Отчёт по лабораторной работе №3

Основы администрирования операционных сетей

Бызова Мария Олеговна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Целью данной работы является получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

2 Задание

1. Прочитайте справочное описание man по командам chgrp, chmod, getfacl, setfacl.
2. Выполните действия по управлению базовыми разрешениями для групп пользователей (раздел 3.3.1).
3. Выполните действия по управлению специальными разрешениями для групп пользователей (раздел 3.3.2).
4. Выполните действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей (раздел 3.3.3).

3 Выполнение лабораторной работы

3.1 Управление базовыми разрешениями

Открываем терминал с учётной записью root: su - (рис. 3.1).

Рис. 3.1: Открытие терминала с учетной записью root

В корневом каталоге создаём каталоги /data/main и /data/third командой: mkdir -p /data/main /data/third. (рис. 3.2).

Рис. 3.2: Создание каталогов

Посмотрим, кто является владельцем этих каталогов. Для этого используем: ls -Al /data. Владельцем каталогов является суперпользователь. (рис. 3.3).

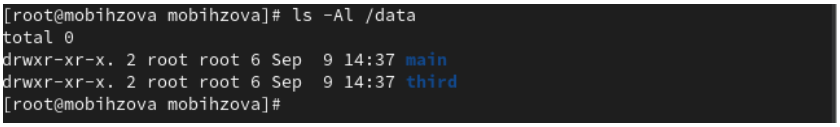

Рис. 3.3: Просмотр владельца каталогов

Прежде чем устанавливать разрешения, изменим владельцев этих каталогов с root на main и third соответственно: chgrp main /data/main и chgrp third /data/third. Теперь владельцем этих каталогов является main и third. (рис. 3.4).

Рис. 3.4: Изменение владельца каталогов

Далее установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам: chmod 770 /data/main и chmod 770 /data/third. После этого проверим права доступа. (рис. 3.5).

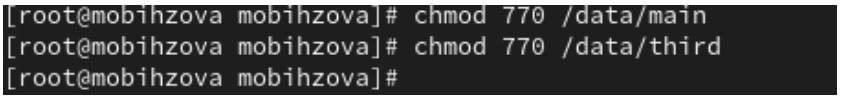

Рис. 3.5: Установка разрешений

В другом терминале перейдём под учётную запись пользователя bob: su - bob (рис. 3.6).

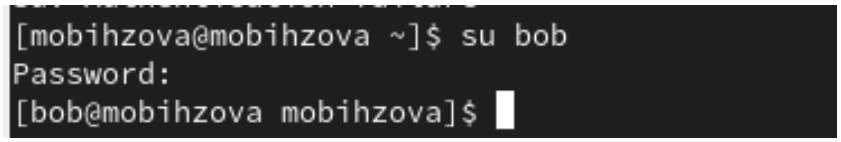

Рис. 3.6: Смена пользователя

Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге: cd /data/main и touch emptyfile. Так как пользователь bob является владельцем каталога main, нам удалось перейти в этот каталог и создать в нём новый файл. (рис. 3.7).

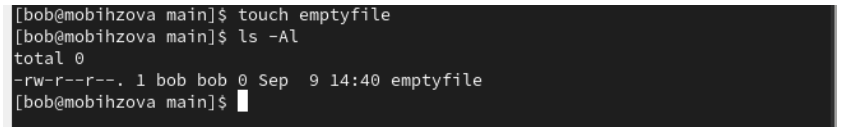

Рис. 3.7: Создание файла в каталоге

Теперь под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Так как пользователь bob не является вла-

дельцем каталога third, нам не удалось перейти в этот каталог и создать в нём новый файл (рис. 3.8).

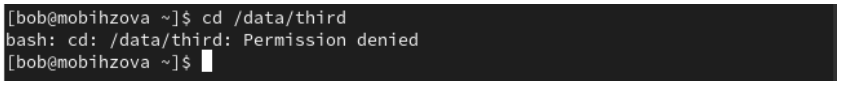

Рис. 3.8: Создание файла в каталоге

3.2 Управление специальными разрешениями

Откроем новый терминал под пользователем alice: su - alice (рис. 3.9).

Рис. 3.9: Смена пользователя

Перейдём в каталог /data/main: cd /data/main (рис. 3.10).

Рис. 3.10: Переход в каталог

В нём создадим два файла, владельцем которых является alice: touch alice1 и touch alice2 (рис. 3.11).

Рис. 3.11: Создание файлов в каталоге

В другом терминале, под учётной записью пользователя bob (пользователь bob является членом группы main, как и alice) (рис. 3.12).

