

Настройка прав доступа

Лабораторная работа № 3

Глобин Никита Анатольевич

20 09 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Информация

```
..... { .columns align=center } :: { .column width="70%" }
```

- Глобин Никита Анатольевич

```
:: :: { .column width="30%" }
```

Управление базовыми разрешениями 1

1. Откроем терминал с учётной записью root

The screenshot shows a desktop environment with a terminal window and a browser window. The terminal window is titled 'Терминал' and shows the command 'naglobin@naglobin:~\$ su -'. The browser window is titled 'Release lab 2.0' and displays a page from esystem.rudn.ru with instructions for managing file permissions.

Предпосылки: в лабораторной работе № 2 были созданы пользователи alice и bob, входящие в группу main, и пользователь carol, входящий в группу third.

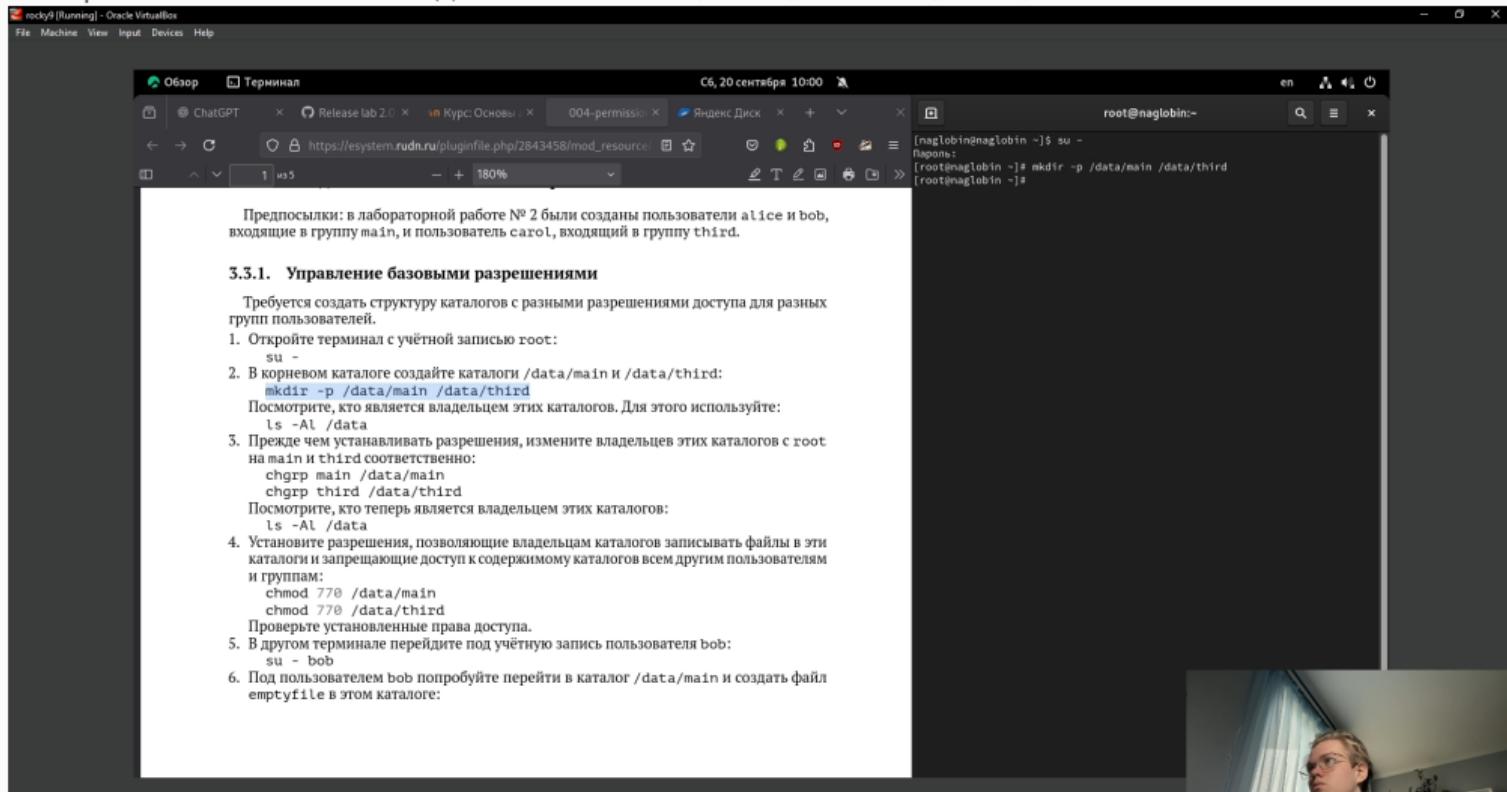
3.3.1. Управление базовыми разрешениями

Требуется создать структуру каталогов с разными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью root:
su -
2. В корневом каталоге создайте каталоги /data/main и /data/third:
mkdir -p /data/main /data/third
Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
ls -Al /data
3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:
chgrp main /data/main
chgrp third /data/third
Посмотрите, кто теперь является владельцем этих каталогов:
ls -Al /data
4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
chmod 770 /data/main
chmod 770 /data/third
Проверьте установленные права доступа.
5. В другом терминале перейдите под учётную запись пользователя bob:
su - bob
6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

Управление базовыми разрешениями 2

2. В корневом каталоге создаем каталоги /data/main и /data/third



Управление базовыми разрешениями 2.2

rocky8 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Обзор Терминал

ChatGPT Release lab 2.0 Курс: Основы 004-permissio Яндекс Диск

https://esystem.rudn.ru/pluginfile.php/2843458/mod_resource/

1 из 5 180%

Сб, 20 сентября 10:00

[root@naglobin ~]\$ su -
Пароль:
[root@naglobin ~]# mkdir -p /data/main /data/third
[root@naglobin ~]# ls -Al /data
итого 0
drwxr-xr-x. 2 root root 6 сен 20 10:00 main
drwxr-xr-x. 2 root root 6 сен 20 10:00 third
[root@naglobin ~]#

3.3.1. Управление базовыми разрешениями

Требуется создать структуру каталогов с различными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью root:
su -
2. В корневом каталоге создайте каталоги /data/main и /data/third:
mkdir -p /data/main /data/third
Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
ls -Al /data
3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:
chgrp main /data/main
chgrp third /data/third
Посмотрите, кто теперь является владельцем этих каталогов:
ls -Al /data
4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
chmod 770 /data/main
chmod 770 /data/third
Проверьте установленные права доступа.
5. В другом терминале перейдите под учётную запись пользователя bob:
su - bob
6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

Управление базовыми разрешениями 3

3. Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно

The screenshot shows a Linux desktop environment with a terminal window and a text editor window.

