Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Калинина Кристина Сергеевна

Содержание

List of Figures

List of Tables

Цель работы

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

Теоретические сведения

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ, discretion — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. [1]

Для каждого файла в Linux задается набор разрешений. Разрешения могут быть следующими:

- r — read — возможность открытия и чтения файла. Для директории это возможность просматривать содержимое директории.
- w — write — возможность изменения файла. Для директории это возможность добавлять, удалять или переименовывать файлы в директории.
- x — execute — возможность выполнения файла (запуска файла). [2]

Набор разрешений состоит из 3 блоков rwx:

- Первый блок rwx определяет права доступа для владельца-пользователя.

- Второй блок rwx определяет права доступа для владельца-группы.
- Третий блок rwx определяет права доступа для всех остальных. [2]

Для каждого файла или директории в Linux задаются права доступа. Они задаются тремя атрибутами: набором разрешений, именем владельца, именем группы.

Набор разрешений — это три блока прав доступа: права доступа для владельца файла, права доступа для группы, права доступа для всех остальных.

Разрешения записываются символами r, w, x.

Набор разрешений состоит из трех блоков и записывается в виде трех rwx, записанных друг за другом в виде одного «слова».

Если какая-либо возможность отключена (запрещена), то вместо соответствующего символа в наборе разрешений ставится прочерк (символ минус). [2]

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе вошла в учётную запись пользователя guest и создала пользователя guest2, а также задала ему пароль (fig. 0.1).

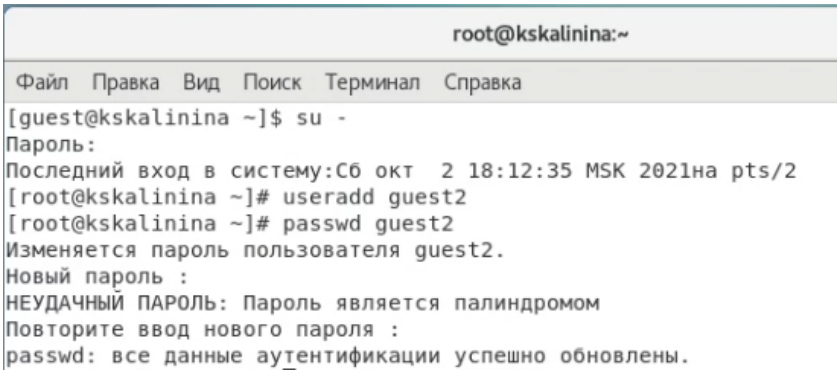

Figure 0.1: Создание учетной записи пользователя guest2

2. Добавила пользователя guest2 в группу guest (fig. 0.2).

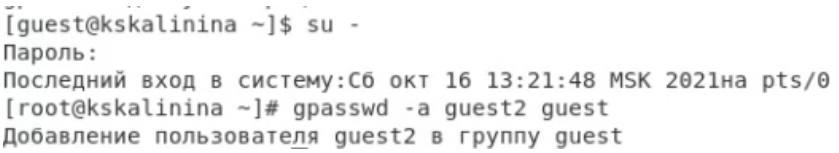

Figure 0.2: Добавление пользователя guest2 в группу guest

3. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли (fig. 0.3).

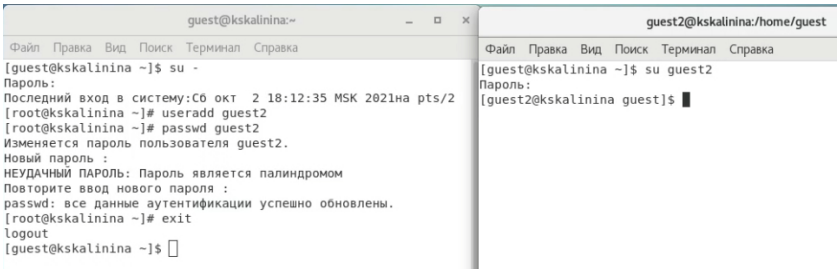

Figure 0.3: Вход в систему от двух пользователей

4. Для обоих пользователей командой pwd определила директорию, в которой я нахожусь. Убедилась в том, что в командной строке отображается тоже самое. Также проверила имя пользователя и основную информацию (fig. 0.4).