Рис. 3.12: Смена пользователя

Перейдём в каталог /data/main: cd/data/main (данный каталог уже был открыт в нашем терминале) и в этом каталоге введём: ls. Мы увидим два файла, созданные пользователем alice. Теперь попробуем удалить файлы, принадлежащие пользователю alice командой: rm -f alice*. Убедимся, что файлы будут удалены пользователем bob (рис. 3.13).

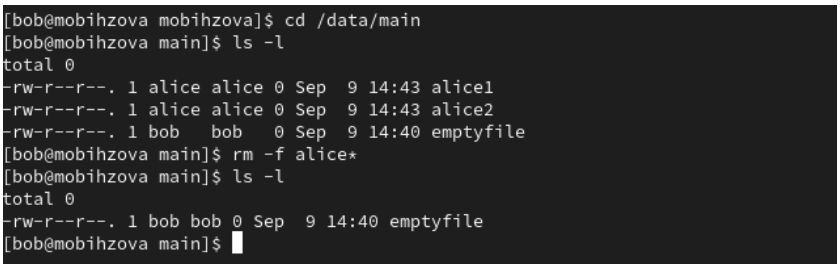

Рис. 3.13: Удаление файлов пользователем bob

После проверки командой ls создадим два файла, которые принадлежат пользователю bob: touch bob1 и touch bob2 (рис. 3.14).

Рис. 3.14: Создание файлов

В терминале под пользователем root установим для каталога /data/main бит идентификатор группы, а также stiky-бит для разделяемого (общего) каталога группы: chmod g+s,o+t /data/main (рис. 3.15).

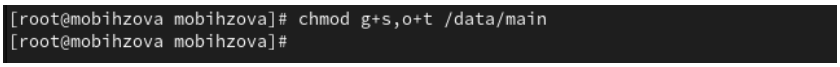

Рис. 3.15: Установка бит идентификатора группы, а также stiky-бита для разделяемого (общего) каталога группы

Переходим в терминал под пользователем alice и создаём в каталоге /data/main файлы alice3 и alice4: touch alice3 и touch alice4. Теперь мы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main: ls и ls -Al /data (рис. 3.16).

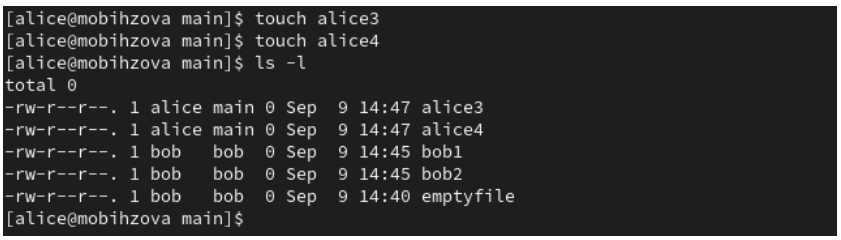

Рис. 3.16: Создание файлов в каталоге

В этом же терминале попробуем удалить файлы, принадлежащие пользователю bob: rm -rf bob*. Убедимся, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов (Operation not permitted) (рис. 3.17).

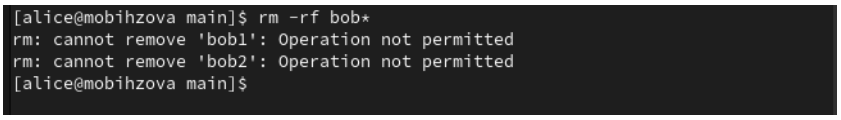

Рис. 3.17: Удаление файлов пользователем alice

3.3 Управление расширенными разрешениями с использованием списков ACL

Откроем терминал с учётной записью root (рис. 3.18).

Рис. 3.18: Смена пользователя

Установим 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:rx /data/main и setfacl -m g:main:rx /data/third (рис. 3.19).

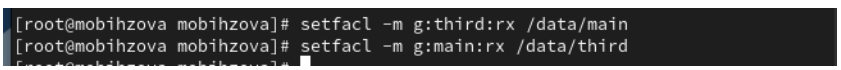

Рис. 3.19: Установка прав

Теперь используем команду getfacl, чтобы убедиться в правильности установки разрешений: getfacl /data/main и getfacl /data/third (рис. 3.20).