Terminal Window:

```
[naglobin@naglobin ~]$ su -  
Пароль:  
[root@naglobin ~]# mkdir -p /data/main /data/third  
[root@naglobin ~]# chgrp main /data/main  
[root@naglobin ~]# chgrp third /data/main  
[root@naglobin ~]# ls -Al /data  
total 0  
drwxr-xr-x. 2 root root 6 сен 20 10:00 main  
drwxr-xr-x. 2 root root 6 сен 20 10:00 third  
[root@naglobin ~]# [root@naglobin ~]# ls -Al /data  
total 0  
drwxr-xr-x. 2 root main 6 сен 20 18:00 main  
drwxr-xr-x. 2 root third 6 сен 20 10:00 third  
[root@naglobin ~]#
```

Text Editor Window:

Требуется создать структуру каталогов с разными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью root:
su -
2. В корневом каталоге создайте каталоги /data/main и /data/third:
mkdir -p /data/main /data/third
Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
ls -Al /data
3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:
chgrp main /data/main
chgrp third /data/third
Посмотрите, кто теперь является владельцем этих каталогов:
ls -Al /data
4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
chmod 770 /data/main
chmod 770 /data/third
Проверьте установленные права доступа.
5. В другом терминале перейдите под учётную запись пользователя bob:
su - bob
6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

Управление базовыми разрешениями 4

4. Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам

The screenshot shows a desktop environment with a terminal window and a browser window. The terminal window is titled 'root@naglobin:~-' and shows a root shell session. The browser window is titled 'rocky9 [Running] - Oracle VirtualBox' and displays a lab assignment page from esystem.rudn.ru.

Terminal Session:

```
[naglobin@naglobin ~]$ su -
Пароль:
[root@naglobin ~]# mkdir -p /data/main /data/second /data/third
[root@naglobin ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 сен 20 10:00 main
drwxr-xr-x. 2 root root 6 сен 20 10:00 second
[root@naglobin ~]# chgrp main /data/main
[root@naglobin ~]# chgrp third /data/second
[root@naglobin ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 сен 20 18:00 main
drwxr-xr-x. 2 root third 6 сен 20 18:00 second
[root@naglobin ~]# chmod 770 /data/main
[root@naglobin ~]# chmod 770 /data/second
[root@naglobin ~]#
```

Browser Content (Lab Assignment):

С6, 20 сентября 10:01

rocky9 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Обзор Терминал ChatGPT Release lab 2.0 Курс: Основы 004-permission Индекс Диск

1 из 5

https://esystem.rudn.ru/pluginfile.php/2843458/mod_resource/

На Main и Second соответственно.

```
chgrp main /data/main
chgrp third /data/second
```

Посмотрите, кто теперь является владельцем этих каталогов:

```
ls -Al /data
```

4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:

```
chmod 770 /data/main
chmod 770 /data/second
```

Проверьте установленные права доступа.

5. В другом терминале перейдите под учётную запись пользователя bob:

```
su - bob
```

6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

Управление базовыми разрешениями 4.2

rocky8 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Обзор Терминал

ChatGPT Release lab 2.0 Курс: Основы... 004-permissio... Яндекс Диск

https://esystem.rudn.ru/pluginfile.php/2843458/mod_resource/1/004-permissio... 1 из 5 180%

Сб, 20 сентября 10:01

на main и third соответственно.
chgrp main /data/main
chgrp third /data/third
Посмотрите, кто теперь является владельцем этих каталогов:
ls -Al /data

4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
chmod 770 /data/main
chmod 770 /data/third
Проверьте установленные права доступа.

5. В другом терминале перейдите под учётную запись пользователя bob:
su - bob
6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

28 Лабораторная работа № 3. Настройка прав доступа

```
cd /data/main
touch emptyfile
ls -Al
```

Опишите и поясните результат этого действия.

