Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Парфенова Елизавета Евгеньевна

Содержание

# 1 Цель работы

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

# 2 Теоретическое введение

Права доступа в операционной системе Linux представляют собой ключевой элемент безопасности, определяющий, какой доступ имеют пользователи и программы к файлам и каталогам. Чтобы посмотреть права пользователя в Linux, необходимо воспользоваться следующей командой [1]:

*ls - l*

Изменить права доступа можно с помощью команды *chmod*. Основной синтаксис команды *chmod* выглядит следующим образом [2]:

*chmod [опции]*

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

* r — read (чтение) — право просматривать содержимое файла;
* w — write (запись) — право изменять содержимое файла;
* x — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

* owner (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но владельцем можно сделать и кого-то другого.
* group (группа) — пользователи с общими заданными правами.
* others (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами [3].

Существуют два основных способа записи прав доступа: символьный и числовой формат. Символьный формат использует читаемые буквы и символы для представления прав доступа, в то время как числовой формат использует числа в восьмеричной системе [1].

В табл. 1 приведено краткое описание стандартных каталогов Unix.

Таблица 1: Формат записи прав доступа системы GNU Linux

| Права доступа | Символьный формат | Числовой формат |
| --- | --- | --- |
| Чтение | r | 4 |
| Запись | w | 2 |
| Выполнение | x | 1 |
| Нет доступа | - | 0 |

# 3 Выполнение лабораторной работы

В установленной нами операциоонной системе в прошлой лабораторной работе мы уже создали пользователя guest. Таким же образом, с помощью команд *useradd guest2* и *passwd guest* создаем нового пользователя и задаем пароль учетной записи, предварительно выполнив вход с правами администратора (рис. 1).

![Создание пользователя guest2](data:application/octet-stream;base64,)

Рис. 1: Создание пользователя guest2

Далее добавляем пользовтаеля guest2 в группу guest командой *gpasswd -a guest2 guest* (рис. 2).

![Добавление guest2 в группу guest](data:application/octet-stream;base64,)

Рис. 2: Добавление guest2 в группу guest

Откроем две консоли и осуществим вход для двух разных пользователей на них, использую права администратора. Командой *pwd* определим директори, в которой находимся и проверим, все ли получилось. (рис. 3) (рис. 4).

![Команда pwd в первой консоли](data:application/octet-stream;base64,)

Рис. 3: Команда pwd в первой консоли

![Команда pwd во второй консоли](data:application/octet-stream;base64,)

Рис. 4: Команда pwd во второй консоли

Как видим, в двух разных консолях мы вошли в разные учетные записи, и вывод команды *pwd* совпадает с приглашение командой строки каждой консоли.

Уточним имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Для этого последовательно введем команды *id*, *id -Gn*, *id -G*, *groups guest* или *groups guest2* в каждую из консолей и сравним результаты. Для пользователя guest (рис. 5) видим id пользователя и id группы, равные 1001, а также то, что он принадлежит одной группе guest, при этом информация при выводе всех команд совпадает. Для пользователя guest2 (рис. 6) информация немного иная: данный пользователь имеет id 1002 и принадлежит уже 2 группам: guest2 с id 1002 и guest с id 1001, то есть к группе 1 пользователя. Информация при выводе каждой команды также совпадает.

![Вывод команд для guest](data:application/octet-stream;base64,)

Рис. 5: Вывод команд для guest

![Вывод команд для guest2](data:application/octet-stream;base64,)

Рис. 6: Вывод команд для guest2

Сравним полученную выше информацию с содержимым файла /etc/group, просмотрев его командой *cat /etc/group*. Нас интересуют последние две строки (рис. 7) : на них видно, что в группе пользователя guest с id 1001 состоит и пользователь guest2, а в группе второго пользователя с id 1002 только он сам. Инормация совпала с предыдущей.

![Содержимое файла /etc/group](data:application/octet-stream;base64,)

Рис. 7: Содержимое файла /etc/group

Выполним регистрацию пользователя guest2 в группе guest от имени пользователя guest2 командой *newgrp guest*. (рис. 8)

![Регистрация пользователя guest2 в группе guest](data:application/octet-stream;base64,)

Рис. 8: Регистрация пользователя guest2 в группе guest

От имени пользователя guest разрешим все действия пользователям группы, изменив права директории /home/guest командой *chmod g+rwx /home/guest*. (рис. 9)

![Выдача всех прав участникам группы](data:application/octet-stream;base64,)

Рис. 9: Выдача всех прав участникам группы

Далее От имени пользователя guest снимем с директории */home/guest/dir1*, которая была создана на прошлой лабораторной, все атрибуты командой *chmod 000 dir1* и проверим правильность выполнения командой *ls -l*(рис. 10)

![Снятие прав с директории dir1](data:application/octet-stream;base64,)

Рис. 10: Снятие прав с директории dir1

Далее, меняя атрибуты у директории dir1 и файла file1 от имени пользова- теля guest и делая проверку от пользователя guest2, опытным путем заполним таблицу 2