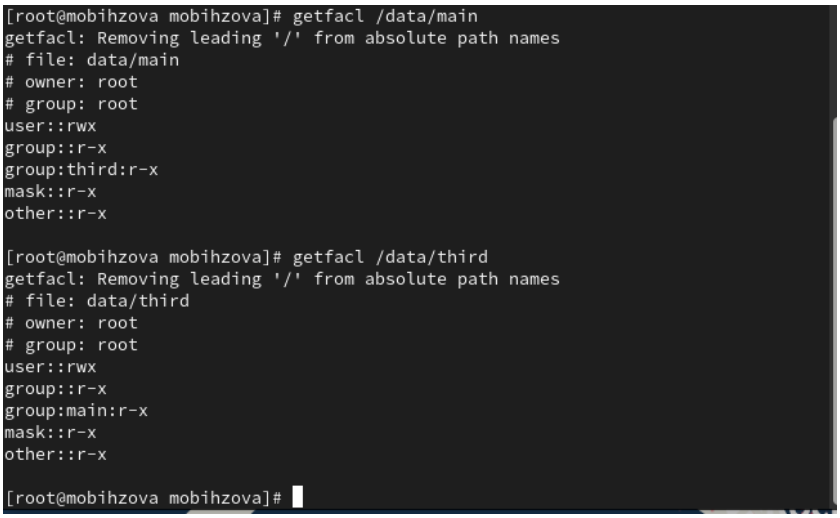

Рис. 3.20: Проверка правильности установки разрешений

Далее создадим новый файл с именем newfile1 в каталоге /data/main: touch /data/main/newfile1. Используем getfacl /data main/newfile1 для проверки текущих назначений полномочий. У пользователя только чтение и запись, у группы и других только чтение (рис. 3.21).

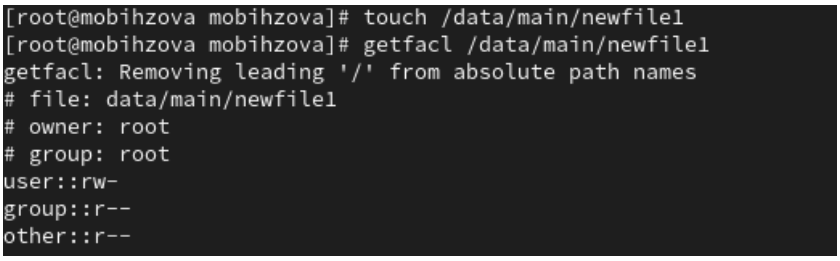

Рис. 3.21: Создание нового файла и проверка текущих назначенных полномочий

Выполним аналогичные действия для каталога /data/third. Видим, что ситуация аналогичная (рис. 3.22).

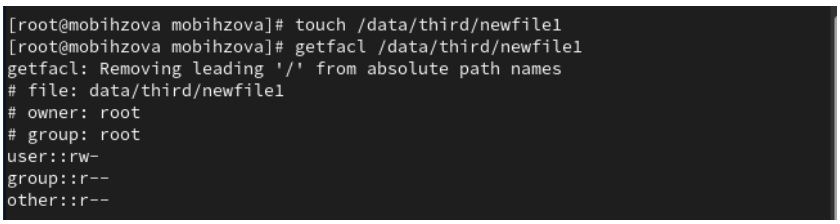

Рис. 3.22: Создание нового файла и проверка текущих назначенных полномочий

Установим ACL по умолчанию для каталога /data/main: setfacl -md:g:third:rwx /data/main и для каталога /data/third: setfacl -m d:g:main:rwx /data/third. (рис. 3.23, рис. 3.24).

Рис. 3.23: Установка ACL по умолчанию

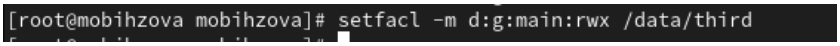

Рис. 3.24: Установка ACL по умолчанию

Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main: touch /data/main/newfile2. Используем getfacl /data/main/newfile2 для проверки текущих назначений полномочий. (рис. 3.25).

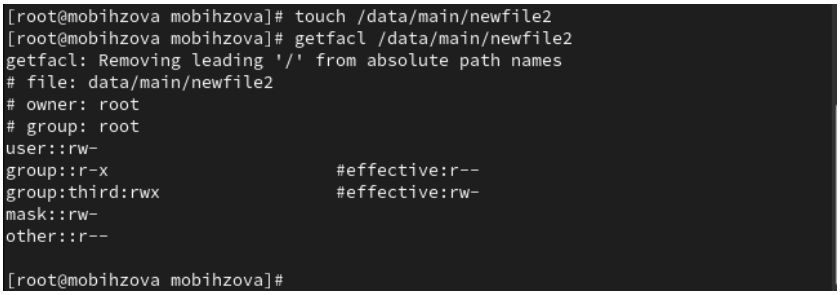

Рис. 3.25: Создание нового файла и проверка текущих назначенных полномочий

Выполним аналогичные действия для каталога /data/third (рис. 3.26).

