Лабораторная работа № 2

Дискреционное разграничение прав в Linux. Основные атрибуты.

Алибаева Данагуль НБибд-01-18

Содержание

# Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (использую учётную запись администратора)
2. Задайте пароль для пользователя guest (использую учётную запись администратора)
3. Войдите в систему от имени пользователя guest.
4. Определите директорию, в которой вы находитесь, командой pwd.
5. Уточните имя вашего пользователя командой whoami.
6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь.
7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.
8. Определите uid пользователя. Определите gid пользователя.
9. Определите существующие в системе директории.
10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home.
11. Создайте в домашней директории поддиректорию dir1.
12. Снимите с директории dir1 все атрибуты dir1 и проверьте её.
13. Попытайтесь создать в директории dir1 файл file1.
14. Заполните таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».
15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните таблицу.

# Теоретическое введение

Атрибуты файла - это набор из девяти основных битов. Определяющих какие из пользователей обладают правами на чтение, запись, а также запуск файлов для выполнения. Данный набор формирует код, называемый режимом доступа к файлу/каталогу. Первые три бита определяют права доступа для владельца. Следующие — для группы пользователей, к которой относится файл и последние три бита — права доступа для всех остальных пользователей в системе. [1]

Существует также ещё четыре дополнительных бита. Которые определяют тип самого файла и задаются непосредственно при создании файла. С помощью команды chmod можно менять основные (и некоторые дополнительные) биты режима доступа. Сделать это может только владелец файла или суперпользователь. Просматривать атрибуты (в том числе и режимы доступа) позволяет команда ls. Таким образом, характер поведения ФС, а также распределение доступа и управление им полностью определяется атрибутами файлов. Которые хранит сама ФС — это самодостаточный и универсальный подход. [1]

Для записи кода режима доступа используется восьмеричная запись чисел. Как уже было отмечено, код доступа содержит три «триады» битов — для пользователя, группы и всех остальных, именно в таком порядке. Битам из первой триады соответствуют значения в восьмеричной записи 400, 200 и 100. Для второй триады (т. е. для группы) — 40, 20 и 10. Наконец, для третьей (все остальные) — 4, 2 и 1. В свою очередь, первому биту в каждой триаде соответствует доступ на чтение (r — «read»). Второму — на запись (w — «write») и третьему — на выполнение, т. е. x — «execute». [1]

Установка бита чтения (r) в одной из триад (или во всех) задаёт право открывать данный файл для чтения соответствующим категориям пользователей. Наличие бита записи (w) позволяет изменять файл. При этом возможно его удаление и/или переименование файла, но только в том случае, если заданы соответствующие биты для его родительского каталога, поскольку именно в его записях хранятся имена файлов. [1]

# Выполнение лабораторной работы

1.Лабораторная работа выполнялась дома со следующими характеристиками техники:

– Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz, 2304 МГц, ядер: 4, логических процессоров: 8

– ОС Майкрософт Windows 10 Pro

– VirtualBox верс. 6.1.26

1. В установленной при выполнении предыдущей лабораторной работы операционной системе запустила терминал и перешла под учетную запись root с помощью команды su (рис. 1)

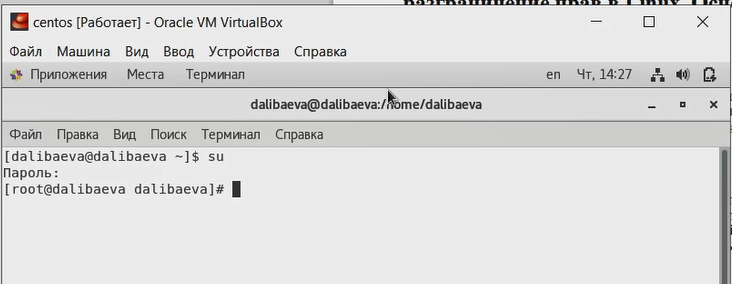


Figure 1: Переход под учетную запись root

1. Создала учётную запись пользователя guest (используя учётную запись администратора): с помощью команды useradd guest (рис. 2)

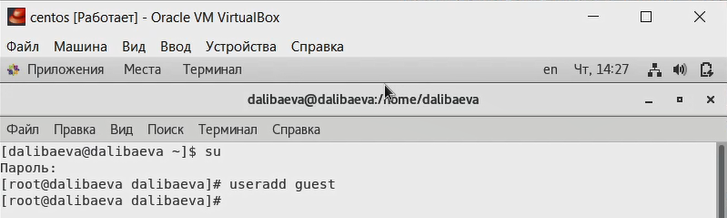


Figure 2: Создание учетной записи пользователя guest

1. Задала пароль для пользователя guest (используя учётную запись администратора): passwd guest (рис. 3)