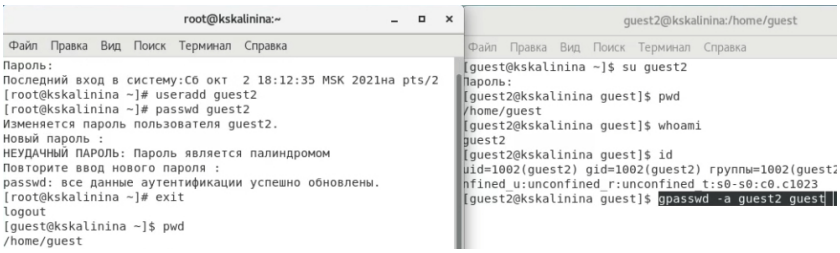

Figure 0.4: Использование команды whoami, id и pwd

5. Определила командами ‘groups guest’ и ‘groups guest2’, в какие группы входят пользователи guest и guest2. Команды ‘id -Gn’ и ‘id -G’ показали id групп и их именования для пользователя, на котором я нахожусь. Информация оказалась аналогичной той, что вывелась после команды ‘groups’ (fig. 0.5).

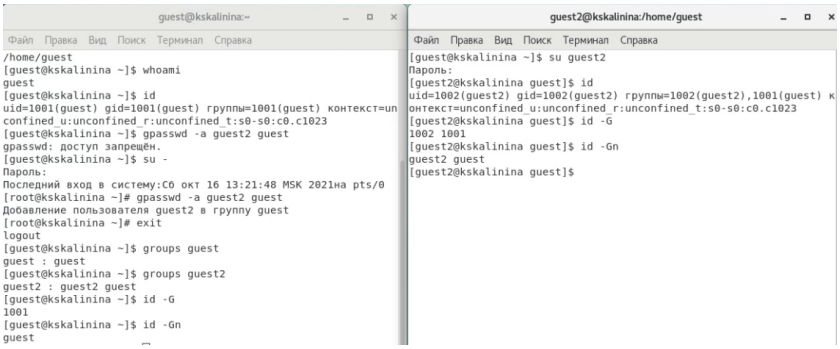

Figure 0.5: Уточнение группы пользователя, и тех, кто также входит в эту группу

6. Просмотрела файл ‘/etc/group’, он показал аналогичную информацию (fig. 0.6).

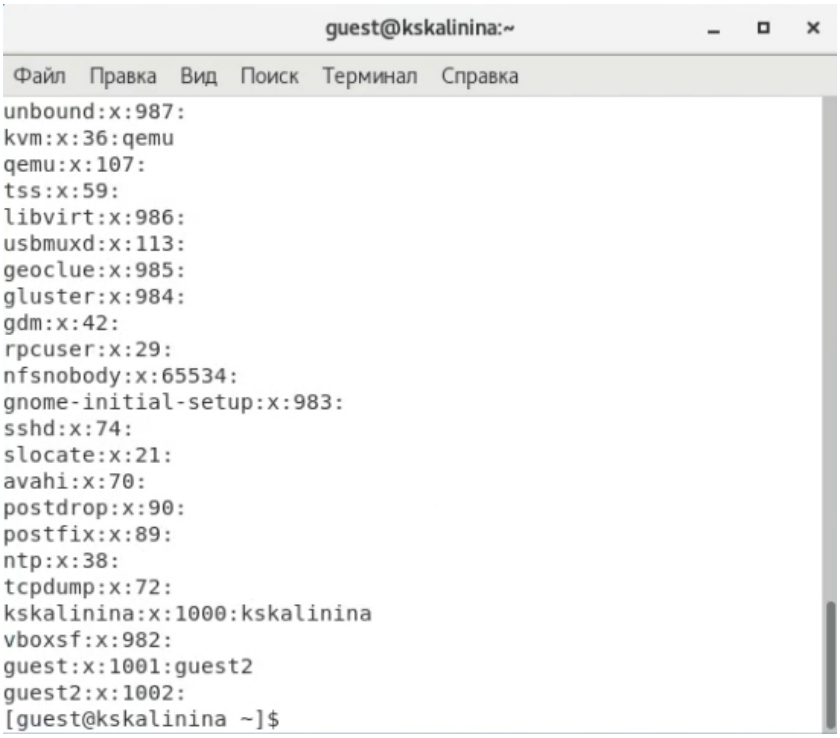

Figure 0.6: Просмотр файла ‘/etc/group’

7. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest (fig. 0.7).

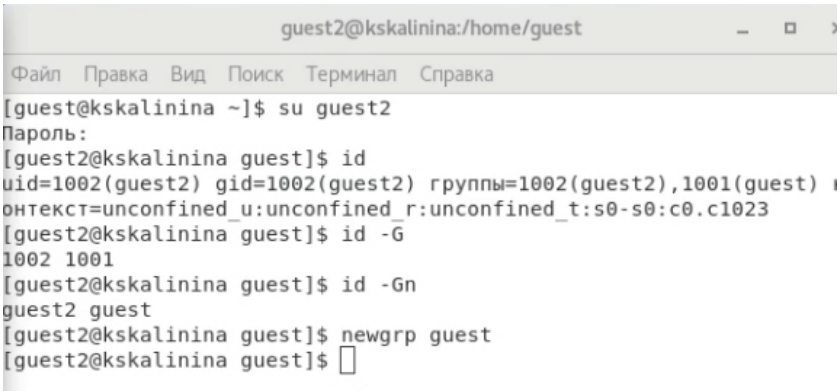

Figure 0.7: Регистрация пользователя guest2 в группе guest

8. От имени пользователя guest изменила права директории ‘/home/guest’, разрешив все действия для пользователей группы (fig. 0.8).