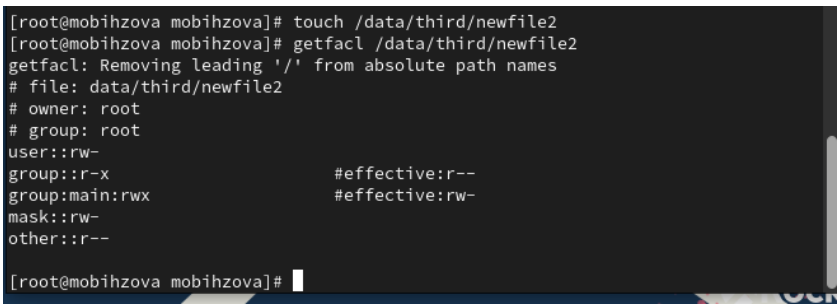

Рис. 3.26: Создание нового файла и проверка текущих назначенных полномочий

Для проверки полномочий группы third в каталоге /data/third войдём в другом терминале под учётной записью члена группы third: su – carol (рис. 3.27).

Рис. 3.27: Смена пользователя

Проверим операции с файлами: rm /data/main/newfile1 и rm /data/main/newfile2. Система не даёт удалить данные файлы (рис. 3.28).

Рис. 3.28: Удаление файлов пользователем carol

Теперь проверим, возможно ли осуществить запись в файл. В файл newfile1 запись осуществить не получилось, а вот в newfile2 всё выполнилось 3.29).

Рис. 3.29: Запись в файл пользователем carol

4 Ответы на контрольные вопросы

1. Как следует использовать команду chown, чтобы установить владельца группы для файла? Приведите пример. chown bob:main /data/third/newfile.

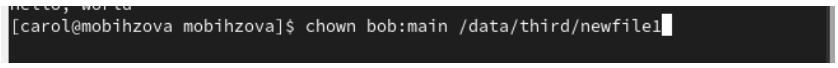

Рис. 4.1: Использование команды chown

2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример. find ~ -user bob -print.

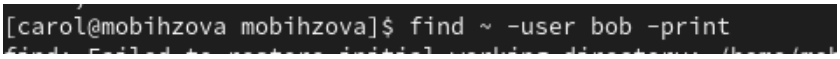

Рис. 4.2: Использование команды find

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 770.

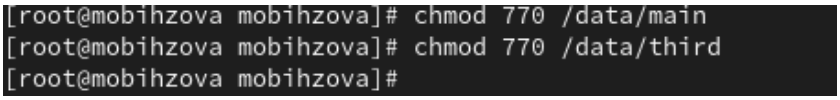

Рис. 4.3: chmod 770

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

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

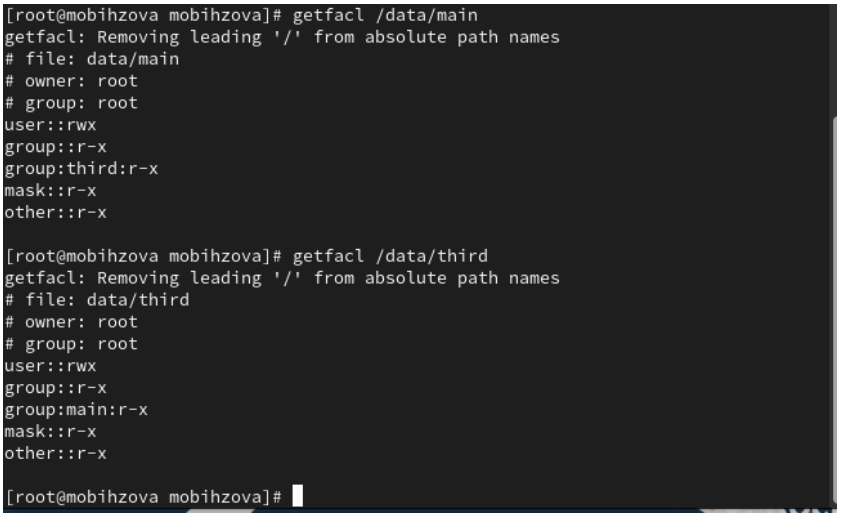

Рис. 4.4: Использование команды getfacl

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. chmod g+s,o+t /data/main.

Рис. 4.5: Использование команды chmod

7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге? setfacl -m g:group:r

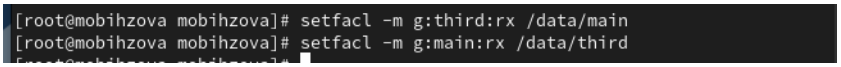

Рис. 4.6: Использование команды setfacl

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. setfacl -dm g:group:r /dir.

9. Какое значение umask нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример. 007.

10. Какая команда гарантирует, что никто не сможет удалить файл myfile случайно? sudo chattr +i myfile.

5 Выводы

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

Список литературы

1. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010.
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — (Системный администратор).
3. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — (Классика Computer Science).
4. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
5. Unix и Linux: руководство системного администратора / Э. Немет, Г. Снайдер, Т.Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.