

Отчёт по лабораторной работе №3

Дискреционное разграничение прав в Linux. Два пользователя

Дарья Эдуардовна Ибатулина

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 5 |
| 2 | Задание | 6 |
| 3 | Теоретическое введение | 7 |
| 4 | Выполнение лабораторной работы | 9 |
| 4.1 | Заполнение таблицы 3.1 | 13 |
| 4.2 | Заполнение таблицы 3.2 | 20 |
| 5 | Выводы | 21 |
| | Список литературы | 22 |

Список иллюстраций

| | | |
|------|--|----|
| 4.1 | Создание нового пользователя и задание пароля для него | 9 |
| 4.2 | Добавление пользователя в группу | 9 |
| 4.3 | Вход в систему от двух пользователей на разных консолях | 10 |
| 4.4 | Вывод рабочей директории для пользователя guest | 10 |
| 4.5 | Вывод рабочей директории для пользователя guest2 | 10 |
| 4.6 | Уточнение групп пользователя guest командой id | 10 |
| 4.7 | Уточнение групп пользователя guest2 командой id | 11 |
| 4.8 | Уточнение групп пользователя guest командой groups | 11 |
| 4.9 | Уточнение групп пользователя guest2 командой groups | 11 |
| 4.10 | Вывод команд id -Gn и id -G для пользователя guest | 11 |
| 4.11 | Вывод команд id -Gn и id -G для пользователя guest2 | 11 |
| 4.12 | Просмотр файла /etc/group | 12 |
| 4.13 | Регистрация пользователя guest2 в группе guest | 12 |
| 4.14 | Разрешение всех действий для пользователей группы guest дирек- тории dir1 | 12 |
| 4.15 | Запрет всех действий для пользователей группы guest директории dir1 | 12 |

Список таблиц

| | | |
|-----|---|----|
| 4.1 | 3.1 Установленные права и разрешённые действия для групп . . | 13 |
| 4.2 | 3.2 Минимальные права для совершения операций от имени пользователей, входящих в группу | 20 |

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

2 Задание

1. Создание нового пользователя;
2. Добавление его в группу;
3. Уточнение имени пользователя, проверка того, в какие группы он входит;
4. Регистрация нового пользователя в группе;
5. Изменение прав директории;
6. Заполнение таблиц: “Установленные права и разрешённые действия для групп” и “Минимальные права для совершения операций от имени пользователей входящих в группу”.

3 Теоретическое введение

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы.

Группы пользователей Linux кроме стандартных root и users, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен.

- daemon - от имени этой группы и пользователя daemon запускаются сервисы, которым необходима возможность записи файлов на диск.
- sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
- sync - позволяет выполнять команду /bin/sync
- games - разрешает играм записывать свои файлы настроек и историю в определенную папку
- man - позволяет добавлять страницы в директорию /var/cache/man
- lp - позволяет использовать устройства параллельных портов
- mail - позволяет записывать данные в почтовые ящики /var/mail/

- `proxy` - используется прокси серверами, нет доступа записи файлов на диск `www-data` - с этой группой запускается веб-сервер, она дает доступ на запись `/var/www`, где находятся файлы веб-документов
- `list` - позволяет просматривать сообщения в `/var/mail`
- `nogroup` - используется для процессов, которые не могут создавать файлов на жестком диске, а только читать, обычно применяется вместе с пользователем `nobody`.
- `adm` - позволяет читать логи из директории `/var/log`
- `tty` - все устройства `/dev/vcs` разрешают доступ на чтение и запись пользователям из этой группы
- `disk` - открывает доступ к жестким дискам `/dev/sd*` `/dev/hd*`, можно сказать, что это аналог `root` доступа.
- `dialout` - полный доступ к серийному порту
- `cdrom` - доступ к CD-ROM
- `wheel` - позволяет запускать утилиту `sudo` для повышения привилегий
- `audio` - управление аудиодрайвером
- `src` - полный доступ к исходникам в каталоге `/usr/src/`
- `shadow` - разрешает чтение файла `/etc/shadow`
- `utmp` - разрешает запись в файлы `/var/log/utmp` `/var/log/wtmp`
- `video` - позволяет работать с видеодрайвером
- `plugdev` - позволяет монтировать внешние устройства USB, CD и т.д.
- `staff` - разрешает запись в папку `/usr/local`

4 Выполнение лабораторной работы

Первые 2 пункта лабораторной работы я уже выполнила в предыдущей работе. Нужно было создать пользователя *guest* и задать для него пароль.

