Лабораторная работа №4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Гудиева Мадина Куйраевна

Содержание

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

Теоретические сведения

Файлам и директориям могут быть установлены атрибуты, о которы помнят далеко не все пользователи. Файловые атрибуты могут использовать администраторы и пользователи для защиты файлов от случайных удалений и изменений, а также их применяют злоумышленники, делая невозможным удаление вредоносного файла. [1]

chattr — изменяет атрибуты файлов на файловых системах ext2fs, ext3, ext4 и частично на других файловых системах Linux.

Формат символьного режима: +-= атрибут.

- «+» обозначает добавление указанных атрибутов к существующим;
- «-» обозначает их снятие;
- «=» обозначает установку только этих атрибутов файлам. [2]

Различают следующие виды расширенных атрибутов.

1. Файл с установленным атрибутом «a» можно открыть только в режиме добавления для записи. Только суперпользователь или процесс, обладающий возможностью CAP_LINUX_IMMUTABLE, может установить или очистить этот атрибут.

- A. При доступе к файлу с установленным атрибутом «A» его запись atime не изменяется. Это позволяет избежать определённого количества дисковых операций ввода-вывода для портативных систем.

    3. Файл с установленным атрибутом «c» автоматически сжимается на диске ядром. При чтении из этого файла возвращаются несжатые данные. Запись в этот файл сжимает данные перед их сохранением на диске. Примечание: обязательно прочтите об ошибках и ограничениях в конце этого раздела. (Примечание: для btrfs: если установлен флаг «c», то нельзя установить флаг «C». Также конфликтует с параметром монтирования btrfs «nodatasum»)
- C. Файл с установленным атрибутом «C» не подлежит обновлению «копирование при записи». Этот флаг поддерживается только в файловых системах, которые выполняют копирование при записи. (Примечание: для btrfs флаг «C» должен быть установлен для новых или пустых файлов. Если он установлен для файла, который уже имеет блоки данных, он не определён, когда блоки, назначенные файлу, будут полностью стабильными. Если для каталога установлен флаг «C», он не повлияет на каталог, но для новых файлов, созданных в этом каталоге, будет установлен атрибут No_COW. Если установлен флаг «C», то флаг «c» не может быть установлен. установленный.)

4. Файл с установленным атрибутом «d» не является кандидатом для резервного копирования при запуске программы dump.

- D. При изменении каталога с установленным атрибутом «D» изменения синхронно записываются на диск; это эквивалентно опции монтирования dirsync, применяемой к подмножеству файлов.

5. Атрибут «e» указывает, что файл использует экстенты для отображения блоков на диске. Его нельзя удалить с помощью chattr.

- E. Файл, каталог или символическая ссылка с установленным атрибутом «E» зашифрованы файловой системой. Этот атрибут нельзя установить или сбросить с помощью chattr, хотя он может быть отображён с помощью lsattr.
- F. Директория с установленным атрибутом «F» указывает, что все поиски путей внутри этого каталога выполняются без учёта регистра. Этот атрибут можно изменить только в пустых каталогах в файловых системах с включённой функцией casefold.

1. Файл с атрибутом «i» не может быть изменён: его нельзя удалить или переименовать, нельзя создать ссылку на этот файл, большую часть метаданных файла нельзя изменить, и файл нельзя открыть в режиме записи. Только суперпользователь или процесс, обладающий возможностью CAP_LINUX_IMMUTABLE, может установить или очистить этот атрибут.

- I. Атрибут «I» используется кодом htree, чтобы указать, что каталог индексируется с использованием хешированных деревьев. Его нельзя установить или очистить с помощью chattr, хотя его можно отобразить с помощью lsattr.

10. Файл с атрибутом «j» имеет все данные, записанные в журнал ext3 или ext4 перед записью в сам файл, если файловая система смонтирована с параметрами «data=ordered» или «data=writeback» и файловая система имеет журнал. Если файловая система смонтирована с параметром «data=journal», все данные файла уже занесены в журнал, и этот атрибут не действует. Только суперпользователь или процесс, обладающий возможностью CAP_SYS_RESOURCE, может установить или очистить этот атрибут.
11. Файл с атрибутом «m» исключается из сжатия в файловых системах, которые поддерживают сжатие файлов.

