Отчёт по лабораторной работе №3

Дискреционное разграничение прав в Linux. Два пользователя

Дарья Эдуардовна Ибатулина

Содержание

# 1 Цель работы

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

# 2 Задание

1. Создание нового пользователя;
2. Добавление его в группу;
3. Уточнение имени пользователя, проверка того, в какие группы он входит;
4. Регистрация нового пользователя в группе;
5. Изменение прав директории;
6. Заполнение таблиц: “Установленные права и разрешённые действия для групп” и “Минимальные права для совершения операций от имени пользователей входящих в группу”.

# 3 Теоретическое введение

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы.

Группы пользователей Linux кроме стандартных root и users, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен.

* daemon - от имени этой группы и пользователя daemon запускаютcя сервисы, которым необходима возможность записи файлов на диск.
* sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
* sync - позволяет выполнять команду /bin/sync
* games - разрешает играм записывать свои файлы настроек и историю в определенную папку
* man - позволяет добавлять страницы в директорию /var/cache/man
* lp - позволяет использовать устройства параллельных портов
* mail - позволяет записывать данные в почтовые ящики /var/mail/
* proxy - используется прокси серверами, нет доступа записи файлов на диск www-data - с этой группой запускается веб-сервер, она дает доступ на запись /var/www, где находятся файлы веб-документов
* list - позволяет просматривать сообщения в /var/mail
* nogroup - используется для процессов, которые не могут создавать файлов на жестком диске, а только читать, обычно применяется вместе с пользователем nobody.
* adm - позволяет читать логи из директории /var/log
* tty - все устройства /dev/vca разрешают доступ на чтение и запись пользователям из этой группы
* disk - открывает доступ к жестким дискам /dev/sd\* /dev/hd\*, можно сказать, что это аналог рут доступа.
* dialout - полный доступ к серийному порту
* cdrom - доступ к CD-ROM
* wheel - позволяет запускать утилиту sudo для повышения привилегий
* audio - управление аудиодрайвером
* src - полный доступ к исходникам в каталоге /usr/src/
* shadow - разрешает чтение файла /etc/shadow
* utmp - разрешает запись в файлы /var/log/utmp /var/log/wtmp
* video - позволяет работать с видеодрайвером
* plugdev - позволяет монтировать внешние устройства USB, CD и т д
* staff - разрешает запись в папку /usr/local

# 4 Выполнение лабораторной работы

Первые 2 пункта лабораторной работы я уже выполнила в предыдущей работе. Нужно было создать пользователя *guest* и задать для него пароль.

1. Создаём второго нового пользователя с именем *guest2* с помощью команд useradd guest2 и passwd guest2(рис. [[1](#fig:001)]).

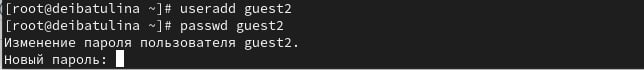


Figure 1: Создание нового пользователя и задание пароля для него

1. Добавляем пользователя *guest2* в группу *guest*, используя команду gpasswd -a guest2 guest (рис. [[2](#fig:002)]).

Figure 2: Добавление пользователя в группу

Figure 2: Добавление пользователя в группу

1. Осуществите вход в систему от двух пользователей на двух разных консолях: *guest* на первой консоли и *guest2* на второй консоли с помощью команды su \*имя пользователя\* (рис. [[3](#fig:003)]).

