Шаблон отчёта по лабораторной работе

Простейший вариант

Лупупа Чилеше

Содержание

# 1 Цель работы

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 Теоретическое введение

Основные права доступа в Linux в первую очередь определяются разрешениями для файлов и каталогов. Эти разрешения обычно представлены тремя наборами атрибутов rwx: Разрешения пользователя (u): применяются к владельцу файла/каталога. Групповые разрешения (g): применяются к членам группы файлов/каталогов. Другие разрешения (o): применить ко всем остальным пользователям. Каждому набору разрешений можно присвоить одно из трех значений: Чтение (r): позволяет просматривать содержимое файла или просматривать содержимое каталога. Запись (w): позволяет изменять содержимое файла или добавлять/удалять элементы в каталоге. Выполнить (x): позволяет выполнить файл или перейти в каталог. Эти разрешения объединяются в строку из 9 символов, первый символ которой представляет тип файла (например, - для обычного файла, d для каталога). Например, строка разрешения rw-r–r– указывает: Владелец имеет права на чтение/запись Группа имеет разрешения только на чтениеДругие имеют разрешения только на чтение

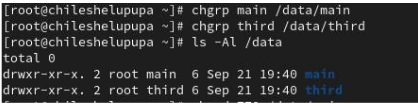
# 4 Выполнение лабораторной работы

1. Откройте терминал с учётной записью root:

su –

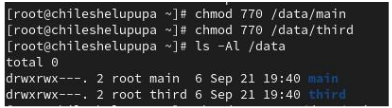
su –

1. 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 (рис. ??)



su –

1. 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



su –

1. 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.

su –

su –

1. В другом терминале перейдите под учётную запись пользователя bob su - bob

su –

su –

1. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталог cd /data/main touch emptyfile ls -Al

su –

su –

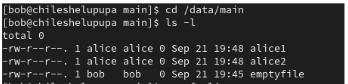
1. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.

su –

su –

##Управление специальными разрешениями

1. Откройте новый терминал под пользователем alice



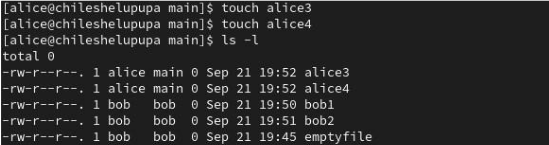
su –

1. Перейдите в каталог /data/main cd /data/main Создайте два файла, владельцем которых является alice: touch alice1 touch alice2

su –

su –

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



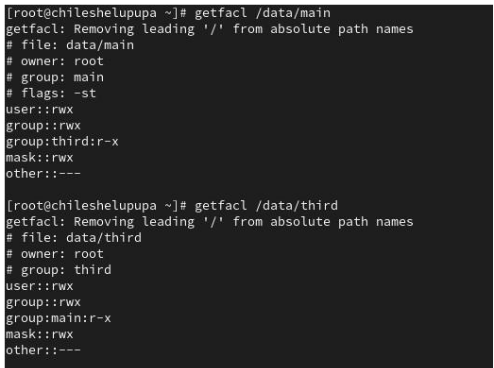
su –

1. Перейдите в каталог /data/main: cd /data/main и в этом каталоге введите: ls -l

su –

su –

1. Создайте два файла, которые принадлежат пользователю bob: touch bob1 touch bob2
2. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы: chmod g+s,o+t /data/main



su –

1. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4: touch alice3 touch alice4 ls -l

su –

su –

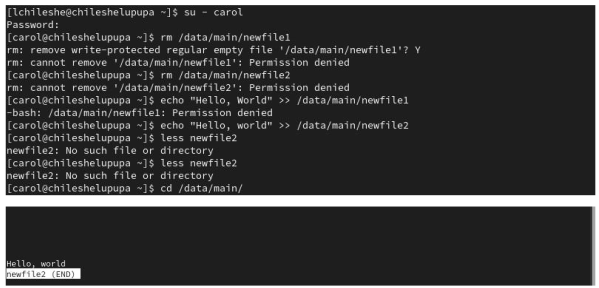
##Управление расширенными разрешениями с ##использованием списков ACL

1. Откройте терминал с учётной записью root su - y
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:rx /data/main setfacl -m g:main:rx /data/third

su –

su –

1. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений: getfacl /data/main getfacl /data/third



su –

1. Создайте новый файл с именем newfile1 в каталоге /data/main: touch /data/main/newfile1 Используйте getfacl /data/main/newfile1
2. Установите ACL по умолчанию для каталога /data/main: setfacl -m d:g:third:rwx /data/main
3. Добавьте ACL по умолчанию для каталога /data/third: setfacl -m d:g:main:rwx /data/third
4. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main: touch /data/main/newfile2
5. 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

# 5 Выводы

Я изучил получение функций для установки основных и специальных прав доступа для групп пользователей в таких системах, как Linux.