Лабораторная работа №3. Настройка прав доступа

Отчёт

Сергеев Даниил Олегович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux. [1]

2 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.

3 Ход выполнения лабораторной работы

3.1 Управление базовыми разрешениями для групп пользователей

Откроем терминал под учётной записью root. В корневом каталоге создадим каталоги /data/main и /data/third и проверим, кто является владельцем этих каталогов. Узнаем, что владелец - root. Теперь сменим владельца этих каталогов с root на main и third. Перепроверим, после установим разрешение владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам.

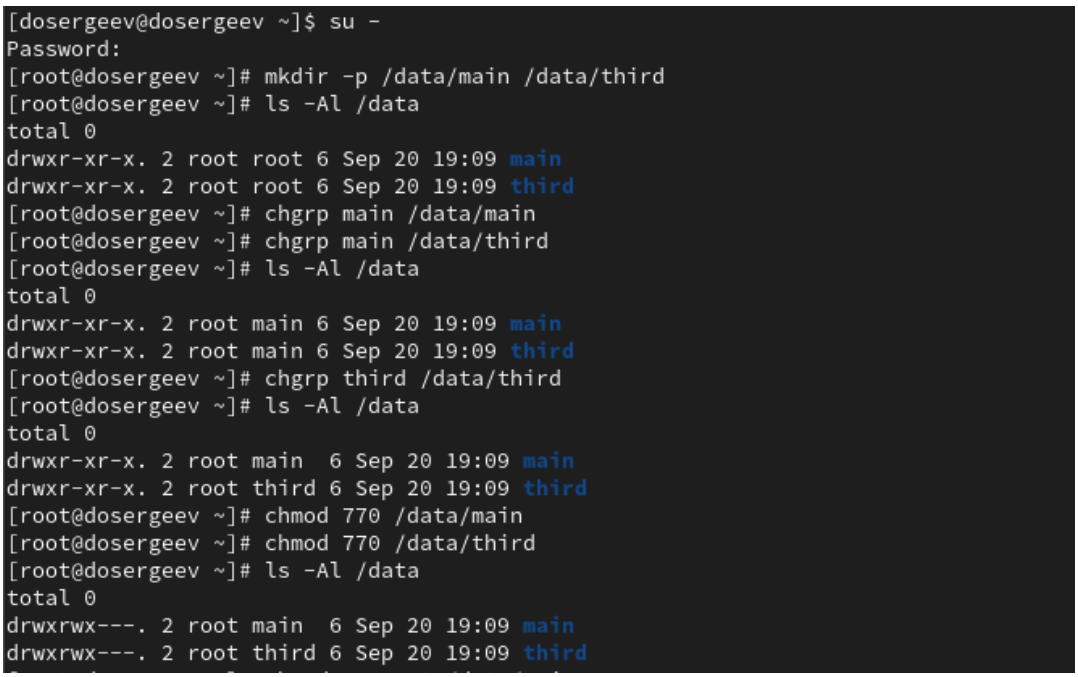

Рис. 3.1: Установка прав доступа и владельца. Проверка выполненных действий

В другом терминале перейдем под учётную запись bob из лабораторной работы №2. Попробуем перейти в катлог /data/main и создать файл emptyfile в этом каталоге. Пользователь bob принадлежит группе main, поэтому мы без проблем создаём файл в каталоге. Теперь попробуем сделать то же самое, но с каталогом /data/third. На этот раз выходит ошибка доступа, так как bob не находится в группе third, файл не создается.

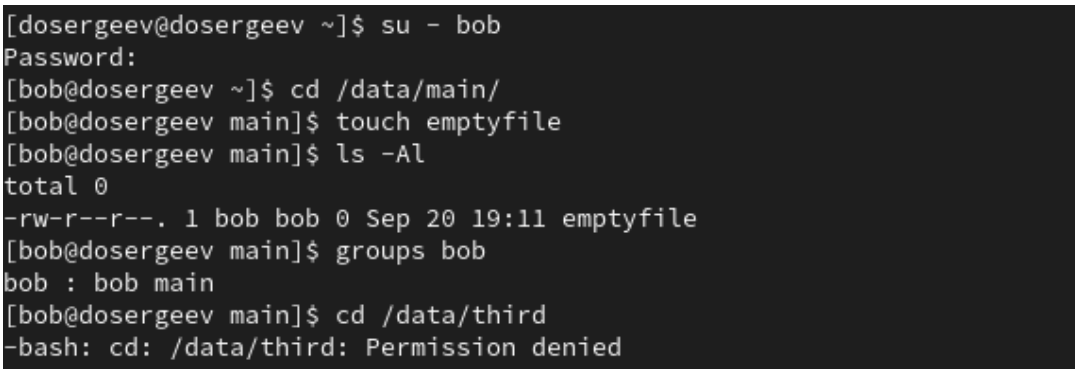

Рис. 3.2: Создание файла в каталогах main и third за пользователя bob

3.2 Управление специальными разрешениями для групп пользователей

Откроем терминал под пользователем alice. Перейдем в каталог /data/main и создадим два файла: alice1, alice2. Их владельцем является alice.

