Лабораторная работа № 3

Основы администрирования операционных систем

Иванов Сергей Владимирович, НПИбд-01-23

20 сентября 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

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

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

Выполнение работы

Создаём каталоги

В корневом каталоге создаем каталоги /data/main и /data/third. Посмотрим, кто является их владельцем.

```
[svivanov1@svivanov1 ~]$ su -
Password:
[root@svivanov1 ~]# mkdir -p /data/main /data/third
[root@svivanov1 ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Sep 20 17:39 main
drwxr-xr-x. 2 root root 6 Sep 20 17:39 third
```

Рис. 1: Создаём каталоги

Меняем владельцев

Изменим владельцев этих каталогов с root на main и third соответственно

```
[root@svivanov1 ~]# chgrp main /data/main
[root@svivanov1 ~]# chgrp third /data/third
[root@svivanov1 ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main  6 Sep 20 17:39 main
drwxr-xr-x. 2 root third 6 Sep 20 17:39 third
[root@svivanov1 ~]# S
```

Рис. 2: Меняем владельцев

Установка разрешений

Установим разрешения, позволяющие владельцам каталогов записывать файлы в них и запрещающие доступ к содержимому другим пользователям.

```
[root@svivanov1 ~]# chmod 770 /data/main
[root@svivanov1 ~]# chmod 770 /data/third
[root@svivanov1 ~]# ls -Al /data
total 0
drwxrwx---. 2 root main  6 Sep 20 17:39 main
drwxrwx---. 2 root third 6 Sep 20 17:39 third
[root@svivanov1 ~]#
```

Рис. 3: Установка разрешений

Учетная запись bob и создание emptyfile

Под пользователем bob перейдем в каталог /data/main и создадим файл emptyfile. Т.к пользователь bob владелец каталога main, нам удалось перейти в него и создать новый файл

```
[svivanov1@svivanov1 ~]$ su - bob
Password:
[bob@svivanov1 ~]$ cd /data/main
[bob@svivanov1 main]$ touch emptyfile
[bob@svivanov1 main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 20 17:47 emptyfile
[bob@svivanov1 main]$
```

Рис. 4: Учетная запись bob и создание emptyfile

Создание файла в /data/third

Передем в каталог /data/third и создадим emptyfile. Т.к пользователь bob не является владельцем каталога, нам не удалось перейти в него и создать новый файл

```
[bob@svivanov1 main]$ cd /data/third
-bash: cd: /data/third: Permission denied
```

Рис. 5: Создание файла в /data/third

Создание файлов alice

Откроем терминал под пользователем alice. Перейдем в каталог /data/main. Создадим 2 файла: alice1, alice2

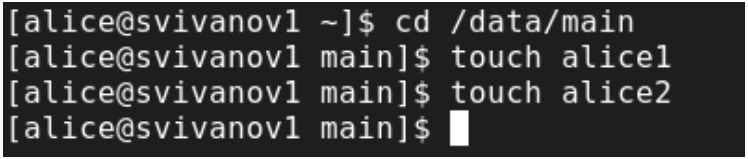

Рис. 6: Создание файлов alice

Удаление файлов alice

Переходим на пользователя bob. Перейдём в каталог /data/main. Мы увидим два файла, созданные пользователем alice. Попробуем удалить файлы, принадлежащие ему. Убедимся, что файлы удалены

```
[bob@svivanov1 ~]$ cd /data/main
[bob@svivanov1 main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 20 17:55 alice1
-rw-r--r--. 1 alice alice 0 Sep 20 17:55 alice2
-rw-r--r--. 1 bob   bob   0 Sep 20 17:47 emptyfile
[bob@svivanov1 main]$ rm -f alice*
[bob@svivanov1 main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 20 17:47 emptyfile
[bob@svivanov1 main]$
```

Рис. 7: Удаление файлов alice

Создание файлов bob

Создадим 2 файла, которые принадлежат пользователю bob: bob1 и bob2

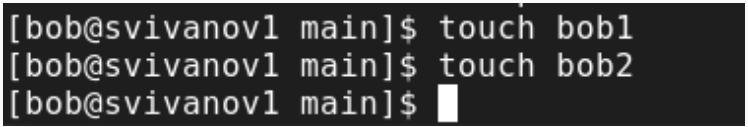

Рис. 8: Создание файлов bob

Бит идентификатора группы

Под пользователем root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого каталога группы

```
[root@svivanov1 ~]# chmod g+s,o+t /data/main
[root@svivanov1 ~]#
```