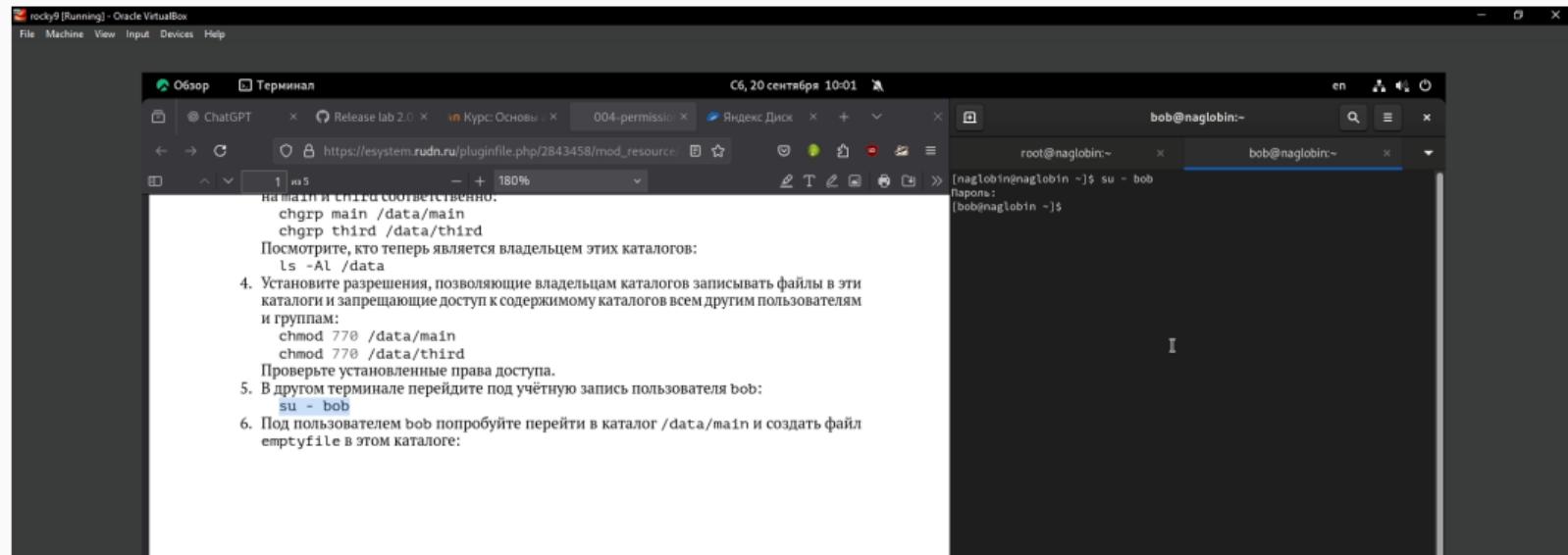
7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.
Опишите и поясните результат этого действия.

```
[naglobin@naglobin ~]$ su -
Пароль:
[root@naglobin ~]# mkdir -p /data/main /data/third
[root@naglobin ~]# ls -Al /data
итого 0
drwxr-xr-x. 2 root root 6 сен 20 10:00 main
drwxr-xr-x. 2 root root 6 сен 20 10:00 third
[root@naglobin ~]# chgrp main /data/main
[root@naglobin ~]# chgrp third /data/third
[root@naglobin ~]# ls -Al /data
итого 0
drwxr-xr-x. 2 root main 6 сен 20 10:00 main
drwxr-xr-x. 2 root third 6 сен 20 10:00 third
[root@naglobin ~]# chmod 770 /data/main
[root@naglobin ~]# chmod 770 /data/third
[root@naglobin ~]# ls -Al /data
итого 0
drwxrwx---. 2 root main 76 сен 20 10:00 main
drwxrwx---. 2 root third 6 сен 20 10:00 third
[root@naglobin ~]#
```

8/39

Управление базовыми разрешениями 5.2

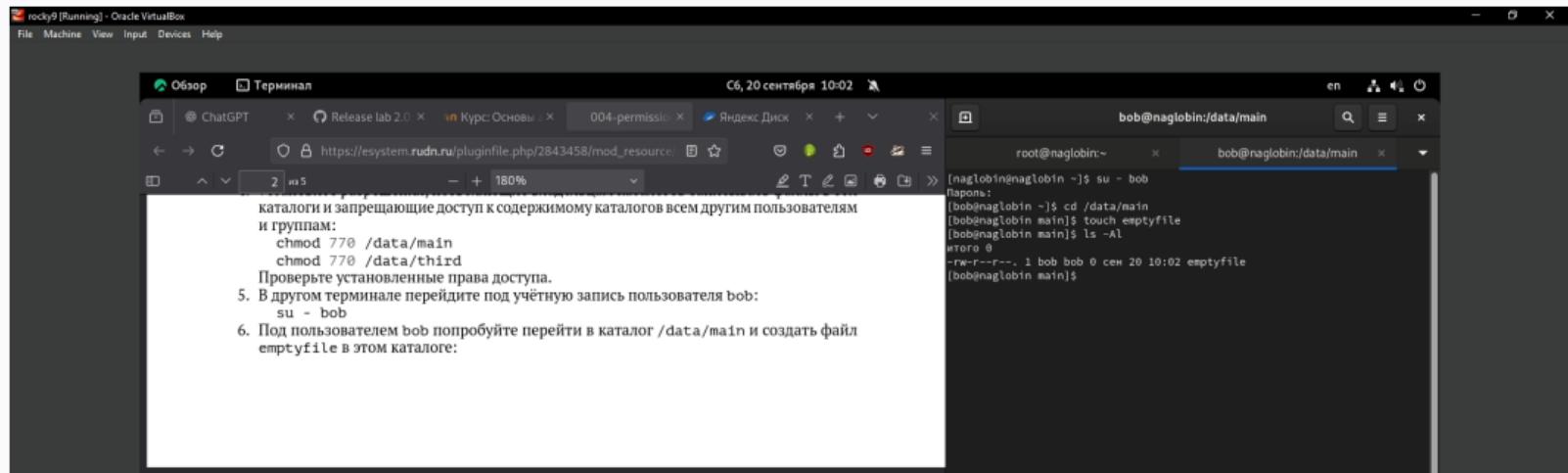
5. В другом терминале перейдем под учётную запись пользователя bob



- cd /data/main
 - touch emptyfile
 - ls -Al
- Опишите и поясните результат этого действия.
7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.

Управление базовыми разрешениями 6

6. Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге



```
cd /data/main
touch emptyfile
ls -Al
```

Опишите и поясните результат этого действия.

7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.

Опишите и поясните результат этого действия.

Управление базовыми разрешениями 7

7. Под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге

The screenshot shows a desktop environment with two terminal windows and a browser window.

Left Terminal:

```
cd /data/main
touch emptyfile
ls -Al
```

Output:

Лабораторная работа № 3. Настройка прав доступа

7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.

Опишите и поясните результат этого действия.

7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.

Опишите и поясните результат этого действия.

Right Terminal:

```
[naglobin@naglobin ~]$ su - bob
Пароль:
[bob@naglobin main]$ cd /data/main
[bob@naglobin main]$ touch emptyfile
[bob@naglobin main]$ ls -Al
total 0
-rw-r--r-- 1 bob bob 0 сен 20 10:02 emptyfile
[bob@naglobin main]$ cd /data/third
[bash: cd: /data/third: Оказано в доступе
[bob@naglobin main]$
```

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также *sticky bit*.

Sticky bit – дополнительный атрибут файлов или каталогов в ОС типа Linux, применявшийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение sticky-бита: 1000, а символьное: +t.

