Отчёт по лабораторной работе №3

Артём Дмитриевич Петлин

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

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.

# 4. Выполнение лабораторной работы

|  |
| --- |
| Рисунок 1: data/main | third |

Открываем терминал с учётной записью root. В корневом каталоге создаём каталоги и смотрим, кто является владельцем этих каталогов. В корневом каталоге создаём каталоги и смотрим, кто является владельцем этих каталогов. Устанавливаем разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам, затем проверяем установленные права доступа.

|  |
| --- |
| Рисунок 2: bob |

В другом терминале переходим под учётную запись пользователя bob. Под пользователем bob пробуем перейти в каталог /data/main и создать файл в этом каталоге. Файл создается, так как пользователь bob находится в группе main. Под пользователем bob пробуем перейти в каталог /data/third и создать файл в этом каталоге. Перейти в каталог не вышло, так как bob не в группе third.

|  |
| --- |
| Рисунок 3: alice |

Открываем новый терминал под пользователем alice. Переходим в каталог /data/main и создаём два файла, владельцем которых является alice.

|  |
| --- |
| Рисунок 4: bob |

В другом терминале переходим под учётную запись пользователя bob. Переходим в каталог /data/main и видим два файла, созданные пользователем alice. Пробуем удалить файлы, принадлежащие пользователю alice, и убеждаемся, что файлы будут удалены пользователем bob. Создаём два файла, которые принадлежат пользователю bob.

|  |
| --- |
| Рисунок 5: sticky-бит |

В терминале под пользователем root устанавливаем для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого каталога группы.

|  |
| --- |
| Рисунок 6: alice |

В терминале под пользователем alice создаём в каталоге /data/main файлы и видим, что созданные файлы принадлежат группе, которая является группой-владельцем каталога.

|  |
| --- |
| Рисунок 7: not permitted |

В терминале под пользователем alice пробуем удалить файлы, принадлежащие пользователю bob, и убеждаемся, что sticky-bit предотвратит удаление этих файлов.

|  |
| --- |
| Рисунок 8: setfacl |

Открываем терминал с учётной записью root. Устанавливаем права на чтение и выполнение в каталоге /data/main для одной группы third и права на чтение и выполнение для другой группы main в соответствующем каталоге /data/third. Используем команду для просмотра прав, чтобы убедиться в правильности установки разрешений.

|  |
| --- |
| Рисунок 9: newfile1 |

Создаём новый файл newfile1 в каталоге /data/main и используем проверку текущих назначений полномочий. Выполняем аналогичные действия для другого каталога /data/third. Файлы newfile1 имеют только базовые права, то есть без унаследования ACL.

|  |
| --- |
| Рисунок 10: newfile2 |

Устанавливаем ACL по умолчанию для каталога /data/main. Добавляем ACL по умолчанию для каталога /data/third. Убеждаемся, что настройки ACL работают, добавив новый файл в каталог и проверив текущие назначения полномочий. Выполняем аналогичные действия для другого каталога.

|  |
| --- |
| Рисунок 11: carol |

Для проверки полномочий группы third в каталоге /data/main входим в другом терминале под учётной записью члена группы third. Проверяем операции с файлами и возможность осуществления записи в файл. Удалить newfile1 можно, так как нет защиты ACL, а дозаписать что-то в файл нельзя, так как нет права записи без унаследования прав ACL.

# 5. Выводы

Мы получили 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,
4. — (Классика Computer Science).
5. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Inde- pendent Publishing Platform, 2016.
6. Unix и Linux: руководство системного администратора / Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.