

Отчёт по лабораторной работе №3

Дискреционное разграничение прав в Linux. Два пользователя

Саргсян Арам Грачьевич

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение работы	9
5	Выводы	20
	Список литературы	21

Список иллюстраций

4.1	Добавление пользователей в группу	9
4.2	Информация о пользователях	10

Список таблиц

4.1	Установленные права и разрешённые действия для групп	11
4.2	Минимальные права для совершения операций	19

1 Цель работы

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

2 Задание

- Произвести работу в консоли с атрибутами от имени пользователя *guest*;
- Составить опытным путем от пользователя *guest2* таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

3 Теоретическое введение

В данной лабораторной работе нам предстоит поработать с правами доступа файлов и директорий. **Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами.

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

- **r** — read (чтение) — право просматривать содержимое файла;
- **w** — write (запись) — право изменять содержимое файла;
- **x** — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

- **owner** (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но владельцем можно сделать и кого-то другого.
- **group** (группа) — пользователи с общими заданными правами.
- **others** (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами.[1]

Чтобы увидеть текущие назначения владельца, нужно использовать команду `ls -l`. Эта команда показывает пользователя и группу-владельца.

Чтобы применить соответствующие разрешения, первое, что нужно учитывать, это владение. Для этого есть команда `chown`. [2]

Для того, чтобы позволить обычным пользователям выполнять программы от имени суперпользователя без знания его пароля была придумана такая вещь, как SUID и SGID биты. Рассмотрим эти полномочия подробнее.

- **SUID** - если этот бит установлен, то при выполнении программы, id пользователя, от которого она запущена заменяется на id владельца файла. Фактически, это позволяет обычным пользователям запускать программы от имени суперпользователя;
- **SGID** - этот флаг работает аналогичным образом, только разница в том, что пользователь считается членом группы, с которой связан файл, а не групп, к которым он действительно принадлежит. Если SGID флаг установлен на каталог, все файлы, созданные в нем, будут связаны с группой каталога, а не пользователя. Такое поведение используется для организации общих папок;
- **Sticky-bit** - этот бит тоже используется для создания общих папок. Если он установлен, то пользователи могут только создавать, читать и выполнять файлы, но не могут удалять файлы, принадлежащие другим пользователям.[3]

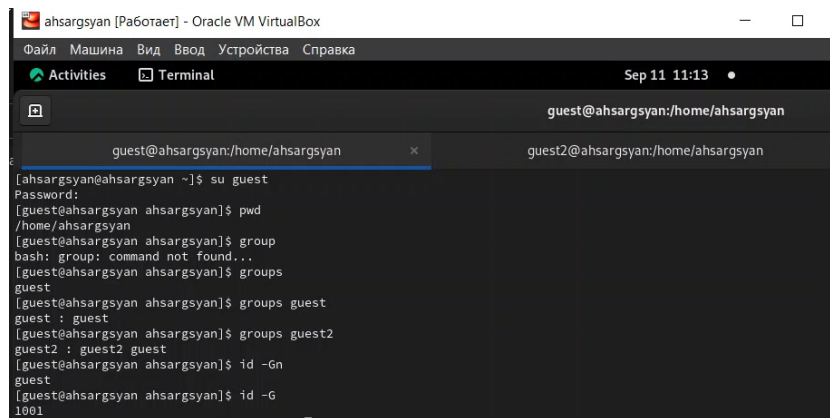
4 Выполнение работы

1. В предыдущей работе в установленной ОС создали учетную запись пользователя guest и задали пароль для пользователя (используя учетную запись администратора) и зашли в эту учетную запись. Аналогично создали второго пользователя guest2 и выполнили вход в эту учетную запись. Добавили пользователя guest2 в группу guest (4.1)

```
[ahsargsyan@ahsargsyan ~]$ sudo -i
[sudo] password for ahsargsyan:
[root@ahsargsyan ~]# useradd guest2
[root@ahsargsyan ~]# passwd guest2
Changing password for user guest2.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ahsargsyan ~]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@ahsargsyan ~]# su guest
[guest@ahsargsyan root]$ exit
exit
[root@ahsargsyan ~]#
```

