

Управление пользователями



Артур
Сагутдинов



Артур Сагутдинов

Начальник IT отдела

ООО «Клинический
институт репродуктивной
медицины»



15+ лет в сфере ИТ



Разрабатываю и внедряю
линуксовую инфраструктуру



[Сисадминский блог](#)



Предисловие

На этом занятии мы **продолжим рассмотрение ОС Linux:**

- разберемся с пользователями и группами;
- научимся работать с атрибутами файлов;
- поговорим о запуске приложений.

План занятия

1. [Предисловие](#)
2. [Пользователи и группы](#)
3. [Права доступа](#)
4. [Запуск приложений](#)
5. [Итоги](#)
6. [Домашнее задание](#)



Пользователи и группы

root

root (superuser, суперпользователь) – обязательный пользователь во всех Linux.

Root может прочитать, удалить или изменить любой файл (следовательно и всё) в системе.

Для root:

UID = 0

GUID = 0

домашний каталог = **/root**

В некоторых дистрибутивах (Ubuntu) пользователю root запрещен вход в систему.



sudo

sudo – временное повышение прав текущего пользователя до root.

/etc/sudoers – список пользователей или групп, которым разрешено использовать sudo

UID

Выполним:

```
user@user:~$ id
```

```
user@user:~$ sudo id
```

UID

Значение UID:

- 1-99 – системные пользователи;
- 500 – ... - пользователи-люди (Red Hat);
- 100-999 – пользователи-службы («стандарт»);
- 1000-4999 – пользователи-люди («стандарт»);
- 5000-9999 – дополнительный пользователи и группы («стандарт»);
- 5000 - ... – пользователи-люди (последние рекомендации Red Hat).

GUID

Значение GUID:

- 100 – «Users»;
- GUID = UID.

Для того, чтобы предоставить доступ к общему ресурсу, следует создать для этих целей отдельную группу и добавлять пользователей в неё.

Домашний каталог

Домашний каталог – место, где пользователь может хранить свои файлы. Все файлы созданные в этом каталоге будут доступны пользователю на чтение и запись.

По умолчанию:

`/home/<имя пользователя>`

Просмотр домашнего каталога:

```
user@user:~$ ls ~
```

Переход в домашний каталог:

```
user@user:~$ cd
```

/etc/passwd

/etc/passwd – файл, содержащий список пользователей системы

```
user@user-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

Пользователь : пароль : UID : GUID : полное_имя : каталог : оболочка

/etc/shadow

/etc/shadow – файл, содержащий список паролей пользователей

```
user@user-VirtualBox:~$ sudo cat /etc/shadow
[sudo] password for user:
root:!:18365:0:99999:7:::
daemon*:18295:0:99999:7:::
bin*:18295:0:99999:7:::
sys*:18295:0:99999:7:::
sync*:18295:0:99999:7:::
games*:18295:0:99999:7:::
man*:18295:0:99999:7:::
lp*:18295:0:99999:7:::
mail*:18295:0:99999:7:::
news*:18295:0:99999:7:::
uucp*:18295:0:99999:7:::
proxy*:18295:0:99999:7:::
www-data*:18295:0:99999:7:::
backup*:18295:0:99999:7:::
list*:18295:0:99999:7:::
irc*:18295:0:99999:7:::
gnats*:18295:0:99999:7:::

```

Пользователь : пароль : дата: мин : макс :::

/etc/group

/etc/group – файл, содержащий список групп пользователей

```
user@user-VirtualBox:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,user
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
```

Группа : пароль : GID : список

/etc/sudoers

Для редактирования применяется команда **visudo**.

Разделы **#Host alias** **#User alias** **#Cmnd alias** позволяют создать списки хостов, пользователей или команд, например:

Students_Alias STUD = student1, student2

Раздел команд:

- **root ALL=(ALL:ALL) ALL** – root может запускать любую команду в любой группе на любом хосте;
- **%admin ALL=(ALL) ALL** – аналогично для группы admin.

login.defs

/etc/login.defs – файл, содержащий параметры входа по умолчанию.