Таблица 2: Установленные права и разрешённые действия для групп

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файл | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d--------- (000) | ---------- (000) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ---------- (000) | - | - | - | - | + | - | - | - |
| d----w---- (020) | ---------- (000) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ---------- (000) | + | + | - | - | + | - | + | - |
| d---r----- (040) | ---------- (000) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ---------- (000) | - | - | - | - | + | + | - | - |
| d---rw---- (060) | ---------- (000) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ---------- (000) | + | + | - | - | + | + | + | - |
| d--------- (000) | ------x--- (010) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ------x--- (010) | - | - | - | - | + | - | - | - |
| d----w---- (020) | ------x--- (010) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ------x--- (010) | + | + | - | - | + | - | + | - |
| d---r----- (040) | ------x--- (010) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ------x--- (010) | - | - | - | - | + | + | - | - |
| d---rw---- (060) | ------x--- (010) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ------x--- (010) | + | + | - | - | + | + | + | - |
| d--------- (000) | -----w---- (020) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | -----w---- (020) | - | - | + | - | + | - | - | - |
| d----w---- (020) | -----w---- (020) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | -----w---- (020) | + | + | + | - | + | - | + | - |
| d---r----- (040) | -----w---- (020) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | -----w---- (020) | - | - | + | - | + | + | - | - |
| d---rw---- (060) | -----w---- (020) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | -----w---- (020) | + | + | + | - | + | + | + | - |
| d--------- (000) | -----wx--- (030) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | -----wx--- (030) | - | - | + | - | + | - | - | - |
| d----w---- (020) | -----wx--- (030) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | -----wx--- (030) | + | + | + | - | + | - | + | - |
| d---r----- (040) | -----wx--- (030) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | -----wx--- (030) | - | - | + | - | + | + | - | - |
| d---rw---- (060) | -----wx--- (030) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | -----wx--- (030) | + | + | + | - | + | + | + | - |
| d--------- (000) | ----r----- (040) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----r----- (040) | - | - | - | + | + | - | - | - |
| d----w---- (020) | ----r----- (040) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----r----- (040) | + | + | - | + | + | - | + | - |
| d---r----- (040) | ----r----- (040) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----r----- (040) | - | - | - | + | + | + | - | - |
| d---rw---- (060) | ----r----- (040) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----r----- (040) | + | + | - | + | + | + | + | - |
| d--------- (000) | ----r-x--- (050) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----r-x--- (050) | - | - | - | + | + | - | - | - |
| d----w---- (020) | ----r-x--- (050) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----r-x--- (050) | + | + | - | + | + | - | + | - |
| d---r----- (040) | ----r-x--- (050) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----r-x--- (050) | - | - | - | + | + | + | - | - |
| d---rw---- (060) | ----r-x--- (050) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----r-x--- (050) | + | + | - | + | + | + | + | - |
| d--------- (000) | ----rw---- (060) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----rw---- (060) | - | - | + | + | + | - | - | - |
| d----w---- (020) | ----rw---- (060) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----rw---- (060) | + | + | + | + | + | - | + | - |
| d---r----- (040) | ----rw---- (060) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----rw---- (060) | - | - | + | + | + | + | - | - |
| d---rw---- (060) | ----rw---- (060) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----rw---- (060) | + | + | + | + | + | + | + | - |
| d--------- (000) | ----rwx--- (070) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----rwx--- (070) | - | - | + | + | + | - | - | - |
| d----w---- (020) | ----rwx--- (070) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----rwx--- (070) | + | + | + | + | + | - | + | - |
| d---r----- (040) | ----rwx--- (070) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----rwx--- (070) | - | - | + | + | + | + | - | - |
| d---rw---- (060) | ----rwx--- (070) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----rwx--- (070) | + | + | + | + | + | + | + | - |

Сравнивая таблицы 2.2 из прошлой лабораторной работы и 3.2 можно сказать, что таблицы одинаковы во всех столбцах кроме кроме столбца “Смена атрибутов файла”, так как это доступно только владельцу, если только вход не осуществлен с правами суперпользователя.

На основе анализа уже заполненной таблицы заполним следующую таблицу, которая указывает на миниммальные права для файла и директории для того или иного действия от имени пользователей, входящих в группу. Получившаяся таблица 3

Таблица 3: Минимальные права для совершения операций от имени пользователей входящих в группу

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | d----wx--- (030) | ---------- (000) |
| Удаление файла | d----wx--- (030) | ---------- (000 |
| Чтение файла | d-----x--- (010) | ----r----- (040) |
| Запись в файл | d-----x--- (010) | -----w---- (020) |
| Переименование файла | d----wx--- (030) | ---------- (000) |
| Создание поддиректории | d----wx--- (030) | ---------- (000) |
| Удаление поддиректории | d----wx--- (030) | ---------- (000) |

# 4 Выводы

Мы получили практические навыки работы в консоли с атрибутами файлов для групп пользователей

# Список литературы

1. Как дать права пользователю Linux: инструкция [Электронный ресурс]. ООО «ТАЙМВЭБ.КЛАУД»., 2024. URL: <https://timeweb.cloud/tutorials/linux/kak-dat-prava-polzovatelyu-linux>.

2. Что делает команда chmod и как ее использовать в Linux [Электронный ресурс]. ОО «Селектел», 2024. URL: <https://selectel.ru/blog/tutorials/what-the-chmod-command-does-and-how-to-use-it-in-linux/>.

3. Права доступа в Linux [Электронный ресурс]. СodeСhick.io, 2024. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.