Отчет по лабораторной работе №3

Дисциплина: Основы администрирования операционных систем

Иванов Сергей Владимирович

Содержание

Список иллюстраций

1 Цель работы

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

2 Задание

1. Прочитать справочное описание man по командам chgrp, chmod, getfacl, setfacl.
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

3 Выполнение лабораторной работы

Откроем терминал с учётной записью root. В корневом каталоге создаем каталоги /data/main и /data/third. Посмотрим, кто является владельцем этих каталогов ls -Al /data. (рис. 1).

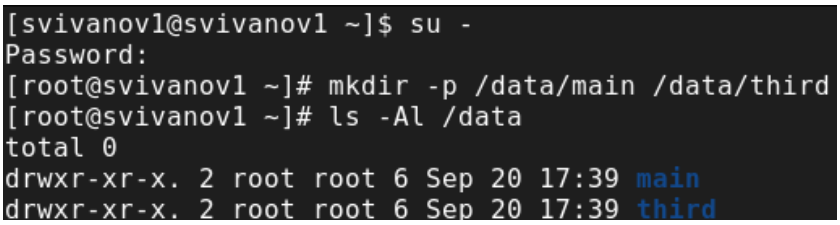

Рис. 3.1: Создаём каталоги

Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно: chgrp main /data/main, chgrp third /data/third. Посмотрим, кто теперь является владельцем этих каталогов (рис. 2).

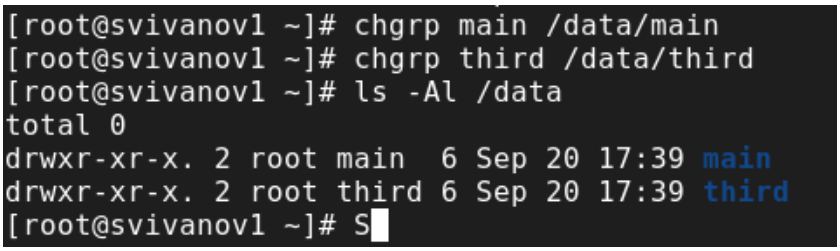

Рис. 3.2: Меняем владельцев

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам. Проверим установленные права доступа. (рис. 3).

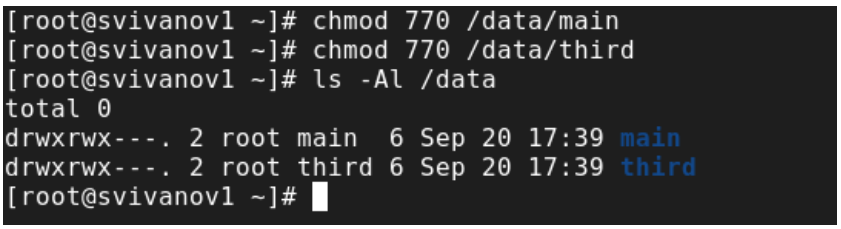

Рис. 3.3: Установка разрешений

В другом терминале перейдём под учётную запись пользователя bob: su – bob. Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге: cd /data/main и touch emptyfile. Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл. (рис. 4).

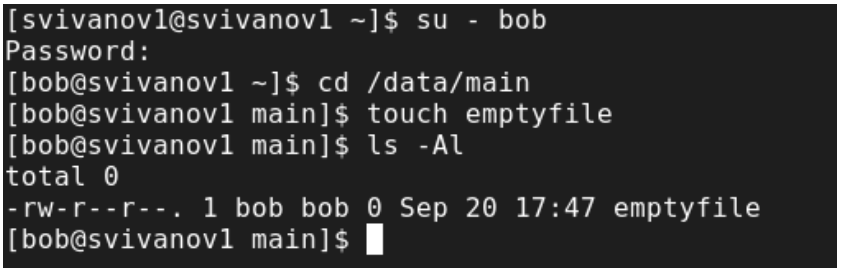

Рис. 3.4: Учетная запись bob и создание emptyfile

Теперь под пользователем bob попробуем 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. 5).

Рис. 3.5: Создание файла в /data/third

Откроем новый терминал под пользователем alice. Перейдем в каталог /data/main. Создадим два файла, владельцем которых является alice: touch alice1, touch alice2 (рис. 6).

