

Настройки прав доступа

Часть 1

Славинский В.В.

20 сентября 2025

Российский университет дружбы народов, Москва, Россия Россия

Информация

..... {.columns align=center} ::: {.column width="70%"}

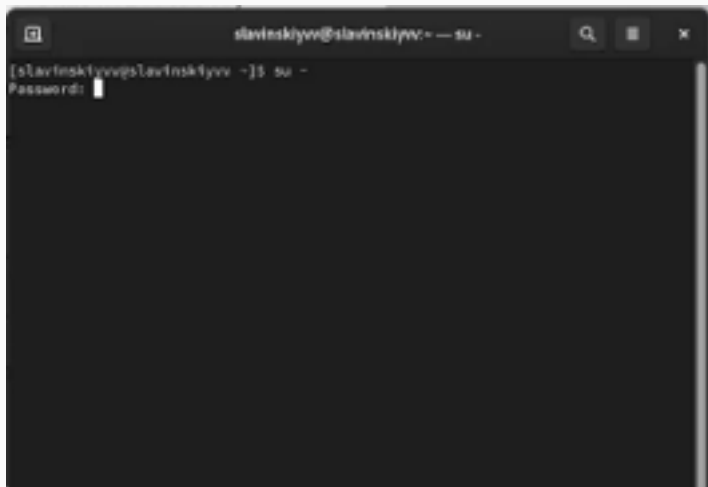
- Славинский Владислав Вадимович
- Студент
- Российский университет дружбы народов
- [1132246169@pfur.ru]

::: ::: {.column width="30%"}

Вводная часть

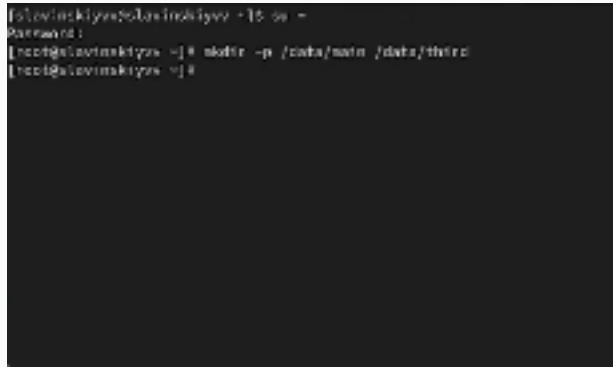
Открытие терминала с root

Откроем терминал с учетной записью root.



Создание каталогов main и third

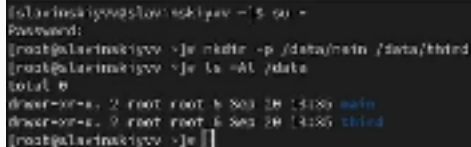
В корневом каталоге создадим каталоги /data/main и /data/third с помощью mkdir.



```
[slovinskiy@elavinskiy ~]$ su -  
Password:  
[root@elavinskiy ~]# mkdir -p /data/main /data/third  
[root@elavinskiy ~]#
```

Рис. 2: sc2

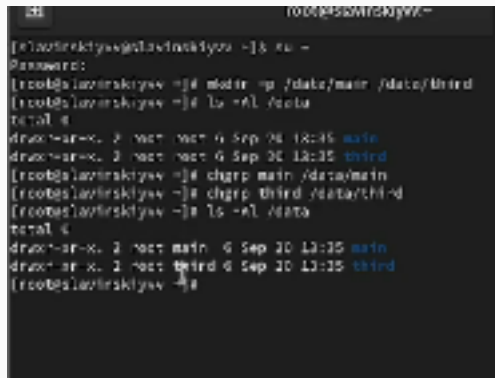
Посмотрим, кто является владельцем этих каталогов, для этого используем команду `ls -Al /data`. Владелец каталогов является root.



```
[root@salavinskiyvv ~]# su -  
Password:  
[root@salavinskiyvv ~]# mkdir -p /data/main /data/third  
[root@salavinskiyvv ~]# ls -Al /data  
total 0  
drwxr-xr-x. 2 root root 4 Sep 20 14:08 main  
drwxr-xr-x. 2 root root 4 Sep 20 14:08 third  
[root@salavinskiyvv ~]#
```

Рис. 3: sc3

Изменим владельцев этих каталогов с root на main и third и посмотрим изменения.



```
root@slavirskiy:~# su -
Password:
[root@slavirskiy ~]# mkdir -p /data/main /data/third
[root@slavirskiy ~]# ls -al /data
total 4
drwxr-xr-x. 2 root root 4 Sep 28 12:45 main
drwxr-xr-x. 2 root root 4 Sep 28 12:45 third
[root@slavirskiy ~]# chgrp main /data/main
[root@slavirskiy ~]# chgrp third /data/third
[root@slavirskiy ~]# ls -al /data
total 4
drwxr-xr-x. 2 root main 4 Sep 28 12:45 main
drwxr-xr-x. 2 root third 4 Sep 28 12:45 third
[root@slavirskiy ~]#
```