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

Рис. 3.3: Создание файлов за alice

В другом терминале перейдем под учётную запись bob и перейдем в каталог /data/main. Проверим файлы в каталоге. После проверки попробуем удалить файлы, принадлежащие alice. Убедимся, что файлы удалены. Они удалились, поэтому создадим файлы bob1 и bob2.

```
[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. 3.4: Удаление и создание файлов за bob в /data/main

В терминале под root установим для каталога /data/main бит идентификатора группы и stiky-бит для общего каталога группы.

```
[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. 3.5: Поставим бит идентификатора группы b stiky-бит для /data/main

Под пользователем alice создадим файл alice3 и alice4. Проверим принадлежность файлов к группе main. Под тем же пользователем попробуем удалить файлы пользователя bob - нам это не удается, так как включен sticky-bit.

Рис. 3.6: Проверка группы и удаление файлов за alice

3.3 Управление расширенными разрешениями с использованием списков ACL для групп пользователей

Откроем терминал с root. Установим права на чтение и выполнение для групп third в каталоге /data/main и main в каталоге /data/third с помощью ACL. Используем getfacl, и увидим что права для соответствующих групп установлены правильно.

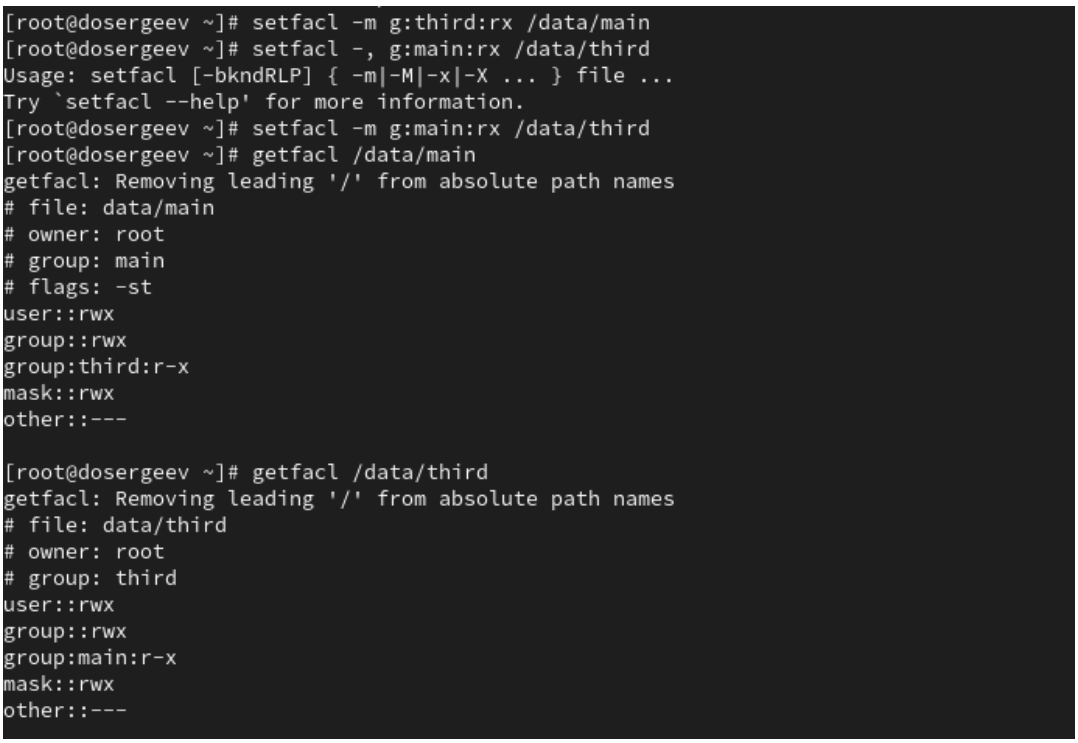

Рис. 3.7: Изменение прав с помощью ACL

Создадим новый файл с именем newfile1 в каталоге /data/main. Проверим полномочия. Владелец имеет права на чтение и запись, группа и остальные имеют только право на чтение. При создании файла, к нему применяется специальная маска, характерная для каждого пользователя. В нашем случае пользователь - root, поэтому файл создался с правами под маской пользователя root по умолчанию. Аналогично поступим для каталога third.

```
[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. 3.8: Создание файла newfile1, проверка его прав доступа

Установим права доступа ACL по умолчанию для каталогов /data/main и /data/third. Убедимся что настройки работают, добавив файл newfile2 и проверив текущие полномочия. Аналогично для каталога /data/third.

```
[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:rw-
group:third:rwx                 #effective:rw-
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:rw-
group:main:rwx                  #effective:rw-
mask::rw-
other::---
```

Рис. 3.9: Установка прав ACL по умолчанию

Для проверки полномочий группы third в каталоге /data/main войдем в другого пользователя carol, члена группы third. Попробуем удалить файл newfile1 и newfile2 - у нас не получится, так как в каталоге main включен sticky-bit, который предотвращает удаление файла, если он не владелец или root. Также попробуем записать в два файла “Hello, world”. Строка запишется только во второй файл, так как для файла newfle1 группе third не выдано право на запись.

```
[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. 3.10: Проверка полномочий группы third в /data/main

4 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
- Напимер 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 получат 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

5 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.

Список литературы

1. Kulyabov, Korolykova. Лабораторная работа №3. Настройка прав доступа. https://esystem.rudn.ru/pluginfile.php/2843458/mod_resource/content/4/004-permissions.pdf; RUDN.