

Лабораторная работа № 3

Дискреционное разграничение прав в Linux. Два пользователя

Сухарев Кирилл

Содержание

Цель работы	5
Условные обозначения и термины	6
Теоретические вводные данные	7
Права доступа к файлам в Linux	7
Основные права доступа к файлам в Linux	7
Просмотр прав доступа	8
Техническое оснащение и выбранные методы проведения работы	10
Выполнение работы	11
Выводы	17
Библиография	18

List of Figures

0.1	Создание нового учётного пользователя	11
0.2	Директории пользователей guest и guest2	11
0.3	Команды groups	12
0.4	Команды id	12
0.5	Файл /etc/group	13
0.6	Регистрация пользователя guest2 в группе guest	13
0.7	Изменение прав доступа	13
0.8	Таблица 3.1	15
0.9	Таблица 3.2	16

List of Tables

Цель работы

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

Условные обозначения и термины

Учетная запись - хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Директория - объект в файловой системе, упрощающий организацию файлов.

uid - номер, назначенный каждому пользователю Linux. Это представление пользователя в ядре Linux.

gid - идентификационный номер основной группы пользователя.

Теоретические вводные данные

Права доступа к файлам в Linux

В операционной системе Linux много функций безопасности. Одна из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

Основные права доступа к файлам в Linux

Изначально каждый файл имел три параметра доступа. Вот они:

- Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;
- Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;
- Выполнение - вы не можете выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу.

Но все эти права были бы бессмысленными, если бы применялись сразу для всех пользователей. Поэтому каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

- Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение.
- Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу.
- Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла.

Именно с помощью этих наборов полномочий устанавливаются права файлов в linux. Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является или к тем, доступ к которым ему разрешен. Только пользователь Root может работать со всеми файлами независимо от их набора их полномочий.

Просмотр прав доступа

Узнать права на файл linux можно командой `ls -l`. За права файлов в linux тут отвечают черточки. Первая это тип файла, который рассмотрен в отдельной статье. Дальше же идут группы прав сначала для владельца, для группы и для всех остальных. Всего девять черточек на права и одна на тип. Рассмотрим значения черточек:

- — - нет прав, совсем;
- -x - разрешено только выполнение файла, как программы но не изменение и не чтение;
- -w- - разрешена только запись и изменение файла;
- -wx - разрешено изменение и выполнение, но в случае с каталогом, вы не можете посмотреть его содержимое;
- r- - права только на чтение;
- r-x - только чтение и выполнение, без права на запись;

- `rw-` - права на чтение и запись, но без выполнения;
- `rwX` - все права;

Техническое оснащение и выбранные методы проведения работы

В качестве среды выполнения лабораторной работы используется менеджер виртуальных машин VirtualBox и установленная с его помощью ОС Centos 7 на базе Linux.

Выполнение работы

1. Используя учётную запись администратора создадим учётную запись пользователя guest2, зададим для него пароль и добавим его в группу guest (fig. 0.1).

