Опросник на позицию linux администратора.

Содержание

Как обновить установленные приложения?

```
user@host:~$ sudo apt-get update && sudo apt-get upgrade -y
```

Как посмотреть кто входил в систему?

```
user@host:~$ last
username1   pts/0        192.168.0.1     Fri Apr  8 11:29   still logged in
username2   pts/0        192.168.0.2     Thu Apr  7 00:43 - 00:49  (00:06)
```

Как посмотреть в реальном времени файл журнала?

```
user@host:~$ tailf -n 200 /path/to/log/file/app.log
```

```
user@host:~$ tail -f -n 200 /path/to/log/file/app.log
```

`-n` - количество выводимых строк от конца файла (по умолчанию 10).

`tailf` — псевдоним `tail -f`.

Как смонтировать NFS шару на постоянку?

Необходимо добавить строку подключения в файл `/etc/fstab`

```
user@host:~$ cat /etc/fstab
...
192.168.0.20:/shared/folder /mount/point/files   nfs   rw, vers=4, sec=sys  0   0
...
```

Для автоматического монтирования после редактирования файла `/etc/fstab` необходимо вызвать `sudo mount -a`.

Где посмотреть информацию о том, какие пользователи могут выполнять команды от имени суперпользователя?

Информация хранится в файле `/etc/sudoers`

```
user@host:~$ sudo cat /etc/sudoers
...
abstractuser ALL=(ALL)       NOPASSWD: ALL
...
```

Как перезагрузить сервис если он завис?

Перезапуск в системах основанных на Debian осуществляется утилитой `systemctl`

```
user@host:~$ sudo systemctl restart application.service
```

Как выгнать пользователя с сервера?

Для того что бы выгнать пользователя с сервера, необходимо узнать PID сессии:

```
user@host:~$ sudo ps ax | grep abstract_user
31553 pts/0    S+     0:00 grep abstract_user
```

`31553` - PID сессии.

Для завершения процесса, посылаем сигнал `kill`

```
user@host:~$ sudo kill 31553
```

Как посмотреть занятые порты?

Есть несколько способов

Утилита `ss`

```
user@host:~$ sudo ss -pt
State     Recv-Q Send-Q    Local Address:Port    Peer Address:Port
ESTAB      0      0        127.0.0.1:45915       127.0.0.1:34482
users:(("klnagent",pid=1694,fd=39))
ESTAB      0      0        10.62.252.176:60908   10.62.252.179:6379
users:(("Tessa.Web.Serve",pid=21817,fd=259))
ESTAB      0      0        127.0.0.1:38962       127.0.0.1:36329
users:(("klnagent",pid=1694,fd=18))
ESTAB      0      0        10.62.252.176:36764   10.62.252.178:postgresql
users:(("Tessa.Web.Serve",pid=21798,fd=827))
ESTAB      0      0        10.62.252.176:https   10.50.40.7:4698
users:(("nginx",pid=18863,fd=51))
SYN-SENT   0      1        10.62.252.176:36496   10.39.66.101:microsoft-ds
...
```

Утилита `netstat`

```
user@host:~$ sudo netstat -ntp
...
tcp        0      0 SPB99-TSA-EAP2.ga:39376 SPB99-TSA-ED:postgresql ESTABLISHED
792/Tessa.Web.Serve
tcp        0      0 SPB99-TSA-EAP2.ga:37478 SPB99-TSA-ED:postgresql ESTABLISHED
21813/Tessa.Web.Ser
tcp        0      0 SPB99-TSA-EAP2.ga:37334 SPB99-TSA-ED:postgresql ESTABLISHED
21817/Tessa.Web.Ser
tcp        0      0 localhost:45915         localhost:34488         ESTABLISHED
1694/klnagent
tcp        0      0 SPB99-TSA-EAP2.ga:https 10.50.40.7:37880        ESTABLISHED
18863/nginx: worker

...
```

Утилита `lsof`

```
user@host:~$ sudo lsof -nP -iTCP:443 -sTCP:ESTABLISHED
COMMAND   PID     USER   FD   TYPE    DEVICE SIZE/OFF NODE NAME
nginx   18863 www-data    3u  IPv4 150794567      0t0  TCP 10.62.252.176:443-
>10.50.40.7:37880 (ESTABLISHED)
nginx   18863 www-data    7u  IPv4 151774916      0t0  TCP 10.62.252.176:443-
>10.50.40.7:29675 (ESTABLISHED)
....
```

Как посчитать количество ошибок в журнале?

Как вариант можно воспользоваться конвейером `stdin` `stdout`.

```
user@host:~$ cat /path/to/file | grep text | wc -l
```

`wc` - утилита для подсчёта вхождений. `-l` - подсчёт строк.

Как добавить сертификат в доверенные?

