

Лабораторная работа №3

Основы администрирования операционных систем

Верниковская Е. А., НПИбд-01-23

16 сентября 2024

Российский университет дружбы народов, Москва, Россия

Вводная часть

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

1. Прочитать справочное описание man по нескольким командам.
2. Выполнить действия по управлению базовыми разрешениями для групп пользователей.
3. Выполнить действия по управлению специальными разрешениями для групп пользователей.
4. Выполнить действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей.

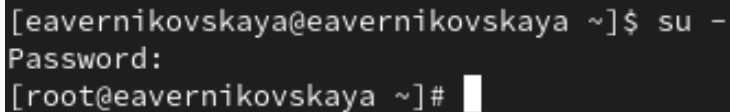
Выполнение лабораторной работы

Открываем терминал и читаем справочное описание man по командам chgrp, chmod, getfacl и setfacl (рис. 1)

```
[eavernikovskaya@eavernikovskaya ~]$ man chgrp  
[eavernikovskaya@eavernikovskaya ~]$ man chmod  
[eavernikovskaya@eavernikovskaya ~]$ man getfacl  
[eavernikovskaya@eavernikovskaya ~]$ man setfacl  
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 1: Команда man

Открываем терминал с учётной записью root: *su -* (рис. 2)



```
[eavernikovskaya@eavernikovskaya ~]$ su -  
Password:  
[root@eavernikovskaya ~]#
```

Рис. 2: Учётная запись root

В корневом каталоге создаём каталоги /data/main и /data/third (рис. 3)

```
[root@eavernikovskaya ~]# mkdir -p /data/main /data/third  
[root@eavernikovskaya ~]#
```

Рис. 3: Создание каталогов /data/main и /data/third

Смотрим, кто является владельцем этих каталогов. Владелец каталогов является суперпользователь root (рис. 4)

```
[root@eavernikovskaya ~]# ls -Al /data/  
total 0  
drwxr-xr-x. 2 root root 6 Sep 15 21:32 main  
drwxr-xr-x. 2 root root 6 Sep 15 21:32 third  
[root@eavernikovskaya ~]#
```

Рис. 4: Информация о каталогах /data/main и /data/third (1)

Далее меняем владельцев этих каталогов с root на main и third соответственно, с помощью команды *chgrp* (рис. 5)

```
[root@eavernikovskaya ~]# chgrp main /data/main  
[root@eavernikovskaya ~]# chgrp third /data/third  
[root@eavernikovskaya ~]#
```

Рис. 5: Изменение владельцев каталогов /data/main и /data/third

Проверяем, кто теперь является владельцем этих каталогов. (рис. 6)

```
[root@eavernikovskaya ~]# ls -Al /data/  
total 0  
drwxr-xr-x. 2 root main  6 Sep 15 21:32 main  
drwxr-xr-x. 2 root third 6 Sep 15 21:32 third  
[root@eavernikovskaya ~]#
```

Рис. 6: Информация о каталогах /data/main и /data/third (2)

Устанавливаем разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам (рис. 7)

```
[root@eavernikovskaya ~]# chmod 770 /data/main/  
[root@eavernikovskaya ~]# chmod 770 /data/third/  
[root@eavernikovskaya ~]#
```

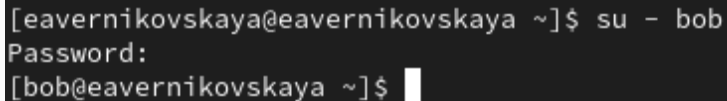
Рис. 7: Установление разрешений

Далее проверяем установленные права доступа (рис. 8)

```
[root@eavernikovskaya ~]# ls -Al /data/  
total 0  
drwxrwx---. 2 root main  6 Sep 15 21:32 main  
drwxrwx---. 2 root third 6 Sep 15 21:32 third  
[root@eavernikovskaya ~]#
```

Рис. 8: Установленные права доступа

В другом терминале переходим под учётную запись пользователя bob: `su - bob` (рис. 9)