Рис. 4.1: Добавление пользователей в группу

2. Выполнили вход в две учетные записи guest guest2 на разных консолях. Для обоих пользователей командой Pwd определили директорию, в которой находимся. Сравнили ее с приглашением командой строки. Уточнили имя нашего пользователя, его группу, кто входит в нее и к каким группам принадлежит он сам. Определили командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравнили выводы команды groups с выводом команд id -Gn и id -G.



```
ahsargsyan [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Activities  Terminal
Sep 11 11:13
guest@ahsargsyan:/home/ahsargsyan
guest@ahsargsyan:/home/ahsargsyan x  guest2@ahsargsyan:/home/ahsargsyan x
[ahsargsyan@ahsargsyan ~]$ su guest
Password:
[guest@ahsargsyan ahsargsyan]$ pwd
/home/ahsargsyan
[guest@ahsargsyan ahsargsyan]$ group
bash: group: command not found...
[guest@ahsargsyan ahsargsyan]$ groups
guest
[guest@ahsargsyan ahsargsyan]$ groups guest
guest : guest
[guest@ahsargsyan ahsargsyan]$ groups guest2
guest2 : guest2 guest
[guest@ahsargsyan ahsargsyan]$ id -Gn
guest
[guest@ahsargsyan ahsargsyan]$ id -G
1001
```

Рис. 4.2: Информация о пользователях

3. После снятия атрибутов заполнили таблицу [4.1]

Обозначения в таблице:

- (1) Создание файла
- (2) Удаление файла
- (3) Запись в файл
- (4) Чтение файла
- (5) Смена директории
- (6) Просмотр файлов в директории
- (7) Переименование файл
- (8) Смена атрибутов файла

Таблица 4.1: Установленные права и разрешённые действия для групп

		Права	Права							
		дирек-	фай-	1	2	3	4	5	6	7
		тории	ла							
-----	-----			-	-	-	-	-	-	-
(000)	(000)									
-----	-----			-	-	-	-	-	-	-
(000)	x---									
	(010)									
-----	-----			-	-	-	-	-	-	-
(000)	w----									
	(020)									
-----	-----			-	-	-	-	-	-	-
(000)	wx---									
	(030)									
-----	---			-	-	-	-	-	-	-
(000)	r-----									
	(040)									
-----	---r-			-	-	-	-	-	-	-
(000)	x---									
	(050)									
-----	---			-	-	-	-	-	-	-
(000)	rw----									
	(060)									
-----	---			-	-	-	-	-	-	-
(000)	rw----									
	(070)									

		Права							
		Права	ва						
		дирек-	фай-	1	2	3	4	5	6
		тории	ла						7
-----x---	-----	-	-	-	+	-	-	-	-
(010)	(000)								
-----x---	-----	-	-	-	+	-	-	-	-
(010)	x---								
	(010)								
-----x---	-----	-	-	+	-	+	-	-	-
(010)	w----								
	(020)								
-----x---	-----	-	-	+	-	+	-	-	-
(010)	wx---								
	(030)								
-----x---	---	-	-	-	+	+	-	-	+
(010)	r-----								
	(040)								
-----x---	---r-	-	-	-	+	+	-	-	+
(010)	x---								
	(050)								
-----x---	---	-	-	+	+	+	-	-	+
(010)	rw----								
	(060)								
-----x---	---	-	-	+	+	+	-	-	+
(010)	rwx---								
	(070)								
----w----	-----	-	-	-	-	-	-	-	-
(020)	(000)								

	Права дирек- тории	Пра- ва фай- ла	1	2	3	4	5	6	7
-----w----- (020)	----- x----	-	-	-	-	-	-	-	-
	(010)								
-----w----- (020)	----- w-----	-	-	-	-	-	-	-	-
	(020)								
-----w----- (020)	----- wx----	-	-	-	-	-	-	-	-
	(030)								
-----w----- (020)	----- r-----	-	-	-	-	-	-	-	-
	(040)								
-----w----- (020)	----r- x----	-	-	-	-	-	-	-	-
	(050)								
-----w----- (020)	----- rw-----	-	-	-	-	-	-	-	-
	(060)								
-----w----- (020)	----- rwx----	-	-	-	-	-	-	-	-
	(070)								
-----wx----- (030)	-----+ (000)	+	+	-	-	+	-	+	-

	Права дирек- тории	Пра- ва фай- ла	1	2	3	4	5	6	7
----wx---	-----	+	+	-	-	+	-	+	-
(030)	x---								
	(010)								
----wx---	-----	+	+	+	-	+	-	+	-
(030)	w----								
	(020)								
----wx---	-----	+	+	+	-	+	-	+	-
(030)	wx---								
	(030)								
----wx---	---	+	+	-	+	+	-	+	+
(030)	r-----								
	(040)								
----wx---	---r-	+	+	-	+	+	-	+	+
(030)	x---								
	(050)								
----wx---	---	+	+	+	+	+	-	+	+
(030)	rw----								
	(060)								
----wx---	---	+	+	+	+	+	-	+	+
(030)	rw----								
	(070)								
---r-----	-----		-	-	-	-	+	-	-
(040)	(000)								

