

Отчет по лабораторной работе 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Шалыгин Георгий Эдуардович

Содержание

1	Цель работы	5
2	Теоретическое введение	6
2.0.1	Изменение владельца	7
2.1	Использование chmod	7
3	Выполнение лабораторной работы	9
4	Выводы	16
	Список литературы	17

Список иллюстраций

3.1	Домашний каталог пользователя guest	9
3.2	Группы доступа пользователя	9
3.3	etc/passwd	9
3.4	Вывод ls -l /home/	10
3.5	Права для новой директории	10
3.6	Изменение прав доступа	11
3.7	Создание файла	11

Список таблиц

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 Linux1.

2 Теоретическое введение

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.

В Linux у каждого файла и каждого каталога есть два владельца: пользователь и группа.

Эти владельцы устанавливаются при создании файла или каталога. Пользователь, который создаёт файл становится владельцем этого файла, а первичная группа, в которую входит этот же пользователь, так же становится владельцем этого файла. Чтобы определить, есть ли у вас как у пользователя права доступа к файлу или каталогу, оболочка проверяет владение ими.

Это происходит в следующем порядке:

1. Оболочка проверяет, являетесь ли вы владельцем файла, к которому вы хотите получить доступ. Если вы являетесь этим владельцем, вы получаете разрешения и оболочка прекращает проверку.

2. Если вы не являетесь владельцем файла, оболочка проверит, являетесь ли вы участником группы, у которой есть разрешения на этот файл. Если вы являетесь участником этой группы, вы получаете доступ к файлу с разрешениями, которые для группы установлены, и оболочка прекратит проверку.
3. Если вы не являетесь ни пользователем, ни владельцем группы, вы получаете права других пользователей (Other).

Чтобы увидеть текущие назначения владельца, вы можете использовать команду **ls -l**. Эта команда показывает пользователя и группу-владельца.

Подробнее в [1].

2.0.1 Изменение владельца

Чтобы применить соответствующие разрешения, первое, что нужно учитывать, это владение. Для этого есть команда **chown**. Синтаксис этой команды несложен для понимания:

```
chown кто что
```

Например, следующая команда меняет владельца каталога `/home/account` на пользователя `linda`:

```
chown linda /home/account
```

2.1 Использование **chmod**

Для управления правами используется команда **chmod**. При использовании **chmod** вы можете устанавливать разрешения для пользователя (user), группы (group) и других (other). Вы можете использовать эту команду в двух режимах: относительный режим и абсолютный режим. В абсолютном режиме три цифры используются для установки основных разрешений.

При настройке разрешений рассчитайте необходимое вам значение. Если вы хотите установить чтение, запись и выполнение для пользователя, чтение и выполнение для группы, а также чтение и выполнение для других в файле /somefile, то вы используете следующую команду **chmod**:

```
chmod 755 /somefile
```

Подробнее в [2].

3 Выполнение лабораторной работы

1. Создадим уч. запись guest и зададим пароль. Войдем в систему под этой уч. записью и проверим домашний каталог (fig. 3.1)

```
[guest@geshalygin ~]$ pwd
/home/guest
[guest@geshalygin ~]$ cd ~
[guest@geshalygin ~]$ pwd
/home/guest
[guest@geshalygin ~]$
```

Рис. 3.1: Домашний каталог пользователя guest

2. Уточним имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Сравним вывод id с выводом команды groups. (fig:002)

Видим, что пользователь входит в группу guest с gid=1001, а uid=1001.

Приглашение командной строки также содержит наименование guest.

```
[guest@geshalygin ~]$ whoami
guest
[guest@geshalygin ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@geshalygin ~]$ groups
guest
[guest@geshalygin ~]$
```

Рис. 3.2: Группы доступа пользователя

3. В файле etc/passwd найдем свою учётную запись (fig. 3.3). gid=1001, а uid=1001.

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

Рис. 3.3: etc/passwd

4. Определим существующие в системе директории командой `ls -l /home/` (fig. 3.4). Видим права 700 для обеих директорий. Сравним с выводом команды `lsattr /home`. Для директории другого пользователя получили ошибку доступа.

```
[guest@geshalygin ~]$ ls -l /home/
total 8
drwx-----. 14 geshalygin geshalygin 4096 Sep 16 17:04 geshalygin
drwx-----. 14 guest      guest      4096 Sep 16 17:23 guest
[guest@geshalygin ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/geshalygin
----- /home/guest
```

Рис. 3.4: Вывод `ls -l /home/`

5. Создадим в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` (fig. 3.5). В данном случае это 755.

```
[guest@geshalygin ~]$ ls -l ~
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 16 17:30 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Music
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Videos
[guest@geshalygin ~]$ lsattr ~
----- /home/guest/Desktop
----- /home/guest/Downloads
----- /home/guest/Templates
----- /home/guest/Public
----- /home/guest/Documents
----- /home/guest/Music
----- /home/guest/Pictures
----- /home/guest/Videos
----- /home/guest/dir1
```

