

Дискреционное разграничение прав в Linux. Основные атрибуты

Николай Мартынов¹

16 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

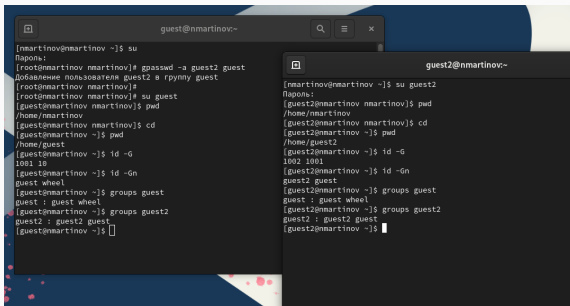
Цели и задачи работы

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



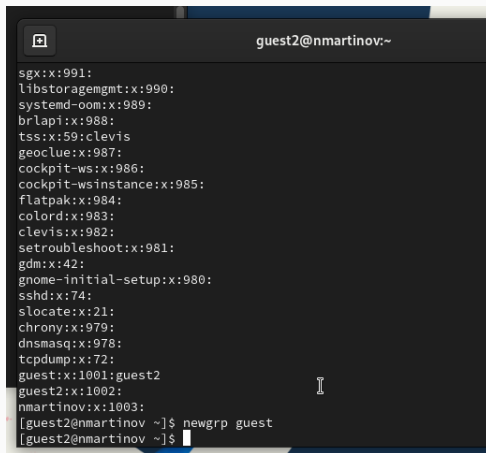
The image shows two terminal windows side-by-side. The left window is titled 'guest@nmartinov:~' and shows the process of creating a user named 'guest' using 'passwd', adding a password, and then switching to the user. It also shows the user's home directory, ID, and group information. The right window is titled 'guest2@nmartinov:~' and shows the process of switching to a user named 'guest2', displaying its home directory, ID, and group information.

```
[nmartinov@nmartinov ~]$ su
Пароль:
[root@nmartinov nmartinov]# passwd -a guest2 guest
Добавление пароля для guest2 с рпмны guest
[root@nmartinov nmartinov]# su guest
[guest@nmartinov nmartinov]$ pwd
/home/nmartinov
[guest@nmartinov nmartinov]$ cd
[guest@nmartinov ~]$ pwd
/home/guest
[guest@nmartinov ~]$ id -G
1001 10
[guest@nmartinov ~]$ id -Gn
guest wheel
[guest@nmartinov ~]$ groups guest
guest : guest wheel
[guest@nmartinov ~]$ groups guest2
guest2 : guest2 guest
[guest@nmartinov ~]$
```

```
[nmartinov@nmartinov ~]$ su guest2
Пароль:
[guest2@nmartinov nmartinov]$ pwd
/home/nmartinov
[guest2@nmartinov nmartinov]$ cd
[guest2@nmartinov ~]$ pwd
/home/guest2
[guest2@nmartinov ~]$ id -G
1002 1001
[guest2@nmartinov ~]$ id -Gn
guest2 guest
[guest2@nmartinov ~]$ groups guest
guest : guest wheel
[guest2@nmartinov ~]$ groups guest2
guest2 : guest2 guest
[guest2@nmartinov ~]$
```

Figure 1: Информация о пользователях

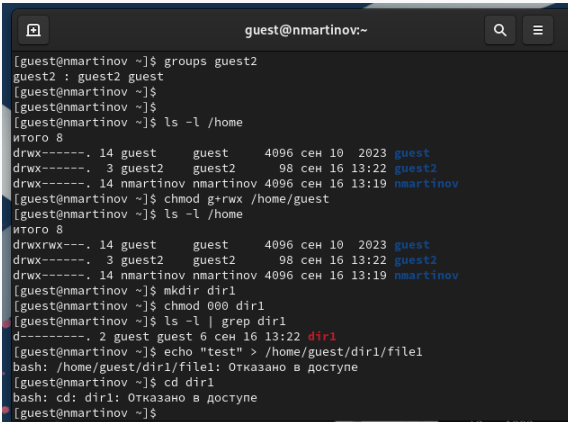
Файл с данными о пользователях

A terminal window titled 'guest2@nmartinov:~' displays the contents of the /etc/group file. The output lists system users and groups with their IDs and shells. At the bottom, the 'newgrp' command is used to switch to the 'guest' group.

```
sgx:x:991:  
libstoragemgmt:x:990:  
systemd-oom:x:989:  
brlapi:x:988:  
tss:x:59:clevis  
geoclue:x:987:  
cockpit-ws:x:986:  
cockpit-wsinstance:x:985:  
flatpak:x:984:  
colord:x:983:  
clevis:x:982:  
setroubleshoot:x:981:  
gdm:x:42:  
gnome-initial-setup:x:980:  
sshd:x:74:  
slocate:x:21:  
chrony:x:979:  
dnsmasq:x:978:  
tcpdump:x:72:  
guest:x:1001:guest  
guest2:x:1002:  
nmartinov:x:1003:  
[guest2@nmartinov ~]$ newgrp guest  
[guest2@nmartinov ~]$
```

