Операционные системы (6 семестр)

Лекция 1.6. Управление правами и пользователями.

Ассистент, к.т.н. Митричев Иван Игоревич

Москва 2018

План лекции

Права доступа и права владения.
•Права доступа к файлам и каталогам.
•Изменение прав доступа.
•Установка прав доступа.

Управление пользователями.
•Хранение учетных записей.
•Регистрация, удаление, блокирование учетных записей.
•Управление паролями.
•Управление группами пользователей.
•Профили пользователей.
•Получение отчетов об активности пользователей.

Права доступа и права владения (DAC)

DAC (Discretionary Access Control) – механизм избирательного управления доступом к файлам, реализован в Unix (пользователи получают доступ к файлам в соответствии со списком доступа).

Каждый пользователь имеет уникальный идентификатор (UID) и может принадлежать различным группам.

У каждого файла есть владелец и группа пользователей, которой принадлежит файл. При создании файла пользователем группа пользователей файла совпадает с первичной группой самого пользователя (GID).

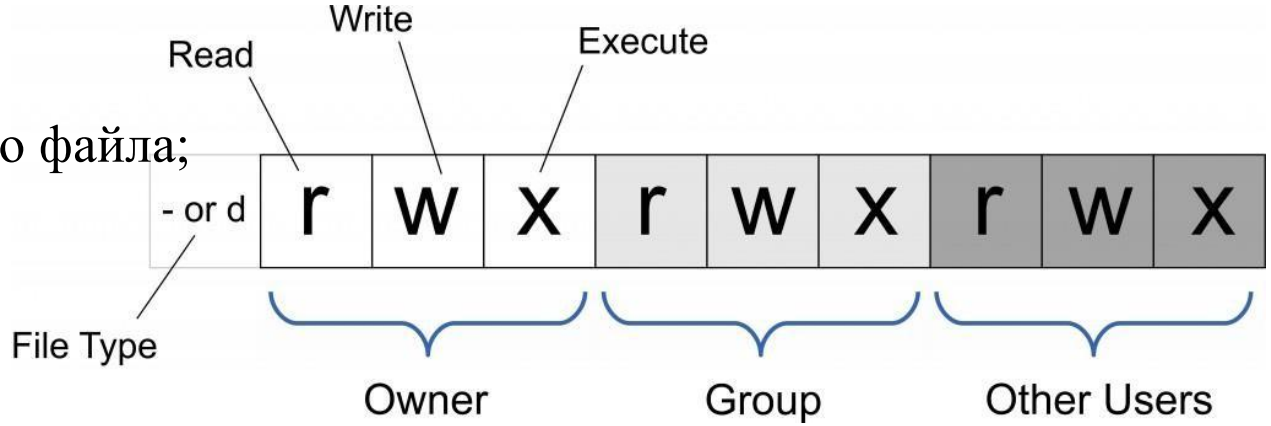
```
$id
uid=1000(user) gid=1000(user)
группы=1000(user),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)

$ > file
$ ls -l file
-rw-rw-r-- 1 user user 0 мар 01 12:51 file
```

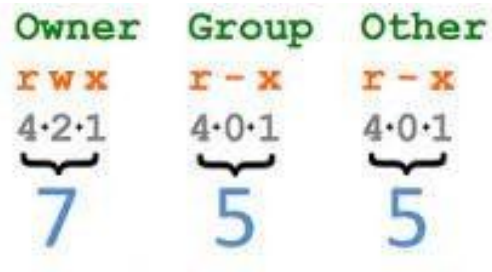
Созданный пользователем user (столбец 3) файл, имеет группу пользователей user (столбец 4).

Права доступа к файлам

- User access (u) – права доступа владельца файла;
- Group access (g) – права доступа группы владельца файла;
- Other access (o) – права доступа для всех остальных.

Символическая нотация
r-- – наличие разрешения на чтение данного файла;
-w- – наличие разрешения на изменение;
--x – наличие разрешения на исполнение.





Восьмеричная нотация — число из трех бит (1/0 = есть/нет) для тройки прав доступа (чтение, запись, исполнение) заданным субъектом (пользователь, группа или другие).