```
[eavernikovskaya@eavernikovskaya ~]$ su - bob
Password:
[bob@eavernikovskaya ~]$
```

Рис. 9: Учётная запись bob

Под пользователем bob пробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге. Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл (рис. 10)

```
[bob@eavernikovskaya ~]$ cd /data/main/  
[bob@eavernikovskaya main]$ touch emptyfile  
[bob@eavernikovskaya main]$ ls -Al  
total 0  
-rw-r--r--. 1 bob bob 0 Sep 15 21:41 emptyfile  
[bob@eavernikovskaya main]$
```

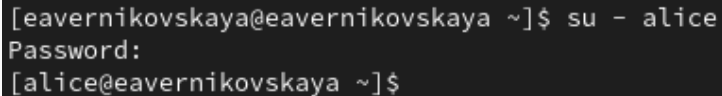
Рис. 10: Каталог /data/main в учётной записи bob и создание файла

Под пользователем bob пробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Так как пользователь bob не является владельцем каталога third, нам не удалось перейти в этот каталог и создать в нём новый файл (рис. 11)

```
[bob@eavernikovskaya main]$ cd /data/third/  
-bash: cd: /data/third/: Permission denied  
[bob@eavernikovskaya main]$
```

Рис. 11: Каталог /data/third в учётной записи bob и создание файла

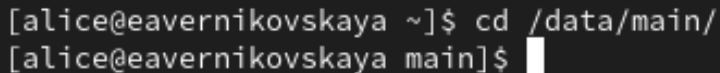
Открываем новый терминал под пользователем alice (рис. 12)



```
[eavernikovskaya@eavernikovskaya ~]$ su - alice  
Password:  
[alice@eavernikovskaya ~]$
```

Рис. 12: Учётная запись alice

Переходим в каталог `/data/main` и создаём два файла, владельцем которых является `alice` (рис. 13), (рис. 14)

A terminal window with a dark background and light-colored text. The first line shows the prompt `[alice@eavernikovskaya ~]$` followed by the command `cd /data/main/`. The second line shows the prompt `[alice@eavernikovskaya main]$` followed by a white cursor block.

```
[alice@eavernikovskaya ~]$ cd /data/main/  
[alice@eavernikovskaya main]$
```

Рис. 13: Переход в каталог `/data/main` под `alice`

```
[alice@eavernikovskaya main]$ touch alice1  
[alice@eavernikovskaya main]$ touch alice2  
[alice@eavernikovskaya main]$
```

Рис. 14: Создание файлов alice1 и alice2

В другом терминале переходим под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice). Далее переходим в каталог /data/main и видим там два файла, созданные пользователем alice (рис. 15)

```
[bob@eavernikovskaya main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 15 21:44 alice1
-rw-r--r--. 1 alice alice 0 Sep 15 21:44 alice2
-rw-r--r--. 1 bob   bob   0 Sep 15 21:41 emptyfile
[bob@eavernikovskaya main]$
```

Рис. 15: Файлы, которые видит bob

Попробуем удалить файлы, принадлежащие пользователю alice. Файлы успешно удалены (рис. 16)

```
[bob@eavernikovskaya main]$ rm -f alice*  
[bob@eavernikovskaya main]$ ls  
emptyfile  
[bob@eavernikovskaya main]$
```

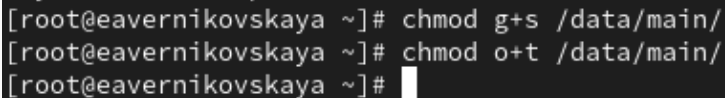
Рис. 16: Удаление файлов (1)

Создаём два файла, которые принадлежат пользователю bob (рис. 17)

```
[bob@eavernikovskaya main]$ touch bob1
[bob@eavernikovskaya main]$ touch bob2
[bob@eavernikovskaya main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 15 21:47 bob1
-rw-r--r--. 1 bob bob 0 Sep 15 21:47 bob2
-rw-r--r--. 1 bob bob 0 Sep 15 21:41 emptyfile
[bob@eavernikovskaya main]$
```

Рис. 17: Создание файлов bob1 и bob2

В терминале под пользователем root устанавливаем для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы `chmod g+s,o+t /data/main` (рис. 18)