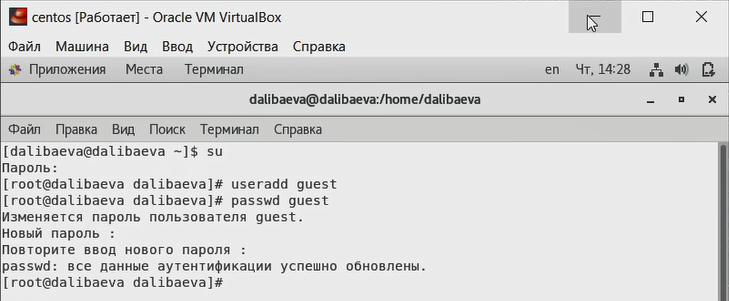


Figure 3: Задание пароля для пользователя guest

1. Вошла в систему от имени пользователя guest (рис. 4)

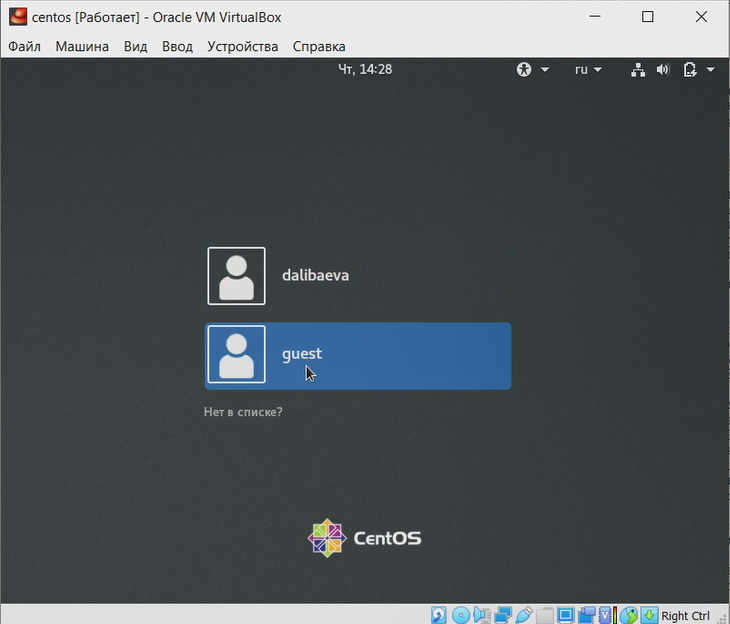


Figure 4: Вход в систему от имени пользователя guest

1. Определила директорию, в которой я нахожусь, командой pwd. Определила, что она является моей домашней директорией (рис. 5)

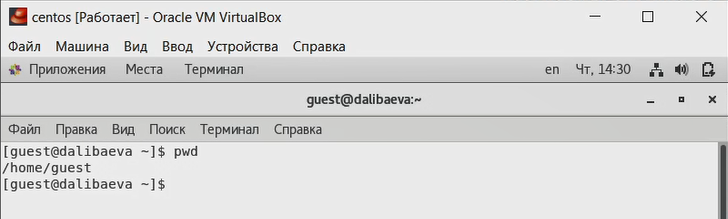


Figure 5: Определение директории

1. Уточнила имя пользователя командой whoami (рис. 6)

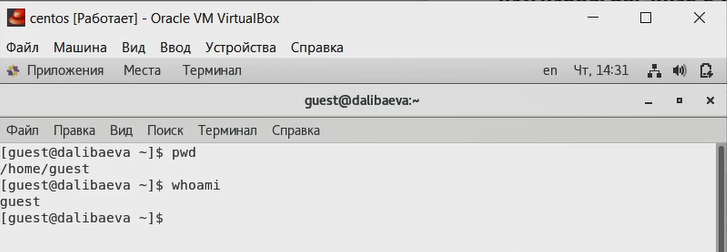


Figure 6: Уточнение имени пользователя

1. Уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Сравнила вывод id с выводом команды groups. Команда groups выводит нам только название группы (рис. 7)

