

Лабораторная работа №3

Настройка прав доступа

Юсупова К. Р.

Российский университет дружбы народов, Москва, Россия

Информация

- Юсупова Ксения Равиловна
- Российский университет дружбы народов
- Номер студенческого билета- 1132247531
- [1132247531@pfur.ru]

Цель работы

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

Выполнение лабораторной работы

Выполнение лабораторной работы

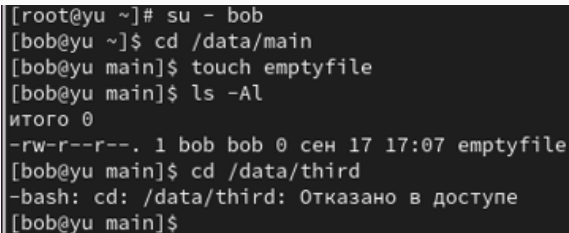
Созданы каталоги /data/main и /data/third с разными правами доступа. Владельцы каталогов изменены с root на группы main и third. Установлены разрешения, позволяющие владельцам записывать файлы и запрещающие доступ другим пользователям.

```
[ksyusha@yu ~]$ su -  
Пароль:  
[root@yu ~]# mkdir -p /data/main /data/third  
[root@yu ~]# ls -Al /data  
итого 0  
drwxr-xr-x. 2 root root 6 сен 17 17:04 main  
drwxr-xr-x. 2 root root 6 сен 17 17:04 third  
[root@yu ~]# chgrp main /data/main  
[root@yu ~]# chgrp third /data/third  
[root@yu ~]# ls -Al /data  
итого 0  
drwxr-xr-x. 2 root main 6 сен 17 17:04 main  
drwxr-xr-x. 2 root third 6 сен 17 17:04 third  
[root@yu ~]# chmod 770 /data/main  
[root@yu ~]# chmod 770 /data/third  
[root@yu ~]# ls -Al /data  
итого 0  
drwxrwx---. 2 root main 6 сен 17 17:04 main  
drwxrwx---. 2 root third 6 сен 17 17:04 third
```

Рис. 1: Выполнили пункты 1-4 из раздела 3.3.1 (Управление базовыми разрешениями)

Выполнение лабораторной работы

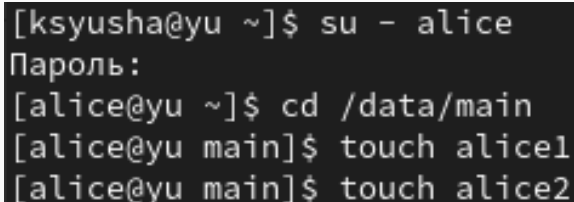
В другом терминале перешли под учётную запись пользователя bob и перешли в каталог /data/main, создали файл emptyfile. В этом каталоге получилось успешно создать файл emptyfile создан, так как bob имеет права на выполнение (x) и запись (w) в каталоге. В каталоге /data/third было отказано в доступе, так как bob не имеет права на выполнение (x) для входа в этот каталог.



```
[root@yu ~]# su - bob
[ bob@yu ~]$ cd /data/main
[ bob@yu main]$ touch emptyfile
[ bob@yu main]$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 17 17:07 emptyfile
[ bob@yu main]$ cd /data/third
-bash: cd: /data/third: Отказано в доступе
[ bob@yu main]$
```

Рис. 2: Выполнили пункты 5-7 из раздела 3.3.1 (Управление базовыми разрешениями)

Открыли новый терминал под пользователем alice и перешли в каталог /data/main. Создали два файла, владельцем которых является alice: touch alice1, touch alice2



```
[ksyusha@yu ~]$ su - alice
Пароль:
[alice@yu ~]$ cd /data/main
[alice@yu main]$ touch alice1
[alice@yu main]$ touch alice2
```

Рис. 3: Выполнили пункты 1 и 2 из раздела 3.3.2 (Управление специальными разрешениями)