1. Создаём второго нового пользователя с именем *guest2* с помощью команд `useradd guest2` и `passwd guest2`(рис. [4.1]).

```
[root@deibatulina ~]# useradd guest2
[root@deibatulina ~]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль: 
```

Рис. 4.1: Создание нового пользователя и задание пароля для него

2. Добавляем пользователя *guest2* в группу *guest*, используя команду `gpasswd -a guest2 guest` (рис. [4.2]).

```
[root@deibatulina ~]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@deibatulina ~]#
```

Рис. 4.2: Добавление пользователя в группу

3. Осуществите вход в систему от двух пользователей на двух разных консолях: *guest* на первой консоли и *guest2* на второй консоли с помощью команды `su *имя пользователя*` (рис. [4.3]).

```
guest@deibatulina:~$ cd
[deibatulina@deibatulina ~]$ su guest
Пароль:
su: Сбой при проверке подлинности
[deibatulina@deibatulina ~]$ su guest
Пароль:
[guest@deibatulina ~]$ cd
[guest@deibatulina ~]$

guest2@deibatulina:~$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@deibatulina ~]$ su root
Пароль:
[root@deibatulina ~]# cd
[root@deibatulina ~]# useradd guest2
[root@deibatulina ~]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
passwd: Ошибка при операциях с маркером проверки подлинности
[root@deibatulina ~]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@deibatulina ~]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@deibatulina ~]# su guest2
[guest2@deibatulina root]$ cd
[guest2@deibatulina ~]$
```

Рис. 4.3: Вход в систему от двух пользователей на разных консолях

4. Далее, выведем рабочую директорию командой `pwd` для обоих пользователей: *guest* (рис. [4.4]) и *guest2* (рис. [4.5]):

```
[guest@deibatulina ~]$ pwd
/home/guest
[guest@deibatulina ~]$
```

Рис. 4.4: Вывод рабочей директории для пользователя *guest*

```
[guest2@deibatulina ~]$ pwd
/home/guest2
[guest2@deibatulina ~]$
```

Рис. 4.5: Вывод рабочей директории для пользователя *guest2*

5. Уточним имя обоих наших пользователей командой `whoami`, группу каждого, кто входит в неё и к каким группам принадлежит он сам командой `id`: *guest* (рис. [4.6]) и *guest2* (рис. [4.7]).

```
[guest@deibatulina ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@deibatulina ~]$
```

Рис. 4.6: Уточнение групп пользователя *guest* командой `id`

```
[guest2@deibatulina ~]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@deibatulina ~]$
```

Рис. 4.7: Уточнение групп пользователя guest2 командой id

6. Определим командами `groups guest` и `groups guest2`, в какие группы входят пользователи: *guest* (рис. [4.8]) и *guest2* (рис. [4.9]). Сравним вывод команды `groups` с выводом команд `id -Gn` и `id -G` для пользователей *guest* (рис. [4.10]) и *guest2* (рис. [4.11]).

Примечательно: * `id -Gn` - выведет названия групп, которым принадлежит пользователь * `id -G` - выведет только код групп, которым принадлежит пользователь

```
[guest@deibatulina ~]$ groups guest
guest : guest
[guest@deibatulina ~]$
```

Рис. 4.8: Уточнение групп пользователя guest командой groups

```
[guest2@deibatulina ~]$ groups guest2
guest2 : guest2 guest
[guest2@deibatulina ~]$
```

Рис. 4.9: Уточнение групп пользователя guest2 командой groups

```
[guest@deibatulina ~]$ groups
guest
[guest@deibatulina ~]$ id -Gn
guest
[guest@deibatulina ~]$ id -G
1001
[guest@deibatulina ~]$
```

Рис. 4.10: Вывод команд `id -Gn` и `id -G` для пользователя guest

```
[guest2@deibatulina ~]$ groups
guest2 guest
[guest2@deibatulina ~]$ id -Gn
guest2 guest
[guest2@deibatulina ~]$ id -G
1002 1001
[guest2@deibatulina ~]$
```

Рис. 4.11: Вывод команд `id -Gn` и `id -G` для пользователя guest2

7. Просмотрим содержимое файла `/etc/group` `cat /etc/group` (рис. [4.12]).

```
[guest@deibatulina ~]$ cat /etc/group | grep 'guest'
guest:x:1001:guest
guest2:x:1002:
[guest@deibatulina ~]$
```

Рис. 4.12: Просмотр файла `/etc/group`

8. От имени пользователя `guest2` выполним регистрацию пользователя `guest2` в группе `guest` командой `newgrp guest` (рис. [4.13]).

```
[guest2@deibatulina ~]$ newgrp guest
[guest2@deibatulina ~]$
```

