

Лабораторная работа №3

Настройка прав доступа

Комягин А.Н.


21 сентября 2024

Российский университет дружбы народов, Москва, Россия

Получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

Выполнение лабораторной работы

Управление базовыми разрешениями



```
root@ankomyagin:~  
[alice@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# mkdir -p /data/main /data/third  
[root@ankomyagin ~]# ls -Al /data  
total 0  
drwxr-xr-x. 2 root root 6 Sep 13 22:19 main  
drwxr-xr-x. 2 root root 6 Sep 13 22:19 third
```

```
drwxr-xr-x. 2 root root 6 Sep 13 22:19 main
[root@ankomyagin ~]# chgrp main /data/main
[root@ankomyagin ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Sep 13 22:19 main
drwxr-xr-x. 2 root root 6 Sep 13 22:19 third
[root@ankomyagin ~]# chgrp third /data/third
[root@ankomyagin ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Sep 13 22:19 main
drwxr-xr-x. 2 root third 6 Sep 13 22:19 third
```

```
drwxrwx---. 2 root main 6 Sep 13 22:19 main
[root@ankomyagin ~]# chmod 770 /data/main
[root@ankomyagin ~]# chmod 770 /data/third
[root@ankomyagin ~]# ls -l /data/
total 0
drwxrwx---. 2 root main 6 Sep 13 22:19 main
drwxrwx---. 2 root third 6 Sep 13 22:19 third
```

попытка редактирования main бобом

```
[ankomyagin@ankomyagin ~]$ su - bob
Password:
su: Authentication failure
[ankomyagin@ankomyagin ~]$ su - bob
Password:
[bob@ankomyagin ~]$ cd /data/main
[bob@ankomyagin main]$ touch emptyfile
[bob@ankomyagin main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 13 22:23 emptyfile
```


Попытка редактирования third бобом

```
[bob@ankomyagin main]$ cd ..  
[bob@ankomyagin data]$ cd  
main/  third/  
[bob@ankomyagin data]$ cd third/  
-bash: cd: third/: Permission denied
```

Управление специальными разрешениями

```
[ankomyagin@ankomyagin ~]$ su alice
Password:
[alice@ankomyagin ankomyagin]$ cd /data/main/
[alice@ankomyagin main]$ touch alice1
[alice@ankomyagin main]$ touch alice2
[alice@ankomyagin main]$
```

удаление файлов элис с учетки боба

```
[bob@ankomyagin data]$ ls
main  third
[bob@ankomyagin data]$ cd main/
[bob@ankomyagin main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 13 22:25 alicel
-rw-r--r--. 1 alice alice 0 Sep 13 22:25 alicel2
-rw-r--r--. 1 bob   bob   0 Sep 13 22:23 emptyfile
[bob@ankomyagin main]$ rm -f alice*
[bob@ankomyagin main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 13 22:23 emptyfile
[bob@ankomyagin main]$
```

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы

```
[root@ankomyagin ~]# chmod g+s,o+t /data/main  
[root@ankomyagin ~]#
```

```
[alice@ankomyagin main]$ touch alice3
[alice@ankomyagin main]$ touch alice4
[alice@ankomyagin main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 13 22:27 alice3
-rw-r--r--. 1 alice main 0 Sep 13 22:27 alice4
-rw-r--r--. 1 bob    bob    0 Sep 13 22:26 bob1
-rw-r--r--. 1 bob    bob    0 Sep 13 22:26 bob2
-rw-r--r--. 1 bob    bob    0 Sep 13 22:23 emptyfile
[alice@ankomyagin main]$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@ankomyagin main]$
```

Управление расширенными разрешениями с использованием списков ACL

работа с разрешениями

```
[root@ankomyagin ~]# su -
[root@ankomyagin ~]# setfacl -m g:third:rx /data/main
[root@ankomyagin ~]# setfacl -m g:main:rx /data/third
[root@ankomyagin ~]# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other::---
```

I

```
[root@ankomyagin ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
group::rwx
group:main:r-x
mask::rwx
other::---
```

```
[root@ankomyagin ~]#
```



```
[root@ankomyagin ~]# touch /data/main/newfile1
[root@ankomyagin ~]# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rw-
group::r--
other::r--

[root@ankomyagin ~]#
```

```
[root@ankomyagin ~]# touch /data/third/newfile1
[root@ankomyagin ~]# getfacl /data/third/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile1
# owner: root
# group: root
user::rw-
group::r--
other::r--

[root@ankomyagin ~]#
```

```
[root@ankomyagin ~]# touch /data/third/newfile2
[root@ankomyagin ~]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::rwx                               #effective:rw-
group:main:rwx                           #effective:rw-
mask::rw-
other::---
```

проверка полномочий пользователя группы third

```
[bob@ankomyagin main]$ su carol
Password:
[carol@ankomyagin main]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? yes
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@ankomyagin main]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@ankomyagin main]$ echo "Hello, world" >> /data/main/newfile1
bash: /data/main/newfile1: Permission denied
[carol@ankomyagin main]$ echo "Hello, world" >> /data/main/newfile2
[carol@ankomyagin main]$
```

Контрольные вопросы

1. Как следует использовать команду `chown`, чтобы установить владельца группы для файла?

Чтобы установить владельца и группу для файла, нужно использовать команду `chown` следующим образом:

`chown :groupname filename`

2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю?

Для этого можно использовать команду `find`:

`find /path/to/search -user username`

3. Как применить разрешения на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп, не устанавливая никаких прав для других?

Используем команду `chmod`:

```
chmod 770 /data/*
```


4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?

chmod +x filename

5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога?

`chmod g+s /path/to/directory`

6. Необходимо, чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они являются. С помощью какой команды можно это сделать?

`chmod g+s,o+t /путь`

7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?

```
setfacl -m g:groupname:r /path/to/directory/*
```

8. Что нужно сделать для гарантии того, что члены группы получают разрешения на чтение для всех файлов в текущем каталоге и во всех его подкаталогах, а также для всех файлов, которые будут созданы в этом каталоге в будущем?

Использовать команду `setfacl` с флагом `-R` (рекурсивно)

`setfacl -R -m g:groupname:rX /path/to/directory`

9. Какое значение `umask` нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы?

`umask 007`

10. Какая команда гарантирует, что никто не сможет удалить файл myfile случайно?

chattr +i myfile

Вывод

В ходе выполнения лабораторной работы я получил навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.