Отчет по Лабораторной работе №8

«Управление доступом в файловой системе EXT3FS»

Группа 2-МВ-4

Ярошевская Д.А.

1. Теоретические сведения.

2. Создать группу пользователей с именем g1 и пользователя с именем a в этой группе, используя режим командной строки.

Создаем группу через **addgroup**.

```
dari@Ubuntu:~$ sudo addgroup g1
[sudo] password for dari:
Adding group `g1' (GID 1001) ...
Done.
```

Создаем пользователя через **adduser**, затем задаем ему пароль.

```
dari@Ubuntu:~$ sudo adduser a
Adding user `a' ...
Adding new group `a' (1002) ...
Adding new user `a' (1001) with group `a' ...
Creating home directory `/home/a' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for a
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Добавлям пользователя **a** в группу **g1**.

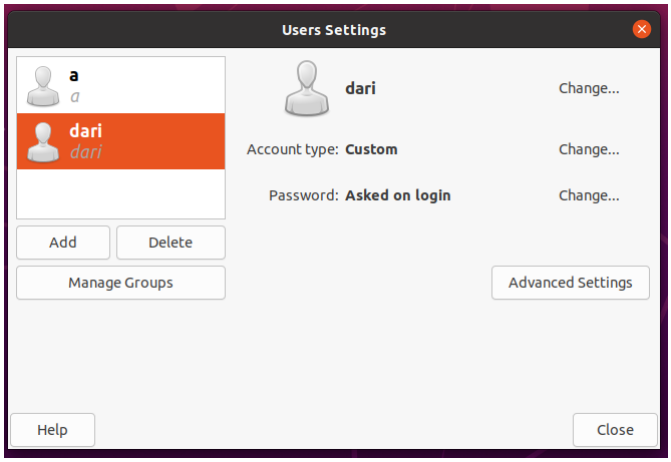
```
dari@Ubuntu:~$ sudo adduser a g1
Adding user `a' to group `g1' ...
Adding user a to group g1
Done.
```

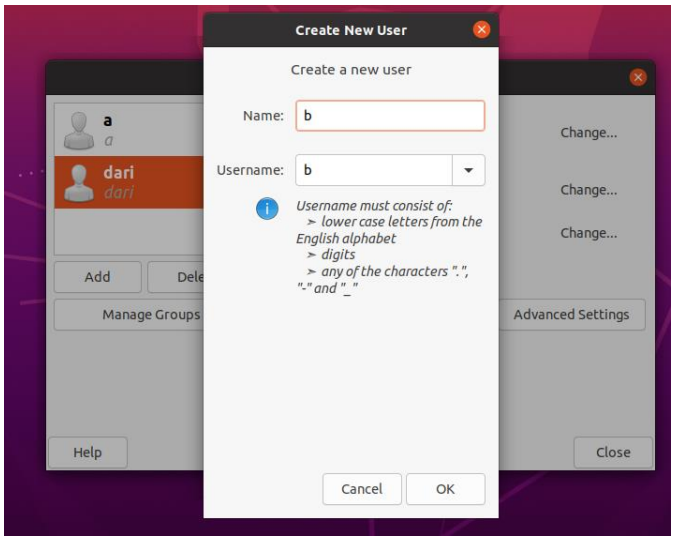
3. Создать группу пользователей с именем g2 и пользователя с именем b в этой группе, используя графический интерфейс пользователя.

Устанавливаем утилиту «Пользователи и группы».

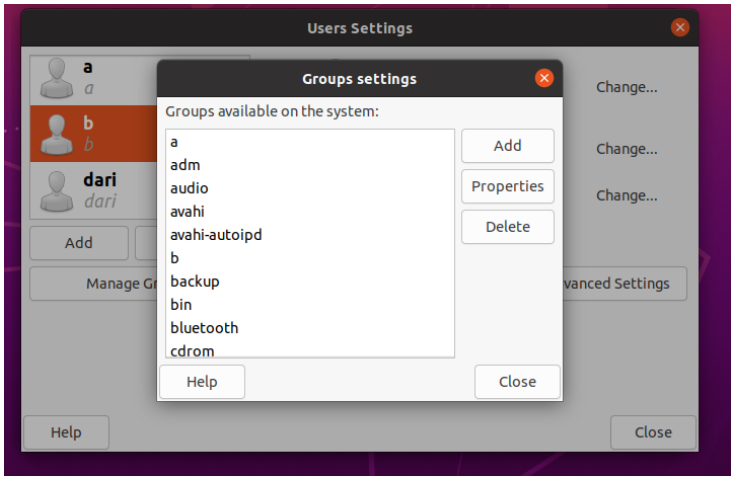
```
dari@Ubuntu:~$ sudo apt-get install gnome-system-tools -y
[sudo] password for dari:
```

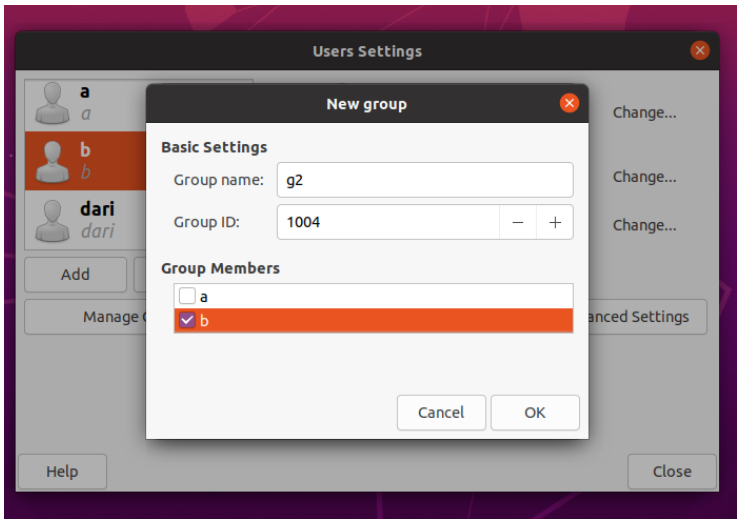
Запускаем, нажимаем **Add**, добавляем пользователя **b**.





Нажимаем **Manage Groups**, **Add**, при создании группы **g2** выбираем пользователя **b**.





4. В домашнем каталоге создать по одному каталогу и файлу на каждого пользователя.

Создаем каталоги через **mkdir**, файлы через **echo >**.