```
[root@eavernikovskaya ~]# chmod g+s /data/main/  
[root@eavernikovskaya ~]# chmod o+t /data/main/  
[root@eavernikovskaya ~]#
```

Рис. 18: Установка бит идентификатора группы и sticky-бит для разделяемого (общего) каталога группы

В терминале под пользователем alice создаём в каталоге /data/main файлы alice3 и alice4. Теперь мы видим, что два созданных нами файла принадлежат группе main, которая является группой-владельцем каталога /data/main (рис. 19)

```
[alice@eavernikovskaya main]$ touch alice3
[alice@eavernikovskaya main]$ touch alice4
[alice@eavernikovskaya main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 15 21:51 alice3
-rw-r--r--. 1 alice main 0 Sep 15 21:51 alice4
-rw-r--r--. 1 bob   bob   0 Sep 15 21:47 bob1
-rw-r--r--. 1 bob   bob   0 Sep 15 21:47 bob2
-rw-r--r--. 1 bob   bob   0 Sep 15 21:41 emptyfile
[alice@eavernikovskaya main]$
```

Рис. 19: Информация о файлах alice3 и alice4

В терминале под пользователем alice пробуем удалить файлы, принадлежащие пользователю bob. Sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов (operation not permitted)(рис. 20)

```
[alice@eavernikovskaya main]$ rm -rf bob*  
rm: cannot remove 'bob1': Operation not permitted  
rm: cannot remove 'bob2': Operation not permitted  
[alice@eavernikovskaya main]$
```

Рис. 20: Удаление файлов (2)

Управление расширенными разрешениями с использованием списков ACL

Открываем терминал с учётной записью root и устанавливаем 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, используя *setfacl -m* (рис. 21)

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

Рис. 21: Установка прав на чтение и выполнение в каталогах для групп

Управление расширенными разрешениями с использованием списков ACL

Используем команду *getfacl*, чтобы убедиться в правильности установки разрешений (рис. 22), (рис. 23)

```
[root@eavernikovskaya ~]# 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::---
```

Рис. 22: Проверка правильности установки разрешений в каталоге main

Управление расширенными разрешениями с использованием списков ACL

```
[root@eavernikovskaya ~]# 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::---  
  
[root@eavernikovskaya ~]#
```

Рис. 23: Проверка правильности установки разрешений в каталоге third

Управление расширенными разрешениями с использованием списков ACL

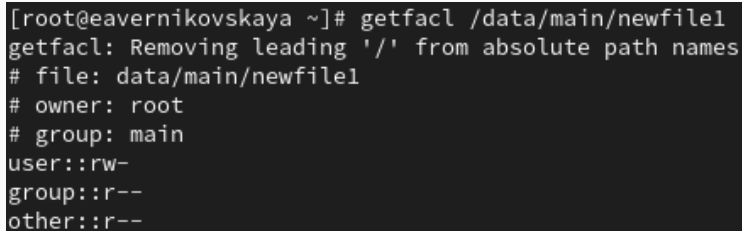
Создаём новый файл с именем newfile1 в каталоге /data/main (рис. 24)

```
[root@eavernikovskaya ~]# cd /data/main/  
[root@eavernikovskaya main]# touch newfile1  
[root@eavernikovskaya main]#
```

Рис. 24: Создание newfile1 в каталоге /data/main

Управление расширенными разрешениями с использованием списков ACL

Используем `getfacl /data/main/newfile1` для проверки текущих назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение. Работать с этим файлом пользователи не могут, потому что мы устанавливали права на чтение и выполнение именно для каталогов, а не для созданных в нём файлов (рис. 25)



```
[root@eavernikovskaya ~]# 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--
```

Рис. 25: Информация о файле newfile1 в каталоге /data/main

Управление расширенными разрешениями с использованием списков ACL

Выполняем аналогичные действия для каталога /data/third. Пояснения те же самые что и к прошлому пункту (рис. 26)