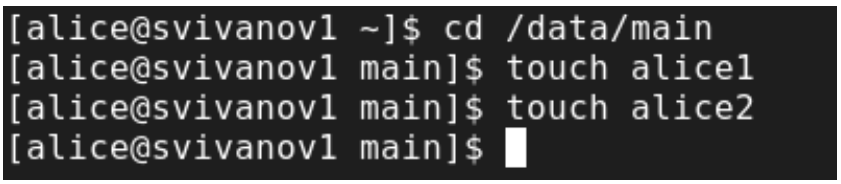

Рис. 3.6: Создание файлов alice

В другом терминале переходим под учётную запись пользователя bob su - bob. Перейдём в каталог cd /data/main и в этом каталоге вводим: ls -l. Мы увидим два файла, созданные пользователем alice. Попробуем удалить файлы, принадлежащие пользователю alice: rm -f alice*. Убедимся, что файлы будут удалены пользователем bob (рис. 7).

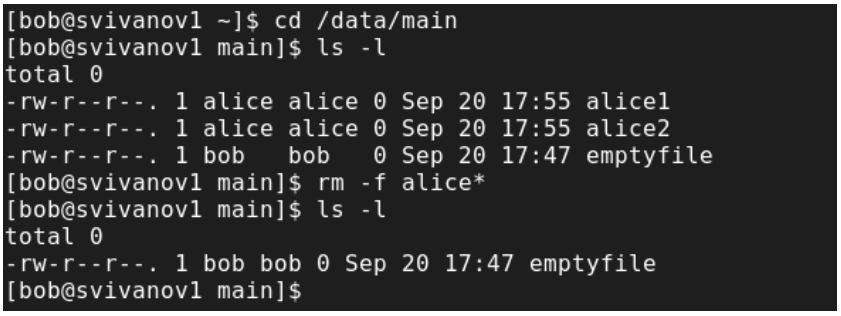

Рис. 3.7: Удаление файлов alice

Создадим два файла, которые принадлежат пользователю bob: touch bob1 и touch bob2 (рис. 8).

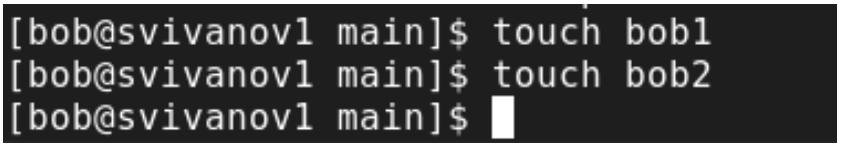

Рис. 3.8: Создание файлов bob

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого каталога группы: chmod g+s,o+t /data/main (рис. 9).

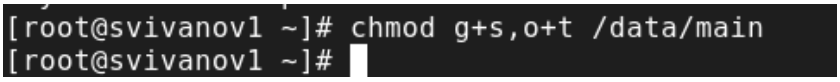

Рис. 3.9: Бит идентификатора группы

В терминале под пользователем alice создадим в каталоге /data/main файлы touch alice3 touch alice4. Теперь мы должны увидеть, что два созданных нами файла принадлежат группе main, которая является группой-владельцем каталога /data/main. (рис. 10).

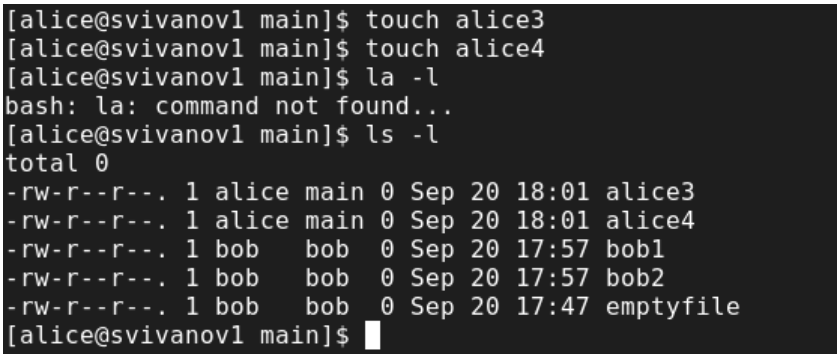

Рис. 3.10: Файлы alice3 и alice4

В терминале под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob: rm -rf bob*. Убеждаемся, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов (рис. 11).