1. Откройте новый терминал под пользователем alice.
2. Перейдите в каталог /data/main:

```
cd /data/main
```

Создайте два файла, владельцем которых является alice:

```
touch alice1
```

```
touch alice2
```

Управление специальными разрешениями 1

1. Откроем новый терминал под пользователем alice

rocky9 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Обзор Терминал

Release lab 2.0 Курс: Основы 004-permission... Яндекс Диск

C6, 20 сентября 10:05

alice@naglobin:~

root@naglobin:~ cd /data/main
bash: cd: /data/main: Оказано в доступе
(naglobin@naglobin:~)\$ su - alice
Пароль:
(alice@naglobin ~)\$ su

1. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге.
Опишите и поясните результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также sticky bit.

Sticky bit – дополнительный атрибут файлов или каталогов в ОС типа Linux, применявшийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение sticky-бита: 1000, а символьное: +t.

1. Откройте новый терминал под пользователем alice.
2. Переийдите в каталог /data/main:

```
cd /data/main
```

Создайте два файла, владельцем которых является alice:

```
touch alice1  
touch alice2
```
3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):

```
su - bob
```
4. Переийдите в каталог /data/main:

```
cd /data/main
```

и в этом каталоге введите:

```
ls -l
```

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:

```
rm -f alice*
```

Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:

```
touch bob1  
touch bob2
```

Управление специальными разрешениями 2

2. Перейдем в каталог /data/main

The screenshot shows a desktop environment with a window titled "rocky9 [Running] - Oracle VirtualBox". Inside, there are two terminal windows and a file manager. The left terminal window has tabs for "Обзор", "Терминал", "ChatGPT", "Release lab 2.0", "Курс: Основы", "004-permission", and "Яндекс Диск". The right terminal window has tabs for "root@naglobin:~" (active), "bob@naglobin:~...", and "alice@naglobin:~...". The active terminal shows a user's session:

```
[naglobin@naglobin ~]$ cd /data/main
bash: cd: /data/main: Отказано в доступе
[naglobin@naglobin ~]$ su - alice
Пароль:
[alice@naglobin ~]$ cd /data/main
[alice@naglobin main]$
```

The file manager shows a list of files and folders, including "emptyfile" and "emptydir". Below the desktop, a list of tasks is visible:

- Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге.
- Опишите и поясните результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также sticky bit.

Sticky bit – дополнительный атрибут файлов или каталогов в ОС типа Linux, применявшийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение sticky-бита: 1000, а символьное: +t.

- Откройте новый терминал под пользователем alice.
- Перейдите в каталог /data/main:
cd /data/main
Создайте два файла, владельцем которых является alice:
touch alice1
touch alice2
- В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):
su - bob
- Перейдите в каталог /data/main:
cd /data/main
и в этом каталоге введите:
ls -l
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
rm -f alice*
- Убедитесь, что файлы будут удалены пользователем bob:
touch bob1
touch bob2

Управление специальными разрешениями 2.2

Создем два файла, владельцем которых является alice

rocky9 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Обзор Терминал

Release lab 2.0 Курс: Основы 004-permissio... Яндекс Диск

C6, 20 сентября 10:05

https://esystem.rudn.ru/pluginfile.php/2843458/mod_resource/

1. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге.
Опишите и поясните результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также sticky bit.

Sticky bit – дополнительный атрибут файлов или каталогов в ОС типа Linux, применяемый в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение sticky-бита: 1000, а символьное: +t.

1. Откройте новый терминал под пользователем alice.
2. Переийдите в каталог /data/main:

```
cd /data/main
```

Создайте два файла, владельцем которых является alice:

```
touch alice1  
touch alice2
```
3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):

```
su - bob
```
4. Переийдите в каталог /data/main:

```
cd /data/main
```

и в этом каталоге введите:

```
ls -l
```

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:

```
rm -f alice*
```

Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:

```
touch bob1  
touch bob2
```

```
[naglobin@naglobin ~]$ cd /data/main  
bash: cd: /data/main: Оказано в доступе  
[naglobin@naglobin ~]$ su - alice  
Password:  
[alice@naglobin ~]$ cd /data/main  
[alice@naglobin main]$ touch alice1  
[alice@naglobin main]$ touch alice2  
[alice@naglobin main]$
```

Управление специальными разрешениями 3

3. В другом терминале перейдем под учётную запись пользователя bob

rocky9 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Обзор Терминал

ChatGPT Release lab 2.0 Курс: Основы 004-permissio... Яндекс Диск

C6, 20 сентября 10:06

bob@naglobin:~

root@na... x bob@nag... x alice@na... x bob@nag... x

[naglobin@naglobin ~]\$ su - bob
Пароль:
(bob@naglobin ~)\$

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также sticky bit.

Sticky bit – дополнительный атрибут файлов или каталогов в ОС типа Linux, применявшийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение sticky-бита: 1000, а символьное: +t.

1. Откройте новый терминал под пользователем alice.
2. Перейдите в каталог /data/main:
`cd /data/main`
Создайте два файла, владельцем которых является alice:
`touch alice1`
`touch alice2`
3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):
`su - bob`
4. Перейдите в каталог /data/main:
`cd /data/main`
и в этом каталоге введите:
`ls -l`
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
`rm -f alice*`
Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:
`touch bob1`
`touch bob2`
6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:
`chmod g+s,+t /data/main`
7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:

Управление специальными разрешениями 4

4. Перейдем в каталог /data/main

rocky9 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Обзор Терминал ChatGPT Release lab 2.0 Курс: Основы 004-permissio... Яндекс Диск

C6, 20 сентября 10:07

или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита chmod. Восьмеричное значение sticky-бита: 1000, а символическое: +t.

1. Откройте новый терминал под пользователем alice.
2. Перейдите в каталог /data/main:
cd /data/main
Создайте два файла, владельцем которых является alice:
touch alice1
touch alice2
3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):
su - bob
4. Перейдите в каталог /data/main:
cd /data/main
и в этом каталоге введите:
ls -l
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
rm -f alice*
Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:
touch bob1
touch bob2
6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:
chmod g+,+t /data/main
7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:
touch alice3
touch alice4
ls -l
Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой владельца каталога /data/main.
В терминале под пользователем alice попробуйте удалить файлы, принадлежащие

```
[naglobin@naglobin ~]$ su - bob
Password:
[bob@naglobin ~]$ cd /data/main
[bob@naglobin main]$ ls -l
итого 0
-rw-r--r--, 1 alice alice 0 сен 20 10:05 alice1
-rw-r--r--, 1 alice alice 0 сен 20 10:05 alice2
-rw-r--r--, 1 bob bob 0 сен 20 10:02 emptyfile
[bob@naglobin main]$ rm -f alice*
[bob@naglobin main]$ ls -l
итого 0
-rw-r--r--, 1 bob bob 0 сен 20 10:02 emptyfile
[bob@naglobin main]$
```

Управление специальными разрешениями 5

5. Создаем два файла, которые принадлежат пользователю bob

The screenshot shows a desktop environment with a terminal window and a browser window.