Пример rxwxr-x--x (751) – пользователь файла имеет все права на доступ к нему (rxw или 7), группа пользователей имеет права на чтение и исполнение файла (r-x или 5), остальные имеют права на исполнение (--x или 1).

Права доступа к каталогам

r – право на чтение названий файлов (вывод содержимого каталогов). Для чтения содержимого требует права x;

w – право изменять (в т.ч. - удалять, создавать) файлы в каталоге, требует права x;

x – право на вход в каталог и доступа к содержащимся внутри каталога файлам, а также чтение индексных записей (метаданных). Поэтому, правильные права для пользователей/групп на каталог должны быть нечетными, также могут отсутствовать (000).

Внимание: право записи на каталог автоматически дает право на удаление, создание файлов в нем, невзирая на права на отдельные файлы! Однако для **редактирования** этих файлов потребуются права **на них**.

Часто используемые права для каталогов

Обозначение 0 (---) означает отсутствие прав (часто используется для запрещения доступа);

Права 5 (r-x) – доступ на переход в каталог и чтение содержимого без возможности редактирования (часто используется);

Права 7 (rwx) – разрешено все (часто используется для предоставления полного доступа).

Другие права используются редко. Например, права 1(--x) на каталог предполагают возможность чтения содержимого файлов в нем, и перехода в него, без возможности просмотра списка содержимого (это неудобно, потому редко используется).

Изменение прав владения

- chown – позволяет менять как владельца файла или каталога, так и группу пользователей файла, может выполнять только суперпользователь
- chgrp – позволяет менять группу пользователей файла. Может выполнить владелец или член группы, а также суперпользователь.

Изменение владельца

```
ll 1.txt
-rw-rw-r-- 1 user user 0 мар 1 12:27 1.txt
sudo chown root 1.txt
ll 1.txt
-rw-rw-r-- 1 root user 0 мар 1 12:27 1.txt
```

опция -R – изменять рекурсивно;
опция -v – получая информацию об изменении.

Изменение группы

```
ll 1.txt
-rw-rw-r-- 1 user user 0 мар 1 12:27 1.txt
chgrp adm 1.txt
ll 1.txt
-rw-rw-r-- 1 user adm 0 мар 1 12:28 1.txt
```

Установка прав доступа

chmod – изменение прав доступа к файлам и каталогам, указанным в качестве аргументов (права указываются в восьмеричной или символьной нотации, изменять права могут суперпользователь и владелец).

```
$ touch 1.txt && ll 1.txt
-rw-rw-r-- 1 user user 0 мар 12 02:42 1.txt

$ chmod 770 1.txt && ll 1.txt
-rwxrwx--- 1 user user 0 мар 12 02:42 1.txt*

$ chmod g-w,o+r 1.txt && ll 1.txt
-rwxr-xr-- 1 user user 0 мар 12 02:42 1.txt*

$ chmod ug=rw,o= 1.txt && ll 1.txt
-rw-rw---- 1 user user 0 мар 12 02:42 1.txt
```

В символьной нотации:
chmod <*класс изменение права*> <*файлы*>
класс один из следующих:
u – доступ владельца;
g – доступ группы владельцев;
o – доступ всех остальных;
a – доступ всех групп пользователей.

Аргумент изменение:
+ – разрешить (добавить);
- – запретить (убрать);
= – установить (переписать).

Автоматическая установка прав доступа

umask – автоматическая установка прав доступа к вновь создаваемым файлам и каталогам (задаваем значение битовой маски, которая вычитается из прав 777 для каталогов и 666 для файлов).

```
$ umask 002
$ mkdir dir1
$ > file1
$ ls -ld dir1
file1
drwxrwxr-x 2     user1 user1  48   Dec 14 20:43    dir1
-rw-rw-r--    1     user1 user1    0   Dec 14 20:43   file1
```

Специальные биты прав доступа

Специальные биты прав доступа

Бит SUID – s в старшей триаде;
SGID – s в средней триаде битов;

```
$ls -ld /tmp
drwxrwxrwt 14 root root 32768 мар 12 02:47 /tmp
```

sticky bit – t в младшей триаде битов.

