

Лабораторная работа №3

Настройка прав доступа

Сергеев Д. О.

20 сентября 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Сергеев Даниил Олегович
- Студент
- Направление: Прикладная информатика
- Российский университет дружбы народов
- 1132246837@pfur.ru

Цель работы

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

Задание

- Прочитать справочное описание `man` по командам `chgrp`, `chmod`, `getfacl`, `setfacl`.
- Выполнить действия по управлению базовыми разрешениями для групп пользователей.
- Выполнить действия по управлению специальными разрешениями для групп пользователей.
- Выполнить действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей.

Ход выполнения лабораторной работы

Управление базовыми разрешениями для групп пользователей

```
[dosergeev@dosergeev ~]$ su -  
Password:  
[root@dosergeev ~]# mkdir -p /data/main /data/third  
[root@dosergeev ~]# ls -Al /data  
total 0  
drwxr-xr-x. 2 root root 6 Sep 20 19:09 main  
drwxr-xr-x. 2 root root 6 Sep 20 19:09 third  
[root@dosergeev ~]# chgrp main /data/main  
[root@dosergeev ~]# chgrp main /data/third  
[root@dosergeev ~]# ls -Al /data  
total 0  
drwxr-xr-x. 2 root main 6 Sep 20 19:09 main  
drwxr-xr-x. 2 root main 6 Sep 20 19:09 third  
[root@dosergeev ~]# chgrp third /data/third  
[root@dosergeev ~]# ls -Al /data  
total 0  
drwxr-xr-x. 2 root main 6 Sep 20 19:09 main  
drwxr-xr-x. 2 root third 6 Sep 20 19:09 third  
[root@dosergeev ~]# chmod 770 /data/main  
[root@dosergeev ~]# chmod 770 /data/third  
[root@dosergeev ~]# ls -Al /data  
total 0  
drwxrwx---. 2 root main 6 Sep 20 19:09 main  
drwxrwx---. 2 root third 6 Sep 20 19:09 third
```

Рис. 1: Установка прав доступа и владельца. Проверка выполненных действий

```
[dosergeev@dosergeev ~]$ su - bob
Password:
[bob@dosergeev ~]$ cd /data/main/
[bob@dosergeev main]$ touch emptyfile
[bob@dosergeev main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 20 19:11 emptyfile
[bob@dosergeev main]$ groups bob
bob : bob main
[bob@dosergeev main]$ cd /data/third
-bash: cd: /data/third: Permission denied
```

Рис. 2: Создание файла в каталогах main и third за пользователя bob

```
[dosergeev@dosergeev ~]$ su - alice  
Password:  
[alice@dosergeev ~]$ cd /data/main/  
[alice@dosergeev main]$ touch alice1  
[alice@dosergeev main]$ touch alice2
```

Рис. 3: Создание файлов за alice

```
[bob@dosergeev main]$ cd /data/main
[bob@dosergeev main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 20 19:14 alice1
-rw-r--r--. 1 alice alice 0 Sep 20 19:14 alice2
-rw-r--r--. 1 bob   bob   0 Sep 20 19:11 emptyfile
[bob@dosergeev main]$ rm -f alice*
[bob@dosergeev main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 20 19:11 emptyfile
[bob@dosergeev main]$ touch bob1
[bob@dosergeev main]$ touch bob2
```

Рис. 4: Удаление и создание файлов за bob в /data/main

```
[root@dosergeev ~]# chmod g+s,o+t /data/main  
[root@dosergeev ~]# ls -Al /data  
total 0  
drwxrws--T. 2 root main  47 Sep 20 19:15 main  
drwxrwx---. 2 root third  6 Sep 20 19:09 third
```

Рис. 5: Поставим бит идентификатора группы b sticky-бит для /data/main

```
[alice@dosergeev main]$ touch alice3
[alice@dosergeev main]$ touch alice4
[alice@dosergeev main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 20 19:16 alice3
-rw-r--r--. 1 alice main 0 Sep 20 19:16 alice4
-rw-r--r--. 1 bob   bob   0 Sep 20 19:15 bob1
-rw-r--r--. 1 bob   bob   0 Sep 20 19:15 bob2
-rw-r--r--. 1 bob   bob   0 Sep 20 19:11 emptyfile
[alice@dosergeev main]$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@dosergeev main]$
```