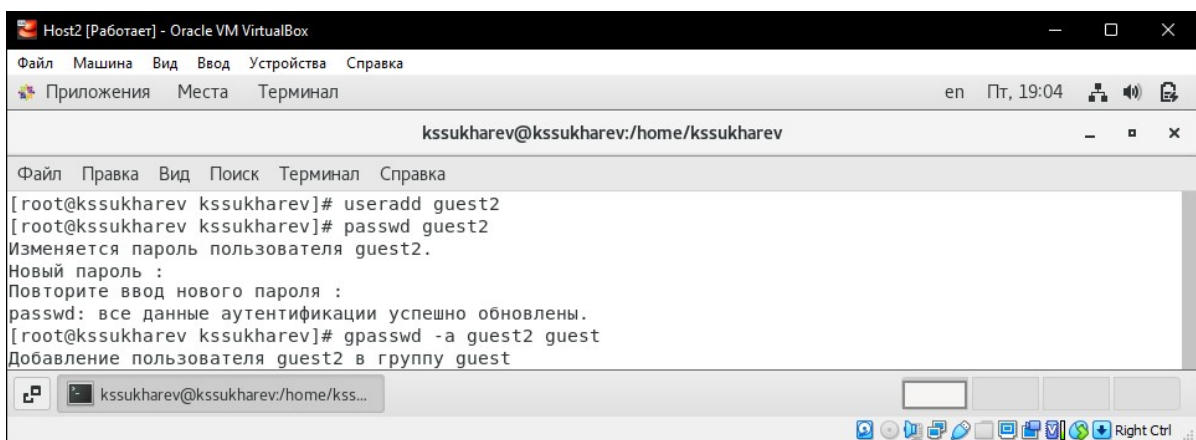


Figure 0.1: Создание нового учётного пользователя

2. Войдем в систему от двух пользователей на двух разных консолях и при помощи команды `pwd` определим директорию. (fig. 0.2).

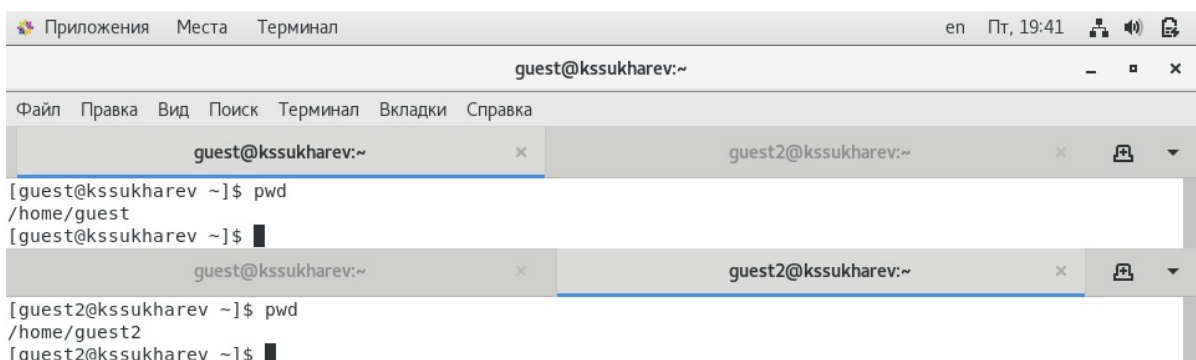
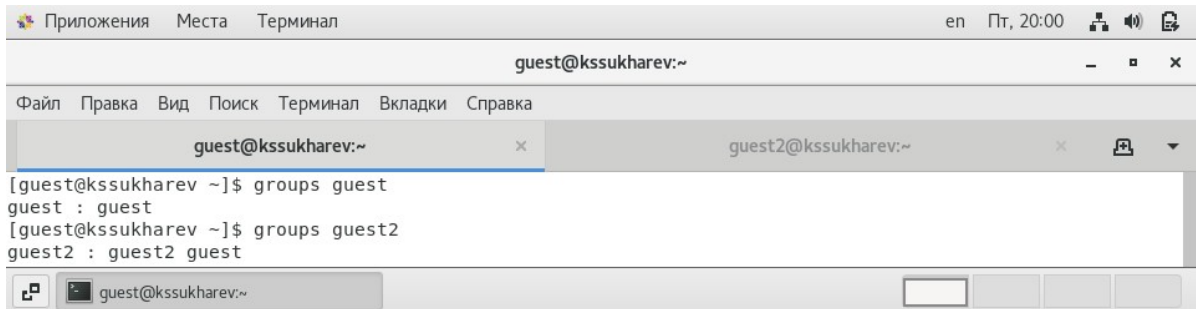