Sticky bit не действует на суперпользователя и владельца директории

Права	Эффект для каталогов	Эффект для файлов
-rws--x--x	—	Команда исполняется от имени владельца файла
-rwx--s--x	—	Команда исполняется от имени группы пользователей файла
drwxrws---	На файлы, создаваемые в каталоге, будет установлена такая же группа, как у каталога	—
drwxrwxrwt	В каталоге можно удалять или переименовывать только собственные файлы	—

Установка специальных битов прав доступа

Специальные биты прав доступа устанавливаются командой chmod в символической нотации (rwsrwsrwt), или когда к восьмеричной нотации прибавлена еще одна цифра

chmod **1**555 — установка sticky bit

chmod **2**555 — установка SGID

chmod **4**555 — установка SUID

Структура учетных записей

Информация о пользователе → /etc/passwd

- имя пользователя;
- пароль (символ x для теневых паролей);
- UID пользователя;
- GID пользователя;
- справочная информация о пользователе;
- домашний каталог;
- оболочка.

Теневые пароли → /etc/shadow

- имя пользователя;
- зашифрованный пароль;
- кол-во дней от начала эпохи Unix (01.01.70) до момента последней смены пароля;
- мин. время жизни пароля;
- макс. время жизни пароля;
- период выдачи предупреждений;
- период до блокировки учетной записи;
- срок жизни учетной записи.

Файл /etc/passwd доступен для чтения всем пользователям.
Использование системы теневых паролей снижает опасность взлома системы.

Регистрация учетных записей пользователей

Правами регистрации пользователей в системе обладает суперпользователь.

useradd <username> ← • регистрация нового пользователя;

Новые записи в /etc/passwd; /etc/shadow.
Создание домашнего каталога.

id <username> ← • получить информацию о пользователе;

useradd -D ← • выдать настройки команды по умолчанию.

Каталог /etc/skel содержит начальное содержимое домашнего каталога, которое копируется в создаваемый домашний каталог пользователя.

Регистрация учетных записей пользователей

Часто используемые опции (начинаются с «-») команды useradd:

- **s – файл оболочки по умолчанию;**
- d – путь к домашнему каталогу;
- **m – необходимо создавать домашний каталог;**
- M – не создавать домашний каталог;
- k – путь к альтернативному каталогу скелета;
- u – назначить UID;
- g – назначить GID (первичную группу);
- G – список групп пользователя;
- e – дата блокировки учетной записи;
- f – срок после устаревания пароля до блокировки учетной записи.

Если пользователь не имеет право входить в сеанс, то ему в качестве оболочки можно указать:

- /bin/false – системная команда, всегда возвращающая код ошибки;
- /dev/null – специальный файл-поглотитель;
- /sbin/nologin – возвращает код ошибки и сообщение о невозможности входа в сеанс.

Изменение учетной записи

usermod <options> <username>

Большая часть опций совпадает с опциями команды useradd.

usermod -s /bin/false classuser ← •смена оболочки в учетной записи.

userdel <username> ← удаление учетной записи

Команда userdel не удаляет файлы пользователя по умолчанию, это нужно сделать вручную или, используя опцию userdel –r <username>.

Управление группами пользователей

Группы пользователей предназначены для совместного доступа группы лиц к файлам.

Информация о группах хранится в файле /etc/group.

Формат записи: <имя группы>:<пароль группы>:<GID группы>:<список пользователей>

`groupadd <groupname>` ← • создание группы;

`groupdel <groupname>` ← • удаление группы;

`gpasswd A <username> <groupname>` • назначение администратора группы;

`gpasswd a <username> <groupname>`
`gpasswd d <username> <groupname>`

- добавление пользователя к группе
- удаление пользователя из группы (администратором группы);

`gpasswd <password>` ← • задать пароль на вход в группу для не членов группы;

`newgrp <groupname>` ← • изменить текущую группу.

