

Лабораторная работа №3

Настройка прав доступа

Ришард Когенгар

18 января 2026

Цель работы

Основная цель

Получение навыков настройки базовых и специальных прав доступа для групп пользователей в ОС типа Linux.

Ход выполнения работы

Подготовка каталогов

- Вход под `root`
- Созданы: `/data/main`, `/data/third`
- Проверены владелец/группа

```
rishard@rishardkogengar:~$ su
Password:
root@rishardkogengar:/home/rishard#
root@rishardkogengar:/home/rishard# mkdir -p /data/main /data/third
root@rishardkogengar:/home/rishard# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Jan 18 13:04 main
drwxr-xr-x. 2 root root 6 Jan 18 13:04 third
root@rishardkogengar:/home/rishard# chgrp main /data/main
root@rishardkogengar:/home/rishard# chgrp third /data/third/
root@rishardkogengar:/home/rishard# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Jan 18 13:04 main
drwxr-xr-x. 2 root third 6 Jan 18 13:04 third
root@rishardkogengar:/home/rishard# chmod 770 /data/main/
root@rishardkogengar:/home/rishard# chmod 770 /data/third/
```

Права 770 и проверка пользователя

- На каталоги выставлено 770
- bob в группе main создаёт файл в /data/main
- Доступ в /data/third для bob запрещён

```
root@rishardkogengar:/home/rishard#  
root@rishardkogengar:/home/rishard# su bob  
bob@rishardkogengar:/home/rishard$ cd /data/main/  
bob@rishardkogengar:/data/main$ touch emptyfile  
bob@rishardkogengar:/data/main$ ls -Al  
total 0  
-rw-r--r--. 1 bob bob 0 Jan 18 13:06 emptyfile  
bob@rishardkogengar:/data/main$ cd /data/third/  
bash: cd: /data/third/: Permission denied  
bob@rishardkogengar:/data/main$
```

Рис. 2: Проверка доступа bob

Поведение без sticky bit

- alice создала файлы в /data/main
- bob смог удалить чужие файлы (запись в каталог разрешена группе)

```
bob@rishardkogengar:/data/main$  
bob@rishardkogengar:/data/main$ su alice  
Password:  
alice@rishardkogengar:/data/main$ cd /data/main/  
alice@rishardkogengar:/data/main$ touch alice1  
alice@rishardkogengar:/data/main$ touch alice2  
alice@rishardkogengar:/data/main$ su bob  
Password:  
bob@rishardkogengar:/data/main$ cd /data/main/  
bob@rishardkogengar:/data/main$ ls -l  
total 0  
-rw-r--r--. 1 alice alice 0 Jan 18 13:08 alice1  
-rw-r--r--. 1 alice alice 0 Jan 18 13:08 alice2  
-rw-r--r--. 1 bob   bob   0 Jan 18 13:06 emptyfile  
bob@rishardkogengar:/data/main$ rm -f alice*  
bob@rishardkogengar:/data/main$ ls -l  
total 0
```

setgid + sticky bit на /data/main

- Включён setgid: новые файлы наследуют группу каталога
- Включён sticky bit: нельзя удалять чужие файлы

```
bob@rishardkogengar:/data/main$ touch bob1
bob@rishardkogengar:/data/main$ touch bob2
bob@rishardkogengar:/data/main$ su
Password:
root@rishardkogengar:/data/main# chmod g+s,o+t /data/main/
root@rishardkogengar:/data/main# su alice
alice@rishardkogengar:/data/main$ touch alice3
alice@rishardkogengar:/data/main$ touch alice4
alice@rishardkogengar:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Jan 18 13:10 alice3
-rw-r--r--. 1 alice main 0 Jan 18 13:10 alice4
-rw-r--r--. 1 bob    bob  0 Jan 18 13:10 bob1
-rw-r--r--. 1 bob    bob  0 Jan 18 13:10 bob2
-rw-r--r--. 1 bob    bob  0 Jan 18 13:06 emptyfile
alice@rishardkogengar:/data/main$ rm -rf bob*
```

- Для /data/main: группе third выдано r-x
- Для /data/third: группе main выдано r-x
- Проверка через getfacl

```
alice@rishardkogengar:/data/main$ su
Password:
root@rishardkogengar:/data/main# setfacl -m g:third:rx /data/main
root@rishardkogengar:/data/main# setfacl -m g:main:rx /data/third
root@rishardkogengar:/data/main# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other::---

root@rishardkogengar:/data/main# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
```

Проблема: ACL не наследуется

- Создан newfile1
- ACL каталога не перешёл на новый файл
- Нужны **default ACL**

```
root@rishardkogengar:/data/main# touch /data/main/newfile1
root@rishardkogengar:/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--

root@rishardkogengar:/data/main# touch /data/third/newfile1
root@rishardkogengar:/data/main# getfacl /data/third/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile1
# owner: root
# group: root
```

Default ACL: наследование включено

- Заданы default ACL для каталогов
- Создан newfile2
- Новый файл получил нужные ACL автоматически

```
root@rishardkogengar:/data/main# setfacl -m d:g:third:rwx /data/main/
root@rishardkogengar:/data/main# setfacl -m d:g:main:rwx /data/third/
root@rishardkogengar:/data/main# touch /data/main/newfile2
root@rishardkogengar:/data/main# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rw-
group::rwx          #effective:rw-
group:third:rwx      #effective:rw-
mask::rw-
other::---

root@rishardkogengar:/data/main# touch /data/third/newfile2
root@rishardkogengar:/data/main# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
```

Проверка доступа пользователем third

- Вход под `carol` (группа `third`)
- Операции доступа/записи зависят от ACL файла и прав на каталог
- Удаление чужих файлов ограничено (sticky bit)

```
root@rishardkogengar:/data/main#  
root@rishardkogengar:/data/main# su carol  
carol@rishardkogengar:/data/main$ rm /data/main/newfile1  
rm: remove write-protected regular empty file '/data/main/newfile1'? y  
rm: cannot remove '/data/main/newfile1': Permission denied  
carol@rishardkogengar:/data/main$ rm /data/main/newfile2  
rm: cannot remove '/data/main/newfile2': Permission denied  
carol@rishardkogengar:/data/main$ echo "Hello world" >> /data/main/newfile1  
bash: /data/main/newfile1: Permission denied  
carol@rishardkogengar:/data/main$ echo "Hello world" >> /data/main/newfile2  
carol@rishardkogengar:/data/main$ █
```

Рис. 8: Проверка `carol`

Выводы

- Настроены базовые права `chmod` и разграничение по группам
- Проверены `setgid` (наследование группы) и `sticky bit` (защита от удаления чужих файлов)
- Настроены `ACL` и `default ACL` для наследования прав на новые файлы