Terminal Window:

```
[naglobin@naglobin ~]$ su - bob
bob:
[bob@naglobin ~]$ cd /data/main
[bob@naglobin main]$ ls -l
итого 0
-rw-r--r--, 1 alice alice 0 сен 20 10:05 alice1
-rw-r--r--, 1 alice alice 0 сен 20 10:05 alice2
-rw-r--r--, 1 bob bob 0 сен 20 10:02 emptyfile
[bob@naglobin main]$ rm -f alice*
[bob@naglobin main]$ ls -l
итого 0
-rw-r--r--, 1 bob bob 0 сен 20 10:02 emptyfile
[bob@naglobin main]$ touch bob1
[bob@naglobin main]$ touch bob2
[bob@naglobin main]$
```

Browser Window:

Address bar: https://esystem.rudn.ru/pluginfile.php/2843458/mod_resource/004-permission

Page content (partial):

```
боб является членом группы main, как и alice):
su - bob
4. Перейдите в каталог /data/main:
cd /data/main
и в этом каталоге введите:
ls -l
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы,
принадлежащие пользователю alice:
rm -f alice*
Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:
touch bob1
touch bob2
6. В терминале под пользователем root установите для каталога /data/main бит иден-
тификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:
chmod g+s,o+t /data/main
7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3
и alice4:
touch alice3
touch alice4
ls -l
Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main,
которая является группой-владельцем каталога /data/main.
8. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие
пользователю bob:
rm -rf bob*
```

Управление специальными разрешениями 6

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

The screenshot shows a desktop environment with a terminal window and a browser window. The terminal window is titled 'root@naglobin:' and contains a command-line session. The browser window is titled 'Терминал' and displays a step-by-step guide for managing file permissions.

Terminal Session:

```
[root@naglobin ~]# su -
Password:
[root@naglobin ~]# mkdir -p /data/main /data/third
[root@naglobin ~]# ls -Al /data
штого 8
drwxr-xr-x 2 root root 6 сен 20 10:00 main
drwxr-xr-x 2 root root 6 сен 20 10:00 third
[root@naglobin ~]# chgrp main /data/main
[root@naglobin ~]# chmod 770 /data/third
[root@naglobin ~]# ls -Al /data
штого 8
drwxr-xr-x 2 root main 6 сен 20 10:00 main
drwxr-xr-x 2 root third 6 сен 20 10:00 third
[root@naglobin ~]# chmod 770 /data/third
[root@naglobin ~]# ls -Al /data
штого 8
drwxrwx--- 2 root main 6 сен 20 10:00 main
drwxrwx--- 2 root third 6 сен 20 10:00 third
[root@naglobin ~]# chmod g+s,o+t /data/main
[root@naglobin ~]#
```

Browser Content (Terminal Guide):

- bob является членом группы main, как и alice:
- su - bob
- Перейдите в каталог /data/main:
cd /data/main
- и в этом каталоге введите:
ls -l
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
rm -f alice*
Убедитесь, что файлы будут удалены пользователем bob.
- Создайте два файла, которые принадлежат пользователю bob:
touch bob1
touch bob2
- В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:
chmod g+s,o+t /data/main
- В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:
touch alice3
touch alice4
ls -l
Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.
- В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob:
rm -rf bob*

Управление специальными разрешениями 7

- В терминале под пользователем alice создаем в каталоге /data/main файлы alice3 и alice4

The screenshot shows a desktop environment with multiple windows. In the foreground, a terminal window titled 'Терминал' is open, showing a command-line session. The session starts with the user 'naglobin' at the prompt [naglobin@naglobin ~]\$. The user runs 'cd /data/main' and then 'ls -l', which lists files: 'alice1', 'alice3', 'alice4', 'bob1', 'bob2', and 'emptyfile'. The user then runs 'rm -rf bob*' to delete files owned by 'bob'. The terminal window has tabs for 'root@naglobin ~', 'alice@naglobin:~', and 'bob@naglobin:~'. In the background, there is a file manager window showing a list of files and a browser window displaying a course page from esystem.rudn.ru.

```
[naglobin@naglobin ~]$ cd /data/main
bash: cd: /data/main: Отказано в доступе
[naglobin@naglobin ~]$ su - alice
Напоминание:
(alice@naglobin main)$ cd /data/main
(alice@naglobin main)$ touch alice1
(alice@naglobin main)$ touch alice3
(alice@naglobin main)$ touch alice4
(alice@naglobin main)$ ls -l
итого 6
-rw-r--r--. 1 alice main 0 сен 20 10:12 alice3
-rw-r--r--. 1 alice main 0 сен 20 10:12 alice4
-rw-r--r--. 1 bob  bob 0 сен 20 10:11 bob1
-rw-r--r--. 1 bob  bob 0 сен 20 10:11 bob2
-rw-r--r--. 1 bob  bob 0 сен 20 10:02 emptyfile
[alice@naglobin main]$
```

4. Перейдите в каталог /data/main:
cd /data/main
и в этом каталоге введите:
ls -l
Вы увидите два файла, созданных пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
rm -f alice*
Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:
touch bob1
touch bob2
6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:
chmod g+s,o+t /data/main
7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:
touch alice3
touch alice4
ls -l
Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.
8. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob:
rm -rf bob*

1. Откроем терминал с учётной записью root
2. Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third

Управление расширенными разрешениями с использованием списков ACL 2

The screenshot shows a Linux desktop environment with a terminal window and a help document.

