

Дискреционное разграничение прав в Linux. Основные атрибуты

Гаглов Олег Мелорович НПИбд-01-20¹

16 сентября, 2022, 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.

Процесс выполнения лабораторной работы

Определяем UID и группу

```
guest  
[guest@omgagloev ~]$ id guest  
uid=1001(guest) gid=1001(guest) groups=1001(guest)  
[guest@omgagloev ~]$ groups  
guest
```

Рис. 1: Информация о пользователе guest

Файл с данными о пользователях

```
ipm:x:0:0:root:/root:/bin/bash
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/nologin
daemon:x:2:2:daemon:/sbin:/bin/nologin
adm:x:3:3:adm:/var/ads:/bin/nologin
lpx:x:4:7:lp:/var/spool/lpd:/bin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:6:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/bin/nologin
operator:x:11:0:operator:/root:/bin/nologin
games:x:12:100:games:/usr/games:/bin/nologin
ftp:x:14:50:FTP User:/var/ftp:/bin/nologin
nobody:x:65534:65534:Kernel Overflow User:/bin/nologin
systemd-coredump:x:999:999:systemd core dumpers:/bin/nologin
dbus:x:81:81:system message bus:/bin/nologin
polkitd:x:998:998:User for polkitd:/bin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/bin/nologin
cvs:x:172:172:RealTimeKit:/proc:/bin/nologin
sssd:x:997:993:User for sssd:/bin/nologin
pipewire:x:996:992:Pipewire System Daemon:/var/run/pipewire:/bin/nologin
libstoragemgmt:x:998:998:daemon account for libstoragemgmt:/usr/bin/nologin
systemd-nx:x:989:989:systemd Userspace OOM Killer:/usr/bin/nologin
tsix:x:59:59:Account used for TPM access/dev/null:/bin/nologin
goocloud:x:988:987:User for goocloud:/var/lib/goocloud:/bin/nologin
cockpit-ws:x:987:986:User for cockpit web service/none/none:/bin/nologin
cockpit-wsInstance:x:986:985:User for cockpit-ws instances/none/none:/bin/nologin
Flatpak:x:985:984:User for Flatpak system helper:/bin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/bin/nologin
clevis:x:983:982:clevis Decryption Framework unprivileged user:/var/cache/levis:/usr/bin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/bin/nologin
gdm:x:42:42:/var/lib/gdm:/bin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/bin/nologin
gnome-initial-setup:x:988:979:1:/run/gnome-initial-setup:/bin/nologin
sblm:x:74:74:Privilege-separated SBL user/share/empty.sblm:/bin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/bin/nologin
dnsmasq:x:978:977:dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/bin/nologin
tcdump:x:72:72:1:/bin/nologin
omniqos:x:1000:1000:omniqos:/home/omniqos:/bin/bash
vboxadd:x:977:1:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:1:/home/guest:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

Рис. 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
guest.X:1001.1001.:/home/guest:/bin/bash
[guest@omgagloev ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Sep 16 14:11 guest
drwx-----. 14 omgagloev omgagloev 4096 Sep 16 13:59 omgagloev
[guest@omgagloev ~]$
```

Рис. 3: Расширенные атрибуты

Атрибуты директории

```
[guest@omgagloev ~]$ mkdir dir1
[guest@omgagloev ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 16 14:19 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Music
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Videos
[guest@omgagloev ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@omgagloev ~]$
```

Рис. 4: Снятие атрибутов с директории

Права и разрешённые действия

```
[guest@omgagloev ~]$ chmod 400 dir1
[guest@omgagloev ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Desktop
dr----- 2 guest guest 19 Sep 16 14:44 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Music
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Videos
```

Рис. 5: Минимальные права для совершения операций

```
[guest@omgagloev ~]$ ls dir1
ls: cannot access 'dir1/file1': Permission denied
file1
```

Рис. 6: Проверка прав

Выведем содержимое файла

```
[guest@omgagloev ~]$ cat dir1/file1  
cat: dir1/file1: Permission denied  
[guest@omgagloev ~]$
```

Рис. 7: Cat

```
[guest@omgagloev ~]$ chmod 100 dir1  
[guest@omgagloev ~]$ ls -l  
total 0  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Desktop  
d--x----- 2 guest guest 19 Sep 16 14:49 dir1  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Documents  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Downloads  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Music  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Pictures  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Public  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Templates  
drwxr-xr-x. 2 guest guest 6 Sep 16 14:09 Videos  
[guest@omgagloev ~]$ cd dir1  
[guest@omgagloev dir1]$ ls  
ls: cannot open directory '.': Permission denied  
[guest@omgagloev dir1]$ chmod 400 file1  
[guest@omgagloev dir1]$ cat file1  
test  
[guest@omgagloev dir1]$
```

Запишем данные в файл

```
test
[guest@omgagloev dir1]$ echo "test"> /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@omgagloev dir1]$
```

Рис. 9: Запись в файл 1

```
test
[guest@omgagloev dir1]$ echo "test"> /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@omgagloev dir1]$ chmod 200 file1
[guest@omgagloev dir1]$ echo "test"> /home/guest/dir1/file1
[guest@omgagloev dir1]$ cat file1
cat: file1: Permission denied
```

Рис. 10: Запись в файл 2

Выводы по проделанной работе

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