Рис. 4.13: Регистрация пользователя `guest2` в группе `guest`

9. От имени пользователя `guest` изменим права директории `/home/guest`, разрешив все действия для пользователей группы с помощью команды `chmod g+rxw /home/guest` (рис. [4.14]).

```
[guest@deibatulina ~]$ chmod g+rxw /home/guest
[guest@deibatulina ~]$
```

Рис. 4.14: Разрешение всех действий для пользователей группы `guest` директории `dir1`

10. От имени пользователя `guest` снимем с директории `/home/guest/dir1` все атрибуты командой `chmod 000 dir1` (рис. [4.15]).

```
[guest@deibatulina ~]$ chmod 000 dir1
[guest@deibatulina ~]$
```

Рис. 4.15: Запрет всех действий для пользователей группы `guest` директории `dir1`

4.1 Заполнение таблицы 3.1

Меняя атрибуты у директории *dir1* и файла *file1* от имени пользователя *guest* и делая проверку от пользователя *guest2*, заполняю таблицу [4.1], определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, в таблице стоит знак “+”, если не разрешена, знак “-”.

Таблица 4.1: 3.1 Установленные права и разрешённые действия для групп

| Права директории | Права файла | Про- смотр фай- Сме- лов ре- ат- на в име- ри- бу- тов фай- | | | | | | | |
|--------------------|----------------|--|----------------------------------|--------------------------|---------------------------|---------------------------|---------------------------|---------------------------|---------------------------------------|
| | | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | ди- рек- то- рии | ди- рек- то- рии | но- ва- ние файл | на ри- бу- тов фай- ла |
| d----- (000) | ----- (000) | - | - | - | - | - | - | - | - |
| d-----x-- (010) | ----- (000) | - | - | - | - | - | - | - | + |
| d----w--- (020) | ----- (000) | - | - | - | - | - | - | - | - |
| d----wx-- (030) | ----- (000) | + | + | - | - | + | - | + | + |
| d---r---- (040) | ----- (000) | - | - | - | - | - | + | - | - |
| d---r-x-- (050) | ----- (000) | - | - | - | - | + | + | - | + |

| | | Права | | | | | | | |
|---------------------|-------------|-------------------|-------------------|------------------|-----------------|---|--|--|--|
| | | Создание файла | Удаление файла | Запись в файл | Чтение файла | Сме- на ди- рек- то- рии | Про- смотр фай- лов в ди- рек- то- рии | Пе- ре- име- но- вание файл | Сме- на ат- ри- бу- тов фай- |
| Права директории | Права файла | ла | ла | файл | ла | рии | рии | файл | ла |
| d---rw--- | ----- | - | - | - | - | - | + | - | - |
| (060) | (000) | | | | | | | | |
| d---rwx-- | ----- | + | + | - | - | + | + | + | + |
| (070) | (000) | | | | | | | | |
| d----- | -----x-- | - | - | - | - | - | - | - | - |
| (000) | (010) | | | | | | | | |
| d-----x-- | -----x-- | - | - | - | - | - | - | - | + |
| (010) | (010) | | | | | | | | |
| d----w--- | -----x-- | - | - | - | - | - | - | - | - |
| (020) | (010) | | | | | | | | |
| d----wx-- | -----x-- | + | + | - | - | + | - | + | + |
| (030) | (010) | | | | | | | | |
| d---r---- | -----x-- | - | - | - | - | - | + | - | - |
| (040) | (010) | | | | | | | | |
| d---r-x-- | -----x-- | - | - | - | - | + | + | - | + |
| (050) | (010) | | | | | | | | |
| d---rw--- | -----x-- | - | - | - | - | - | + | - | - |
| (060) | (010) | | | | | | | | |
| d---rwx-- | -----x-- | + | + | - | - | + | + | + | + |
| (070) | (010) | | | | | | | | |