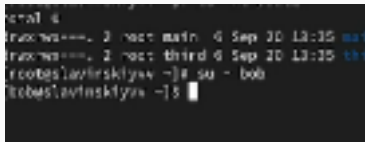
Рис. 4: sc4

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам. Проверяем изменения, как видим, у нас все применилось.

```
total 0
drwxr-xr-x. 2 root main  6 Sep 20 13:25 main
drwxr-xr-x. 2 root third 6 Sep 20 13:25 third
root@slavinskiy: ~# chmod T70 /data/main
root@slavinskiy: ~# chmod T70 /data/third
root@slavinskiy: ~# ls -Al /data
total 0
drwxr-xr-x. 2 root main  6 Sep 20 13:25 main
drwxr-xr-x. 2 root third 6 Sep 20 13:25 third
root@slavinskiy: ~#
```

Рис. 5: sc5

Далее перейдем на учетную запись bob.



```
root@ ~  
root@ ~ # su - bob  
bob@slavinskiy ~$
```

Рис. 6: sc6

Создание файла под пользователем bob в каталоге /data/main

Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге. Видим, что владельцем является bob и группа тоже bob.

```
brkstraxmm: 2 root third 6 Sep 28 13:55 third
[root@localhost ~]# su - bob
[bob@localhost ~]# cd /data/main
[bob@localhost ~]# touch emptyfile
[bob@localhost ~]# ls -la
total 0
-rw-r--r-- 1 bob bob 0 Sep 28 13:55 emptyfile
```

Рис. 7: sc7

Создание файла в каталоге /data/third

Под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Как видим, нам выводится Permission denied или же отказано в доступе, все из-за того, что пользователь bob входил в группу main, а не в группе third.

```
total 0
-rw-r--r-- 1 bob bob 0 Sep 19 13:04 emptyfile
[bob@slavinskiye main]$ cd /data/third/
-bash: cd: /data/third/: Permission denied
[bob@slavinskiye main]$ cd /data/third/
-bash: cd: /data/third/: Permission denied
[bob@slavinskiye main]$ cd
[bob@slavinskiye ~]$ cd /data/third/
-bash: cd: /data/third/: Permission denied
[bob@slavinskiye ~]$
```

Рис. 8: sc8

Переключение на другую учетную запись

Переключимся на учётную запись пользователя alice.

```
[bob@slawinskyyv ~]$ cd  
[bob@slawinskyyv ~]$ cd /data/third/  
-bash: cd: /data/third/: Permission denied  
[bob@slawinskyyv ~]$ su - alice  
Password:  
[alice@slawinskyyv ~]$
```

Рис. 9: sc9

Перейдем в каталог /data/main и создадим два файла, владельцем которых является alice.

```
bob@slavinskiyyv ~]$ su - alice
alice@slavinskiyyv ~]$ cd /data/main
alice@slavinskiyyv main]$ touch alice1
alice@slavinskiyyv main]$ touch alice2
alice@slavinskiyyv main]$
```

Рис. 10: sc10

Перейдем под учётную запись пользователя bob.

A terminal window showing a user switch. The prompt is [alice@slavinskiyvm: ~]\$ and the command is su - bob. The prompt changes to [bob@slavinskiyvm: ~]\$ and there is a cursor at the end.

```
[alice@slavinskiyvm: ~]$ su - bob
Password:
[bob@slavinskiyvm: ~]$
```

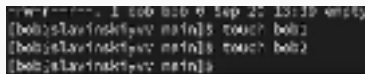
Рис. 11: sc11

Перейдем в каталог `/data/main`. Введем команду `ls -l`, чтобы увидеть файлы `alice`, и попробуем удалить файлы. Как видим, через пользователя `bob`, мы смогли удалить файлы `alice` в каталоге `main`.

```
bob@alaxinaksyev: main$ ls -l
total 0
-rw-r--r-- 1 alice alice 0 Sep 20 18:45 alice1
-rw-r--r-- 1 alice alice 0 Sep 20 18:45 alice2
-rw-r--r-- 1 bob  bob  0 Sep 20 18:22 emptyfile
bob@alaxinaksyev: main$ rm -f alice*
bob@alaxinaksyev: main$ ls -l
total 0
-rw-r--r-- 1 bob bob 0 Sep 20 18:22 emptyfile
bob@alaxinaksyev: main$
```

Рис. 12: sc12

Создадим два файла, которые принадлежат пользователю bob.