Terminal Window:

```
[root@naglobin ~]# su -  
Пароль:  
[root@naglobin ~]# mkdir -p /data/main /data/third  
[root@naglobin ~]# ls -Al /data  
ицтого 0  
drwxr-xr-x. 2 root root 6 сен 20 10:00 main  
drwxr-xr-x. 2 root third 6 сен 20 10:00 third  
[root@naglobin ~]# chgrp main /data/main  
[root@naglobin ~]# chgrp third /data/third  
[root@naglobin ~]# ls -Al /data  
ицтого 0  
drwxr-xr-x. 2 root main 6 сен 20 10:00 main  
drwxr-xr-x. 2 root third 6 сен 20 10:00 third  
[root@naglobin ~]# chmod 770 /data/main  
[root@naglobin ~]# chmod 770 /data/third  
[root@naglobin ~]# ls -Al /data  
ицтого 0  
drwxrwx---. 2 root main 6 сен 20 10:00 main  
drwxrwx---. 2 root third 6 сен 20 10:00 third  
[root@naglobin ~]# chmod g+s,o+t /data/main  
[root@naglobin ~]# setfacl -m g:third:rwx /data/main  
[root@naglobin ~]# setfacl -m g:main:rwx /data/third  
[root@naglobin ~]#
```

Help Document:

Установить разрешения для группы:

```
setfacl -m "g:group:permissions" <file/dir>
```

Наследование записи ACL родительского каталога:

```
setfacl -dN "entry" <dir>
```

Удаление записи ACL:

```
setfacl -x "entry" <file/dir>
```

Синтаксис команды getfacl:

```
getfacl <file/dir>
```

Применим команды setfacl и getfacl для выполнения поставленной задачи.

1. Откройте терминал с учётной записью root
su -
2. Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third:
setfacl -m g:third:rwx /data/main
setfacl -m g:main:rwx /data/third
3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main
getfacl /data/third
4. Создайте новый файл с именем newfile1 в каталоге /data/main:
touch /data/main/newfile1
Используйте
getfacl /data/main/newfile1
для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему.
5. Выполните аналогичные действия для каталога /data/third. Дайте пояснения.
6. Установите ACL по умолчанию для каталога /data/main:
setfacl -m d:g:third:rwx /data/main
7. Добавьте ACL по умолчанию для каталога /data/third:
setfacl -m d:g:main:rwx /data/third
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:
touch /data/main/newfile2

Управление расширенными разрешениями с использованием списков ACL 3

4. Создаем новый файл с именем newfile1 в каталоге /data/main

The screenshot shows a desktop environment with a terminal window and a browser window. The terminal window is titled 'root@naglobin:' and displays a command-line session. The browser window is titled '004-permission' and shows a page from esystem.rudn.ru with instructions for managing ACL permissions.

Terminal Session:

```
root@naglobin:~# ls -Al /data
drwxr-xr-x. 2 root main 6 сен 20 10:00 main
drwxr-xr-x. 2 root third 6 сен 20 10:00 third
[root@naglobin ~]# chmod 770 /data/main
[root@naglobin ~]# chmod 770 /data/third
[root@naglobin ~]# ls -Al /data
总用量 0
drwxrwx---. 2 root main 6 сен 20 10:00 main
drwxrwx---. 2 root third 6 сен 20 10:00 third
[root@naglobin ~]# chmod g+s,ott /data/main
[root@naglobin ~]# setfacl -m g:third:rwx /data/main
[root@naglobin ~]# setfacl -m g:main:rwx /data/third
[root@naglobin ~]# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# Flags: -s-
user::rwx
group::rwx
group:third:rwx
mask::rwx
other::---

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

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

Browser Content (Instructions):

Установить разрешения для группы:
setfacl -m "g:group:permissions" <file/dir>

Наследование записи ACL родительского каталога:
setfacl -dm "entry" <dir>

Удаление записи ACL:
setfacl -x "entry" <file/dir>

Синтаксис команды getfacl:
getfacl <file/dir>

Применим команды setfacl и getfacl для выполнения поставленной задачи.

- Откройте терминал с учётной записью root
su -
- Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third:
setfacl -m g:third:rwx /data/main
setfacl -m g:main:rwx /data/third
- Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main
getfacl /data/third
- Создайте новый файл с именем newfile1 в каталоге /data/main:
touch /data/main/newfile1
Используйте
getfacl /data/main/newfile1
для проверки текущих назначений полномочий. Какие права доступа у этого файла?
Объясните, почему.
- Выполните аналогичные действия для каталога /data/third. Дайте пояснения.
- Установите ACL по умолчанию для каталога /data/main:
setfacl -m d:g:third:rwx /data/main
- Добавьте ACL по умолчанию для каталога /data/third:
setfacl -m d:g:main:rwx /data/third
- Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:
touch /data/main/newfile2

Управление расширенными разрешениями с использованием списков ACL 4

5. Установим ACL по умолчанию для каталога /data/main

rocky9 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Обзор Терминал ChatGPT Release lab 2.0 Курс: Основы 004-permission... Яндекс Диск

C6, 20 сентября 10:18

root@naglobin:~

root@naglobin:~

alice@naglobin:~

bob@naglobin:~/

Установить разрешения для группы:
setfacl -m "g:group:permissions" <file/dir>

Наследование записи ACL родительского каталога:
setfacl -dm "entry" <dir>

Удаление записи ACL:
setfacl -x "entry" <file/dir>

Синтаксис команды getfacl:
getfacl <file/dir>

Применим команды setfacl и getfacl для выполнения поставленной задачи.

- Откройте терминал с учётной записью root
su -
- Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third:
setfacl -m g:third:rwx /data/main
setfacl -m g:main:rwx /data/third
- Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main
getfacl /data/third
- Создайте новый файл с именем newfile1 в каталоге /data/main:
touch /data/main/newfile1
Используйте
getfacl /data/main/newfile1
для проверки текущих назначений полномочий. Какие права доступа у этого файла?
Объясните, почему.
- Выполните аналогичные действия для каталога /data/third. Дайте пояснения.
- Установите ACL по умолчанию для каталога /data/main:
setfacl -m d:g:third:rwx /data/main
- Добавьте ACL по умолчанию для каталога /data/third:
setfacl -m d:g:main:rwx /data/third
- Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:
touch /data/main/newfile2

