

Дискреционное разграничение прав в Linux. Основные атрибуты

Джафер Идрисов¹

7 марта, 2025, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

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

Процесс выполнения лабораторной работы

Определяем UID и группу двух пользователей

```
didrisov@didrisov:~$ su guest
Пароль:
guest@didrisov:/home/didrisov$
guest@didrisov:/home/didrisov$ su
Пароль:
root@didrisov:/home/didrisov# useradd guest2
root@didrisov:/home/didrisov# passwd guest2
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: пароль успешно обновлен
root@didrisov:/home/didrisov# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
root@didrisov:/home/didrisov#
root@didrisov:/home/didrisov# su guest
guest@didrisov:/home/didrisov$ pwd
/home/didrisov
guest@didrisov:/home/didrisov$ cd
/home/guest
guest@didrisov:~$ pwd
/home/guest
guest@didrisov:~$ id -G
1001
guest@didrisov:~$ id -Gn
guest
guest@didrisov:~$ groups guest
guest : guest
guest@didrisov:~$ groups guest2
guest2 : guest2 guest
guest@didrisov:~$
```

```
didrisov@didrisov:~$ su guest2
Пароль:
guest2@didrisov:/home/didrisov$ pwd
/home/didrisov
guest2@didrisov:/home/didrisov$ cd
/home/guest2
guest2@didrisov:~$ id -G
1003 1001
guest2@didrisov:~$ id -Gn
guest2 guest
guest2@didrisov:~$ groups guest
guest : guest
guest2@didrisov:~$ groups guest2
guest2 : guest2 guest
guest2@didrisov:~$
```

Рис. 1: Информация о пользователях

Файл с данными о пользователях

```
ircd.x:172.172:ircd.x:/usr/sbin/nologin
geoclue:x:997:996:User for geoclue:/var/lib/geoclue:/sbin/nologin
sssd:x:996:995:User for sssd:/run/sss:/sbin/nologin
libstoragemgmt:x:994:994:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-coredump:x:993:993:systemd Core Dumper:/usr/sbin/nologin
wsdd:x:992:992:Web Services Dynamic Discovery host daemon:/sbin/nologin
clevis:x:991:991:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:990:990:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
pipewire:x:989:989:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
flatpak:x:988:988:Flatpak system helper:/usr/sbin/nologin
gdm:x:42:42:GNOME Display Manager:/var/lib/gdm:/usr/sbin/nologin
gnome-initial-setup:x:987:986:/run/gnome-initial-setup:/sbin/nologin
dnsmasq:x:986:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
design:x:985:984:Group for the design signing daemon:/run/design:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:984:983:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:tcpdump:/usr/sbin/nologin
gnome-remote-desktop:x:981:981:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
guest:x:1001:1001:./home/guest:/bin/bash
didrisov:x:1002:1002:./home/didrisov:/bin/bash
guest2:x:1003:1003:./home/guest2:/bin/bash
guest2@didrisov:~$ newgrp guest
guest2@didrisov:~$
```

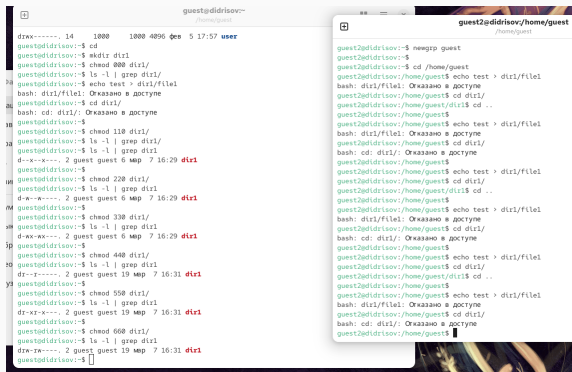
Рис. 2: Содержимое файла /etc/group

Атрибуты директории

```
guest@didrisov:~$ cd
guest@didrisov:~$ chmod g+rxw /home/guest
guest@didrisov:~$ ls -l /home
итого 8
drwx-----. 14 didrisov didrisov 4096 мар 7 16:21 didrisov
drwxrwx---. 3 guest guest 78 фев 5 19:27 guest
drwx-----. 3 guest2 guest2 78 мар 7 16:23 guest2
drwx-----. 14 1000 1000 4096 фев 5 17:57 user
guest@didrisov:~$ cd
guest@didrisov:~$ mkdir dir1
guest@didrisov:~$ chmod 000 dir1/
guest@didrisov:~$ ls -l | grep dir1/
guest@didrisov:~$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
guest@didrisov:~$ cd dir1/
bash: cd: dir1/: Отказано в доступе
guest@didrisov:~$ █
```