A terminal window showing the execution of the 'touch' command to create files for user 'bob'. The prompt is '[bob@slavinskijv: ~]\$'. The first command is 'touch bob1', followed by 'touch bob2'. The prompt returns after each command. The final line shows the prompt '[bob@slavinskijv: ~]\$' without a command.

```
[bob@slavinskijv: ~]$ touch bob1  
[bob@slavinskijv: ~]$ touch bob2  
[bob@slavinskijv: ~]$
```

Рис. 13: sc13

Установка бит идентификатора группы и sticky-бит для общего каталога группы

Под пользователем root установим для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы.

```
root@kali:~#  
[root@kali:~]# chmod g+px /data/main  
[root@kali:~]#
```

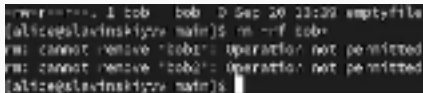
Рис. 14: sc14

Под пользователем alice создадим в каталоге /data/main файлы alice3 и alice4. Здесь мы видим, что два этих файла принадлежать групппе main

```
total 0
-rw-r--r--. 1 alice main 0 Sep 20 13:48 alice3
-rw-r--r--. 1 alice main 0 Sep 20 13:48 alice4
-rw-r--r--. 1 bob  bob  0 Sep 20 13:48 bob1
-rw-r--r--. 1 bob  bob  0 Sep 20 13:48 bob2
-rw-r--r--. 1 bob  bob  0 Sep 20 13:49 emptyfile
[alice@elastinsky: /data/main]$
```

Рис. 15: sc15

Под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob с помощью команды: `rm -rf bob*`. Sticky-bit предотвратил удаление, поскольку alice не является создателем файлов, но alice является создателем каталога, поэтому все равно alice сможет все удалить.

A terminal window showing a file listing and a failed removal command. The file listing shows a directory 'bob' owned by 'bob' with the sticky bit set. The command 'rm -rf bob*' is executed, but it fails with the message 'rm: cannot remove 'bob/b': operation not permitted' for both the directory and the file inside it.

```
alice@slavinskiy:~$ ls -ld bob
drwxr-xr-x 1 bob  bob  0 Sep 20 23:39 empty-file
alice@slavinskiy:~$ rm -rf bob*
rm: cannot remove 'bob/b': operation not permitted
rm: cannot remove 'bob/b': operation not permitted
alice@slavinskiy:~$
```

Рис. 16: sc16

Переключимся в терминале на учётную запись пользователя root



```
root@kali:~# su alessandra -s /bin/bash  
[alessandra@kali:~]$ su -  
Password:  
[root@kali:~#]#
```

Рис. 17: sc17

Установим права на чтение и выполнение в каталоге `/data/main` для группы `third` и права на чтение и выполнение для группы `main` в каталоге `/data/third`.



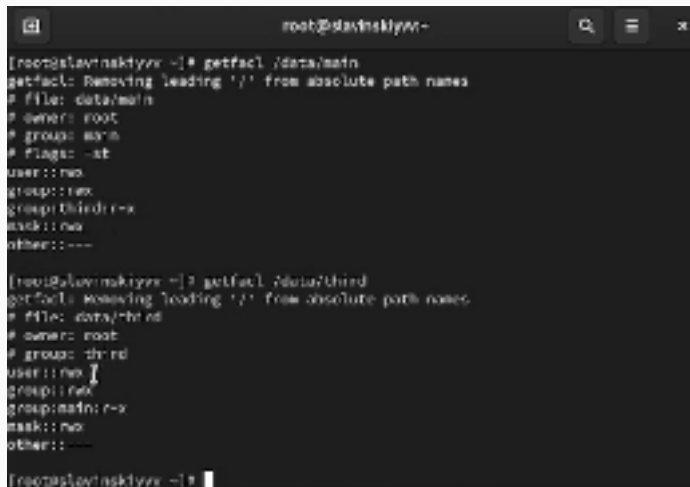
```

Password:
[root@alavinskiiy ~]# setfacl -m g:third:rx /data/main
[root@alavinskiiy ~]# setfacl -m g:main:rx /data/third
[root@alavinskiiy ~]#
```

Рис. 18: sc18

Проверка разрешений

Используем команду `getfacl`, чтобы убедиться в правильности установки разрешений. Как видим, в каталоге `main` высвечивается `third`, а для `third-main`.