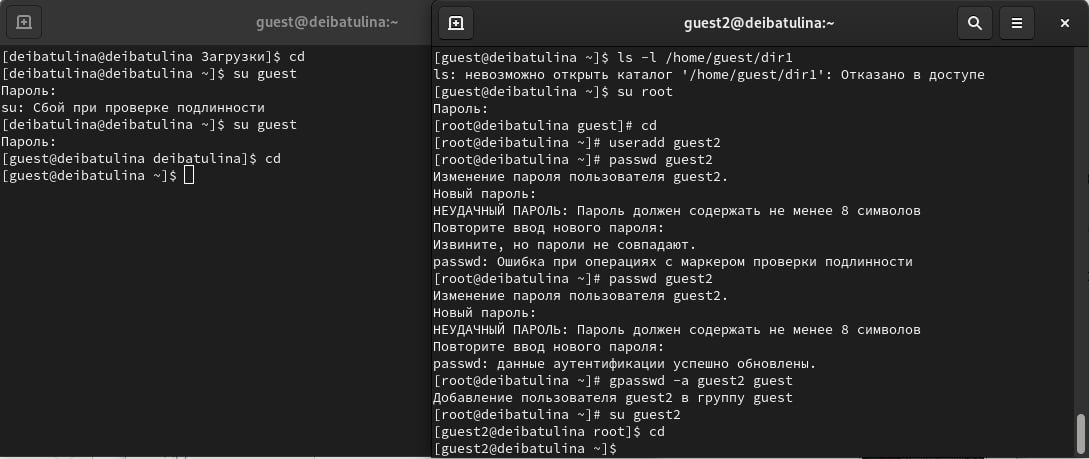


Figure 3: Вход в систему от двух пользователей на разных консолях

1. Далее, выведем рабочую директорию командой pwd для обоих пользователей: *guest* (рис. [[4](#fig:004)]) и *guest2* (рис. [[5](#fig:005)]):

Figure 4: Вывод рабочей директории для пользователя guest

Figure 4: Вывод рабочей директории для пользователя guest

Figure 5: Вывод рабочей директории для пользователя guest2

Figure 5: Вывод рабочей директории для пользователя guest2

1. Уточним имя обоих наших пользователей командой whoami, группу каждого, кто входит в неё и к каким группам принадлежит он сам командой id: *guest* (рис. [[6](#fig:006)]) и *guest2* (рис. [[7](#fig:007)]).

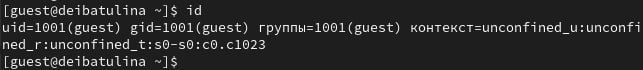


Figure 6: Уточнение групп пользователя guest командой id

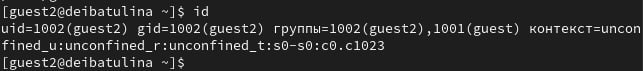


Figure 7: Уточнение групп пользователя guest2 командой id

1. Определим командами groups guest и groups guest2, в какие группы входят пользователи: *guest* (рис. [[8](#fig:008)]) и *guest2* (рис. [[9](#fig:009)]). Сравним вывод команды groups с выводом команд id -Gn и id -G для пользователей *guest* (рис. [[10](#fig:010)]) и *guest2* (рис. [[11](#fig:011)]).

Примечательно: \* id -Gn - выведет названия групп, которым принадлежит пользователь \* id -G - выведет только код групп, которым принадлежит пользователь

Figure 8: Уточнение групп пользователя guest командой groups

Figure 8: Уточнение групп пользователя guest командой groups

Figure 9: Уточнение групп пользователя guest2 командой groups

Figure 9: Уточнение групп пользователя guest2 командой groups



Figure 10: Вывод команд id -Gn и id -G для пользователя guest



Figure 11: Вывод команд id -Gn и id -G для пользователя guest2

1. Просмотрим содержимое файла */etc/group* cat /etc/group (рис. [[12](#fig:012)]).

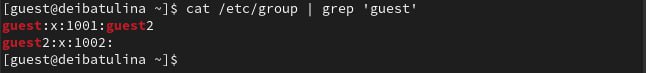


Figure 12: Просмотр файла /etc/group

1. От имени пользователя *guest2* выполним регистрацию пользователя *guest2* в группе *guest* командой newgrp guest (рис. [[13](#fig:013)]).

Figure 13: Регистрация пользователя guest2 в группе guest

Figure 13: Регистрация пользователя guest2 в группе guest

1. От имени пользователя *guest* изменим права директории */home/guest*, разрешив все действия для пользователей группы с помощью команды chmod g+rwx /home/guest (рис. [[14](#fig:014)]).

Figure 14: Разрешение всех действий для пользователей группы guest директории dir1

Figure 14: Разрешение всех действий для пользователей группы guest директории dir1

1. От имени пользователя *guest* снимем с директории */home/guest/dir1* все атрибуты командой chmod 000 dirl (рис. [[15](#fig:015)]).

Figure 15: Запрет всех действий для пользователей группы guest директории dir1

Figure 15: Запрет всех действий для пользователей группы guest директории dir1

## 4.1 Заполнение таблицы 3.1

Меняя атрибуты у директории *dir1* и файла *file1* от имени пользователя *guest* и делая проверку от пользователя *guest2*, заполняю таблицу [[1](#tbl:std-dir)], определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, в таблице стоит знак “+”, если не разрешена, знак “-”.

Table 1: 3.1 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) | + | + | + | + | + | + | + | + |

## 4.2 Заполнение таблицы 3.2

На основе таблицы 3.1 заполняю следующую таблицу [[2](#tbl:std-dir1)].

Table 2: 3.2 Минимальные права для совершения операций от имени пользователей, входящих в группу

| Операция | Права на директорию | 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) |

# 5 Выводы

Я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

# Список литературы