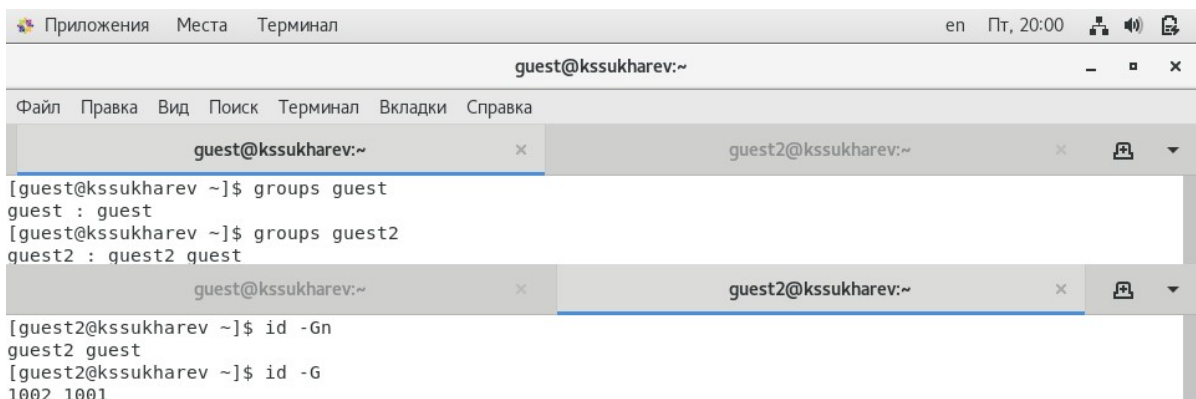
Figure 0.2: Директории пользователей guest и guest2

3. Выполним команды `groups guest` и `groups guest2` (fig. 0.3), чтобы определить, в какие группы входят указанные пользователи. Сравним вывод этих команд с выводом команды `id -Gn` и `id -G` (fig. 0.4). Обе команды сообщают, что пользователь `guest` находится только в группе `guest`, а пользователь `guest2` - в группах `guest` и `guest2`.



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

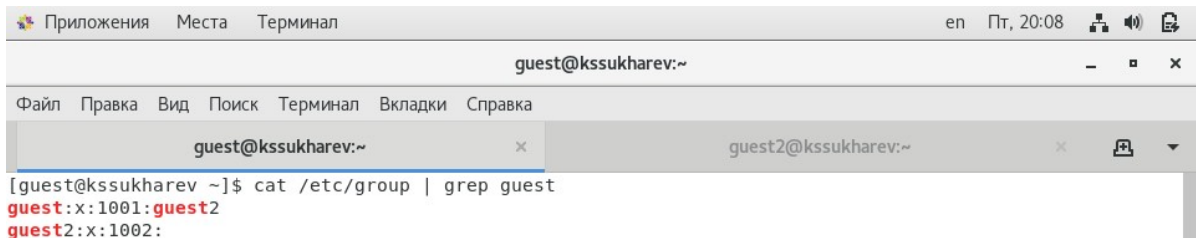
Figure 0.3: Команды `groups`



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

Figure 0.4: Команды `id`

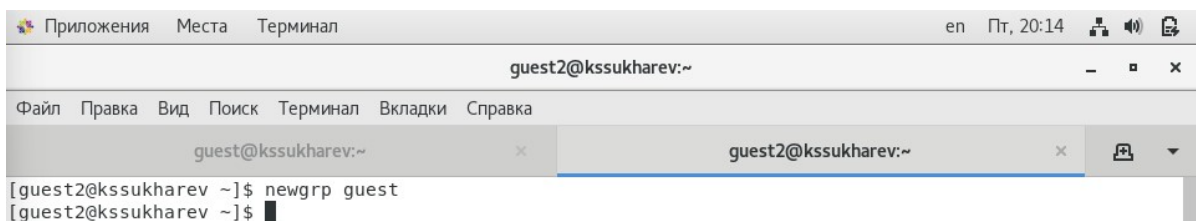
4. Просмотрим файл `/etc/group`. В нем содержится список групп, а также список пользователей внутри этой группы. (fig. 0.5).



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

Figure 0.5: Файл /etc/group

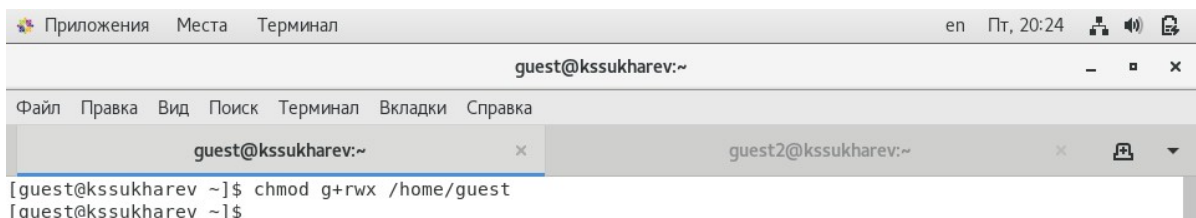
- От имени пользователя guest2 выполним регистрацию этого пользователя в группе guest командой `newgrp guest`(fig. 0.6).



```
guest2@kssukharev:~  
[guest2@kssukharev ~]$ newgrp guest  
[guest2@kssukharev ~]$
```