Рис. 6: Проверка группы и удаление файлов за alice

Управление расширенными разрешениями с использованием списков ACL для групп пользователей

```
[root@dosergeev ~]# setfacl -m g:third:rx /data/main
[root@dosergeev ~]# setfacl -, g:main:rx /data/third
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try 'setfacl --help' for more information.
[root@dosergeev ~]# setfacl -m g:main:rx /data/third
[root@dosergeev ~]# 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@dosergeev ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
group::rwx
group:main:r-x
mask::rwx
other:---
```

Рис. 7: Изменение прав с помощью ACL

Управление расширенными разрешениями с использованием списков ACL для групп пользователей

```
[root@dosergeev ~]# touch /data/main/newfile1
[root@dosergeev ~]# getfacl /data/main/
alice3      alice4      bob1        bob2        emptyfile  newfile1
[root@dosergeev ~]# 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@dosergeev ~]# touch /data/third/newfile1
[root@dosergeev ~]# getfacl /data/third/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile1
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

Рис. 8: Создание файла newfile1, проверка его прав доступа

Управление расширенными разрешениями с использованием списков ACL для групп пользователей

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



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

Рис. 9: Установка прав ACL по умолчанию

Управление расширенными разрешениями с использованием списков ACL для групп пользователей

```
[alice@dosergeev main]$ su - carol
Password:
[carol@dosergeev ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'?
[carol@dosergeev ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@dosergeev ~]$ groups
users third
[carol@dosergeev ~]$ ls /data/main
alice3 alice4 bob1 bob2 emptyfile newfile1 newfile2
[carol@dosergeev ~]$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Permission denied
[carol@dosergeev ~]$ echo "Hello, world" >> /data/main/newfile2
[carol@dosergeev ~]$ cat /data/main/newfile2
Hello, world
```

Рис. 10: Проверка полномочий группы third в /data/main

Ответы на контрольные вопросы

1. Как следует использовать команду `chown`, чтобы установить владельца группы для файла?
 - Чтобы установить владельца группы и группу: `chown пользователь:группа файл`, или же `chown :группа файл`.
 - Например из лабораторной работы: `chown carol:third /data/main/*` установит для всех файлов в каталоге `main` владельца `carol` и группу `third`.
2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю?
 - Можно использовать
 - `find / -user пользователь`
 - `find / -uid UID_пользователя`.

3. Как применить разрешения на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп, не устанавливая никаких прав для других?
- Можно использовать команду `chmod` с ключем `-R`
 - Например используем `chmod -R ug=rwx,o-rwx /data`
4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?
- Можно использовать команду `chmod +x файл`

5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога?
- Для этого нужно поставить SGID с помощью команды `chmod` с опцией `+s`.
 - Например используем `chmod g+s /data/main` - все файлы в каталоге будут созданы с группой `main`.
6. Необходимо, чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они являются. С помощью какой команды можно это сделать?
- Для этого нужно поставить sticky-бит. Это можно сделать с помощью команды: `chmod +t` каталог

7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?
- Используем команду `setfacl -R -m g:группа:r *` для рекурсивного изменения прав доступа в текущем каталоге.

8. Что нужно сделать для гарантии того, что члены группы получают разрешения на чтение для всех файлов в текущем каталоге и во всех его подкаталогах, а также для всех файлов, которые будут созданы в этом каталоге в будущем?
- Сначала нужно установить право на чтение для текущих файлов: `setfacl -R -m g:группа:r каталог`
 - Потом установить права для умолчанию для будущих файлов: `setfacl -m d:g:группа:r каталог`
 - Например для каталога `/data/third` можно сразу прописать `setfacl -R -m d:g:dosergeev:r /data/main`.

9. Какое значение `umask` нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы?
- Нужно использовать команду `umask`.
 - Например чтобы другие пользователи не получали какие-либо разрешения на новые файлы напишем `umask 007(rwxrwx—)` для установление маски по умолчанию для текущего пользователя
10. Какая команда гарантирует, что никто не сможет удалить файл `myfile` случайно?
- Используем команду `chattr` с атрибутом `+i`. Он устанавливает файл как неизменяемый, что защищает его от любых изменений, в том числе и удаления.
 - Например: `chattr +i файл`

Вывод

В результате выполнения лабораторной работы я получил навыки настройки базовых и специальных прав доступа для групп пользователей в Linux, в том числе с использованием ACL.