		Права	Права							
		дирек-	ва							
		тории	фай-	1	2	3	4	5	6	7
			ла							
---	r-----	-----	-	-	-	-	-	+	-	-
(040)	x---									
	(010)									
---	r-----	-----	-	-	-	-	-	+	-	-
(040)	w----									
	(020)									
---	r-----	-----	-	-	-	-	-	+	-	-
(040)	wx---									
	(030)									
---	r-----	---	-	-	-	-	-	+	-	-
(040)	r-----									
	(040)									
---	r-----	---r-	-	-	-	-	-	+	-	-
(040)	x---									
	(050)									
---	r-----	---	-	-	-	-	-	+	-	-
(040)	rw----									
	(060)									
---	r-----	---	-	-	-	-	-	+	-	-
(040)	rw----									
	(070)									
---	r-x---	-----	-	-	-	-	+	+	-	-
(050)	(000)									

	Права дирек- тории	Пра- ва фай- ла	1	2	3	4	5	6	7
---	r-x---	-----	-	-	-	+	+	-	-
(050)	x---								
	(010)								
---	r-x---	-----	-	-	+	-	+	+	-
(050)	w----								
	(020)								
---	r-x---	-----	-	-	+	-	+	+	-
(050)	wx---								
	(030)								
---	r-x---	---	-	-	-	+	+	+	-
(050)	r-----								+
	(040)								
---	r-x---	---r-	-	-	-	+	+	+	-
(050)	x---								+
	(050)								
---	r-x---	---	-	-	+	+	+	+	-
(050)	rw----								+
	(060)								
---	r-x---	---	-	-	+	+	+	+	-
(050)	rwx---								+
	(070)								
---	rw----	-----	-	-	-	-	+	-	-
(060)	(000)								

		Права	Права							
		дирек-	ва							
		тории	фай-	1	2	3	4	5	6	7
			ла							
---	rw----	-----	-	-	-	-	-	+	-	-
(060)	x---									
	(010)									
---	rw----	-----	-	-	-	-	-	+	-	-
(060)	w----									
	(020)									
---	rw----	-----	-	-	-	-	-	+	-	-
(060)	wx---									
	(030)									
---	rw----	----	-	-	-	-	-	+	-	-
(060)	r-----									
	(040)									
---	rw----	---r-	-	-	-	-	-	+	-	-
(060)	x---									
	(050)									
---	rw----	----	-	-	-	-	-	+	-	-
(060)	rw----									
	(060)									
---	rw----	----	-	-	-	-	-	+	-	-
(060)	rwx---									
	(070)									
---	rwx---	-----+	+	+	-	-	+	+	+	-
(070)	(000)									

	Права дирек- тории	Пра- ва фай- ла	1	2	3	4	5	6	7
---rwx---	-----	+	+	-	-	+	+	+	-
(070)	x---								
	(010)								
---rwx---	-----	+	+	+	-	+	+	+	-
(070)	w----								
	(020)								
---rwx---	-----	+	+	+	-	+	+	+	-
(070)	wx---								
	(030)								
---rwx---	---	+	+	-	+	+	+	+	+
(070)	r-----								
	(040)								
---rwx---	---r-	+	+	-	+	+	+	+	+
(070)	x---								
	(050)								
---rwx---	---	+	+	+	+	+	+	+	+
(070)	rw----								
	(060)								
---rwx---	---	+	+	+	+	+	+	+	+
(070)	rwx---								
	(070)								

На основании заполненной таблицы я определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила таблицу [4.2]. Для заполнения последних двух строк

опытным путем проверила минимальные права для создания и удаления поддиректории.

Таблица 4.2: Минимальные права для совершения операций

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)

Сравнивая таблицу 3.1. с такой же таблицей из предыдущей лабораторной работы, могу сказать, что они одинаковы. Единственное различие только в том, что в предыдущий раз я присваивала права владельцу, а в этот раз группе.

5 Выводы

В ходе выполнения работы, мы приобрели практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Права доступа в Linux [Электронный ресурс]. 2023. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.
2. Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask) [Электронный ресурс]. 2023. URL: <https://habr.com/ru/articles/469667/>.
3. Права доступа к файлам в Linux [Электронный ресурс]. 2023. URL: <https://losst.pro/prava-dostupa-k-fajlam-v-linux>.