

Дискреционное разграничение прав в Linux. Основные атрибуты

Никита Надежда¹

12 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

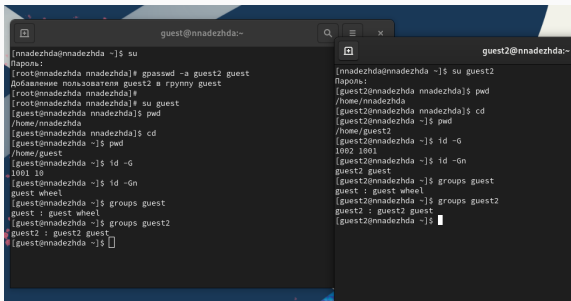
Цели и задачи работы

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

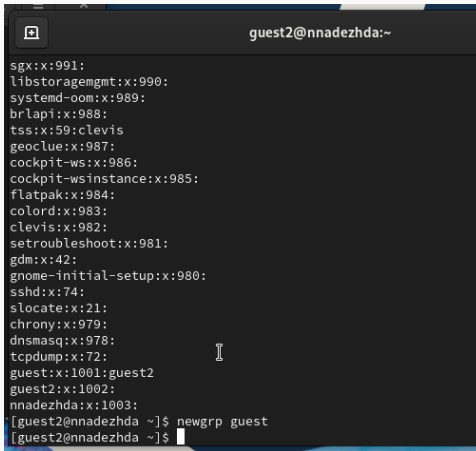


The image shows two terminal windows side-by-side. The left window, titled 'guest@nnadezhda:-', shows the process of creating a user named 'guest' using 'gpsswd -a guest2 guest', adding a password, and then switching to the 'guest' user. The right window, titled 'guest2@nnadezhda:-', shows the user 'guest2' logging in, changing to their home directory, and running 'id -G' and 'groups guest' to verify their UID and group membership.

```
guest@nnadezhda:~$ su
[nnadezhda@nnadezhda ~]$ gpsswd -a guest2 guest
Добавление пользователя guest2 в rpymy guest
[nnadezhda@nnadezhda ~]$ su guest
[guest@nnadezhda ~]$ pwd
/home/nnadezhda
[guest@nnadezhda ~]$ cd
[guest@nnadezhda ~]$ pwd
/home/guest
[guest@nnadezhda ~]$ id -G
1001 10
[guest@nnadezhda ~]$ id -Gn
guest wheel
[guest@nnadezhda ~]$ groups guest
guest : guest wheel
[nnadezhda@nnadezhda ~]$ su guest2
[guest2@nnadezhda ~]$ pwd
/home/nnadezhda
[guest2@nnadezhda ~]$ cd
[guest2@nnadezhda ~]$ pwd
/home/guest2
[guest2@nnadezhda ~]$ id -G
1002 1001
[guest2@nnadezhda ~]$ id -Gn
guest2 guest
[guest2@nnadezhda ~]$ groups guest
guest2 : guest2 guest
[guest2@nnadezhda ~]$
```

Figure 1: Информация о пользователях

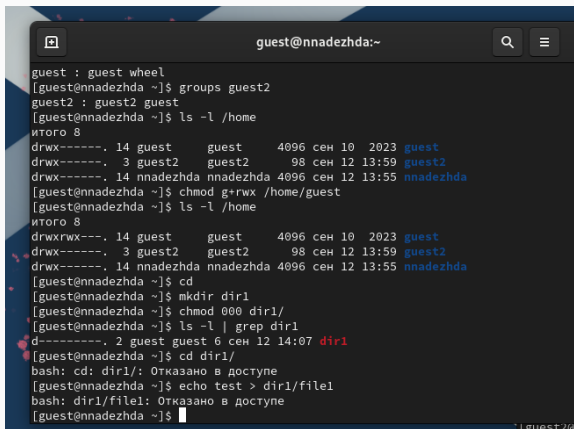
Файл с данными о пользователях

A terminal window with a dark background and light text. The title bar at the top reads "guest2@nnadezhda:~". The terminal displays the output of a command, showing a list of system and user groups in the format "groupname:x:gid:". The groups listed are: sgx, libstoragemgmt, systemd-oom, brlapi, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, sshd, slocate, chrony, dnsmasq, tcpdump, guest, guest2, nnadezhda, and a new group named "guest" created at the bottom. The prompt changes from a root shell to a regular shell after the "newgrp" command.

```
guest2@nnadezhda:~  
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:  
nnadezhda:x:1003:  
[guest2@nnadezhda ~]$ newgrp guest  
[guest2@nnadezhda ~]$
```