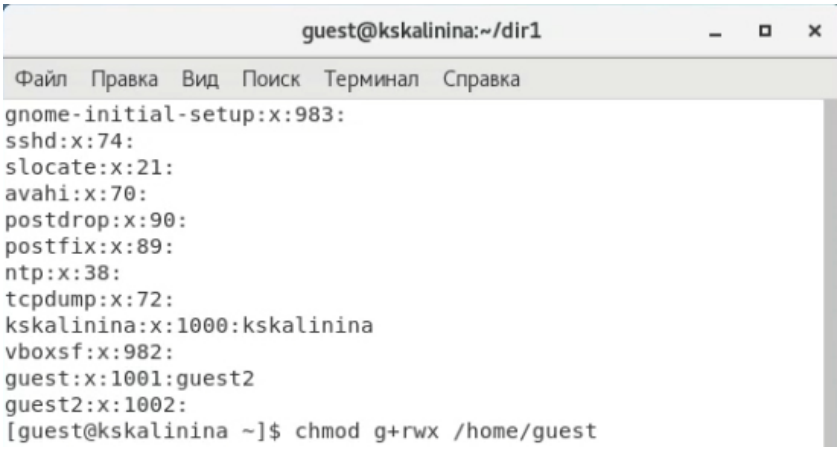

Figure 0.8: Изменение прав директории '/home/guest'

9. Заполнила таблицу «Установленные права и разрешённые действия для групп» (fig. 0.10). Для этого я создала в директории 16 файлов с разными правами на каждом(по два на каждые права для удобства). После этого я меняла права dir1 на guest и пробовала взаимодействовать с каждым из этих файлов на guest2, также пыталась зайти внутрь папки и просмотреть её содержимое (fig. 0.9). Таким образом я проделала необходимые действия с каждым вариантов прав директории и прав файла на пользователе guest2 .