Figure 0.6: Регистрация пользователя guest2 в группе guest

- От имени пользователя guest изменим права директории `/home/guest`, разрешив все действия для пользователей группы (fig. 0.7).



```
guest@kssukharev:~  
[guest@kssukharev ~]$ chmod g+rwX /home/guest  
[guest@kssukharev ~]$
```

Figure 0.7: Изменение прав доступа

- Выполним анализ прав доступа на директорию `dir1` и файла `file1`. Менять права будем от имени пользователя guest, а выполнять проверку - от пользователя guest2. Результаты будем заносить в табл. 3.1 (fig. 0.8). Для проверки будут использоваться следующие команды:

- Создание файла: `echo "test" > dir1/file2`

- Удаление файла: `rm dir1/file1`
- Запись в файл: `echo "test" > dir1/file1`
- Чтение файла: `cat dir1/file1`
- Смена директории: `cd dir1`
- Просмотр файлов в директории: `ls dir1`
- Переименование файла: `mv dir1/file1 dir1/file2`
- Смена атрибутов файла: `chattr +d dir1/file1`

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименования файла	Смена атрибутов файла
d--- --- (000)	--- --- (000)	-	-	-	-	-	-	-	-
d--- --- (000)	--- -X --- (010)	-	-	-	-	-	-	-	-
d--- --- (000)	--- -W --- (020)	-	-	-	-	-	-	-	-
d--- --- (000)	--- -WX --- (030)	-	-	-	-	-	-	-	-
d--- --- (000)	--- r- --- (040)	-	-	-	-	-	-	-	-
d--- --- (000)	--- r-X --- (050)	-	-	-	-	-	-	-	-
d--- --- (000)	--- rW- --- (060)	-	-	-	-	-	-	-	-
d--- --- (000)	--- rwx --- (070)	-	-	-	-	-	-	-	-
d--- -X --- (010)	--- --- (000)	-	-	-	-	+	-	-	-
d--- -X --- (010)	--- -X --- (010)	-	-	-	-	+	-	-	-
d--- -X --- (010)	--- -W --- (020)	-	-	+	-	+	-	-	-
d--- -X --- (010)	--- -WX --- (030)	-	-	+	-	+	-	-	-
d--- -X --- (010)	--- r- --- (040)	-	-	-	+	+	-	-	-
d--- -X --- (010)	--- r-X --- (050)	-	-	-	+	+	-	-	-
d--- -X --- (010)	--- rW- --- (060)	-	-	+	+	+	-	-	-
d--- -X --- (010)	--- rwx --- (070)	-	-	+	+	+	-	-	-
d--- -W- --- (020)	--- --- (000)	-	-	-	-	-	-	-	-
d--- -W- --- (020)	--- -X --- (010)	-	-	-	-	-	-	-	-
d--- -W- --- (020)	--- -W --- (020)	-	-	-	-	-	-	-	-
d--- -W- --- (020)	--- -WX --- (030)	-	-	-	-	-	-	-	-
d--- -W- --- (020)	--- r- --- (040)	-	-	-	-	-	-	-	-
d--- -W- --- (020)	--- r-X --- (050)	-	-	-	-	-	-	-	-
d--- -W- --- (020)	--- rW- --- (060)	-	-	-	-	-	-	-	-
d--- -W- --- (020)	--- rwx --- (070)	-	-	-	-	-	-	-	-
d--- -WX --- (030)	--- --- (000)	+	+	-	-	+	-	+	-
d--- -WX --- (030)	--- -X --- (010)	+	+	-	-	+	-	+	-
d--- -WX --- (030)	--- -W --- (020)	+	+	+	-	+	-	+	-
d--- -WX --- (030)	--- -WX --- (030)	+	+	+	-	+	-	+	-
d--- -WX --- (030)	--- r- --- (040)	+	+	-	+	+	-	+	-