Рис. 3.5: Права для новой директории

6. Снимем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверим с её помощью правильность выполнения команды `ls -l` (fig. 3.6).

```
[guest@geshalygin ~]$ chmod 000 dir1
[guest@geshalygin ~]$ ls -l ~
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 17:23 Desktop
d----- . 2 guest guest 6 Sep 16 17:30 dir1
```

Рис. 3.6: Изменение прав доступа

7. Попробуем создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 (fig. 3.7). Т.к. права были изменены в прошлом пункте, выскакивает ошибка доступа.

```
[guest@geshalygin ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@geshalygin ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
```

Рис. 3.7: Создание файла

8. Поочередно меняя права доступа для директории и файла заполним таблицу:

Права	Смена	Создание	Удаление	Запись	Чтение	Директория	Просмотр	Переименование	Смена атрибутов
директории	файла	файла	файла	файла	файла	директории	файлов в директории	файла	файла
		touch	rm	echo	cat	cd	ls	mv	chmod
0	0	-	-	-	-	-	-	-	-
0	100	-	-	-	-	-	-	-	-
0	200	-	-	-	-	-	-	-	-
0	300	-	-	-	-	-	-	-	-
0	400	-	-	-	-	-	-	-	-
0	500	-	-	-	-	-	-	-	-
0	600	-	-	-	-	-	-	-	-

Пра- ва	Со- зда- ние	Уда- ние	За- пись	Чте- ние	Сме- на	Просмотр	Пере- имено- вание	Смена атрибу- тов
ди- рек- то- рии	Пра- ва фай- ла	зда- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	файлов в директо- рии	Смена атрибу- тов файла
0	700	-	-	-	-	-	-	-
100	0	-	-	-	-	+	-	+
100	100	-	-	-	-	+	-	+
100	200	-	-	+	-	+	-	+
100	300	-	-	+	-	+	-	+
100	400	-	-	+	+	+	-	+
100	500	-	-	+	+	+	-	+
100	600	-	-	+	+	+	-	+
100	700	-	-	+	+	+	-	+
200	0	-	-	-	-	-	-	-
200	100	-	-	-	-	-	-	-
200	200	-	-	-	-	-	-	-
200	300	-	-	-	-	-	-	-
200	400	-	-	-	-	-	-	-
200	500	-	-	-	-	-	-	-
200	600	-	-	-	-	-	-	-
200	700	-	-	-	-	-	-	-
300	0	+	+	-	-	+	-	+
300	100	+	+	-	-	+	-	+
300	200	+	+	+	-	+	-	+
300	300	+	+	+	-	+	-	+
300	400	+	+	+	+	+	-	+
300	500	+	+	+	+	+	-	+

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись в файл	Чте- ние фай- ла	Сме- на	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
300	600	+	+	+	+	-	+	+
300	700	+	+	+	+	-	+	+
400	0	-	-	-	-	+	-	-
400	100	-	-	-	-	+	-	-
400	200	-	-	-	-	+	-	-
400	300	-	-	-	-	+	-	-
400	400	-	-	-	-	+	-	-
400	500	-	-	-	-	+	-	-
400	600	-	-	-	-	+	-	-
400	700	-	-	-	-	+	-	-
500	0	-	-	+	+	+	-	+
500	100	-	-	+	+	+	-	+
500	200	-	+	+	+	+	-	+
500	300	-	+	+	+	+	-	+
500	400	-	+	+	+	+	-	+
500	500	-	+	+	+	+	-	+
500	600	-	+	+	+	+	-	+
500	700	-	+	+	+	+	-	+
600	0	-	-	-	-	+	-	-
600	100	-	-	-	-	+	-	-
600	200	-	-	-	-	+	-	-
600	300	-	-	-	-	+	-	-
600	400	-	-	-	-	+	-	-

Пра- ва	Со- зда- ние	Уда- ние	За- пись	Чте- ние	Сме- на	Просмотр	Пере- имено- вание	Смена
ди- рек- то- рии	Пра- ва фай- ла	фай- ла	фай- ла	в файл	фай- ла	рек- то- рии	файлов в директо- рии	атрибу- тов файла
600	500	-	-	-	-	-	+	-
600	600	-	-	-	-	-	+	-
600	700	-	-	-	-	-	+	-
700	0	+	+	+	-	+	+	+
700	100	+	+	+	-	+	+	+
700	200	+	+	+	-	+	+	+
700	300	+	+	+	-	+	+	+
700	400	+	+	+	+	+	+	+
700	500	+	+	+	+	+	+	+
700	600	+	+	+	+	+	+	+
700	700	+	+	+	+	+	+	+

9. И результаты моделирования (fig. ??)

Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	300	0
Удаление файла	300	0
Чтение файла	100	400
Запись в файл	100	200
Переименование файла	300	0

Операция	Минимальные права на директорию	Минимальные права на файл
Создание поддиректории	300	0
Удаление поддиректории	300	0

4 Выводы

В ходе 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 Linux1.

Список литературы

1. Кетов Д.В. Внутреннее устройство Linux. BHV, 2017. 124 с.
2. Л. М. Ухлинов. Управление доступом в ОС GNU /Linux . ОКБ САПР», Москва, Россия, 2010.