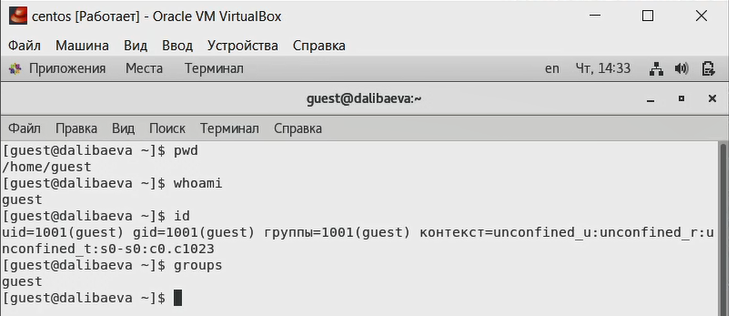


Figure 7: Уточнение группы имени пользователя

1. Сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. В командной строке у нас выводится еще и имя пользователя.
2. Просмотрела файл /etc/passwd командой cat /etc/passwd (рис. 8). Нашла в нём свою учётную запись (рис. 9). Определила uid пользователя, который равен 1001. Определила gid пользователя, который равен 1001. Сравнила найденные значения с полученными в предыдущих пунктах и сделала вывод, что они равны.

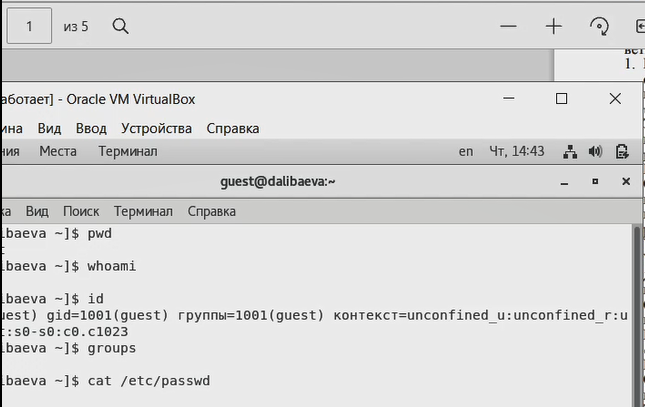


Figure 8: Просмотр файла /etc/passwd

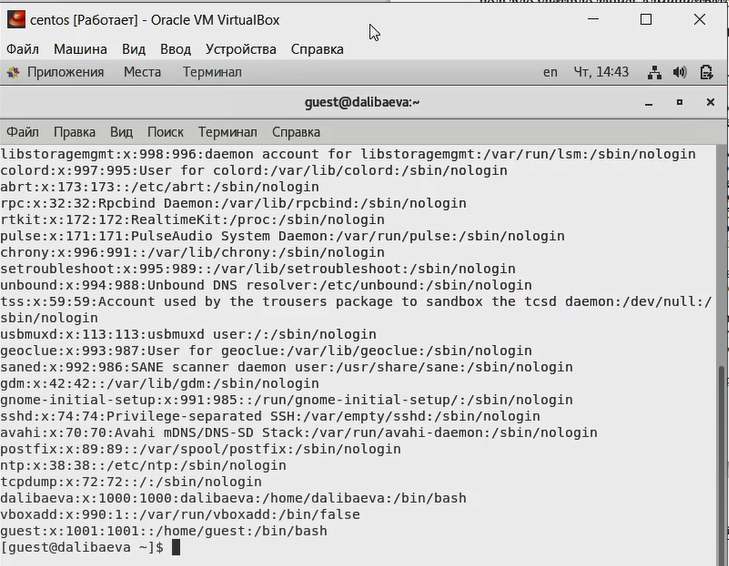


Figure 9: Поиск учетной записи

1. Определила существующие в системе директории командой ls -l /home/. Это dalibaeva и guest (рис. 10). На директориях установлены полные права у владельца. Это чтение, запись и запуск директории. У группы и остальных пользователей нет никаких прав.



Figure 10: Определение существующих директорий

1. Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home. Мне удалось увидеть расширенные атрибуты поддиректории guest, но не dalibaeva (рис. 11).

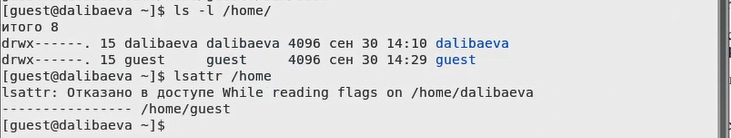


Figure 11: Расширенные атрибуты на поддиректориях

1. Создала в домашней директории поддиректорию dir1 командой mkdir dir1 (рис. 12). Определила, командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис. 13). Владельцу выставлены полные права доступа (чтение, запись, запуск директории), группе пользователей – полные права, остальным пользователям – только чтение и запуск. На директорию dir1 не выставлено никаких расширенных атрибутов.