d--- -WX --- (030)	--- r-X --- (050)	+	+	-	+	+	-	+	-
d--- -WX --- (030)	--- rW- --- (060)	+	+	+	+	+	-	+	-
d--- -WX --- (030)	--- rwx --- (070)	+	+	+	+	+	-	+	-
d--- r- --- (040)	--- --- (000)	-	-	-	-	-	+	-	-
d--- r- --- (040)	--- -X --- (010)	-	-	-	-	-	+	-	-
d--- r- --- (040)	--- -W --- (020)	-	-	-	-	-	+	-	-
d--- r- --- (040)	--- -WX --- (030)	-	-	-	-	-	+	-	-
d--- r- --- (040)	--- r- --- (040)	-	-	-	-	-	+	-	-
d--- r- --- (040)	--- r-X --- (050)	-	-	-	-	-	+	-	-
d--- r- --- (040)	--- rW- --- (060)	-	-	-	-	-	+	-	-
d--- r- --- (040)	--- rwx --- (070)	-	-	-	-	-	+	-	-
d--- r-X --- (050)	--- --- (000)	-	-	-	-	+	+	-	-
d--- r-X --- (050)	--- -X --- (010)	-	-	-	-	+	+	-	-
d--- r-X --- (050)	--- -W --- (020)	-	-	+	-	+	+	-	-
d--- r-X --- (050)	--- -WX --- (030)	-	-	+	-	+	+	-	-
d--- r-X --- (050)	--- r- --- (040)	-	-	-	+	+	+	-	-
d--- r-X --- (050)	--- r-X --- (050)	-	-	-	+	+	+	-	-
d--- r-X --- (050)	--- rW- --- (060)	-	-	+	+	+	+	-	-
d--- r-X --- (050)	--- rwx --- (070)	-	-	+	+	+	+	-	-
d--- rW- --- (060)	--- --- (000)	-	-	-	-	-	+	-	-
d--- rW- --- (060)	--- -X --- (010)	-	-	-	-	-	+	-	-
d--- rW- --- (060)	--- -W --- (020)	-	-	-	-	-	+	-	-
d--- rW- --- (060)	--- -WX --- (030)	-	-	-	-	-	+	-	-
d--- rW- --- (060)	--- r- --- (040)	-	-	-	-	-	+	-	-
d--- rW- --- (060)	--- r-X --- (050)	-	-	-	-	-	+	-	-
d--- rW- --- (060)	--- rW- --- (060)	-	-	-	-	-	+	-	-
d--- rW- --- (060)	--- rwx --- (070)	-	-	-	-	-	+	-	-
d--- rwx --- (070)	--- --- (000)	+	+	-	-	+	+	+	-
d--- rwx --- (070)	--- -X --- (010)	+	+	-	-	+	+	+	-
d--- rwx --- (070)	--- -W --- (020)	+	+	+	-	+	+	+	-
d--- rwx --- (070)	--- -WX --- (030)	+	+	+	-	+	+	+	-
d--- rwx --- (070)	--- r- --- (040)	+	+	-	+	+	+	+	-
d--- rwx --- (070)	--- r-X --- (050)	+	+	-	+	+	+	+	-
d--- rwx --- (070)	--- rW- --- (060)	+	+	+	+	+	+	+	-
d--- rwx --- (070)	--- rwx --- (070)	+	+	+	+	+	+	+	-

Figure 0.8: Таблица 3.1

8. По результатам таблицы 3.1 заполним таблицу 3.2 (fig. 0.9).

Операция	Минимальные права на директорию	Минимальные 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)

Figure 0.9: Таблица 3.2

Выводы

Права доступа используются для управления возможностями различных групп пользователей системы по отношению к директориям и файлам.

Библиография

1. Группы пользователей Linux // Losst. 2020. URL: <https://losst.ru/gruppy-polzovatelej-linux> (Дата обращения: 15.10.2021).
2. Права доступа к файлам в Linux. // Losst. 2020. URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux> (Дата обращения: 15.10.2021).
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..