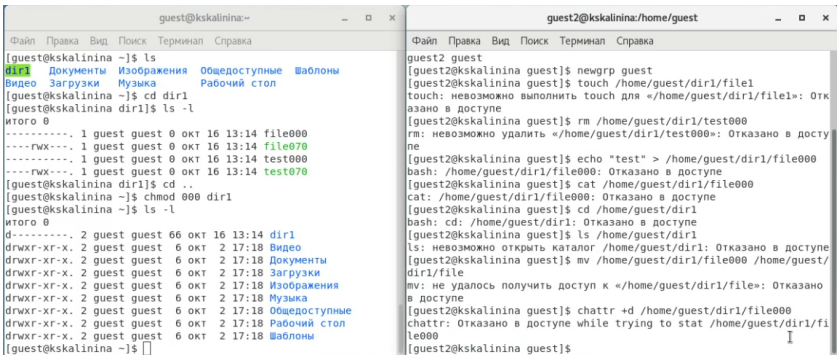

Figure 0.9: Процесс заполнения таблицы

Права директории	Права файла	Создание файла	Удаление файла	Запись файла	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов
d (000)	(000)	-	-	-	-	-	-	-	-
d----x---(010)	(000)	-	-	-	-	+	-	-	-
d----w----(020)	(000)	-	-	-	-	-	-	-	-
d----wx---(030)	(000)	+	+	-	-	+	-	+	-
d---r-----(040)	(000)	-	-	-	-	-	+	-	-
d---r-x---(050)	(000)	-	-	-	-	+	+	-	-
d---rw----(060)	(000)	-	-	-	-	-	+	-	-
d---rwx---(070)	(000)	+	+	-	-	+	+	+	-
d (000)	------x---(010)	-	-	-	-	-	-	-	-
d----x---(010)	------x---(010)	-	-	-	-	+	-	-	-
d----w----(020)	------x---(010)	-	-	-	-	-	-	-	-
d----wx---(030)	------x---(010)	+	+	-	-	+	-	+	-
d---r-----(040)	------x---(010)	-	-	-	-	-	+	-	-
d---r-x---(050)	------x---(010)	-	-	-	-	+	+	-	-
d---rw----(060)	------x---(010)	-	-	-	-	-	+	-	-
d---rwx---(070)	------x---(010)	+	+	-	-	+	+	+	-
d (000)	-----w----(020)	-	-	-	-	-	-	-	-
d----x---(010)	-----w----(020)	-	-	+	-	+	-	-	-
d----w----(020)	-----w----(020)	-	-	-	-	-	-	-	-
d----wx---(030)	-----w----(020)	+	+	+	-	+	-	+	-
d---r-----(040)	-----w----(020)	-	-	-	-	-	+	-	-
d---r-x---(050)	-----w----(020)	-	-	+	-	+	+	-	-
d---rw----(060)	-----w----(020)	-	-	-	-	-	+	-	-
d---rwx---(070)	-----w----(020)	+	+	+	-	+	+	+	-
d (000)	-----wx---(030)	-	-	-	-	-	-	-	-
d----x---(010)	-----wx---(030)	-	-	+	-	+	-	-	-
d----w----(020)	-----wx---(030)	-	-	-	-	-	-	-	-
d----wx---(030)	-----wx---(030)	+	+	+	-	+	-	+	-
d---r-----(040)	-----wx---(030)	-	-	-	-	-	+	-	-
d---r-x---(050)	-----wx---(030)	-	-	+	-	+	+	-	-
d---rw----(060)	-----wx---(030)	-	-	-	-	-	+	-	-
d---rwx---(070)	-----wx---(030)	+	+	+	-	+	+	+	-
d (000)	----r-----(040)	-	-	-	-	-	-	-	-
d----x---(010)	----r-----(040)	-	-	-	+	+	-	-	-
d----w----(020)	----r-----(040)	-	-	-	-	-	-	-	-
d----wx---(030)	----r-----(040)	+	+	-	+	+	-	+	-
d---r-----(040)	----r-----(040)	-	-	-	-	-	+	-	-
d---r-x---(050)	----r-----(040)	-	-	-	+	+	+	-	-
d---rw----(060)	----r-----(040)	-	-	-	-	-	+	-	-
d---rwx---(070)	----r-----(040)	+	+	-	+	+	+	+	-
d (000)	----r-x---(050)	-	-	-	-	-	-	-	-
d----x---(010)	----r-x---(050)	-	-	-	+	+	-	-	-
d----w----(020)	----r-x---(050)	-	-	-	-	-	-	-	-
d----wx---(030)	----r-x---(050)	+	+	-	+	+	-	+	-
d---r-----(040)	----r-x---(050)	-	-	-	-	-	+	-	-
d---r-x---(050)	----r-x---(050)	-	-	-	+	+	+	-	-
d---rw----(060)	----r-x---(050)	-	-	-	-	-	+	-	-
d---rwx---(070)	----r-x---(050)	+	+	-	+	+	+	+	-
d (000)	----rw----(060)	-	-	-	-	-	-	-	-
d----x---(010)	----rw----(060)	-	-	+	+	+	-	-	-
d----w----(020)	----rw----(060)	-	-	-	-	-	-	-	-
d----wx---(030)	----rw----(060)	+	+	+	+	+	-	+	-
d---r-----(040)	----rw----(060)	-	-	-	-	-	+	-	-
d---r-x---(050)	----rw----(060)	-	-	+	+	+	+	-	-
d---rw----(060)	----rw----(060)	-	-	-	-	-	+	-	-
d---rwx---(070)	----rw----(060)	+	+	+	+	+	+	+	-
d (000)	----rwx---(070)	-	-	-	-	-	-	-	-
d----x---(010)	----rwx---(070)	-	-	+	+	+	-	-	-
d----w----(020)	----rwx---(070)	-	-	-	-	-	-	-	-
d----wx---(030)	----rwx---(070)	+	+	+	+	+	-	+	-
d---r-----(040)	----rwx---(070)	-	-	-	-	-	+	-	-
d---r-x---(050)	----rwx---(070)	-	-	+	+	+	+	-	-
d---rw----(060)	----rwx---(070)	-	-	-	-	-	+	-	-
d---rwx---(070)	----rwx---(070)	+	+	+	+	+	+	+	-

Figure 0.10: Таблица «Установленные права и разрешённые действия для групп»

10. На основе полученной информации из таблицы прошлого пункта (fig. 0.10), я смогла определить те или иные минимально необходимые права для выполнения операций внутри директории dir1 от имени пользователей входящих в группу (guest2). Так как в предыдущем пунте не требовалось создавать подкаталог, я дополнительно попробовала создать dir2 внутри dir1 (меняя права dir1) и удалить её, используя пользователя guest2 (fig. 0.11).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	-
Удаление поддиректории	030	-

Figure 0.11: Таблица “Минимальные права для совершения операций от имени пользователей входящих в группу”

Выводы

Таким образом я успешно приобрела практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Дискреционное разграничение доступа Linux. // Debianinstall. 2018. URL: https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/ (дата обращения 16.10.2021).

2. Права доступа к файлам в Linux. // Pingvinus. 2018.URL: https://pingvinus.ru/note/file-permissions (дата обращения 16.10.2021).

3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..