

Лабораторная работа № 2.

Дискреционное разграничение прав в Linux. Основные атрибуты

Сунгурова Мариян Мухсиновна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
3.1	Создание нового пользователя	7
4	Выводы	16
	Список литературы	17

Список иллюстраций

3.1	Создание нового пользователя guest	7
3.2	Создание нового пользователя guest	7
3.3	Вход под новым пользователем	8
3.4	Просмотр информации о пользователе	8
3.5	Просмотр информации о пользователе	8
3.6	Просмотр информации о пользователе	9
3.7	Просмотр информации о пользователе	9
3.8	Просмотр информации о пользователе	9
3.9	Просмотр информации о пользователе	10

Список таблиц

3.1	Установленные права и разрешённые действия	11
3.2	Минимальные права для совершения операций	14

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Теоретическое введение

При работе с командой `chmod` важно понимать основные права доступа, которые назначают файлам или каталогам. В Linux используется три основных типа прав доступа[1]:

- Чтение (Read) — обозначается буквой «r». Предоставляет возможность просматривать содержимое файла или каталога.
- Запись (Write) — обозначается буквой «w». Позволяет создавать, изменять и удалять файлы внутри каталога, а также изменять содержимое файла.
- Выполнение (Execute) — обозначается буквой «x». Дает разрешение на выполнение файла или на вход в каталог.

Каждый из указанных выше типов прав доступа может быть назначен трем группам пользователей:

- Владелец (Owner) — пользователь, который является владельцем файла или каталога.
- Группа (Group) — группа пользователей, к которой принадлежит файл или каталог.
- Остальные пользователи (Others) — все остальные пользователи системы.

Комбинация этих базовых прав доступа для каждой из групп пользователей определяет полный набор прав доступа для файла или каталога.

3 Выполнение лабораторной работы

3.1 Создание нового пользователя

В установленной при выполнении предыдущей лабораторной работы ОС создадим учетную запись пользователя guest (рис. fig. 3.1), и установим пароль пользователя guest (рис. fig. 3.2).

```
[mmsungurova@mmsungurova ~]$ sudo useradd guest

Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

    №1) Уважайте частную жизнь других.
    №2) Думайте, прежде что-то вводить.
    №3) С большой властью приходит большая ответственность.

[sudo] пароль для mmsungurova:
[mmsungurova@mmsungurova ~]$ useradd guest
useradd: пользователь «guest» уже существует
[mmsungurova@mmsungurova ~]$
```

Рис. 3.1: Создание нового пользователя guest

```
[root@mmsungurova ~]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@mmsungurova ~]#
```

Рис. 3.2: Создание нового пользователя guest

Войдем в систему от имени пользователя guest. Определим директорию, в которой мы находимся, командой `pwd`. Сравнив её с приглашением командной строки, увидим, что она называется как наш пользователь. Она является домашней директорией. (рис. fig. 3.3)

```
[root@mmsungurova ~]# su - guest
[guest@mmsungurova ~]$ pwd
/home/guest
[guest@mmsungurova ~]$
```

Рис. 3.3: Вход под новым пользователем

Уточним имя нашего пользователя командой `whoami`. (рис. fig. ??)

```
[guest@mmsungurova ~]$ cd
[guest@mmsungurova ~]$ pwd
/home/guest
[guest@mmsungurova ~]$
[guest@mmsungurova ~]$ whoami
guest
[guest@mmsungurova ~]$ id
uid=1001(guest) gid=1001(guest) gpyrnnw=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@mmsungurova ~]$
```

С помощью команды

`id` также увидим имя пользователя и его `id 1001` и группу `guest` с `id 1001`. (рис. fig. ??)
Сравнивая вывод `id` с выводом команды `groups`, можно увидеть, что пользователь входит только в одну группу (в этом случае указывается только ее название). (рис. fig. 3.4)

```
[guest@mmsungurova ~]$ groups
guest
[guest@mmsungurova ~]$
```

Рис. 3.4: Просмотр информации о пользователе

Посмотрим файл `/etc/passwd` командой `cat /etc/passwd` и увидим, что `uid` и `gid` пользователя равен `1001`, что также было видно из предыдущих выводов команд (рис. fig. 3.5).

```
[guest@mmsungurova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@mmsungurova ~]$
```

Рис. 3.5: Просмотр информации о пользователе

Определим существующие в системе директории командой `ls -l /home/` - это `guest` и `mmsungurova`, правами на чтение, запись и изменение директорий владеет только их владелец. (рис. fig. 3.6).


```
[guest@mmsungurova ~]$ ls -l /home/
итого 4
drwx-----.  4 guest      guest      92 сен 11 21:06 guest
drwx-----. 14 mmsungurova mmsungurova 4096 сен 11 21:02 mmsungurova
[guest@mmsungurova ~]$
```

Рис. 3.6: Просмотр информации о пользователе

Также с помощью команды `lsattr` увидим, что для домашней директории не установлены расширенные атрибуты, а для других пользователей мы не можем это посмотреть. (рис. fig. 3.6)

Создадим в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Затем, воспользуемся командами `ls -l` и `lsattr`. (рис. fig. 3.7). Увидим, что для владельца этой директории есть все права, а для группы и остальных доступно только чтение и вход (не доступно внесение изменений), также видно, что никаких расширенных атрибутов не установлено.

```
[guest@mmsungurova ~]$ mkdir dir1
[guest@mmsungurova ~]$ ls -l
итого 0
drwxr-xr-x.  2 guest guest 6 сен 11 21:14 dir1
[guest@mmsungurova ~]$ lsattr
----- ./dir1
[guest@mmsungurova ~]$
```

Рис. 3.7: Просмотр информации о пользователе

Затем снимем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверим выполнение с помощью команды `ls -l`. (рис. fig. 3.8)

```
----- ./dir1
[guest@mmsungurova ~]$ chmod 000 dir1
[guest@mmsungurova ~]$ ls -l
итого 0
d-----.  2 guest guest 6 сен 11 21:14 dir1
[guest@mmsungurova ~]$
```

Рис. 3.8: Просмотр информации о пользователе

Также попытаемся создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Однако, так как мы забрали право на

запись в эту директорию, то получим отказ в создании. А введя команду `ls -l /home/guest/dir1` увидим, что просмотр директории также запрещен (рис. 3.9).

```
[guest@mmsungurova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@mmsungurova ~]$ ls -l /home/
итого 4
drwx-----. 4 guest      guest      92 сен 11 21:06 guest
drwx-----. 14 mmsungurova mmsungurova 4096 сен 11 21:02 mmsungurova
[guest@mmsungurova ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/mmsungurova
----- /home/guest
[guest@mmsungurova ~]$ mkdir dir1
[guest@mmsungurova ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 11 21:14 dir1
[guest@mmsungurova ~]$ lsattr
----- ./dir1
[guest@mmsungurova ~]$ chmod 000 dir1
[guest@mmsungurova ~]$ ls -l
итого 0
d-----.. 2 guest guest 6 сен 11 21:14 dir1
[guest@mmsungurova ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Отказано в доступе
[guest@mmsungurova ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@mmsungurova ~]$
```

Рис. 3.9: Просмотр информации о пользователе

В табл. 3.1 приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Таблица 3.1: Установленные права и разрешённые действия

Права директории	Права файла	Про- Пе- Сме- смотр ре- на Сме- фай- име- ат- на лов в но- ри- зда- ле- За- Чте- ди- ди- ва- бу- ние ние пись ние рек- рек- ние тов фай- фай- в фай- то- то- фай- фай- ла ла файл ла рии рии ла ла							
		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	ва- ние фай- ла	бу- тов фай- ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(000)	(100)	-	-	-	-	-	-	-	-
d(100)	(100)	-	-	-	-	+	-	-	+
d(200)	(100)	-	-	-	-	-	-	-	-
d(300)	(100)	+	+	-	-	+	-	+	+
d(400)	(100)	-	-	-	-	-	+	-	-
d(500)	(100)	-	-	-	-	+	+	-	+
d(600)	(100)	-	-	-	-	-	+	-	-
d(700)	(100)	+	+	-	-	+	+	+	+
d(000)	(200)	-	-	-	-	-	-	-	-
d(100)	(200)	-	-	+	-	+	-	-	+
d(200)	(200)	-	-	-	-	-	-	-	-

							Про- смотр	Пе- ре-	Сме- на	
							Сме- на	фай- лов в	име- но-	ат- ри-
							ди- рек-	ди- рек-	ва- ние	бу- тов
Права директории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	то- рии	то- рии	фай- ла	фай- ла	
d(300)	(200)	+	+	+	-	+	-	+	+	
d(400)	(200)	-	-	-	-	-	+	-	-	
d(500)	(200)	-	-	+	-	+	+	-	+	
d(600)	(200)	-	-	-	-	-	+	-	-	
d(700)	(200)	+	+	+	-	+	+	+	+	
d(000)	(300)	-	-	-	-	-	-	-	-	
d(100)	(300)	-	-	+	-	+	-	-	+	
d(200)	(300)	-	-	-	-	-	-	-	-	
d(300)	(300)	+	+	+	-	+	-	+	+	
d(400)	(300)	-	-	-	-	-	+	-	-	
d(500)	(300)	-	-	+	-	+	+	-	+	
d(600)	(300)	-	-	-	-	-	+	-	-	
d(700)	(300)	+	+	+	-	+	+	+	+	
d(000)	(400)	-	-	-	-	-	-	-	-	
d(100)	(400)	-	-	-	+	+	-	-	+	
d(200)	(400)	-	-	-	-	-	-	-	-	
d(300)	(400)	+	+	-	+	+	-	+	+	
d(400)	(400)	-	-	-	-	-	+	-	-	
d(500)	(400)	-	-	-	+	+	+	-	+	
d(600)	(400)	-	-	-	-	-	+	-	-	
d(700)	(400)	+	+	-	+	+	+	+	+	

Права директории	Права файла	Про- Пе- Сме- смотр ре- на Сме- фай- име- ат- на лов в но- ри- ди- ди- ва- бу- рек- рек- ние тов то- то- фай- фай- рии рии ла ла							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Сме- на ди- рек- то- рии	Сме- на ди- рек- то- рии	Сме- на ди- рек- то- рии
d(000)	(500)	-	-	-	-	-	-	-	-
d(100)	(500)	-	-	-	+	+	-	-	+
d(200)	(500)	-	-	-	-	-	-	-	-
d(300)	(500)	+	+	-	+	+	-	+	+
d(400)	(500)	-	-	-	-	-	+	-	-
d(500)	(500)	-	-	-	+	+	+	-	+
d(600)	(500)	-	-	-	-	-	+	-	-
d(700)	(500)	+	+	-	+	+	+	+	+
d(000)	(600)	-	-	-	-	-	-	-	-
d(100)	(600)	-	-	+	+	+	-	-	+
d(200)	(600)	-	-	-	-	-	-	-	-
d(300)	(600)	+	+	+	+	+	-	+	+
d(400)	(600)	-	-	-	-	-	+	-	-
d(500)	(600)	-	-	+	+	+	+	-	+
d(600)	(600)	-	-	-	-	-	+	-	-
d(700)	(600)	+	+	+	+	+	+	+	+
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(700)	-	-	-	-	-	+	-	-

Права директории	Права файла					Сме-	Про-	Пе-	Сме-
		Со-	Уда-			на	смотр	ре-	на
		зда-	ле-	За-	Чте-	ди-	фай-	име-	ат-
		ние	ние	пись	ние	рек-	лов в	но-	ри-
		фай-	фай-	в	фай-	то-	ди-	ва-	бу-
		ла	ла	файл	ла	рии	рек-	фай-	тов
		ла	ла	файл	ла	рии	рии	ла	фай-
		ла	ла	файл	ла	рии	рии	ла	ла
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(700)	+	+	+	+	+	+	+	+

На основании заполненной выше таблицы определим минимально необходимые права для выполнения операций внутри директории, заполним 3.2

Таблица 3.2: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переиме- нование файла	d(300)	(000)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

4 Выводы

В результате выполнения данной лабораторной работы были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Граннеман С. Linux. Карманный справочник. 2-е изд. Вильямс, 2019. 464 с.