1. Скопировать все сертификаты в цепочке в /usr/local/share/ca-certificates/ в BASE64 кодировке с расширением .crt
2. update-ca-certificates
3. Проверяем соединение: openssl s_client -CApath /etc/ssl/certs/ -connect hostname:port

Как перечитать конфигурацию Nginx без перезапуска.

```
user@host:~$ sudo /usr/sbin/nginx -s reload
```

Как добавить пользователя?

Вся информация о пользователях находится в файле `/etc/passwd`. Мы могли бы создать пользователя linux просто добавив его туда, но так делать не следует, поскольку для этой задачи существуют специальные утилиты. Одна из таких утилит, это useradd. Рассмотрим ее подробнее.

КОМАНДА USERADD

```
user@host:~$ sudo useradd опции имя_пользователя

-b - базовый каталог для размещения домашнего каталога пользователя, по умолчанию
/home;
-c - комментарий к учетной записи;
-d - домашний каталог, в котором будут размещаться файлы пользователя;
-e - дата, когда учетная запись пользователя будет заблокирована, в формате ГГГГ-ММ-
ДД;
-f - заблокировать учетную запись сразу после создания;
-g - основная группа пользователя;
-G - список дополнительных групп;
-k - каталог с шаблонами конфигурационных файлов;
-l - не сохранять информацию о входах пользователя в lastlog и faillog;
-m - создавать домашний каталог пользователя, если он не существует;
-M - не создавать домашнюю папку;
-N - не создавать группу с именем пользователя;
-o - разрешить создание пользователя linux с неуникальным идентификатором UID;
-p - задать пароль пользователя;
-r - создать системного пользователя, не имеет оболочки входа, без домашней директории
и с идентификатором до SYS_UID_MAX;
-s - командная оболочка для пользователя;
-u - идентификатор для пользователя;
-D - отобразить параметры, которые используются по умолчанию для создания
пользователя. Если вместе с этой опцией задать еще какой-либо параметр, то его
значение по умолчанию будет переопределено.
```

Создадим пользователя с паролем и оболочкой `/bin/bash`

```
user@host:~$ sudo useradd -p password -s /bin/bash test1
```

Для того чтобы получать доступ к системным ресурсам пользователю нужно быть участником групп, у которых есть доступ к этим ресурсам. Дополнительные группы пользователя задаются с помощью параметра -G. Например, разрешим пользователю читать логи, использовать cdrom и пользоваться sudo:

```
user@host:~$ sudo useradd -G adm,cdrom,wheel -p password -s /bin/bash test2
```

Также, можно установить дату, когда аккаунт пользователя будет отключен автоматически, это может быть полезно для пользователей, которые будут работать временно:

```
user@host:~$ sudo useradd -G adm,cdrom,wheel -p password -s /bin/bash -e 01:01:2018
test2
```

Некоторых пользователей интересует создание пользователя с правами root linux, это очень просто делается с помощью useradd, если комбинировать правильные опции. Нам всего лишь нужно разрешить создавать пользователя с неуникальным uid, установить идентификатор в 0 и идентификатор основной группы тоже в 0. Команда будет выглядеть вот так:

```
user@host:~$ sudo useradd -o -u 0 -g 0 -s /bin/bash newroot
```

Как посмотреть список групп пользователя?

Все группы, созданные в системе, находятся в файле `/etc/group`. Посмотрев содержимое этого файла, вы можете узнать список групп linux, которые уже есть в вашей системе. И вы будете удивлены.

```
user@host:~$ sudo cat /etc/group
```

Посмотреть группы linux, в которых состоит пользователь можно командой

```
user@host:~$ groups
```

Добавить пользователя в группу можно командой usermod

```
user@host:~$ sudo usermod -a -G имя_группы имя_пользователя
```

Удалить пользователя из группы в linux можно той же командой с опцией R:

```
user@host:~$ sudo usermod -R группа пользователь
```

Как сменить владельца файла?

Синтаксис chown, как и других подобных команд linux очень прост

```
user@host:~$ chown пользователь опции /путь/к/файлу

-c, --changes - подробный вывод всех выполняемых изменений;
-f, --silent, --quiet - минимум информации, скрыть сообщения об ошибках;
--dereference - изменять права для файла к которому ведет символическая ссылка вместо
самой ссылки (поведение по умолчанию);
-h, --no-dereference - изменять права символических ссылок и не трогать файлы, к
которым они ведут;
--from - изменять пользователя только для тех файлов, владельцем которых является
указанный пользователь и группа;
-R, --recursive - рекурсивная обработка всех подкаталогов;
-H - если передана символическая ссылка на директорию - перейти по ней;
-L - переходить по всем символическим ссылкам на директории;
-P - не переходить по символическим ссылкам на директории (по умолчанию).
```

Для рекурсивного изменения владельца и группы каталога, добавьте опцию -R:

```
user@host:~$ sudo chown -R root:root ./dir3
```

Изменить группу и владельца на www-data только для тех каталогов и файлов, у которых владелец и группа root в каталоге /dir3:

```
user@host:~$ sudo chown --from=root:root www-data:www-data -cR ./
```

Как сменить права на файл?

