

Дискреционное разграничение прав в Linux. Основные атрибуты

Конева Анастасия Михайловна НБИбд-02-18¹

30 сентября, 2021, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

1. Создать нового пользователя “guest”
2. Создать новому пользователю пароль
3. Скопировать образ виртуальной машины в папку, созданную на предыдущем шаге.
4. Определить те или иные минимально необходимые права для выполнения операций внутри директории

Процесс выполнения лабораторной работы

Создание пользователя

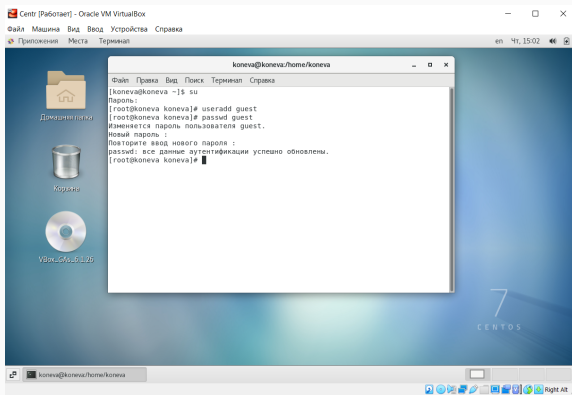
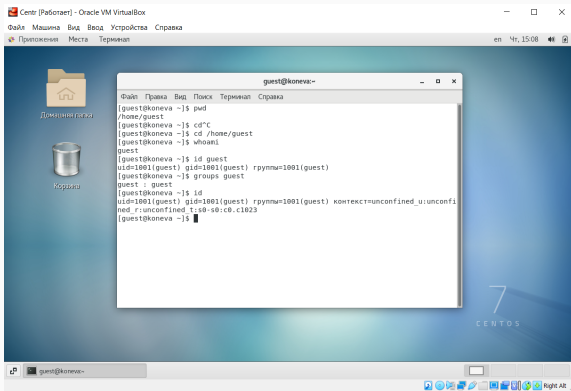


Figure 1: Создание нового пользователя guest

Информация о пользователе

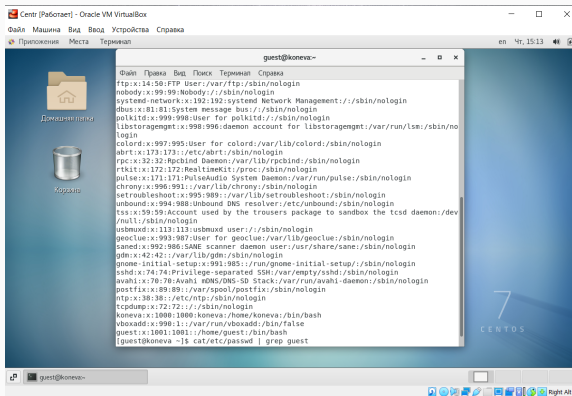


The screenshot shows a CentOS 7 desktop environment within an Oracle VM VirtualBox window. The desktop has a blue background with a large number '7' and the word 'CENTOS'. There are two icons on the left: 'Домашняя папка' (Home folder) and 'Корзина' (Trash). A terminal window titled 'guest@koneva:~' is open in the center, displaying the following commands and their outputs:

```
guest@koneva ~]$ pwd
/home/guest
guest@koneva ~]$ cd /C
guest@koneva ~]$ cd /home/guest
guest@koneva ~]$ whoami
guest
guest@koneva ~]$ id guest
uid=1001(guest) gid=1001(guest) rпymмы=1001(guest)
guest@koneva ~]$ groups guest
guest : guest
guest@koneva ~]$ id
uid=1001(guest) gid=1001(guest) rпymмы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
guest@koneva ~]$
```

Figure 2: Информация о пользователе guest

Файл с данными о пользователях



The screenshot shows a CentOS 7 desktop environment. A terminal window is open, displaying the contents of the `/etc/passwd` file. The desktop background is blue with a large number '7' and the word 'CENTOS'. There are icons for 'Домашняя папка' (Home folder) and 'Корзина' (Trash). The terminal window title is 'guest@koneva:~'. The file content is as follows:

```
File Edit View Search Terminal Help
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:999:998>User for polkitd:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995>User for colord:/var/lib/colord:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
chrony:x:996:991:/var/lib/chrony:/sbin/nologin
setroubleshoot:x:995:989:/var/lib/setroubleshoot:/sbin/nologin
unbound:x:994:988:Unbound DNS resolver:/etc/unbound:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
usbnuxd:x:113:113:usbnuxd user:/sbin/nologin
geoclue:x:993:987>User for geoclue:/var/lib/geoclue:/sbin/nologin
sane:x:992:986:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:991:985:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/empty/ssh:/sbin/nologin
avahi:x:78:78:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
koneva:x:1000:1000:koneva:/home/koneva:/bin/bash
vboxadd:x:998:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@koneva ~]$ cat/etc/passwd | grep guest
```

Figure 3: Содержимое файла `/etc/passwd`

Доступ к домашним директориям

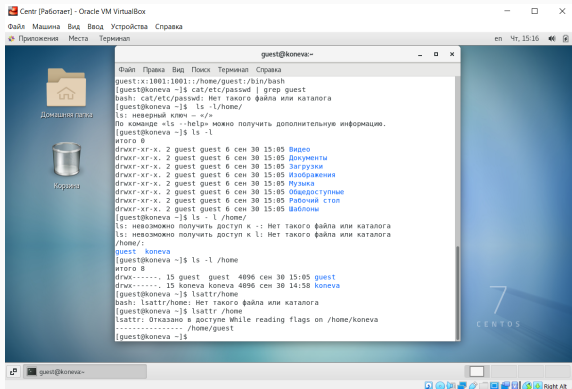


Figure 4: Расширенные атрибуты

Атрибуты директории

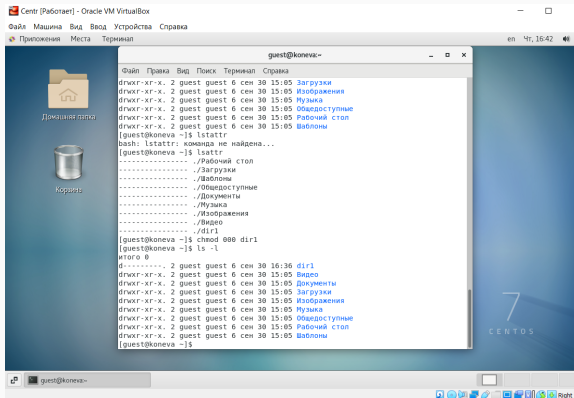


Figure 5: Снятие атрибутов с директории

Права и разрешённые действия

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла.	d-wx----- (300)	0
Удаление файла	d-wx----- (300)	0
Чтение файла	d--x----- (100)	r----- (400)
Запись в файл	d--x----- (100)	-w----- (200)
Переименование файла	d-wx----- (300)	0
Создание поддиректории	d-wx----- (300)	0
Удаление поддиректории	d-wx----- (300)	0

Figure 6: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.