Управление паролями

```
passwd <options> <username>
```

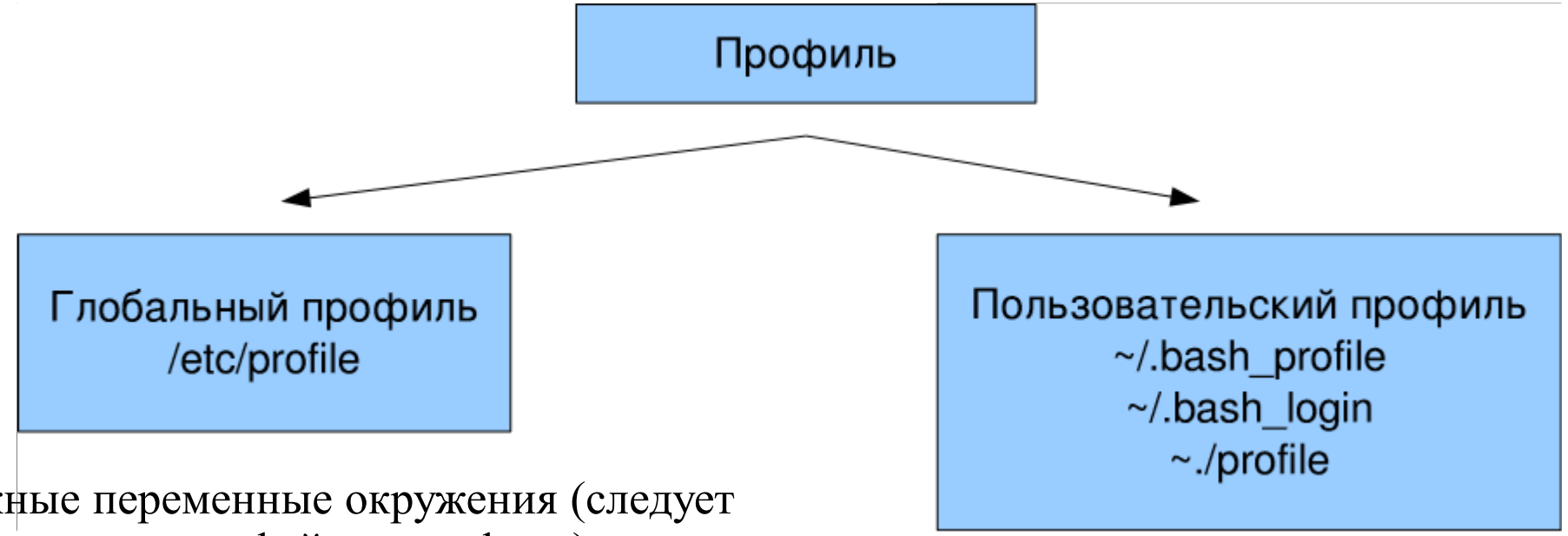
-l – блокировка;
-u – разблокирование;
-S – текущее состояние пароля;
-d – удаление пароля;
-n – период запрета смены пароля;
-x – максимальный срок использования пароля;
-w – период предупреждений;
-i – период после устаревания пароля до блокировки.

Блокирование учетной записи

```
# id lisa
uid=503(lisa) gid=503(lisa) groups=503(lisa),22(cdrom)  #
cat /etc/shadow
lisa:$2a$08$Z4jZgPzM2GDVguFd4TRF3ubB:14316::::::
# passwd -l lisa
# cat /etc/shadow
lisa:!$2a$08$Z4jZgPzM2GDVguFd4TRF3ubB:14316::::::
```

После блокирования учетной записи в первой позиции второго поля файла /etc/shadow перед шифрованным паролем пользователя появляется знак восклицания.

Профили пользователей



Важные переменные окружения (следует устанавливать в файлах профиля):

- PATH – путь поиска исполняемых файлов;
- TERM – тип терминала;
- USER – имя пользователя;
- HOME – путь к домашнему каталогу.

```
PATH = $PATH:$HOME/bin
export PATH
```

Переменные окружения должны быть созданы командой export.