Синтаксис команды для смены прав

```
user@host:~$ chmod опции права /путь/к/файлу
```

Есть три основных вида прав:

`r` - чтение; `w` - запись; `x` - выполнение; `s` - выполнение от имени суперпользователя (дополнительный);

Есть три категории пользователей, для которых вы можете установить эти права на файл linux:

`u` - владелец файла; `g` - группа файла; `o` - все остальные пользователи;

Синтаксис настройки прав такой:

В качестве действий могут использоваться знаки "+" — включить или "-" — отключить. Рассмотрим несколько примеров:

- `u+x` — разрешить выполнение для владельца;
- `ugo+x` — разрешить выполнение для всех;
- `ug+w` — разрешить запись для владельца и группы;
- `o-x` — запретить выполнение для остальных пользователей;
- `ugo+rwx` — разрешить все для всех;

Но права можно записывать не только таким способом. Есть еще восьмеричный формат записи, он более сложен для понимания, но пишется короче и проще. Я не буду рассказывать как считать эти цифры, просто запомните какая цифра за что отвечает, так проще:

- `0` — никаких прав;
- `1` — только выполнение;
- `2` — только запись;
- `3` — выполнение и запись;
- `4` — только чтение;
- `5` — чтение и выполнение;
- `6` — чтение и запись;
- `7` - чтение запись и выполнение.

ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ CHMOD

Сначала самый частый случай - разрешить выполнения скрипта владельцу

```
user@host:~$ chmod u+x file
```

Или можно воспользоваться цифровой записью

```
user@host:~$ chmod 766 file
```

Для того чтобы поменять права на все файлы в папке используйте опцию -R:

```
user@host:~$ chmod -R ug+rw dir
```

Как посмотреть сколько занимает директория?

СИНТАКСИС И ОПЦИИ КОМАНДЫ DU

```
user@host:~$ du опции /путь/к/папке

-a, --all - выводить размер для всех файлов, а не только для директорий, по умолчанию
размер выводится только для папок;
-B, --block-size - указать единицы вывода размера, доступно: K,M,G,T,P,E,Z,Y для 1024
и KB, MB и так далее для 1000;
-c, --total - выводить в конце общий размер всех папок;
-d, --max-depth - максимальная глубина вложенности директорий;
-h, --human-readable - выводить размер в единицах измерения удобных для человека;
--inodes - выводить информацию об использованию inode;
-L, --dereference - следовать по всем символическим ссылкам;
-l, --count-links - учитывать размер файла несколько раз для жестких ссылок;
-P, --no-dereference - не следовать по символическим ссылкам, это поведение
используется по умолчанию;
-S, --separate-dirs - не включать размер подпапок в размер папки;
--si - выводить размер файлов и папок в системе си, используется 1000 вместо 1024;
-s, --summarize - выводить только общий размер;
-t, --threshold - не учитывать файлы и папки с размером меньше указанного;
--time - отображать время последней модификации для файла или папки, вместо времени
модификации можно выводить такие метки: atime, access, use, ctime;
-X, --exclude - исключить файлы из подсчёта;
-x, --one-file-system - пропускать примонтированные файловые системы;
--version - вывести версию утилиты.
```

По умолчанию размер выводится в байтах. Для того чтобы размер выводился в более читабельном виде используйте опцию `-h`*:*

```
user@host:~$ du -h /var
```

Если надо выводить размер не только папок, но и файлов, которые там находятся, используйте опцию `-a`*:*

```
user@host:~$ du -ha /var
```

Для того чтобы вывести только общий размер всех файлов и папок нужно применить опцию -s:

```
user@host:~$ du -hs /var
```

Ещё можно вывести строчку с общим размером всей папки. Правда использовать эту возможность есть смысл только с опцией `-S`*, потому что общий размер папки во всех других случаях и так отображается:*

```
user@host:~$ du -hSc /var
```

Если вам надо исключить какие-либо файлы из подсчёта, следует использовать опцию `--exclude`. *Например, давайте исключим все лог файлы:*

```
user@host:~$ du -hac --exclude="*.log"
```

Чтобы данные были более наглядными их желательно отсортировать. Встроенной поддержки сортировки в du linux нет, зато можно воспользоваться утилитой sort с опцией -h. Эта опция нужна чтобы сортировались единицы измерения в понятном для чтения формате:

```
user@host:~$ du -h /var | sort -h
```