Figure 2: Содержимое файла /etc/group

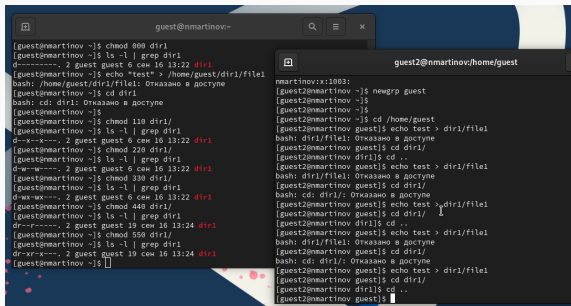
Атрибуты директории

A terminal window titled 'guest@nmartinov:~' with search and menu icons. It shows a series of commands and their outputs. The user first checks the groups of 'guest2', then lists the contents of '/home' with long options. They then change permissions of '/home/guest' to 'g+rx'. After another listing, they create a directory 'dir1' and set its permissions to '000'. Finally, they list files containing 'dir1', create a file inside it, and attempt to change the directory, which is denied.

```
guest@nmartinov:~  
[guest@nmartinov ~]$ groups guest2  
guest2 : guest2 guest  
[guest@nmartinov ~]$  
[guest@nmartinov ~]$  
[guest@nmartinov ~]$ ls -l /home  
итого 8  
drwx-----, 14 guest      guest      4096 сен 10  2023 guest  
drwx-----,  3 guest2     guest2     98 сен 16 13:22 guest2  
drwx-----, 14 nmartinov  nmartinov 4096 сен 16 13:19 nmartinov  
[guest@nmartinov ~]$ chmod g+rx /home/guest  
[guest@nmartinov ~]$ ls -l /home  
итого 8  
drwxrwx---, 14 guest      guest      4096 сен 10  2023 guest  
drwx-----,  3 guest2     guest2     98 сен 16 13:22 guest2  
drwx-----, 14 nmartinov  nmartinov 4096 сен 16 13:19 nmartinov  
[guest@nmartinov ~]$ mkdir dir1  
[guest@nmartinov ~]$ chmod 000 dir1  
[guest@nmartinov ~]$ ls -l | grep dir1  
d-----,  2 guest guest 6 сен 16 13:22 dir1  
[guest@nmartinov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@nmartinov ~]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@nmartinov ~]$
```

Figure 3: Снятие атрибутов с директории

Заполнение таблицы



```
guest@nmartinov:~$ chmod 800 dir1
[guest@nmartinov ~]$ ls -l | grep dir1
d-----, 2 guest guest 6 сен 16 13:22 dir1
[guest@nmartinov ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@nmartinov ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@nmartinov ~]$
[guest@nmartinov ~]$ chmod 110 dir1/
[guest@nmartinov ~]$ ls -l | grep dir1
d-x--x---, 2 guest guest 6 сен 16 13:22 dir1
[guest@nmartinov ~]$ chmod 220 dir1/
[guest@nmartinov ~]$ ls -l | grep dir1
d-w-r-----, 2 guest guest 6 сен 16 13:22 dir1
[guest@nmartinov ~]$ chmod 330 dir1/
[guest@nmartinov ~]$ ls -l | grep dir1
d-wx-wx---, 2 guest guest 6 сен 16 13:22 dir1
[guest@nmartinov ~]$ chmod 440 dir1/
[guest@nmartinov ~]$ ls -l | grep dir1
dr--r-----, 2 guest guest 10 сен 16 13:24 dir1
[guest@nmartinov ~]$ chmod 550 dir1/
[guest@nmartinov ~]$ ls -l | grep dir1
dr-xr-x---, 2 guest guest 19 сен 16 13:24 dir1
[guest@nmartinov ~]$

nmartinov:x:1003:
[guest2@nmartinov ~]$ newgrp guest
[guest2@nmartinov ~]$
[guest2@nmartinov ~]$ cd /home/guest
[guest2@nmartinov guest]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@nmartinov guest]$ cd dir1/
[guest2@nmartinov dir1]$ cd ..
[guest2@nmartinov guest]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@nmartinov guest]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest2@nmartinov guest]$ echo test > dir1/file1
[guest2@nmartinov dir1]$ cd ..
[guest2@nmartinov guest]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@nmartinov guest]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest2@nmartinov guest]$ echo test > dir1/file1
[guest2@nmartinov dir1]$ cd ..
[guest2@nmartinov guest]$
```

Figure 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)	----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)

Figure 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.