```
PASS_MIN_DAYS    0
PASS_WARN_AGE    7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN          1000
UID_MAX          60000
# System accounts
#SYS_UID_MIN      100
#SYS_UID_MAX      999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN          1000
GID_MAX          60000
# System accounts
#SYS_GID_MIN      100
#SYS_GID_MAX      999

#
# Max number of login retries if password is bad. This will most likely be
--More--
```

Пользователи: useradd

```
cat /etc/default/useradd
```

```
user@user:~$ useradd -D
```

```
user@user:~$ sudo useradd xakep
```

```
user@user:~$ sudo useradd xakep -s /bin/bash
```

```
user@user:~$ useradd -c "Test User" -e 2021-12-31 test
```

```
user@user:~$ su - test
```

Пользователи: редактирование

```
user@user:~$ usermod --lock xakep
```

```
user@user:~$ usermod -p password xakep
```

```
user@user:~$ sudo passwd xakep
```

```
user@user:~$ sudo userdel xakep
```

Группы: редактирование

```
user@user:~$ groupadd ctf
```

```
user@user:~$ groupmod -n ctf ftc
```

```
user@user:~$ sudo groupdel ftc
```

Ограничение ресурсов

/etc/security/limits.conf – файл, содержащий ограничения ресурсов

```
# - maxsyslogins - max number of logins on the system
# - priority - the priority to run user process with
# - locks - max number of file locks the user can hold
# - sigpending - max number of pending signals
# - msgqueue - max memory used by POSIX message queues (bytes)
# - nice - max nice priority allowed to raise to values: [-20, 19]
# - rtprio - max realtime priority
# - chroot - change root to directory (Debian-specific)
#
#<domain>      <type>  <item>      <value>
#
#*              soft    core        0
#root           hard    core        100000
#*              hard    rss         10000
#@student       hard    nproc       20
#@faculty       soft    nproc       20
#@faculty       hard    nproc       50
#ftp            hard    nproc       0
#ftp            -       chroot       /ftp
#@student       -       maxlogins    4

# End of file
```



Права доступа

Атрибуты файла

1. Права пользователя
(r, w, x, -).
2. Права группы.
3. Права «всех других».

r w x r w - r - x

4 2 1 4 2 0 4 0 1

7 6 5

```
user@user-VirtualBox:~$ ls -l
total 2196
-r----- 1 root root 1052672 авг  7 14:43 back
drwxr-xr-x 2 1210 root  4096 окт 23 18:54 community-rules
drwxr-xr-x 2 user user  4096 окт 24 22:42 Desktop
drwxr-xr-x 7 user user  4096 окт 24 22:44 dockpot
drwxr-xr-x 2 user user  4096 июл 27 17:18 Documents
drwxr-xr-x 3 user user  4096 ноя  9 07:46 Downloads
drwxr-xr-x 6 user user  4096 окт 25 21:15 dtk-dist
-rw-rw-r-- 1 user user 993280 окт 25 21:13 dtk.tar
drwxrwxr-x 5 user user  4096 апр 16  2020 go
drwxr-xr-x 6 root root  4096 окт 24 22:59 mhn
drwxr-xr-x 2 user user  4096 апр 13  2020 Music
drwxr-xr-x 2 user user  4096 окт 30 17:17 Pictures
drwxr-xr-x 5 user user  4096 апр 20  2020 projects
drwxr-xr-x 2 user user  4096 апр 13  2020 Public
drwxr-xr-x 7 user user  4096 окт 24 23:31 servletpot
drwxr-xr-x 2 user user  4096 апр 13  2020 Templates
-rw-r--r-- 1 user user 138994 ноя  6 08:00 test.svg
drwxr-xr-x 2 user user  4096 апр 13  2020 Videos
```

Атрибуты каталога

Биты доступа:

- **r** – чтение содержимого каталога;
- **w** – право создания / изменения / удаления файлов каталога;
- **x** – позволяет делать текущий каталог рабочим (pwd).

Специальные биты

Setuid (suid) – позволяет пользователю выполнять программу с правами владельца (**s** в атрибутах файла).