| Права директории | Права файла | <div> <div>Про- смотр фай-</div> <div>Сме- на ре- ат-</div> <div>Сме- лов ре- ва-</div> <div>на в име- но- бу-</div> <div>ри- бу- тов фай-</div> </div> | | | | | | | |
|---------------------|-------------|---|----------------------------------|--------------------------|---------------------------|-----------------------------------|-----------------------------------|---------------------------|---------------------------------|
| | | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | Сме- ди- рек- то- рии | Сме- ди- рек- то- рии | на име- ние файл | ри- бу- тов фай- ла |
| d----- | -----w--- | - | - | - | - | - | - | - | - |
| (000) | (020) | | | | | | | | |
| d-----x-- | -----w--- | - | - | + | - | - | - | - | + |
| (010) | (020) | | | | | | | | |
| d----w--- | -----w--- | - | - | - | - | - | - | - | - |
| (020) | (020) | | | | | | | | |
| d----wx-- | -----w--- | + | + | + | - | + | - | + | + |
| (030) | (020) | | | | | | | | |
| d---r---- | -----w--- | - | - | - | - | - | + | - | - |
| (040) | (020) | | | | | | | | |
| d---r-x-- | -----w--- | - | - | + | - | + | + | - | + |
| (050) | (020) | | | | | | | | |
| d---rw--- | -----w--- | - | - | - | - | - | + | - | - |
| (060) | (020) | | | | | | | | |
| d---rwx-- | -----w--- | + | + | + | - | + | + | + | + |
| (070) | (020) | | | | | | | | |
| d----- | -----wx-- | - | - | - | - | - | - | - | - |
| (000) | (030) | | | | | | | | |
| d-----x-- | -----wx-- | - | - | + | - | - | - | - | + |
| (010) | (030) | | | | | | | | |

| | | Продолжение таблицы 1 | | | | | | | |
|---------------------|-------------|----------------------------------|----------------------------------|--------------------------|---------------------------|---|--|--|---|
| Права директории | Права файла | Права доступа к файлу | | | | | | | |
| | | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | Сме- на ди- рек- то- рии | Про- смотр фай- лов в ди- рек- то- рии | Пе- ре- име- но- вание файл | Сме- на ри- бу- тов фай- ла |
| d----w--- | -----wx-- | - | - | - | - | - | - | - | - |
| (020) | (030) | | | | | | | | |
| d----wx-- | -----wx-- | + | + | + | - | + | - | + | + |
| (030) | (030) | | | | | | | | |
| d---r---- | -----wx-- | - | - | - | - | - | + | - | - |
| (040) | (030) | | | | | | | | |
| d---r-x-- | -----wx-- | - | - | + | - | + | + | - | + |
| (050) | (030) | | | | | | | | |
| d---rw--- | -----wx-- | - | - | - | - | - | + | - | - |
| (060) | (030) | | | | | | | | |
| d---rwx-- | -----wx-- | + | + | + | - | + | + | + | + |
| (070) | (030) | | | | | | | | |
| d----- | ----r---- | - | - | - | - | - | - | - | - |
| (000) | (040) | | | | | | | | |
| d-----x-- | ----r---- | - | - | - | + | + | - | - | + |
| (010) | (040) | | | | | | | | |
| d----w--- | ----r---- | - | - | - | - | - | - | - | - |
| (020) | (040) | | | | | | | | |
| d----wx-- | ----r---- | + | + | - | + | + | - | + | + |
| (030) | (040) | | | | | | | | |

| Права директории | Права файла | <div> <div>Про- смотр фай-</div> <div>Сме- на ре- ат-</div> <div>Сме- лов ре- ва-</div> <div>на в име-</div> <div>на ди- рек-</div> <div>Уда- ле- ние</div> <div>За- пись в</div> <div>Чте- ние фай-</div> <div>Созда- ние фай-</div> </div> | | | | | | | |
|---------------------|-------------|--|----|------|----|-----|-----|------|----|
| | | ла | ла | файл | ла | рии | рии | файл | ла |
| d---r---- | ----r---- | - | - | - | - | - | + | - | - |
| (040) | (040) | | | | | | | | |
| d---r-x-- | ----r---- | - | - | - | + | + | + | - | + |
| (050) | (040) | | | | | | | | |
| d---rw--- | ----r---- | - | - | - | - | - | + | - | - |
| (060) | (040) | | | | | | | | |
| d---rwx-- | ----r---- | + | + | - | + | + | + | + | + |
| (070) | (040) | | | | | | | | |
| d----- | ----r-x-- | - | - | - | - | - | - | - | - |
| (000) | (050) | | | | | | | | |
| d-----x-- | ----r-x-- | - | - | - | + | + | - | - | + |
| (010) | (050) | | | | | | | | |
| d----w--- | ----r-x-- | - | - | - | - | - | - | - | - |
| (020) | (050) | | | | | | | | |
| d----wx-- | ----r-x-- | + | + | - | + | + | - | + | + |
| (030) | (050) | | | | | | | | |
| d---r---- | ----r-x-- | - | - | - | - | - | + | - | - |
| (040) | (050) | | | | | | | | |
| d---r-x-- | ----r-x-- | - | - | - | + | + | + | - | + |
| (050) | (050) | | | | | | | | |