Рис. 9: Бит идентификатора группы

Файлы alice3 и alice4

Под пользователем alice создадим в каталоге /data/main файлы alice3 и alice4. Мы видим, что 2 этих файла принадлежат группе main, которая является владельцем каталога /data/main.

```
[alice@svivanov1 main]$ touch alice3
[alice@svivanov1 main]$ touch alice4
[alice@svivanov1 main]$ la -l
bash: la: command not found...
[alice@svivanov1 main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 20 18:01 alice3
-rw-r--r--. 1 alice main 0 Sep 20 18:01 alice4
-rw-r--r--. 1 bob   bob  0 Sep 20 17:57 bob1
-rw-r--r--. 1 bob   bob  0 Sep 20 17:57 bob2
-rw-r--r--. 1 bob   bob  0 Sep 20 17:47 emptyfile
[alice@svivanov1 main]$
```

Рис. 10: Файлы alice3 и alice4

Пробуем удалить файлы

Под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob. Убеждаемся, что sticky-bit предотвратит удаление этих файлов.

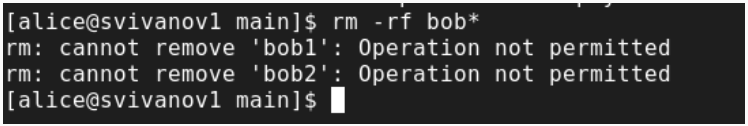

Рис. 11: Пробуем удалить файлы

Установка прав

Под пользователем 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

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

Рис. 12: Установка прав

Правильность установки разрешений

Используем команду getfacl, чтобы убедиться в правильности установки разрешений

```
[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::---
```

Проверка полномочий

Создадим newfile1 в каталоге /data/main. Используем getfacl для проверки текущих назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение.

```
[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. 14: Проверка полномочий

Проверка полномочий

Выполним аналогичные действия для каталога /data/third.

```
[root@svivanov1 ~]# touch /data/third/newfile2
[root@svivanov1 ~]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::r--
other::r--

[root@svivanov1 ~]#
```

Рис. 15: Проверка полномочий

Установка ACL по умолчанию

Установим ACL по умолчанию для каталогов /data/main и /data/third.
Убедимся, что настройки ACL работают, добавив новый файл в каталог.

```
[root@svivanov1 ~]# setfacl -m d:g:third:rwx /data/main
[root@svivanov1 ~]# setfacl -m d:g:main:rwx /data/third
[root@svivanov1 ~]# touch /data/main/newfile2
[root@svivanov1 ~]# 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@svivanov1 ~]#
```

Рис. 16: Установка ACL по умолчанию

Установка ACL по умолчанию

Выполним аналогичные действия для каталога /data/third

```
[root@svivanov1 ~]# touch /data/third/newfile3
[root@svivanov1 ~]# getfacl /data/third/newfile3
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile3
# owner: root
# group: root
user::rw-
group::rwx                      #effective:rw-
group:main:rwx                  #effective:rw-
mask::rw-
other::---
```

Рис. 17: Установка ACL по умолчанию

Проверка операций с файлами

Проверим операции с файлами: rm /data/main/newfile1 и rm /data/main/newfile2. Система не даёт удалить данные файлы.

```
[svivanov1@svivanov1 ~]$ su - carol
Password:
[carol@svivanov1 ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@svivanov1 ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@svivanov1 ~]$
```

Рис. 18: Проверка операций с файлами

Проверка операций с файлами

Проверим, возможно ли осуществить запись в файл. В файл newfile1 запись осуществить не получилось, а вот в newfile2 всё выполнилось

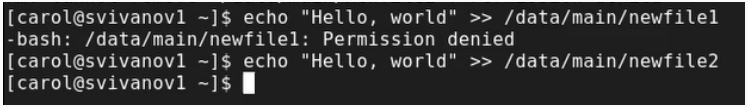

Рис. 19: Проверка операций с файлами

Вывод

Вывод

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

Список литературы

https://esystem.rudn.ru/mod/page/view.php?id=1098933