Рис. 3: Снятие атрибутов с директории

Заполнение таблицы



The image displays two terminal windows. The left window, titled 'guest@didrisov:~', shows a series of commands and their outputs. It starts with 'drwx-----, 14 1000 1000 4096 Dec 5 17:57 user', followed by 'guest@didrisov:~\$ cd /home/guest'. Then, it runs 'mkdir dir1' and 'chmod 000 dir1'. A 'ls -l | grep dir1' command shows a directory listing. A 'bash: dir1/file1: Оказано в доctype' error is shown. The user then runs 'cd dir1/' and 'echo test > dir1/file1'. This process is repeated for multiple directories (dir1, dir2, etc.), with the output of 'ls -l | grep dir1' showing the growing list of directories and files. The right window, titled 'guest2@didrisov:/home/guest', shows a similar process starting with 'newgrp guest' and 'cd /home/guest'. It then runs 'echo test > dir1/file1' and 'cd dir1/' to create files in the subdirectories. Both windows show the progression of creating a directory structure and populating it with files.

```
guest@didrisov:~  
drwx-----, 14 1000 1000 4096 Dec 5 17:57 user  
guest@didrisov:~$ cd /home/guest  
guest@didrisov:~$ mkdir dir1  
guest@didrisov:~$ chmod 000 dir1/  
guest@didrisov:~$ ls -l | grep dir1  
bash: dir1/file1: Оказано в доctype  
guest@didrisov:~$ cd dir1/  
bash: cd: dir1/: Оказано в доctype  
guest@didrisov:~$  
guest@didrisov:~$ chmod 110 dir1/  
guest@didrisov:~$ ls -l | grep dir1/  
guest@didrisov:~$ ls -l | grep dir1  
d-x-x-x---, 2 guest guest 6 Мб 7 16:29 dir1  
guest@didrisov:~$  
guest@didrisov:~$ chmod 220 dir1/  
guest@didrisov:~$ ls -l | grep dir1  
d-x-x-x---, 2 guest guest 6 Мб 7 16:29 dir1  
guest@didrisov:~$  
guest@didrisov:~$ chmod 330 dir1/  
guest@didrisov:~$ ls -l | grep dir1  
d-x-x-x---, 2 guest guest 6 Мб 7 16:29 dir1  
guest@didrisov:~$  
guest@didrisov:~$ chmod 440 dir1/  
guest@didrisov:~$ ls -l | grep dir1  
dr--r-----, 2 guest guest 19 Мб 7 16:31 dir1  
guest@didrisov:~$  
guest@didrisov:~$ chmod 550 dir1/  
guest@didrisov:~$ ls -l | grep dir1  
dr-xr-x---, 2 guest guest 19 Мб 7 16:31 dir1  
guest@didrisov:~$  
guest@didrisov:~$ chmod 660 dir1/  
guest@didrisov:~$ ls -l | grep dir1  
drw-r-----, 2 guest guest 19 Мб 7 16:31 dir1  
guest@didrisov:~$  
guest@didrisov:~$  
guest2@didrisov:/home/guest  
guest2@didrisov:~$ newgrp guest  
guest2@didrisov:~$  
guest2@didrisov:~$ cd /home/guest  
guest2@didrisov:/home/guest$ echo test > dir1/file1  
bash: dir1/file1: Оказано в доctype  
guest2@didrisov:/home/guest$ cd dir1/  
guest2@didrisov:/home/guest/dir1$ cd ..  
guest2@didrisov:/home/guest$  
guest2@didrisov:/home/guest$ echo test > dir1/file1  
bash: dir1/file1: Оказано в доctype  
guest2@didrisov:/home/guest$ cd dir1/  
bash: cd: dir1/: Оказано в доctype  
guest2@didrisov:/home/guest$  
guest2@didrisov:/home/guest$ echo test > dir1/file1  
bash: dir1/file1: Оказано в доctype  
guest2@didrisov:/home/guest$ cd dir1/  
guest2@didrisov:/home/guest/dir1$ cd ..  
guest2@didrisov:/home/guest$  
guest2@didrisov:/home/guest$ echo test > dir1/file1  
bash: dir1/file1: Оказано в доctype  
guest2@didrisov:/home/guest$ cd dir1/  
bash: cd: dir1/: Оказано в доctype  
guest2@didrisov:/home/guest$  
guest2@didrisov:/home/guest$ echo test > dir1/file1  
bash: dir1/file1: Оказано в доctype  
guest2@didrisov:/home/guest$ cd dir1/  
bash: cd: dir1/: Оказано в доctype  
guest2@didrisov:/home/guest$  
guest2@didrisov:/home/guest$ echo test > dir1/file1  
bash: dir1/file1: Оказано в доctype  
guest2@didrisov:/home/guest$ cd dir1/  
bash: cd: dir1/: Оказано в доctype  
guest2@didrisov:/home/guest$
```

Рис. 4: Заполнение таблицы

Права и разрешённые действия

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)	----- (040)
Запись в файл	d----x--- (010)	----- (020)
Переименование файла	d---wx--- (030)	----- (000)
Создание поддиректории	d---wx--- (030)	----- (000)
Удаление поддиректории	d---wx--- (030)	----- (000)

Рис. 5: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения работы, мы смогли приобрести практические навыки работы в консоли с атрибутами файлов для групп пользователей.