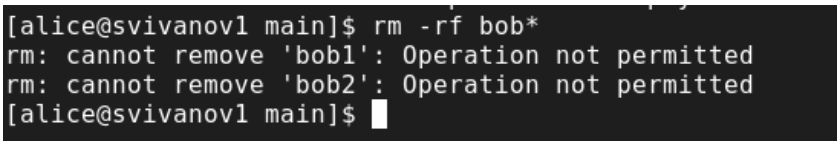

Рис. 3.11: Пробуем удалить файлы

Откроем терминал с учётной записью root. Установим 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: setfacl -m g:third:rx /data/main и setfacl -m g:main:rx /data/third (рис. 12).

```
[root@svivanov1 ~]# setfacl -m g:third:rx /data/main
[root@svivanov1 ~]# setfacl -m g:main:rx /data/third
```

Рис. 3.12: Установка прав

Используем команду getfacl, чтобы убедиться в правильности установки разрешений: getfacl /data/main и getfacl /data/third (рис. 13)

```
[root@svivanov1 ~]# 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@svivanov1 ~]# 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. 3.13: Правильность установки разрешений

Создадим новый файл с именем newfile1 в каталоге /data/main: touch /data/и main/newfile1. Используем getfacl /data/main/newfile1 для проверки текущих назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение. (рис. 14).

```
[root@svivanov1 ~]# touch /data/main/newfile1
[root@svivanov1 ~]# 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. 3.14: Проверка полномочий

Выполним аналогичные действия для каталога /data/third. (рис. 15).

Рис. 3.15: Проверка полномочий

Установим ACL по умолчанию для каталогов /data/main и /data/third. setfacl -m d:g:third:rwx /data/main и setfacl -m d:g:main:rwx /data/third. Убедимся, что настройки ACL работают, добавив новый файл в каталог touch /data/main/newfile2. Используем getfacl /data/main/newfile2 для проверки текущих назначений полномочий (рис. 16).

Рис. 3.16: Установка ACL по умолчанию

Выполним аналогичные действия для каталога /data/third (рис. 17)

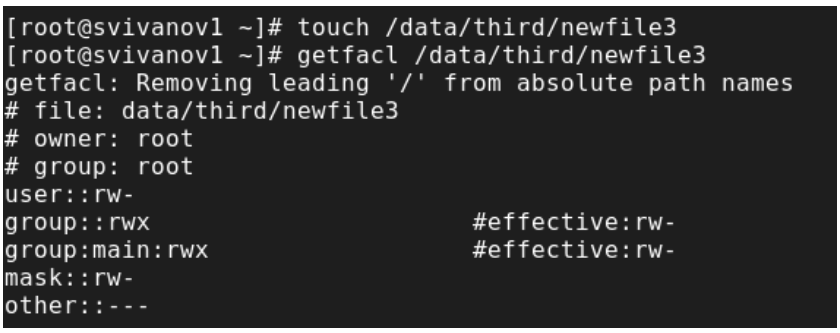

Рис. 3.17: Установка ACL по умолчанию

Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third: su - carol. Проверим операции с файлами: rm /data/main/newfile1 и rm /data/main/newfile2. Система не даёт удалить данные файлы. (рис. 18)

Рис. 3.18: Проверка операций с файлами

Проверим, возможно ли осуществить запись в файл: echo “Hello, world” » /data/main/newfile1 и echo “Hello, world” » /data/main/newfile2. В файл newfile1 запись осуществить не получилось, а вот в newfile2 всё выполнилось (рис. 19)

Рис. 3.19: Проверка операций с файлами

4 Контрольные вопросы

1. Как следует использовать команду chown, чтобы установить владельца группы для файла? Приведите пример.

chown bob:main /data/third/newfile.

2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример.

find ~ -user bob -print.

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? Приведите пример.

chmod 770 /data/main

4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?

chmod +x file

5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога? Приведите пример.

getfacl “имя каталога”. getfacl /data/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? Приведите пример.

chmod g+s,o+t /data/main

7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?

setfacl -m g:group:r . setfacl -m g:third:rx /data/main

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? Приведите пример.

setfacl -dm g:group:r /dir.

9. Какое значение umask нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример.

7.

10. Какая команда гарантирует, что никто не сможет удалить файл myfile случайно?

sudo chattr +i myfile.

5 Выводы

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