```
user@Asus:~$ ls -l /bin/sudo  
-rwsr-xr-x 1 root root 166056 янв 19 17:21 /bin/sudo
```

Setgid (sgid) – работает аналогично **setuid**, но для группы.

Sticky – в таком каталоге пользователь может удалять только свои файлы (**t** в атрибутах файла).

```
user@Asus:~$ ls -ld /tmp/  
drwxrwxrwt 23 _root root 4096 янв 28 07:10 /tmp/
```

Для большей безопасности при монтировании ФС можно указать параметр **nosuid** для отключения флагов **suid** и **setgid**.



chmod

chmod (change mode) – утилита для изменения прав доступа

- chmod **+x** <file> chmod **-x** <file>
- chmod **g+r** <file> chmod **g-r** <file>
- chmod **o+w** <file> chmod **o-w** <file>
- chmod **660** <file>
- chmod **u+s** <file> – установка SUID
- chmod **g+s** <file> – установка SGID
- chmod **+t** <file> – установка Sticky

chown, chgrp

chown (change owner) – утилита для изменения владельца файла.

```
user@user:~$ chown student file1
```

chgrp (change group) – утилита для изменения групп.

```
user@user:~$ chgrp student file1
```

umask

umask (user mask) – задает биты доступа, устанавливаемые по умолчанию для всех новых файлов.

Заметим, что **бит X** никогда не устанавливается для созданных файлов.

Umask обладает «инверсной» логикой, т.е. единицы в маске задают нули в правах доступа. Поэтому, для обычного пользователя **umask=0002** или **-rw-rw-r--**

По аналогии:

umask=0000 или **-rw-rw-rw-**



Запуск приложений

Выполнение команды в консоли

1. Набираем команду и нажимаем «Enter».
2. оболочка (`bash` и т.д.) разбирает путь, параметры.
3. Если введена внутренняя команда, то запускается её выполнение.
4. Если введена внешняя команда / имя приложения вместе с путем, то запускается выполнение приложения.
5. Если введена внешняя команда / имя приложения и путь не указан, то оболочка просматривает все каталоги в переменной `$PATH`. Если приложение найдено, оно запускается на выполнение

Переменная PATH

Переменная **\$PATH** (путь) – список каталогов, разделенных символом «;»

Просмотр \$PATH:

```
user@user:~$ echo $PATH
```

```
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Переменная \$PATH может быть задана для:

- текущего пользователя;
- всех пользователей;
- текущей сессии.

Выполнение команды из текущего каталога

Если программа **my_prog** находится в каталоге `/home/user/` и мы выполним `cd /home/user/`, то запустить программу можно следующим образом:

`./my_prog`

`~/my_prog`

`/home/user/my_prog`

Основные переменные окружения

- `HOME=/home/user` – домашний каталог пользователя;
- `LOGNAME=user` – имя пользователя в текущей оболочке;
- `PWD=/home/user` – текущий рабочий каталог;
- `SHELL=/bin/bash` – командная оболочка;
- `LC_*=ru_RU.UTF-8` – переменные для локализации;
- `LANG=en_US.UTF-8` – язык системы.



Итоги

Итоги

Сегодня мы:

- рассмотрели добавление, удаление и редактирование пользователей ОС Linux, а также запуск команд;
- научились работать с атрибутами файлов.

Домашнее задание

Давайте посмотрим ваше [домашнее задание](#).

- Вопросы по домашней работе задавайте в чате учебной группы и/или в разделе “Вопросы по заданию”.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

⌘ нетология

**Задавайте вопросы и
пишите отзыв о лекции!**

Артур Сагутдинов