```
drwxr-xr-x. 2 root third 6 сен 20 10:00 third
[root@naglobin ~]# chmod 770 /data/main
[root@naglobin ~]# chmod 770 /data/third
[root@naglobin ~]# ls -Al /data
 всего 0
drwxrwx---. 2 root main 6 сен 20 10:00 main
drwxrwx---. 2 root third 6 сен 20 10:00 third
[root@naglobin ~]# chmod g+s,ot+ /data/main
[root@naglobin ~]# setfacl -m g:third:dirx /data/main
[root@naglobin ~]# setfacl -m g:main:rwx /data/third
[root@naglobin ~]# 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::---

[root@naglobin ~]# 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@naglobin ~]# touch /data/main/newfile1
[root@naglobin ~]# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rwx
group::r-x
group:third:r-x
mask::rwx
other::---

[root@naglobin ~]# setfacl -m d:g:third:rwx /data/main
```

Управление расширенными разрешениями с использованием списков ACL 5

6. Добавим ACL по умолчанию для каталога /data/third

rocky9 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Обзор Терминал ChatGPT Release lab 2.0 Курс: Основы 004-permission... Яндекс Диск

C6, 20 сентября 10:18

root@naglobin:~

Установить разрешения для группы:
setfacl -m "g:group:permissions" <file/dir>

Наследование записи ACL родительского каталога:
setfacl -dm "entry" <dir>

Удаление записи ACL:
setfacl -x "entry" <file/dir>

Синтаксис команды getfacl:
getfacl <file/dir>

Применим команды setfacl и getfacl для выполнения поставленной задачи.

- Откройте терминал с учётной записью root
su -
- Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third:
setfacl -m g:third:rwx /data/main
setfacl -m g:main:rwx /data/third
- Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main
getfacl /data/third
- Создайте новый файл с именем newfile1 в каталоге /data/main:
touch /data/main/newfile1
Используйте
getfacl /data/main/newfile1
для проверки текущих назначений полномочий. Какие права доступа у этого файла?
Объясните, почему.
Выполните аналогичные действия для каталога /data/third. Дайте пояснения.
- Установите ACL по умолчанию для каталога /data/main:
setfacl -m d:g:third:rwx /data/main
- Добавьте ACL по умолчанию для каталога /data/third:
setfacl -m d:g:main:rwx /data/third
- Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:
touch /data/main/newfile2

```
[root@naglobin ~]# chmod 770 /data/main
[root@naglobin ~]# chmod 770 /data/third
[root@naglobin ~]# ls -Al /data
кого 0
drwxrwx---. 2 root main 6 сем 20 10:00 main
drwxrwx---. 2 root third 6 сем 20 10:00 third
[root@naglobin ~]# chmod g+s,=t /data/main
[root@naglobin ~]# setfacl -m g:third:rwx /data/main
[root@naglobin ~]# setfacl -m g:main:rwx /data/third
[root@naglobin ~]# 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::---

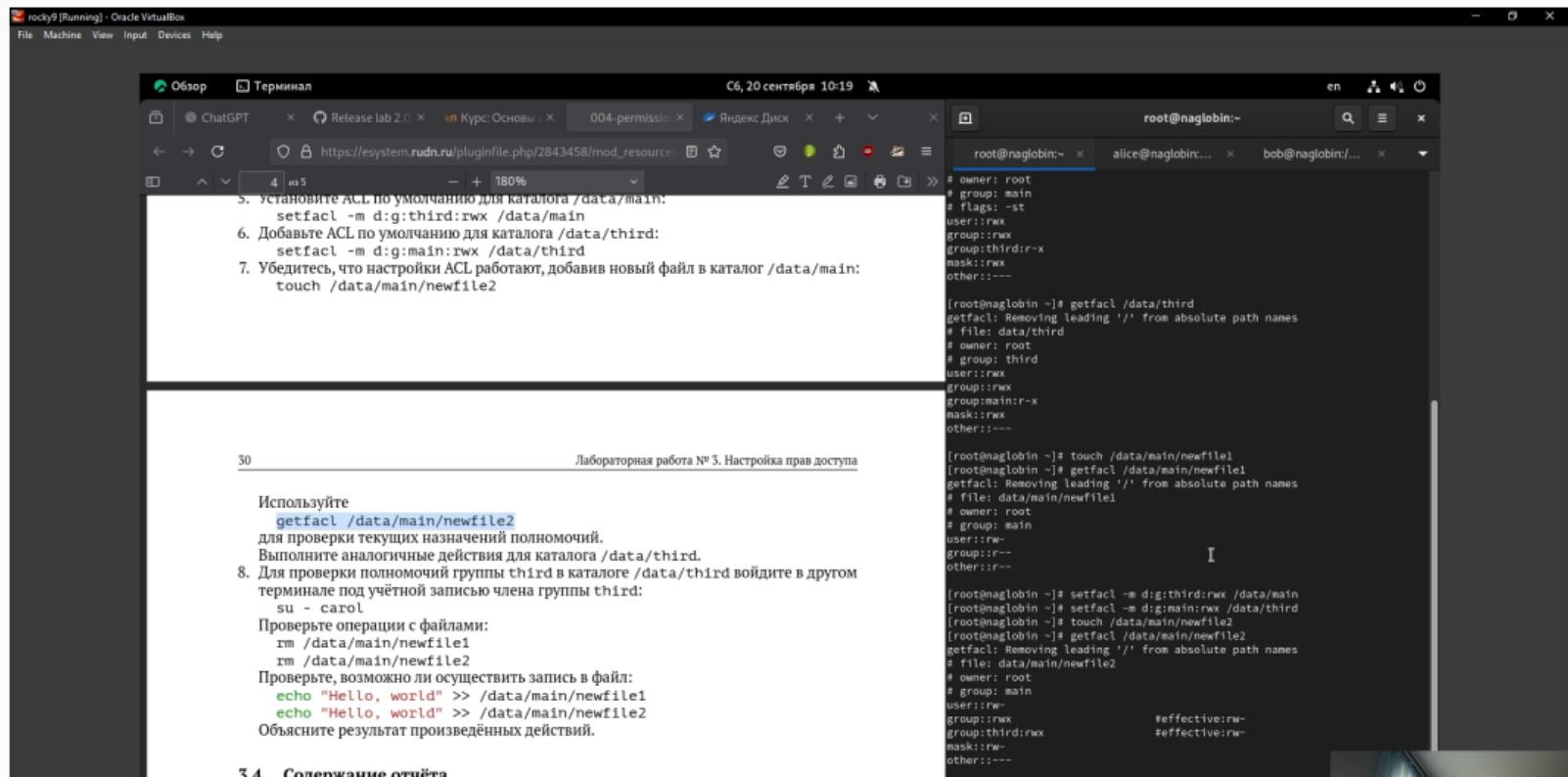
[root@naglobin ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
group::rwx
group:main:r-x
mask::rwx
other::---

[root@naglobin ~]# touch /data/main/newfile1
[root@naglobin ~]# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rwx
group::rwx
group:main:r-x
mask::rwx
other::---

[root@naglobin ~]# setfacl -m d:g:third:rwx /data/main
[root@naglobin ~]# setfacl -m d:g:main:rwx /data/third
```

Управление расширенными разрешениями с использованием списков ACL 6

7. Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main



Управление расширенными разрешениями с использованием списков ACL 6.2

Выполним аналогичные действия для каталога /data/third

The screenshot shows a desktop environment with a terminal window and a browser window. The terminal window is titled 'root@naglobin:~-' and displays a series of commands related to SELinux file context manipulation. The browser window shows a lab exercise page from RUDN University.

Terminal Window Content:

```
# owner: root
# group: third
user::rwx
group::rwx
group::main:r-x
mask::rwx
other::---

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

[root@naglobin ~]# setfacl -m d:third:rwx /data/main
[root@naglobin ~]# setfacl -m d:main:rwx /data/third
[root@naglobin ~]# touch /data/main/newfile2
[root@naglobin ~]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rwx
group::rwx
group::third:rwx
mask::rwx
other::---

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

Browser Window Content (Lab Exercise Page):

Лабораторная работа № 3. Настройка прав доступа

30

Используйте
getfacl /data/main/newfile2
для проверки текущих назначений полномочий.
Выполните аналогичные действия для каталога /data/third.

8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:
su - carol
Проверьте операции с файлами:
rm /data/main/newfile1
rm /data/main/newfile2
Проверьте, возможно ли осуществить запись в файл:
echo "Hello, world" >> /data/main/newfile1
echo "Hello, world" >> /data/main/newfile2
Объясните результат произведённых действий.

Section-Header:

3.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:

- скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
- подробное описание произведенных действий;

26/39

Управление расширенными разрешениями с использованием списков ACL 7

8. Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third

rocky9 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Обзор Терминал

ChatGPT Release lab 2.0 Курс: Основы... 004-permissio... Яндекс Диск

https://esystem.rudn.ru/pluginfile.php/2843458/mod_resource/

root@na... alice@na... bob@na... carol@na...

en

06, 20 сентября 10:27

[naglobin@naglobin ~]\$ su - carol

Пароль:

[carol@naglobin ~]\$ rm /data/main/newfile1

rm: удалить защищенный от записи пустой обычный файл '/data/main/newfile1'? у

rm: невозможно удалить '/data/main/newfile1': Отказано в доступе

[carol@naglobin ~]\$ rm /data/main/newfile2

rm: невозможно удалить '/data/main/newfile2': Отказано в доступе

[carol@naglobin ~]\$

Лабораторная работа № 3. Настройка прав доступа

30

Используйте
getfacl /data/main/newfile2
для проверки текущих назначений полномочий.
Выполните аналогичные действия для каталога /data/third.
8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:
su - carol
Проверьте операции с файлами:
rm /data/main/newfile1
rm /data/main/newfile2
Проверьте, возможно ли осуществить запись в файл:
echo "Hello, world" >> /data/main/newfile1
echo "Hello, world" >> /data/main/newfile2
Объясните результат произведённых действий.

3.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.

Управление расширенными разрешениями с использованием списков ACL 7.2

Проверим операции с файлами и возможно ли осуществить запись в файл

The screenshot shows a desktop environment with a terminal window and a browser window. The terminal window is titled 'carol@naglobin:' and shows a user attempting to delete files and echo content into them, demonstrating permission errors. The browser window shows a lab guide for 'Лабораторная работа № 3. Настройка прав доступа'.

Лабораторная работа № 3. Настройка прав доступа

30

Используйте
getfacl /data/main/newfile2
для проверки текущих назначений полномочий.
Выполните аналогичные действия для каталога /data/third.
8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:
su - carol
Проверьте операции с файлами:
rm /data/main/newfile1
rm /data/main/newfile2
Проверьте, возможно ли осуществить запись в файл:
echo "Hello, world" >> /data/main/newfile1
echo "Hello, world" >> /data/main/newfile2
Объясните результат произведённых действий.

3.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание произведённых в соответствии с заданием настройками;
 - результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы (по возможности подтверждённые скриншотами).

Контрольные вопросы 1

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

Команда chown позволяет изменить владельца и/или группу файла.chown :

Контрольные вопросы 2

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

Команда find позволяет искать файлы по владельцу.`find / -user alice`

Контрольные вопросы 3

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? Приведите пример. chmod -R 770 /data

Контрольные вопросы 4

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

`chmod +x`

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

Для этого используется бит setgid на каталоге. chmod g+s /data/main

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? Приведите пример.

Для этого применяется sticky-bit. После установки sticky-бита только владельцы файлов (или root) смогут их удалять, даже если каталог доступен другим. `chmod +t /data/main`

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

```
setfacl -m g::r
```

8. Что нужно сделать для гарантии того, что члены группы получат 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? Приведите пример.

Нужно использовать ACL по умолчанию (default ACL). `setfacl -R -m g:third:r setfacl -d -m g:third:rwx`

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

Значение umask: 007

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

Самый простой способ — запретить запись в каталог или установить атрибут “immutable”.

Результаты

В ходе выполнения лабораторной работы №3 мы научились настраивать базовые, специальные и расширенные права доступа в операционной системе Linux. Были изучены команды chmod, chgrp, chown, getfacl, setfacl, а также их применение на практике.