```
dari@Ubuntu:~$ mkdir a
dari@Ubuntu:~$ echo > a/a.txt
dari@Ubuntu:~$ mkdir b
```

```
dari@Ubuntu:~$ echo > b/b.txt
```

5. Разрешить группе чтение, владельцу - чтение и запись файла. Для каталога группе разрешить чтение и выполнение. Для выполнения задания использовать запись прав в 8 сс и маску прав.

Устанавливаем права доступа с помощью команды **chmod**.

Для файла используем восьмеричное представление **640** (6 - права на чтение и запись для владельца, 4 - права на чтение для группы, 0 - отсутствие прав для остальных групп пользователей). Можем проверить результат через ls –l.

```
dari@Ubuntu:~/a$ chmod 640 a.txt
dari@Ubuntu:~/a$ ls -l
total 4
-rw-r----- 1 dari dari 1 ноя 10 16:37 a.txt
```

Для каталога используем маску прав g=rx (g – группа, rx – чтение и выполнение).

```
dari@Ubuntu:~$ chmod g=rx b
dari@Ubuntu:~$ ls -l
total 44
drwxrwxr-x 2 dari dari 4096 ноя 10 16:37 a
drwxr-xr-x 2 dari dari 4096 ноя 10 16:38 b
```

6. На один из созданных каталогов установить sticky-бит.

Каталог с установленным sticky-битом означает, что удалить файл из этого каталога может только владелец файла или суперпользователь.

Устанавливаем с помощью **chmod** и ключа **+t** (добавление к текущим правам).

```
dari@Ubuntu:~$ chmod +t b
dari@Ubuntu:~$ ls -l
total 44
drwxrwxr-x 2 dari dari 4096 ноя 10 16:37 a
drwxr-xr-t 2 dari dari 4096 ноя 10 16:38 b
```

7. Записать в каталог со sticky-битом по копии файла от каждого пользователя бригады, выполнить удаление записанных файлов (проверка действия sticky-бита).

Записываем файл от пользователя **dari**, проверяем его наличие в каталоге. С помощью **su –l** переключаемся на пользователя **b**, уже от его лица просматриваем каталог.

```
dari@Ubuntu:~$ cp /etc/group b
dari@Ubuntu:~$ ls b
b.txt  group
dari@Ubuntu:~$ su -l b
Password:
b@Ubuntu:~$ ls /home/dari/b
b.txt  group
```

Пытаемся удалить скопированный файл, доступ закрыт.

```
b@Ubuntu:~$ rm /home/dari/b/group
rm: remove write-protected regular file '/home/dari/b/group'? y
rm: cannot remove '/home/dari/b/group': Permission denied
```

Переключаемся обратно на создателя файла, от его лица успешно удаляем.

```
b@Ubuntu:~$ su -l dari
Password:
dari@Ubuntu:~$ rm b/group
dari@Ubuntu:~$ ls b
b.txt
```

8. Скопировать один из выполняемых файлов, созданных в работе 5 в один из созданных каталогов и установить ему бит SGID. С помощью команды ls –l получить результаты установки.

Копируем файл и просматриваем его права до установки SGID.

```
b@Ubuntu:~$ cp /home/dari/Yaroshevskaya/1/group /home/b/
```

```
b@Ubuntu:~$ ls -l /home/b
total 4
-rw-r--r-- 1 b b 1039 ноя 11 13:00 group
```

Устанавлиаем бит SGID с помощью **chmod g+x** (без перезаписывания обычных прав) и проверяем: появилась буква S, что говорит об установке бита. Ее регистр означает, что группа для этого файла ранее не имела прав на выполнение.

```
b@Ubuntu:~$ ls -l /home/b
total 4
-rw-r-Sr-- 1 b b 1039 ноя 11 13:00 group
```

9. Проверить, установлена ли поддержка ACL-списков на компьютере, на котором выполняется лабораторная работа.

Используем команду **getfacl**, которая предназначена для отображения ACL-списка указанного файла. Все работает.

```
dari@Ubuntu:~$ getfacl Yaroshevskaya
# file: Yaroshevskaya
# owner: dari
# group: dari
user::rwx
group::rwx
other::r-x
```

10. Установить для одного из созданных каталогов правила по умолчанию и получить результаты установки с помощью утилиты getfacl.

Просматриваем ACL-список каталога **a**.

```
dari@Ubuntu:~$ getfacl a
# file: a
# owner: dari
# group: dari
user::rwx
group::rwx
other::r-x
```

С помощью команды **setfacl** устанавливаем правила по умолчанию (ключ **–d**), ключ **–m** – модификация указанных ACL. Для пользователя **b** делаем доступными только права чтения с помощью **u:b:r--**.

```
dari@Ubuntu:~$ setfacl -d -m u:b:r-- a
```

Проверяем установленные правила.

```
dari@Ubuntu:~$ setfacl -d -m u:b:r-- a
dari@Ubuntu:~$ getfacl a
# file: a
# owner: dari
# group: dari
user::rwx
group::rwx
other::r-x
default:user::rwx
default:user:b:r--
default:group::rwx
default:mask::rwx
default:other::r-x
```