

Linux

Пользователи и права доступа

- Учётные записи пользователей и групп
- Команды и файлы управления учётными записями
- Права доступа к файлам



Для разграничения прав доступа к файлам, в системе существуют пользователи и группы пользователей.

/etc/passwd – файл, в котором хранятся учётные записи пользователей;

/etc/group – файл, в котором хранится перечень групп, а также списки пользователей, которые в них входят;

В целях безопасности, пароли пользователей и групп хранятся в отдельных файлах в виде хеш-сумм, а к самим файлам доступ ограничен.

/etc/shadow – файл с данными о паролях пользователей

/etc/gshadow – файл с данными о паролях групп



- 1: Account (login)
- 2: Password (x)
- 3: UID (User ID)
- 4: GID (Group ID)
- 5: GECOS
- 6: Home directory
- 7: Shell

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
roman:x:500:500:R:/home/roman:/bin/bash
```

- 1: **Account** (login) – имя пользователя
- 2: **Password** (x) – когда-то давно здесь хранили пароль, теперь только метку 'x'
- 3: **UID** (User ID) – числовой идентификатор пользователя в системе
- 4: **GID** (Group ID) – числовой идентификатор базовой группы, в которую входит пользователь
- 5: **GECOS** – общая информация о пользователе. Поле имело свой формат, редко используется
- 6: **Home directory** – домашний каталог пользователя
- 7: **Shell** – оболочка пользователя.

В некоторых случаях подставляют оболочку-пустышку /sbin/nologin для запрета входа в систему

```
root:$1$RuHQ/nGS$AKGPIhviW9ESxn64x34541:14783:0:99999:7:::  
bin:*:14783:0:99999:7:::  
daemon:*:14783:0:99999:7:::  
adm:*:14783:0:99999:7:::  
lp:*:14783:0:99999:7:::  
shutdown:*:14783:0:99999:7:::  
halt:*:14783:0:99999:7:::  
mail:*:14783:0:99999:7:::  
operator:*:14783:0:99999:7:::  
games:*:14783:0:99999:7:::  
ftp:*:14783:0:99999:7:::  
nobody:*:14783:0:99999:7:::  
roman:$1$O1F0LdLp$iebVRX7OjQosHJqWhys1H/:14783:0:99999:7:::
```

- 1: **Login** – имя пользователя
- 2: **Password** – информация о пароле. Обычно представлен в виде хеша
- 3: Кол-во дней с 1 января 1970 когда пароль последний раз был изменён
- 4: Кол-во дней, через которые пароль можно будет изменить
- 5: Кол-во дней, через которые пароль должен быть изменён
- 6: Кол-во дней до окончания срока действия пароля, когда система просит его сменить
- 7: Кол-во дней после устаревания пароля, через которые учётная запись будет заблокирована
- 8: Кол-во дней с 1 января 1970 когда пользователь был заблокирован.
- 9: Резервное поле

- 1: Имя группы
 - 2: Пароль
 - 3: GID (Group ID)
числовой идентификатор группы
 - 4: Перечень пользователей, которые входят в данную группу (через запятую)
- Каждый пользователь имеет свою основную (базовую) группу.
 - Пользователь может входить более чем в одну группу.
 - Группа также может иметь пароль (соответствующие хеш-суммы хранятся в файле /etc/gshadow)

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
man:x:15:
games:x:20:
screen:x:84:
```

По работе с пользователями:

useradd – создание учётной записи пользователя

userdel – удаление учётной записи пользователя

usermod – изменение учётной записи пользователя

passwd – смена токена аутентификации (пароля)

По работе с группами:

groupadd – создание учётной записи группы

groupdel – удаление учётной записи группы

groupmod – изменение учётной записи пользователя

gpasswd – смена токена аутентификации

chage – изменение временных политик по пользователю

vipw (vigr) – редактирование конфигурационных файлов пользователей (групп)

pwck (grpck) – проверка целостности файлов учётных записей пользователей (групп).

Команды, с помощью которых обычный пользователь может изменить информацию своей учётной записи

chsh – изменить командную оболочку пользователя

chfn – изменить пользовательскую информацию

passwd – изменить пароль (хеш)

Специфичные для оболочки команды

umask – задание прав доступа по-умолчанию для создаваемых файлов и каталогов

ulimit – ограничение пользователя по кол-ву процессов, открытых файлов и т.д.