- N. Файл с установленным атрибутом «N» указывает, что файл содержит данные, хранящиеся внутри самого inode. Его нельзя установить или очистить с помощью chattr, хотя его можно отобразить с помощью lsattr.
- P. Директория с установленным атрибутом «P» будет обеспечивать иерархическую структуру для идентификаторов проектов. Это означает, что файлы и каталоги, созданные в директории, будут наследовать идентификатор проекта каталога, операции переименования ограничены, поэтому, когда файл или каталог перемещается в другой каталог, идентификаторы проекта должны совпадать. Кроме того, жёсткая ссылка на файл может быть создана только в том случае, если идентификатор проекта для файла и целевой каталог совпадают.

19. Когда файл с установленным атрибутом «s» удаляется, его блоки обнуляются и записываются обратно на диск. Примечание: обязательно прочтите об ошибках и ограничениях в конце этого раздела.

- S. При изменении файла с установленным атрибутом «S» изменения синхронно записываются на диск; это эквивалентно опции монтирования «sync», применяемой к подмножеству файлов.

20. Файл с атрибутом «t» не будет иметь фрагмент частичного блока в конце файла, объединённого с другими файлами (для тех файловых систем, которые поддерживают

объединение хвостов).

- T. Директория с атрибутом «T» будет считаться вершиной иерархии каталогов для целей распределителя блоков Орлова. Это подсказка распределителю блоков, используемому ext3 и ext4, что подкаталоги в этом каталоге не связаны и, следовательно, должны быть разделены для целей распределения. Например, очень хорошая идея установить атрибут «T» в каталоге /home, чтобы /home/john и /home/mary были помещены в отдельные группы блоков. Для каталогов, где этот атрибут не установлен, распределитель блоков Орлова будет пытаться сгруппировать подкаталоги ближе друг к другу, где это возможно.

21. Когда файл с установленным атрибутом «u» удаляется, его содержимое сохраняется. Это позволяет пользователю запрашивать его восстановление. Примечание: обязательно прочтите об ошибках и ограничениях в конце этого раздел.
22. Атрибут «x» может быть установлен для каталога или файла. Если атрибут установлен в существующем каталоге, он будет унаследован всеми файлами и подкаталогами, которые впоследствии будут созданы в каталоге. Если существующий каталог содержал некоторые файлы и подкаталоги, изменение атрибута в родительском каталоге не изменяет атрибуты этих файлов и подкаталогов.

- V. Для файла с установленным атрибутом «V» включена функция проверки подлинности. Он не может быть записан, и файловая система будет автоматически проверять все данные, считанные из неё, по криптографическому хешу, который покрывает всё содержимое файла, например через дерево Меркла. Это позволяет эффективно аутентифицировать файл. Этот атрибут нельзя установить или сбросить с помощью chattr, хотя он может быть отображён с помощью lsattr. [1]

Выполнение лабораторной работы

1. От имени пользователя guest определила расширенные атрибуты файла ‘/home/guest/dir1/file1’ (fig. 1).

```
[guest@gudievamadina dir1]$ lsattr /home/guest/dir1/file1
---------------- /home/guest/dir1/file1
```

Figure 1: Расширенные атрибуты файла ‘/home/guest/dir1/file1’

2. Установила на файл file1 права, разрешающие чтение и запись для владельца файла (fig. 2).

```
[guest@gudievamadina dir1]$ chmod 600 file1
[guest@gudievamadina dir1]$ lsattr /home/guest/dir1/file1
---------------- /home/guest/dir1/file1
[guest@gudievamadina dir1]$ ls -l file1
-rw-------. 1 guest guest 0 сен 29 22:16 file1
```

Figure 2: Смена прав файла ‘/home/guest/dir1/file1’

3. Попробовала установить на файл /home/guest/dir1/file1 расширенный атрибут ‘a’ от имени пользователя guest. Получила отказ от выполнения операции (fig. 3).

```
[guest@gudievamadina dir1]$ chattr +a /home/guest/dir1/file1
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1
```

Figure 3: Попытка смены расширенного атрибута файла ‘/home/guest/dir1/file1’