Выполнение лабораторной работы

В другом терминале перешли под учётную запись пользователя bob и в каталог /data/main. Увидели два файла, созданные пользователем alice. Удалили файлы, принадлежащие пользователю alice; убедились что файлы будут удалены пользователем bob. Затем создали два файла, которые принадлежат пользователю bob: touch bob1, touch bob2

```
[ksyusha@yu ~]$ su - bob
Пароль:
[bob@yu ~]$ cd /data/main
[bob@yu main]$ ls -l
итого 0
-rw-r--r--. 1 alice alice 0 сен 17 17:16 alice1
-rw-r--r--. 1 alice alice 0 сен 17 17:16 alice2
-rw-r--r--. 1 bob  bob  0 сен 17 17:07 emptyfile
[bob@yu main]$ rm -f alice*
[bob@yu main]$ ls -l
итого 0
-rw-r--r--. 1 bob bob 0 сен 17 17:07 emptyfile
[bob@yu main]$ touch bob1
[bob@yu main]$ touch bob2
```

Рис. 4: Выполнили пункты 3-5 из раздела 3.3.2 (Управление специальными разрешениями)

В терминале под пользователем root установили для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы



```
[ksyusha@yu ~]$ su -  
Пароль:  
[root@yu ~]# chmod g+s,o+t /data/main
```

Рис. 5: Выполнили пункт 6 из раздела 3.3.2 (Управление специальными разрешениями)

Выполнение лабораторной работы

В терминале под пользователем alice создали в каталоге /data/main файлы alice3 и alice4; затем увидели, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main. Пользователь alice не может удалить файлы bob благодаря sticky-bit. Новые файлы наследуют группу каталога благодаря SGID

```
[alice@yu main]$ touch alice3
[alice@yu main]$ touch alice4
[alice@yu main]$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 17 17:20 alice3
-rw-r--r--. 1 alice main 0 сен 17 17:20 alice4
-rw-r--r--. 1 bob   bob   0 сен 17 17:18 bob1
-rw-r--r--. 1 bob   bob   0 сен 17 17:18 bob2
-rw-r--r--. 1 bob   bob   0 сен 17 17:07 emptyfile
[alice@yu main]$ rm -rf bob*
rm: невозможно удалить 'bob1': Операция не позволена
rm: невозможно удалить 'bob2': Операция не позволена
```

Рис. 6: Выполнили пункты 7 и 8 из раздела 3.3.2 (Управление специальными разрешениями)

Выполнение лабораторной работы

Открыли терминал с учётной записью root; установили 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. Затем использовали команду getfacl, чтобы убедиться в правильности установки разрешений

```
[root@yu ~]# su -
[root@yu ~]# setfacl -m g:third:rx /data/main
[root@yu ~]# setfacl -m g:third:rx /data/third
[root@yu ~]# 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@yu ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
group::rwx
group:third:r-x
```

Выполнение лабораторной работы

Создали новый файл с именем newfile1 в каталоге /data/main, затем использовали проверку текущих назначений полномочий. Созданы файлы до и после установки ACL. Файл newfile2 унаследовал ACL, newfile1 - нет.

```
[root@yu ~]# touch /data/main/newfile1
[root@yu ~]# 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@yu ~]# setfacl -m d:g:third:rwX /data/main
[root@yu ~]# setfacl -m d:g:main:rwX /data/third
[root@yu ~]# touch /data/main/newfile2
[root@yu ~]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
```

Выполнение лабораторной работы

Проверили операции с файлами, и поняли что пользователь carol (группа third) может записывать в файл с ACL (newfile2), но не может удалять файлы из-за отсутствия прав на каталог

```
[ksyusha@yu ~]$ su - carol
Пароль:
[carol@yu ~]$ rm /data/main/newfile1
rm: удалить защищённый от записи пустой обычный файл '/data/main/newfile1'?^[
[carol@yu ~]$ rm /data/main/newfile1
rm: удалить защищённый от записи пустой обычный файл '/data/main/newfile1'? y
rm: невозможно удалить '/data/main/newfile1': Отказано в доступе
[carol@yu ~]$ rm /data/main/newfile2
rm: невозможно удалить '/data/main/newfile2': Отказано в доступе
[carol@yu ~]$ echo "Hello, world" >> /data/main/newfile1
-bash: /data/main/newfile1: Отказано в доступе
[carol@yu ~]$ echo "Hello, world" >> /data/main/newfile2
[carol@yu ~]$
```

Рис. 9: Выполнили пункт 8 из раздела 3.3.3 (Управление расширенными разрешениями с использованием списков ACL)

Выводы

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