```
[root@eavernikovskaya ~]# touch /data/third/newfile1
[root@eavernikovskaya ~]# 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. 26: Информация о файле newfile1 в каталоге /data/third

Управление расширенными разрешениями с использованием списков ACL

Устанавливаем ACL по умолчанию для каталога /data/main, с помощью *setfacl -m d:g:third:rwX* (рис. 27)

```
[root@eavernikovskaya ~]# setfacl -m d:g:third:rwX /data/main/  
[root@eavernikovskaya ~]#
```

Рис. 27: Установка ACL по умолчанию для каталога /data/main

Управление расширенными разрешениями с использованием списков ACL

Устанавливаем ACL по умолчанию для каталога /data/third (рис. 28)

```
[root@eavernikovskaya ~]# setfacl -m d:g:main:rwX /data/third/  
[root@eavernikovskaya ~]#
```

Рис. 28: Установка ACL по умолчанию для каталога /data/third

Управление расширенными разрешениями с использованием списков ACL

Добавляем новый файл newfile2 в каталог /data/main и проверяем, что настройки ACL работают (рис. 29), (рис. 30)

```
[root@eavernikovskaya ~]# touch /data/main/newfile2  
[root@eavernikovskaya ~]#
```

Рис. 29: Создание newfile2 в каталоге /data/main

Управление расширенными разрешениями с использованием списков ACL

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]# █

Рис. 30: Информация о файле newfile2 в каталоге /data/main

Управление расширенными разрешениями с использованием списков ACL

Выполняем аналогичные действия для каталога /data/third (рис. 31), (рис. 32)

```
[root@eavernikovskaya ~]# touch /data/third/newfile2  
[root@eavernikovskaya ~]#
```

Рис. 31: Создание newfile2 в каталоге /data/third

Управление расширенными разрешениями с использованием списков ACL

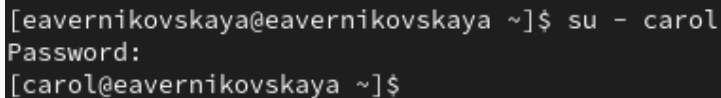
```
[root@eavernikovskaya ~]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::rwx                               #effective:rw-
group:main:rwx                           #effective:rw-
mask::rw-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

Рис. 32: Информация о файле newfile2 в каталоге /data/third

Для созданных файлов группы main возможны действия от пользователей группы third и наоборот

Управление расширенными разрешениями с использованием списков ACL

Далее заходим в другом терминале под учётной записью члена группы third - это carol (рис. 33)



```
[eavernikovskaya@eavernikovskaya ~]$ su - carol
Password:
[carol@eavernikovskaya ~]$
```

Рис. 33: Учётная запись carol

Управление расширенными разрешениями с использованием списков ACL

Далее проверяем операции с файлами newfile1 и newfile2. Пытаемся их удалить. Система не даёт нам этого сделать, так как удаление файлов это действие с каталогом, а к каталогу main у группы third нет полномочий (рис. 34)

```
[carol@eavernikovskaya ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@eavernikovskaya ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@eavernikovskaya ~]$
```

Рис. 34: Проверка операции удаления

Управление расширенными разрешениями с использованием списков ACL

Далее пытаемся осуществить запись в файлы. Система не даёт осуществить запись в newfile1, но разрешает сделать это в файле newfile2, так как ранее мы установили определённые разрешения (рис. 35)

```
[carol@eavernikovskaya ~]$ echo "Hello< world" >> /data/main/newfile1  
-bash: /data/main/newfile1: Permission denied  
[carol@eavernikovskaya ~]$ echo "Hello< world" >> /data/main/newfile2  
[carol@eavernikovskaya ~]$
```

Рис. 35: Проверка операции записи в файл

Подведение итогов

В ходе выполнения лабораторной работы мы получили навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

1. Лабораторная работа №3 [Электронный ресурс] URL:
https://esystem.rudn.ru/pluginfile.php/2400684/mod_resource/content/4/004-permissions.pdf