4. Зашла на другую консоль с правами администратора. Попробовала установить расширенный атрибут ‘a’ на файл /home/guest/dir1/file1 от имени суперпользователя (fig. 4).

```
[guest@gudievamadina dir1]$ su -
Пароль:
[root@gudievamadina ~]# chattr +a /home/guest/dir1/file1
```

Figure 4: Смена расширенного атрибута файла '/home/guest/dir1/file1'

5. От пользователя guest проверила правильность установления атрибута (fig. 5).

```
[guest@gudievamadina dir1]$ lsattr /home/guest/dir1/file1
-----a---------- /home/guest/dir1/file1
```

Figure 5: Проверка правильности смены расширенного атрибута файла '/home/guest/dir1/file1'

6. Выполнила дозапись в файл file1 слова «test», убедилась, что слово 'test' было успешно записано (fig. 6).

```
[guest@gudievamadina dir1]$ echo "test" >> /home/guest/dir1/file1
[guest@gudievamadina dir1]$ cat /home/guest/dir1/file1
test
```

Figure 6: Дозапись слова 'test' в файл '/home/guest/dir1/file1'

7. Попробовала удалить файл file1, стереть имеющуюся в нём информацию, переименовать, а также сменить права на файл. Получила отказ (fig. 7).

```
[guest@gudievamadina dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Операция не позволена
[guest@gudievamadina dir1]$ mv file1 file2
mv: невозможно переместить «file1» в «file2»: Операция не позволена
[guest@gudievamadina dir1]$ chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
```

Figure 7: Отказ на команды при расширенном атрибуте 'a'

8. Сняла расширенный атрибут 'a' с файла '/home/guest/dir1/file1' и повторила проделанные ранее команды. Всё прошло успешно (fig. 8, fig. 9).

```
[guest@gudievamadina dir1]$ su
Пароль:
[root@gudievamadina dir1]# chattr -a /home/guest/dir1/file1
```

Figure 8: Снятие расширенного атрибута 'a'

```
[guest@gudievamadina dir1]$ echo "abcd" > /home/guest/dir1/file1
[guest@gudievamadina dir1]$ mv file1 file2
[guest@gudievamadina dir1]$ chmod 000 file1
chmod: невозможно получить доступ к «file1»: Нет такого файла или каталога
[guest@gudievamadina dir1]$ chmod 000 file2
```

Figure 9: Успешное повторное выполнение команд

9. Установила расширенный атрибут 'i' на файл /home/guest/dir1/file1 от имени суперпользователя. Повторила проделанные ранее команды. В данном случае не удалось даже дозаписать в файл. Таким образом я получила отказ на выполнение всех команд (fig. 10, fig. 11).

```
[root@gudievamadina dir1]# chattr +i /home/guest/dir1/file1
[root@gudievamadina dir1]# exit
exit
[guest@gudievamadina dir1]$ lsattr file1
----i----------- file1
[guest@gudievamadina dir1]$ cat file1
test
[guest@gudievamadina dir1]$ echo "test2" >> file1
bash: file1: Отказано в доступе
[guest@gudievamadina dir1]$ echo "abcd" >> file1
bash: file1: Отказано в доступе
[guest@gudievamadina dir1]$ mv file1 file2
mv: невозможно переместить «file1» в «file2»: Операция не позволена
[guest@gudievamadina dir1]$ rm file1
rm: удалить защищенный от записи обычный файл «file1»? y
rm: невозможно удалить «file1»: Операция не позволена
[guest@gudievamadina dir1]$ chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
[guest@gudievamadina dir1]$
```

Figure 10: Установка расширенного атрибута 'i'

Выводы

Таким образом я успешно приобрела практические навыки работы в консоли с расширенными атрибутами файлов.

Список литературы

1. Атрибуты файлов в Linux. // ZaLinux.ru. 2021. URL: https://zalinux.ru/?p=6440 (дата обращения 30.10.2021).
2. Изменение атрибутов (флагов) на файлах в Unix/Linux. // linux-notes.com. 2015. URL: https://linux-notes.org/izmenenie-atributov-flagov-na-fajlah-v-unix-linux/ (дата обращения 30.10.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..