Отчет по лабораторной работе 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Шалыгин Георгий Эдуардович

Содержание

# 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.

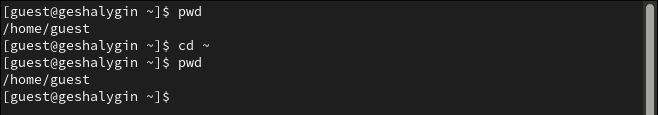
При настройке разрешений рассчитайте необходимое вам значение. Если вы хотите установить чтение, запись и выполнение для пользователя, чтение и выполнение для группы, а также чтение и выполнение для других в файле /somefile, то вы используете следующую команду **chmod**:

chmod 755 /somefile

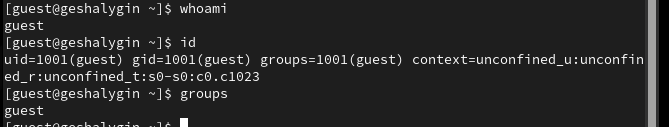
Подробнее в [2].

# 3 Выполнение лабораторной работы

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

* 
* Рис. 1: Домашний каталог пользователя guest

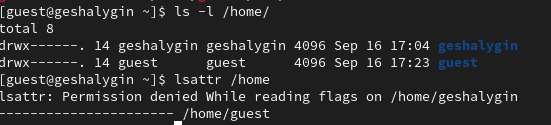
1. Уточним имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Сравним вывод id с выводом команды groups. (fig:002)

* Видим, что пользователь входит в группу guest с gid=1001, а uid=1001.
* Приглашение командной строки также содержит наименование guest.
* 
* Рис. 2: Группы доступа пользователя

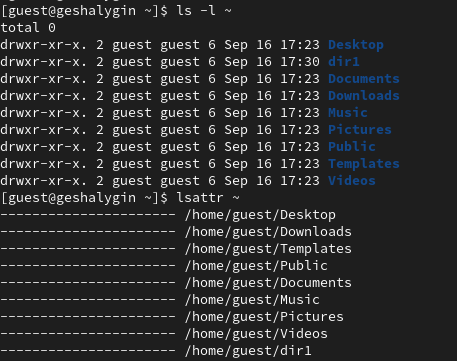
1. В файле etc/passwd найдем свою учётную запись (fig. 3). gid=1001, а uid=1001.

* etc/passwd
* Рис. 3: etc/passwd

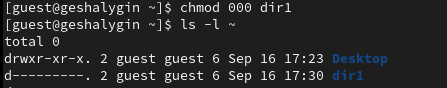
1. Определим существующие в системе директории командой ls -l /home/ (fig. 4). Видим права 700 для обеих директорий. Сравним с выводом команды lsattr /home. Для директории другого пользователя получили ошибку доступа.

* 
* Рис. 4: Вывод ls -l /home/

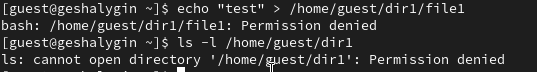
1. Создадим в домашней директории поддиректорию dir1 командой mkdir dir1 Определим командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (fig. 5). В данном случае это 755.

* 
* Рис. 5: Права для новой директории

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

* 
* Рис. 6: Изменение прав доступа

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

* 
* Рис. 7: Создание файла

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

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | touch | rm | echo | cat | cd | ls | mv | chmod |
| 0 | 0 | - | - | - | - | - | - | - | - |
| 0 | 100 | - | - | - | - | - | - | - | - |
| 0 | 200 | - | - | - | - | - | - | - | - |
| 0 | 300 | - | - | - | - | - | - | - | - |
| 0 | 400 | - | - | - | - | - | - | - | - |
| 0 | 500 | - | - | - | - | - | - | - | - |
| 0 | 600 | - | - | - | - | - | - | - | - |
| 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 | + | + | + | + | + | - | + | + |
| 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 | - | - | - | - | - | + | - | - |
| 600 | 500 | - | - | - | - | - | + | - | - |
| 600 | 600 | - | - | - | - | - | + | - | - |
| 600 | 700 | - | - | - | - | - | + | - | - |
| 700 | 0 | + | + | + | - | + | + | + | + |
| 700 | 100 | + | + | + | - | + | + | + | + |
| 700 | 200 | + | + | + | - | + | + | + | + |
| 700 | 300 | + | + | + | - | + | + | + | + |
| 700 | 400 | + | + | + | + | + | + | + | + |
| 700 | 500 | + | + | + | + | + | + | + | + |
| 700 | 600 | + | + | + | + | + | + | + | + |
| 700 | 700 | + | + | + | + | + | + | + | + |

1. И результаты моделирования (fig. **¿fig:008?**)

* 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 |
| 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.