A terminal window titled 'root@slavinskiyyr-' with search, list, and close icons in the top right. The terminal shows two commands and their outputs. The first command is 'getfacl /data/main', and the output shows permissions for file 'data/main' owned by 'root' and group 'main', with a 'third' group listed in the permissions. The second command is 'getfacl /data/third', and the output shows permissions for file 'data/third' owned by 'root' and group 'third', with a 'main' group listed in the permissions.

```
[root@slavinskiyyr ~]# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -at
user::no
group::no
group:third:r-x
mask::no
other::---
```

```
[root@slavinskiyyr ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::no
group::no
group:main:r-x
mask::no
other::---
```

```
[root@slavinskiyyr ~]#
```

Полномочия файла newfile1

Создадим новый файл с именем newfile1 в каталоге /data/main и используем getfacl /data/main/newfile1 для проверки текущих назначений полномочий. Видим, что для пользователя у нас полномочия для записи и чтения, а для группы только для чтения. Так же владельцами являются пользователь root и группа main.

```
root@slavinskiyy: ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rw-
group::r--
other::r--

root@slavinskiyy: ~]# cd /data/main
root@slavinskiyy: /data/main]# touch /data/main/newfile1
root@slavinskiyy: /data/main]# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rw-
group::r--
other::r--
```


Полномочия файла newfile1 в каталоге third

Сделаем тоже самое, только в каталоге /data/third и видим, что владелец группы является уже не third, а root.

```
# group: third
user: orw-
group: orw-
other: orw-

[root@salvatore:~]# cd
[root@salvatore:~]# cd /data/third/
[root@salvatore:third]# touch /data/third/newfile1
[root@salvatore:third]# getfacl /data/third/newfile1
getfacl: removing leading '/' from absolute path names
# file: data/third/newfile1
# owner: root
# group: root
user:: orw-
group:: orw-
other:: orw-
```

Рис. 21: sc21

Установим ACL по умолчанию для каталога /data/main.

```
stf@sc22:~$  
[root@slavinskysv ~]# cd /data/main  
[root@slavinskysv ~]# setfacl -m d::trind:rwx /data/main  
[root@slavinskysv ~]#
```

Рис. 22: sc22

Добавим ACL по умолчанию для каталога /data/third.

```
[root@slavinskijv ~]# cd /data/third
[root@slavinskijv ~]# setfacl -m d:sg:third:rwx /data/main
[root@slavinskijv ~]# setfacl -m d:sg:main:rwx /data/third
[root@slavinskijv ~]#
```

Рис. 23: sc23

Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main. Видим, что что настройки работают, полномочия для third тоже есть.

```
root@elawinaki-pv ~# setfacl -m d:group:main:rx /data/main
root@elawinaki-pv ~# touch /data/main/newfile0
root@elawinaki-pv ~# getfacl /data/main/newfile0
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile0
# owner: root
# group: main
user::rw-
group:rwx
group:third:rwx
mask::rw-
other::---
root@elawinaki-pv ~#
```

Рис. 24: sc24

Проверка настроек

Сделаем те же действия только для каталога /data/third. Теперь у группы third есть полномочия в каталоге main.

```
# owner: root
# group: main
user::rw-
group::rwx
group:third:rwx
mask::rw-
other::---

[root@slavinskiyy ~]# touch /data/third/newfile2
[root@slavinskiyy ~]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::rwx
group:main:rwx
mask::rw-
other::---

[root@slavinskiyy ~]#
```

Рис. 25: sc25

Для проверки полномочий группы third войдем под учётной записью члена группы third.

```
other::--  
other::--  
[rus@alevinskijye ~]$ su - carol  
[carol@alevinskijye ~]$
```

Рис. 26: sc26

Проверка операций с файлами

Попробуем удалить newfile1 и newfile2 и осуществить запись в эти файлы. Как видим, удалось записать только в newfile2, поскольку мы применили настройки для newfile2 для записи и чтения, а для newfile1 только для чтения.

```
other:---
[root@slavinskiyy ~]# touch /data/ibind/newfile2
[root@slavinskiyy ~]# getfacl /data/ibind/newfile2
facl: Removing leading '/' from absolute path names
# file: data/ibind/newfile2
# owner: root
# group: root
user::rw-
group::rwx          seffect::reim-
group::admin:rw-    seffect::reim-
mask::rw-
other:---

[root@slavinskiyy ~]# su - carol
carol@slavinskiyy ~$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1': y
rm: cannot remove '/data/main/newfile1': Permission denied
carol@slavinskiyy ~$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
carol@slavinskiyy ~$ echo "hello, world!" >> /data/main/newfile1
baad: /data/main/newfile1: Permission denied
```