- /etc/login.defs** – файл, содержащий различные параметры, которые задаются по-умолчанию создаваемым пользователям
- /etc/skel** – каталог с набором файлов внутри, которые будут помещены в домашний каталог нового пользователя
- /etc/shells** – файл с перечнем доступных оболочек
- /sbin/nologin** (/usr/sbin/nologin) – специальная оболочка, которая не пускает пользователя в систему. При этом, она сообщает, что пользователю не разрешен вход в систему
- /etc/nologin.txt** – сообщение, которое будет выводиться в случае, если у пользователя оболочка /sbin/nologin
- /etc/nologin** – наличие этого файла блокирует вход в систему всех обычных пользователей. Содержимое этого файла выводится при попытке таких пользователей войти в систему

id – отобразить id пользователя и групп, в которые он входит

users – отобразить имена пользователей, которые на текущий момент работают в системе

w – показать кто вошел в систему и что сейчас делает

who – показать кто вошел в систему

groups – показать группы, в которые пользователь входит

last – показать историю заходов пользователей в систему

uptime – показать как долго работает система + среднюю нагрузку на сервер

su – позволяет запускать команды от имени другого пользователя или группы

- Можно перейти в оболочку другого пользователя и работать в ней, можно запустить всего одну команду от имени другого пользователя (с ключом -c)
- Опция ' - ' (она же -l, --login) – имитирует вход в систему под указанным пользователем (влияет на переменные окружения)
- У не root-пользователей спрашивает пароль того пользователя, под которым хотим выполнять команды

newgrp – способ сменить текущую основную группу.

sudo – программа, с помощью которой суперпользователь может дать возможность определённым пользователям и группам запускать привилегированные программы

/etc/sudoers – файл настроек команды sudo.

Редактировать этот файл обычными редакторами настоятельно не рекомендуется, т.к. если будет допущена ошибка – механизм sudo работать не будет. Это чревато нарушением работы служб и пользователей, которые в своей работе полагаются на sudo.

visudo – специальный редактор, для внесения изменений в файл /etc/sudoers. Производит проверку синтаксиса по выходу из редактора.

Грамотно настроенный функционал sudo позволяет реже входить в систему под учётной записью суперпользователя.

Права доступа

Каждый файл в системе имеет права доступа к нему

Права доступа распределяются между:

- владельцем файла
- группой, владеющей файлом
- остальными пользователями

	U	G	O
	7	5	4
access	r w x	r - x	r - -
enabled	1 1 1	1 0 1	1 0 0
binary	4 2 1	4 2 1	4 2 1
result	4 2 1	4 0 1	4 0 0
total	7	5	4

Обозначение прав доступа:

- **r** (read), 4 – чтение
Файл: просмотр содержимого
Каталог: просмотр списка файлов (содержимого таблицы direntry)
- **w** (write), 2 – запись
Файл: изменение файла
Каталог: добавление, удаление, переименование файлов (изменение direntry)
- **x** (eXecute), 1 – исполнение
Файл: запуск файла на исполнение
Каталог: переход в каталог
- **s** (setuid), 4 – подмена идентификатора EUID процесса на UID владельца исполняемого файла. Для каталога – все создаваемые вложения имеют такой же UID, как и у владельца этого каталога.
- **S** (setgid), 2 – подмена идентификатора EGID процесса на GID исполняемого файла
- **t** (sticky), 1 – каталог для добавления. В каталоге с этим битом любой пользователь может создавать свои файлы. Удалить эти файлы может только:
1) суперпользователь, 2) владелец каталога, 3) владелец этих файлов.

chmod (change mode) – утилита для изменения прав доступа к файлам (каталогам). Работает как с числовым представлением прав доступа, так и с символьным

Примеры:

chmod u+x file - разрешить владельцу запускать файл на исполнение

chmod o-rwx file - запретить всякие действия над файлом для всех остальных

chmod g=rx file - группе разрешено читать и запускать файл на исполнение

chmod 755 file - задать права доступа “rwx r-x r-x”

chmod 4744 file - задать права доступа “rws r-- r--”

chmod 1777 dir – задать права доступа на каталог “rwx rwx rwt”

chown (change owner) – утилита для изменения владельца (группы) указанного файла или каталога.

Синтаксис:

```
chown [options] NewOwner[:NewGroup] file ...
```

Примеры:

chown userok file – сменить владельца файла file на userok

chown userok:grp file – сменить одновременно и владельца на userok, и группу на grp

chown :grp file – сменить группу на grp (аналогично **chgrp**)

chown -R userok Dir – сменить владельца каталога Dir и владельцев всех его вложений рекурсивно на userok