Лабораторная работа № 3.

Настройка прав доступа

Диана Алексеевна Садова

Содержание

# 1 Цель работы

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

# 2 Последовательность выполнения работы

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

## 2.1 Управление базовыми разрешениями

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

1. Откройте терминал с учётной записью root:(рис. 1).

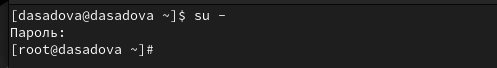


Рис. 1: Переходим в учётную запись root

1. В корневом каталоге создайте каталоги /data/main и /data/third:(рис. 2).

Создаем каталоги /data/main и /data/third в корневом каталоге

Рис. 2: Создаем каталоги /data/main и /data/third в корневом каталоге

Посмотрите, кто является владельцем этих каталогов. Для этого используйте:(рис. 3).

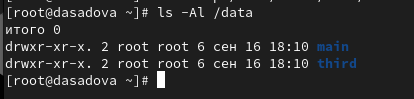


Рис. 3: Просматириваем кто является владельцем каталогов

1. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:(рис. 4).

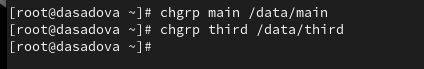


Рис. 4: Изменяем владельцев каталогов main и third

Посмотрите, кто теперь является владельцем этих каталогов:(рис. 5).

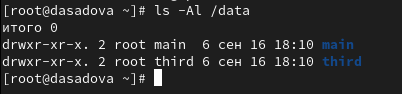


Рис. 5: Просматириваем кто является владельцем каталогов

1. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам. Проверьте установленные права доступа(рис. 6).

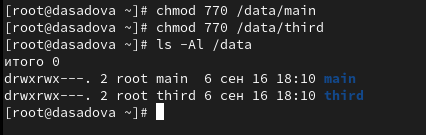


Рис. 6: Устанавливаем и приверяем разрешение

1. В другом терминале перейдите под учётную запись пользователя bob:(рис. 7).

Переходим к учётной запись пользователя bob

Рис. 7: Переходим к учётной запись пользователя bob

1. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:(рис. 8).

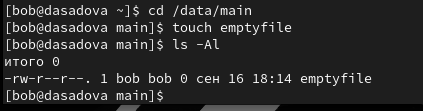


Рис. 8: Переходим в каталог и создаем файл

Опишите и поясните результат этого действия.

Пользователь bob может создать файл в каталоге main, так как имет права достура в каталоге

1. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.(рис. 9).

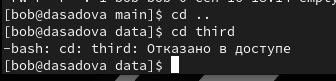


Рис. 9: Переходим в каталог и создаем файл

Опишите и поясните результат этого действия.

Пользователь bob не может создать файл в каталоге third, так как сам не пренадлежит к этому каталогу и не имеет прав доступа

## 2.2 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, применяющийся 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 stiky-бита: 1000, а символьное: +t.

1. Откройте новый терминал под пользователем alice.(рис. 10).

Переходим к учётной запись пользователя alice

Рис. 10: Переходим к учётной запись пользователя alice

1. Перейдите в каталог /data/main:(рис. 11).

Переходим в каталог

Рис. 11: Переходим в каталог

Создайте два файла, владельцем которых является alice:(рис. 12).

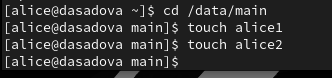


Рис. 12: Создаем два файла

1. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):(рис. 13).

Переходим к учётной запись пользователя bob

Рис. 13: Переходим к учётной запись пользователя bob

1. Перейдите в каталог /data/main:(рис. 14).

Переходим в каталог

Рис. 14: Переходим в каталог

и в этом каталоге введите:(рис. 15).

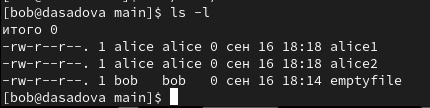


Рис. 15: Просматриваем всю информацию о файлах

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:(рис. 16).

Пробуем удалить файл

Рис. 16: Пробуем удалить файл

Убедитесь, что файлы будут удалены пользователем bob.(рис. 17).

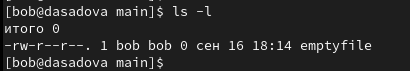


Рис. 17: Убедимся в том что файлы удалены

1. Создайте два файла, которые принадлежат пользователю bob:(рис. 18).

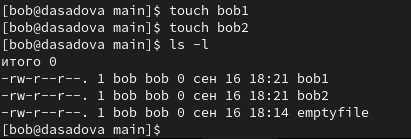


Рис. 18: Создаем файлы

1. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы:(рис. 19).

Устанавливаем бит идентификатора группы, а так же stiky-бит

Рис. 19: Устанавливаем бит идентификатора группы, а так же stiky-бит

1. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:(рис. 20).

Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.(рис. 20).

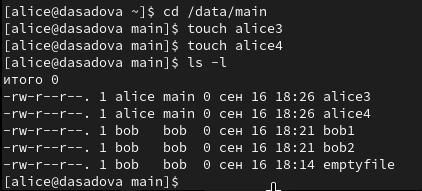


Рис. 20: Создаем файлы и проверяем их группы

1. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob:(рис. 21).

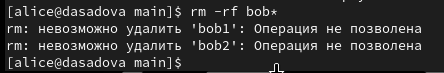


Рис. 21: Пробуем удалить файлы

Убедитесь, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов. Обратите внимание: поскольку пользователь alice является владельцем каталога /data/main, то он может удалить все свои файлы в любом случае.