| | | Про- смотр фай- Пе- на Сме- лов ре- ат- на в име- ри- уда- ле- За- Чте- ди- ди- но- бу- ние ние пись ние рек- рек- ва- тов фай- фай- в фай- то- то- ние фай- ла ла файл ла рии рии файл ла | | | | | | | |
|---------------------|-------------|--|----------------------------------|--------------------------------|---------------------------|---|--|---|---------------------------------------|
| Права директории | Права файла | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл ла | Чте- ние фай- ла | Сме- на ди- рек- то- рии | Сме- лов ди- рек- то- рии | Пе- ре- име- ние файл ла | на ри- бу- тов фай- ла |
| d---rw--- | ----r-x-- | - | - | - | - | - | + | - | - |
| (060) | (050) | | | | | | | | |
| d---rwx-- | ----r-x-- | + | + | - | + | + | + | + | + |
| (070) | (050) | | | | | | | | |
| d----- | ----rw--- | - | - | - | - | - | - | - | - |
| (000) | (060) | | | | | | | | |
| d-----x-- | ----rw--- | - | - | + | + | - | - | - | + |
| (010) | (060) | | | | | | | | |
| d----w--- | ----rw--- | - | - | - | - | - | - | - | - |
| (020) | (060) | | | | | | | | |
| d----wx-- | ----rw--- | + | + | + | + | + | - | + | + |
| (030) | (060) | | | | | | | | |
| d---r---- | ----rw--- | - | - | - | - | - | + | - | - |
| (040) | (060) | | | | | | | | |
| d---r-x-- | ----rw--- | - | - | + | + | + | + | - | + |
| (050) | (060) | | | | | | | | |
| d---rw--- | ----rw--- | - | - | - | - | - | + | - | - |
| (060) | (060) | | | | | | | | |
| d---rwx-- | ----rw--- | + | + | + | + | + | + | + | + |
| (070) | (060) | | | | | | | | |

| Права директории | Права файла | <div> <div>Про- смотр фай-</div> <div>Сме- на</div> <div>Сме- лов</div> <div>ре- ат-</div> <div>на</div> <div>име- ри-</div> <div>бу-</div> <div>тов</div> <div>фай-</div> </div> | | | | | | | |
|---------------------|-------------|---|----------------------------------|--------------------------|---------------------------|---------------------------|---------------------------|---------------------------|----|
| | | Со- зда- ние фай- ла | Уда- ле- ние фай- ла | За- пись в файл | Чте- ние фай- ла | ди- рек- то- рии | ди- рек- то- рии | но- ва- ние файл | ла |
| d----- | ----rwx-- | - | - | - | - | - | - | - | - |
| (000) | (070) | | | | | | | | |
| d-----x-- | ----rwx-- | - | - | + | + | + | - | - | + |
| (010) | (070) | | | | | | | | |
| d----w--- | ----rwx-- | - | - | - | - | - | - | - | - |
| (020) | (070) | | | | | | | | |
| d----wx-- | ----rwx-- | + | + | + | + | + | - | + | + |
| (030) | (070) | | | | | | | | |
| d---r---- | ----rwx-- | - | - | - | - | - | + | - | - |
| (040) | (070) | | | | | | | | |
| d---r-x-- | ----rwx-- | - | - | + | + | + | + | - | + |
| (050) | (070) | | | | | | | | |
| d---rw--- | ----rwx-- | - | - | - | - | - | + | - | - |
| (060) | (070) | | | | | | | | |
| d---rwx-- | ----rwx-- | + | + | + | + | + | + | + | + |
| (070) | (070) | | | | | | | | |

4.2 Заполнение таблицы 3.2

На основе таблицы 3.1 заполняю следующую таблицу [4.2].

Таблица 4.2: 3.2 Минимальные права для совершения операций от имени пользователей, входящих в группу

| Операция | Права на директорию | Права на файл |
|------------------------|---------------------|-----------------|
| Создание файла | d----wx-- (030) | ----- (000) |
| Удаление файла | d----wx-- (030) | ----- (000) |
| Чтение файла | d-----x-- (010) | ----r---- (040) |
| Запись в файл | d-----x-- (010) | -----w--- (020) |
| Переименование файла | d----wx-- (030) | ----- (000) |
| Создание поддиректории | d----wx-- (030) | ----- (000) |
| Удаление поддиректории | d----wx-- (030) | ----- (000) |

5 Выводы

Я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы