

# **Отчёт по лабораторной работе №2**

**Дискреционное разграничение прав в Linux. Основные атрибуты**

Саргсян Арам Грачьевич

# Содержание

1	Цель работы	5
2	Теоритическое введение	6
3	Выполнение лабораторной работы	8
4	Вывод	13
	Список литературы	14

# Список иллюстраций

3.1	создание пользователя . . . . .	8
3.2	проверка данных . . . . .	8
3.3	изменение прав . . . . .	9

## Список таблиц

3.1	Установленные права и разрешённые действия . . . . .	10
3.2	Минимальные права для совершения операций . . . . .	12

# 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 Теоритическое введение

Настройка прав доступа пользователей в Linux осуществляется с использованием механизма управления правами файлов и каталогов. Основные особенности этой настройки включают:

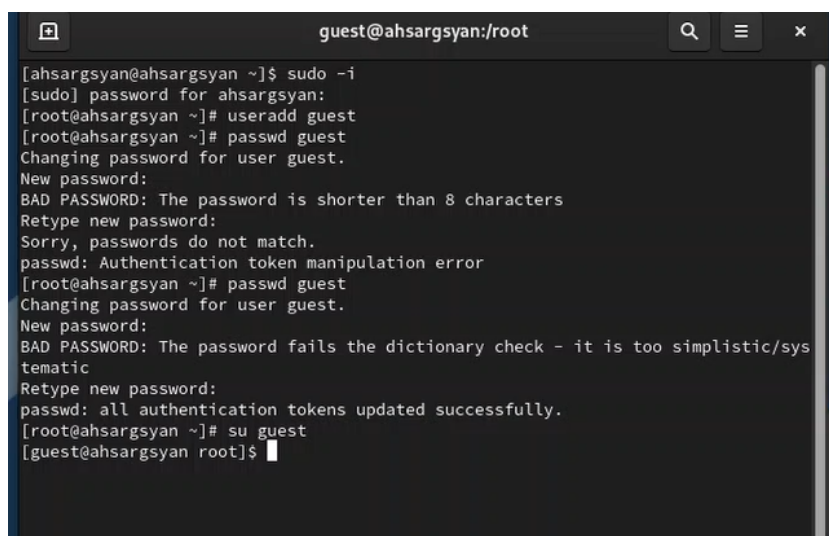
1. Роли пользователей: В Linux существуют разные роли пользователей, такие как обычные пользователи, администраторы (суперпользователи), и другие пользовательские группы. Каждая роль имеет свои права и ограничения.
2. Права доступа: Права доступа к файлам и каталогам определяются для трех основных категорий пользователей: владельцев файла, группы и всех остальных. Эти права включают в себя чтение (r), запись (w) и выполнение (x).
3. Команды `chmod` и `chown`: Для изменения прав доступа и владельцев файлов и каталогов в Linux используются команды `chmod` и `chown`. `chmod` позволяет изменять права доступа, а `chown` - владельцев.
4. Наследование прав: Права доступа могут быть унаследованы от родительских каталогов. Это означает, что если у родительского каталога есть определенные права доступа, то новые файлы и подкаталоги в нем будут иметь те же права по умолчанию.
5. Переменные права доступа: В Linux также существует концепция переменных прав доступа, таких как SUID (Set User ID), SGID (Set Group ID) и sticky bit. Они позволяют изменять поведение файлов и каталогов в отношении прав доступа и выполняемых команд.

6. Управление группами: В Linux пользователи могут быть объединены в группы. Права доступа могут быть назначены как для отдельных пользователей, так и для групп, что позволяет более гибко управлять доступом.
7. Аудит и журналирование: Linux предоставляет средства аудита и журналирования, которые позволяют отслеживать действия пользователей и проверять соответствие прав доступа установленным политикам.

Настройка прав доступа пользователей в Linux является фундаментальным аспектом безопасности и управления файловой системой. Она позволяет определить, кто имеет доступ к каким файлам и какие операции с ними могут быть выполнены, обеспечивая таким образом защиту данных и системы ([1], [2], [3]).

### 3 Выполнение лабораторной работы

1. В установленной ранее ОС создали пользователя guest, задали ему пароль и зашли в систему под данного пользователя (Рис. 3.1)



```
guest@ahsargsyan:/root
[ahsargsyan@ahsargsyan ~]$ sudo -i
[sudo] password for ahsargsyan:
[root@ahsargsyan ~]# useradd guest
[root@ahsargsyan ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@ahsargsyan ~]# passwd guest
Changing password for user guest.
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 ~]# su guest
[guest@ahsargsyan root]$
```

Рис. 3.1: создание пользователя

2. Уточнил имя пользователя, группы, в которые он входит (Рис. 3.2)



```
[root@ahsargsyan guest]# su guest
[guest@ahsargsyan ~]$ 12345678\
> ^C
[guest@ahsargsyan ~]$ ls
[guest@ahsargsyan ~]$ whoami
guest
[guest@ahsargsyan ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@ahsargsyan ~]$ groups
guest
```

Рис. 3.2: проверка данных



3. В установленной ранее ОС создали пользователя guest, задали ему пароль и зашли в систему под данного пользователя (Рис. 3.3)

```
guest:x:1001:1001::/home/guest:/bin/bash
[guest@ahsargsyan ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@ahsargsyan ~]$ ls -l /home
total 4
drwx-----, 17 ahsargsyan ahsargsyan 4096 Sep  7 10:38 ahsargsyan
drwx-----,  6 guest      guest      142 Sep 11 10:59 guest
[guest@ahsargsyan ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/ahsargsyan
----- /home/guest
[guest@ahsargsyan ~]$ mkdir dir1
[guest@ahsargsyan ~]$ ls -l
total 0
drwxr-xr-x, 2 guest guest 6 Sep 11 11:03 dir1
[guest@ahsargsyan ~]$ lsattr
----- ./dir1
[guest@ahsargsyan ~]$ echo "test" > /home/guest/dir1/file1
[guest@ahsargsyan ~]$ rm /home/guest/dir1/file1
[guest@ahsargsyan ~]$ chmod 000 dir1
[guest@ahsargsyan ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@ahsargsyan ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@ahsargsyan ~]$
```

Рис. 3.3: изменение прав

4. Заполнил таблицу (@#tbl:rules) .

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

Таблица 3.1: Установленные права и разрешённые действия

Права директории	Права файла	1	2	3	4	5	6	7	8
d------(000)	------(000)	-	-	-	-	-	-	-	-
d--x------(100)	------(000)	-	-	-	-	+	-	-	+
d-w------(200)	------(000)	-	-	-	-	-	-	-	-
d-wx------(300)	------(000)	+	+	-	-	+	-	+	+
dr------(400)	------(000)	-	-	-	-	-	-	-	-
dr-x------(500)	------(000)	-	-	-	-	+	+	-	+
drw------(600)	------(000)	-	-	-	-	-	-	-	-
drwx------(700)	------(000)	+	+	-	-	+	+	+	+
d------(000)	---x------(100)	-	-	-	-	-	-	-	-
d--x------(100)	---x------(100)	-	-	-	-	+	-	-	+
d-w------(200)	---x------(100)	-	-	-	-	-	-	-	-
d-wx------(300)	---x------(100)	+	+	-	-	+	-	+	+
dr------(400)	---x------(100)	-	-	-	-	-	-	-	-
dr-x------(500)	---x------(100)	-	-	-	-	+	+	-	+
drw------(600)	---x------(100)	-	-	-	-	-	-	-	-
drwx------(700)	---x------(100)	+	+	-	-	+	+	+	+
d------(000)	--w------(200)	-	-	-	-	-	-	-	-
d--x------(100)	--w------(200)	-	-	+	-	+	-	-	+
d-w------(200)	--w------(200)	-	-	-	-	-	-	-	-
d-wx------(300)	--w------(200)	+	+	+	-	+	-	+	+
dr------(400)	--w------(200)	-	-	-	-	-	-	-	-
dr-x------(500)	--w------(200)	-	-	+	-	+	+	-	+
drw------(600)	--w------(200)	-	-	-	-	-	-	-	-
drwx------(700)	--w------(200)	+	+	+	-	+	+	+	+
d------(000)	--wx------(300)	-	-	-	-	-	-	-	-
d--x------(100)	--wx------(300)	-	-	+	-	+	-	-	+

Права директории	Права файла	1	2	3	4	5	6	7	8
d-w------(200)	--wx------(300)	-	-	-	-	-	-	-	-
d-wx------(300)	--wx------(300)	+	+	+	-	+	-	+	+
dr------(400)	--wx------(300)	-	-	-	-	-	-	-	-
dr-x------(500)	--wx------(300)	-	-	+	-	+	+	-	+
drw------(600)	--wx------(300)	-	-	-	-	-	-	-	-
drwx------(700)	--wx------(300)	+	+	+	-	+	+	+	+
d------(000)	-r------(400)	-	-	-	-	-	-	-	-
d--x------(100)	-r------(400)	-	-	-	+	+	-	-	+
d-w------(200)	-r------(400)	-	-	-	-	-	-	-	-
d-wx------(300)	-r------(400)	+	+	-	+	+	-	+	+
dr------(400)	-r------(400)	-	-	-	-	-	-	-	-
dr-x------(500)	-r------(400)	-	-	-	+	+	+	-	+
drw------(600)	-r------(400)	-	-	-	-	-	-	-	-
drwx------(700)	-r------(400)	+	+	-	+	+	+	+	+
d------(000)	-r-x------(500)	-	-	-	-	-	-	-	-
d--x------(100)	-r-x------(500)	-	-	-	+	+	-	-	+
d-w------(200)	-r-x------(500)	-	-	-	-	-	-	-	-
d-wx------(300)	-r-x------(500)	+	+	-	+	+	-	+	+
dr------(400)	-r-x------(500)	-	-	-	-	-	-	-	-
dr-x------(500)	-r-x------(500)	-	-	-	+	+	+	-	+
drw------(600)	-r-x------(500)	-	-	-	-	-	-	-	-
drwx------(700)	-r-x------(500)	+	+	-	+	+	+	+	+
d------(000)	-rw------(600)	-	-	-	-	-	-	-	-
d--x------(100)	-rw------(600)	-	-	+	+	+	-	-	+
d-w------(200)	-rw------(600)	-	-	-	-	-	-	-	-
d-wx------(300)	-rw------(600)	+	+	+	+	+	-	+	+
dr------(400)	-rw------(600)	-	-	-	-	-	-	-	-

Права директории	Права файла	1	2	3	4	5	6	7	8
dr-x----- (500)	-rw----- (600)	-	-	+	+	+	+	-	+
drw----- (600)	-rw----- (600)	-	-	-	-	-	-	-	-
drwx----- (700)	-rw----- (600)	+	+	+	+	+	+	+	+
d----- (000)	-rwx----- (700)	-	-	-	-	-	-	-	-
d--x----- (100)	-rwx----- (700)	-	-	+	+	+	-	-	+
d-w----- (200)	-rwx----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	-rwx----- (700)	+	+	+	+	+	-	+	+
dr----- (400)	-rwx----- (700)	-	-	-	-	-	-	-	-
dr-x----- (500)	-rwx----- (700)	-	-	+	+	+	+	-	+
drw----- (600)	-rwx----- (700)	-	-	-	-	-	-	-	-
drwx----- (700)	-rwx----- (700)	+	+	+	+	+	+	+	+

5. На основании таблицы выше определили минимально необходимые права для выполнения операций внутри директории dir1 и заполнили таблицу 3.2 .

Таблица 3.2: Минимальные права для совершения операций

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

## **4 Вывод**

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.

## Список литературы

1. Vugt S. van. Red Hat RHCSA/RHCE 7 Cert Guide: Red Hat Enterprise Linux 7 (EX200 and EX300). Pearson, 2015.
2. Chiang J.K., Yen E.H.-W., Chen Y.-H. Authentication, Authorization and File Synchronization in Hybrid Cloud: On Case of Google Docs, Hadoop and Linux Local Hosts. IEEE, 2013.
3. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. 2-е изд. БХВ-Петербург, 2010. 656 с.