## 2.3 Управление расширенными разрешениями с использованием списков ACL

В этом упражнении продолжим работать в созданных ранее каталогах /data/main и /data/third. В предыдущих упражнениях для группы main были установлены разрешения на каталог /data/main, а у группы third — на каталог /data/third.

Требуется установить для группы third разрешения на чтение в каталоге /data/main, а для группы main — разрешения на чтение в каталоге /data/third. Затем требуется установить права доступа по умолчанию, чтобы убедиться в правильности установки разрешений для новых элементов этих каталогов. Для этого будет использоваться пакет acl и команды setfacl (для установки прав) и getfacl (для просмотра установленных прав).

Кратко опишем синтаксис команды setfacl.

Установить разрешения для пользователя:

setfacl -m “u:user:permissions”

Установить разрешения для группы:

setfacl -m “g:group:permissions”

Наследование записи ACL родительского каталога:

setfacl -dm “entry”

Удаление записи ACL:

setfacl -x “entry”

Синтаксис команды getfacl:

getfacl

Применим команды setfacl и getfacl для выполнения поставленной задачи.

1. Откройте терминал с учётной записью root(рис. 22).

Переходим в учётную запись root

Рис. 22: Переходим в учётную запись root

1. 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:(рис. 23).

Устанавливаем права чтения

Рис. 23: Устанавливаем права чтения

1. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:(рис. 24),(рис. 25).

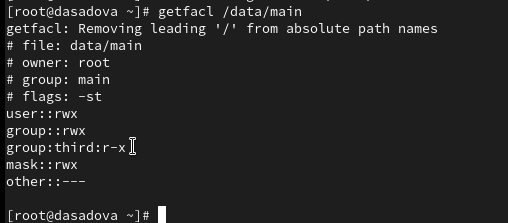


Рис. 24: Используем команду getfacl для main

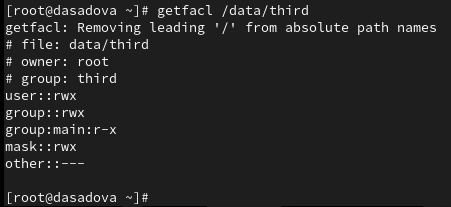


Рис. 25: Используем команду getfacl для third

1. Создайте новый файл с именем newfile1 в каталоге /data/main:(рис. 26).

Создаем файл newfile1

Рис. 26: Создаем файл newfile1

Используйте getfacl /data/main/newfile1 для проверки текущих назначений полномочий. Какие права доступа у этого файла?

Объясните, почему.

Права доступа у файла “-rw-r–r–” - это значит что владелец файла имеет права только на чтение и запись (rw), а группа и остальные пользователи — только на чтение (r)

Выполните аналогичные действия для каталога /data/third. Дайте пояснения.(рис. 27).

Создаем файл newfile2

Рис. 27: Создаем файл newfile2

1. Установите ACL по умолчанию для каталога /data/main:(рис. 28).

Устанавили ACL для /data/main

Рис. 28: Устанавили ACL для /data/main

1. Добавьте ACL по умолчанию для каталога /data/third:(рис. 29).

Устанавили ACL для /data/third

Рис. 29: Устанавили ACL для /data/third

1. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main. Используйте getfacl /data/main/newfile2 для проверки текущих назначений полномочий.(рис. 30).



Рис. 30: Добавляем новый файл в main

Выполните аналогичные действия для каталога /data/third.(рис. 31).

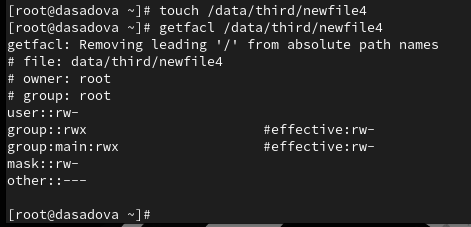


Рис. 31: Добавляем новый файл в third

1. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:(рис. 32).

Переходим к учётной запись пользователя carol

Рис. 32: Переходим к учётной запись пользователя carol

Проверьте операции с файлами:(рис. 33).

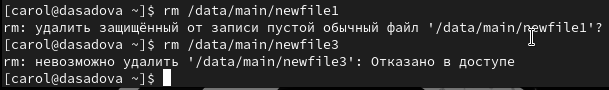


Рис. 33: Пытаемся удалить файлы из каталогов

Проверьте, возможно ли осуществить запись в файл:(рис. 34),(рис. 35).

Пытаемся записать “Hello, world” в файл

Рис. 34: Пытаемся записать “Hello, world” в файл

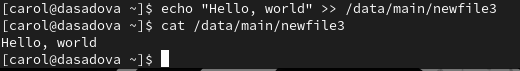


Рис. 35: Пытаемся записать “Hello, world” в файл

Объясните результат произведённых действий.

В первом случае у нас отказ в доступе - это связанно с правами доступа файла newfile1. Пользователь carol, который записанн в каталоге third не имеет прав доступа редактировать файла newfile1 не своего каталога (каталога main).

Во втором случае получилось записать в файл newfile3, так как его прова доступа разрешают редактировать его другим пользователям (остальные пользователи)

# 3 Выводы

Получили навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux. Больше узнали о правах доступа пользователей # Список литературы{.unnumbered}