8 МБ	Архив Gzip
duplicity-full.20200510T143549Z.manifest	2 КБ	Файл MANIFEST
duplicity-full.20200510T143549Z.vol1.diff.tar.gz	200.0 МБ	Архив Gzip
duplicity-full.20200510T143549Z.vol2.diff.tar.gz	200.0 МБ	Архив Gzip
duplicity-full.20200510T143549Z.vol3.diff.tar.gz	200.0 МБ	Архив Gzip
duplicity-full.20200510T143549Z.vol4.diff.tar.gz	199.9 МБ	Архив Gzip
duplicity-full.20200510T143549Z.vol5.diff.tar.gz	199.9 МБ	Архив Gzip
duplicity-full.20200510T143549Z.vol6.diff.tar.gz	200.0 МБ	Архив Gzip
duplicity-full.20200510T143549Z.vol7.diff.tar.gz	76.9 МБ	Архив Gzip
duplicity-inc.20200510T143549Z.to.20200510T144646Z.manifest	178 Б	Файл MANIFEST
duplicity-inc.20200510T143549Z.to.20200510T144646Z.vol1.diff.tar.gz	232 КБ	Архив Gzip
duplicity-new-signatures.20200510T143549Z.to.20200510T144646Z.sig...	925 КБ	Архив Gzip

- 11) Данное решение конечно нельзя назвать оптимальным и много вопросов не было решено. Таких, как: защита файлов бэкапа от взлома, сохранение на различные

носители, отсутствие единого интерфейса с информацией о том, какие бэкапы были выполнены или завершились с ошибкой. Тем не менее данный подход кажется менее трудоемким и более легким в сопровождении, нежели создание своих собственных скриптов с запуском из кронтаб.

- 12) Из-за недостатка времени проверка полного восстановления после краха не производилась.

---

## Тюнинг сервера

В конфиг nginx добавляем следующее

Максимальный размер буфера для хранения тела запроса клиента  
`client_body_buffer_size 1K;`

Максимальный размер буфера для хранения заголовков запроса клиента  
`client_header_buffer_size 1k;`

Максимальный размер тела запроса клиента, прописанный в поле Content-Length заголовка. Если сервер должен поддерживать загрузку файлов, это значение необходимо увеличить  
`client_max_body_size 1k;`

Количество и размер буферов для чтения большого заголовка запроса клиента  
`large_client_header_buffers 2 1k;`

Таймаут при чтении тела запроса клиента  
`client_body_timeout 10;`

Таймаут при чтении заголовка запроса клиента  
`client_header_timeout 10;`

Таймаут, по истечению которого keep-alive соединение с клиентом не будет закрыто со стороны сервера  
`keepalive_timeout 5 5;`

Таймаут при передаче ответа клиенту  
`send_timeout 10;`

Ограничиваем количество доступных методов обращения к Web-серверу  
`if ($request_method !~ ^(GET|HEAD|POST)$ ) {  
return 444;  
}`

Блокируем менеджеры загрузки

```
if ($http_user_agent ~* LWP::Simple|BBBike|wget) {  
return 403;  
}
```

Блокируем некоторые типы ботов

```
if ($http_user_agent ~* msnbot|scrapbot) {  
return 403;  
}
```

Блокируем Referrer-спам

```
if ( $http_referer ~* (babes|forsale|girl|jewelry|love|nudist|organic|poker|porn|sex|teen) )  
{  
return 403;  
}
```

В sysctl внесены следующие параметры

```
net.ipv4.tcp_timestamps = 1  
net.netfilter.nf_conntrack_tcp_loose=0  
net.netfilter.nf_conntrack_max=2000000  
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.all.secure_redirects = 0  
net.ipv4.conf.all.send_redirects = 0  
net.ipv4.tcp_max_orphans = 65536  
net.ipv4.tcp_fin_timeout = 10  
net.ipv4.tcp_keepalive_time = 1800  
net.ipv4.tcp_keepalive_intvl = 15  
net.ipv4.tcp_keepalive_probes = 5  
net.ipv4.tcp_max_syn_backlog = 4096  
net.ipv4.tcp_synack_retries = 1  
net.ipv4.tcp_orphan_retries = 0  
net.ipv4.tcp_sack = 1  
net.ipv4.tcp_congestion_control = htcp  
net.ipv4.tcp_no_metrics_save = 1  
net.ipv4.route.flush = 1  
net.ipv4.conf.all.rp_filter = 1  
net.ipv4.conf.lo.rp_filter = 1  
net.ipv4.conf.ens3.rp_filter = 1  
net.ipv4.conf.default.rp_filter = 1  
net.ipv4.conf.all.accept_source_route = 0  
net.ipv4.conf.lo.accept_source_route = 0
```

```
net.ipv4.conf.ens3.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.ip_local_port_range = 1024 65535
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_rfc1337 = 1
net.ipv4.ip_forward = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.core.somaxconn = 65535
net.core.netdev_max_backlog = 1000
```

Почитать про них можно <http://adminunix.ru/nastrojka-sysctl/>