Отчет по лабораторной работе 3

Дискреционное разграничение прав в Linux. Два пользователя

Шалыгин Георгий Эдуардович

Содержание

# 1 Цель работы

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

# 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 guest2. пароль. Добавим пользователя guest2 в группу guest. Определим домашние каталоги для пользователей (fig. 1).

* 
* Рис. 1: Домашние каталоги

1. Уточним имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id (fig:002).

* Видим, что пользователь guest входит в группу guest с id=1001.
* Пользователь guest2 имеет id=1002 и входит так же в группу (кроме 1002) guest с id=1001.
* 
* Рис. 2: Группы доступа пользователей

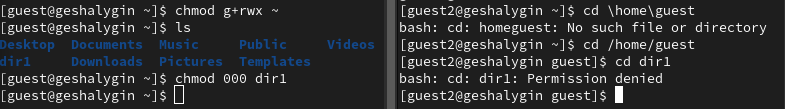
1. В файле etc/passwd найдем ту же информацию о группах (fig. 3).

* etc/passwd
* Рис. 3: etc/passwd

1. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой newgrp guest

* Регистрация guest2
* Рис. 4: Регистрация guest2

1. Заполним таблицу доступа. Ниже guest2 отказано в доступе к директории, доступ к которой изменен guest на 000 (fig. 5).

* 
* Рис. 5: Права для новой директории

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 |
| 0 | 0 | - | - | - | - | - | - |  |  |
| 0 | 10 | - | - | - | - | - | - | - | - |
| 0 | 20 | - | - | - | - | - | - | - | - |
| 0 | 30 | - | - | - | - | - | - | - | - |
| 0 | 40 | - | - | - | - | - | - | - | - |
| 0 | 50 | - | - | - | - | - | - | - | - |
| 0 | 60 | - | - | - | - | - | - | - | - |
| 0 | 70 | - | - | - | - | - | - | - | - |
| 10 | 0 | - | - | - | - | + | - | - | - |
| 10 | 10 | - | - | - | - | + | - | - | - |
| 10 | 20 | - | - | - | - | + | - | - | - |
| 10 | 30 | - | - | - | - | + | - | - | - |
| 10 | 40 | - | - | - | - | + | - | - | - |
| 10 | 50 | - | - | - | - | + | - | - | - |
| 10 | 60 | - | - | - | - | + | - | - | - |
| 10 | 70 | - | - | - | - | + | - | - | - |
| 20 | 0 | - | - | - | - | - | - | - | - |
| 20 | 10 | - | - | - | - | - | - | - | - |
| 20 | 20 | - | - | - | - | - | - | - | - |
| 20 | 30 | - | - | - | - | - | - | - | - |
| 20 | 40 | - | - | - | - | - | - | - | - |
| 20 | 50 | - | - | - | - | - | - | - | - |
| 20 | 60 | - | - | - | - | - | - | - | - |
| 20 | 70 | - | - | - | - | - | - | - | - |
| 30 | 0 | + | + | - | - | + | - | + | + |
| 30 | 10 | + | + | - | - | + | - | + | + |
| 30 | 20 | + | + | + | - | + | - | + | + |
| 30 | 30 | + | + | + | - | + | - | + | + |
| 30 | 40 | + | + | + | + | + | - | + | + |
| 30 | 50 | + | + | + | + | + | - | + | + |
| 30 | 60 | + | + | + | + | + | - | + | + |
| 30 | 70 | + | + | + | + | + | - | + | + |
| 40 | 0 | - | - | - | - | - | + | - | - |
| 40 | 10 | - | - | - | - | - | + | - | - |
| 40 | 20 | - | - | - | - | - | + | - | - |
| 40 | 30 | - | - | - | - | - | + | - | - |
| 40 | 40 | - | - | - | - | - | + | - | - |
| 40 | 50 | - | - | - | - | - | + | - | - |
| 40 | 60 | - | - | - | - | - | + | - | - |
| 40 | 70 | - | - | - | - | - | + | - | - |
| 50 | 0 | - | - | - | + | + | + | - | + |
| 50 | 10 | - | - | - | + | + | + | - | + |
| 50 | 20 | - | - | + | + | + | + | - | + |
| 50 | 30 | - | - | + | + | + | + | - | + |
| 50 | 40 | - | - | + | + | + | + | - | + |
| 50 | 50 | - | - | + | + | + | + | - | + |
| 50 | 60 | - | - | + | + | + | + | - | + |
| 50 | 70 | - | - | + | + | + | + | - | + |
| 60 | 0 | - | - | - | - | - | + | - | - |
| 60 | 10 | - | - | - | - | - | + | - | - |
| 60 | 20 | - | - | - | - | - | + | - | - |
| 60 | 30 | - | - | - | - | - | + | - | - |
| 60 | 40 | - | - | - | - | - | + | - | - |
| 60 | 50 | - | - | - | - | - | + | - | - |
| 60 | 60 | - | - | - | - | - | + | - | - |
| 60 | 70 | - | - | - | - | - | + | - | - |
| 70 | 0 | + | + | - | - | + | + | + | + |
| 70 | 10 | + | + | - | - | + | + | + | + |
| 70 | 20 | + | + | - | - | + | + | + | + |
| 70 | 30 | + | + | - | - | + | + | + | + |
| 70 | 40 | + | + | - | - | + | + | + | + |
| 70 | 50 | + | + | - | - | + | + | + | + |
| 70 | 60 | + | + | - | - | + | + | + | + |
| 70 | 70 | + | + | - | - | + | + | + | + |

1. Минимальные права для совершения операций

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | 030 | 0 |
| Удаление файла | 030 | 0 |
| Чтение файла | 010 | 040 |
| апись в файл | 010 | 020 |
| Переименование файла | 030 | 0 |
| Создание поддиректории | 030 | 0 |
| Удаление поддиректории | 030 | 0 |

# 4 Выводы

В ходе работы были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей.

# 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.