Figure 2: Содержимое файла /etc/group

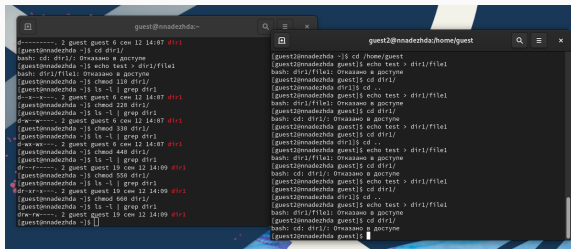
Атрибуты директории

A terminal window titled 'guest@nnadezhda:~' with search and menu icons. It shows a series of commands and their outputs. The user sets 'guest' as the wheel group, then 'guest2' as the group for 'guest'. They list the contents of /home, showing files owned by 'guest' and 'nnadezhda'. Then, they change permissions of /home/guest to 'g+rx'. They list /home again. Then they change directory to /home/guest, create a subdirectory 'dir1', and change its permissions to '000'. Finally, they list 'dir1' and see a directory entry owned by 'guest' with permissions 'd-----'. They attempt to change directory to 'dir1' but are denied access. They then create a file 'file1' in 'dir1' and are also denied access. The prompt returns to the root of the directory.

```
guest : guest wheel
[guest@nnadezhda ~]$ groups guest2
guest2 : guest2 guest
[guest@nnadezhda ~]$ ls -l /home
иторо 8
drwx-----, 14 guest      guest      4096 сен 10  2023 guest
drwx-----, 3 guest2     guest2     98 сен 12 13:59 guest2
drwx-----, 14 nnadezhda nnadezhda 4096 сен 12 13:55 nnadezhda
[guest@nnadezhda ~]$ chmod g+rx /home/guest
[guest@nnadezhda ~]$ ls -l /home
иторо 8
drwxrwx---, 14 guest      guest      4096 сен 10  2023 guest
drwx-----, 3 guest2     guest2     98 сен 12 13:59 guest2
drwx-----, 14 nnadezhda nnadezhda 4096 сен 12 13:55 nnadezhda
[guest@nnadezhda ~]$ cd
[guest@nnadezhda ~]$ mkdir dir1
[guest@nnadezhda ~]$ chmod 000 dir1/
[guest@nnadezhda ~]$ ls -l | grep dir1
d-----, 2 guest guest 6 сен 12 14:07 dir1
[guest@nnadezhda ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@nnadezhda ~]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@nnadezhda ~]$
```

Figure 3: Снятие атрибутов с директории

Заполнение таблицы



The image shows two terminal windows. The left window, titled 'guest@nnadezhda:~', displays the output of a recursive directory listing command. The output shows a tree structure of directories and files, with permissions, owner, group, size, and date for each entry. The right window, titled 'guest2@nnadezhda:/home/guest', shows the same command being executed from a different directory, resulting in a similar output structure.

```
guest@nnadezhda:~  
d----- 2 guest guest 6 cew 12 14:07 dir1/  
[guest@nnadezhda ~]$ cd dir1/  
bash: cd: dir1/: Ошибка: не существует  
[guest@nnadezhda ~]$ echo test > dir1/file1  
bash: dir1/file1: Ошибка: не существует  
[guest@nnadezhda ~]$ chmod 110 dir1/  
[guest@nnadezhda ~]$ ls -l | grep dir1  
d-x-x-x----- 2 guest guest 6 cew 12 14:07 dir1/  
[guest@nnadezhda ~]$ chmod 220 dir1/  
[guest@nnadezhda ~]$ ls -l | grep dir1  
d-x-x-x----- 2 guest guest 6 cew 12 14:07 dir1/  
[guest@nnadezhda ~]$ chmod 330 dir1/  
[guest@nnadezhda ~]$ ls -l | grep dir1  
d-x-x-x----- 2 guest guest 6 cew 12 14:07 dir1/  
[guest@nnadezhda ~]$ chmod 440 dir1/  
[guest@nnadezhda ~]$ ls -l | grep dir1  
dr--r----- 2 guest guest 19 cew 12 14:09 dir1  
[guest@nnadezhda ~]$ chmod 550 dir1/  
[guest@nnadezhda ~]$ ls -l | grep dir1  
dr-xr-x----- 2 guest guest 19 cew 12 14:09 dir1  
[guest@nnadezhda ~]$ chmod 660 dir1/  
[guest@nnadezhda ~]$ ls -l | grep dir1  
drw-rw----- 2 guest guest 19 cew 12 14:09 dir1  
[guest@nnadezhda ~]$
```

```
guest2@nnadezhda:/home/guest  
[guest2@nnadezhda ~]$ cd /home/guest  
[guest2@nnadezhda ~]$ echo test > dir1/file1  
bash: dir1/file1: Ошибка: не существует  
[guest2@nnadezhda ~]$ cd dir1/  
[guest2@nnadezhda dir1]$ cd ..  
[guest2@nnadezhda ~]$ echo test > dir1/file1  
bash: dir1/file1: Ошибка: не существует  
[guest2@nnadezhda ~]$ cd dir1/  
[guest2@nnadezhda dir1]$ cd ..  
[guest2@nnadezhda ~]$ echo test > dir1/file1  
bash: dir1/file1: Ошибка: не существует  
[guest2@nnadezhda ~]$ cd dir1/  
[guest2@nnadezhda dir1]$ cd ..  
[guest2@nnadezhda ~]$ echo test > dir1/file1  
bash: dir1/file1: Ошибка: не существует  
[guest2@nnadezhda ~]$ cd dir1/  
[guest2@nnadezhda dir1]$ cd ..  
[guest2@nnadezhda ~]$ echo test > dir1/file1  
bash: dir1/file1: Ошибка: не существует  
[guest2@nnadezhda ~]$ cd dir1/  
[guest2@nnadezhda dir1]$ cd ..  
[guest2@nnadezhda ~]$
```

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.