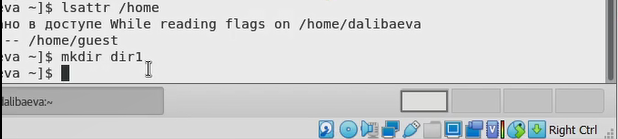


Figure 12: Создание поддиректории dir1

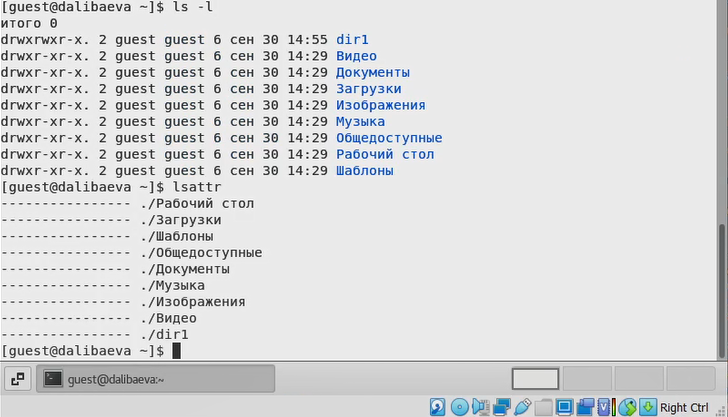


Figure 13: Определение прав доступа и расширенных атрибутов

1. Сняла с директории dir1 все атрибуты командой chmod 000 dir1 и проверила с её помощью правильность выполнения команды ls -l (рис. 14).

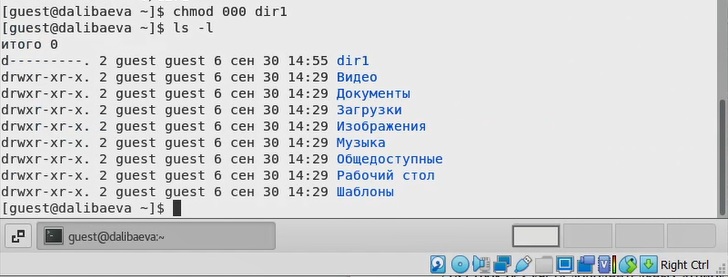


Figure 14: Снятие атрибутов

1. Попыталась создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 (рис. 15). При попытке, я получила отказ в доступе, так как в прошлом пункте убрала владельцу права доступа на запись. Сообщение об ошибке никак не отразилось на создании файла. Попыталась проверить командой ls -l /home/guest/dir1, находится ли файл file1 внутри директории dir1, но мне было отказано в доступе (рис. 15).

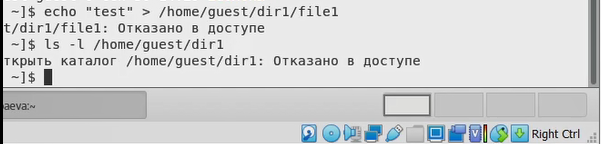


Figure 15: Попытка создания файла

1. Заполнила таблицу «Установленные права и разрешённые действия» (см. табл. 1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».
2. На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнила табл. 2.2 (см. табл. 2).

Table 1: Установленные права и разрешённые действия

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| d— (000) | — (000) | - | - | - | - | - | - | - | - |
| d— (000) | –x (100) | - | - | - | - | - | - | - | - |
| d— (000) | -w- (200) | - | - | - | - | - | - | - | - |
| d— (000) | -wx (300) | - | - | - | - | - | - | - | - |
| d— (000) | r– (400) | - | - | - | - | - | - | - | - |
| d— (000) | r-x (500) | - | - | - | - | - | - | - | - |
| d— (000) | rw- (600) | - | - | - | - | - | - | - | - |
| d— (000) | rwx (700) | - | - | - | - | - | - | - | - |
| d–x (100) | — (000) | - | - | - | - | + | - | - | + |
| d–x (100) | –x (100) | - | - | - | - | + | - | - | + |
| d–x (100) | -w- (200) | - | - | + | - | + | - | - | + |
| d–x (100) | -wx (300) | - | - | + | - | + | - | - | + |
| d–x (100) | r– (400) | - | - | - | + | + | - | - | + |
| d–x (100) | r-x (500) | - | - | - | + | + | - | - | + |
| d–x (100) | rw- (600) | - | - | + | + | + | - | - | + |
| d–x (100) | rwx (700) | - | - | + | + | + | - | - | + |
| d-w- (200) | — (000) | - | - | - | - | - | - | - | - |
| d-w- (200) | –x (100) | - | - | - | - | - | - | - | - |
| d-w- (200) | -w- (200) | - | - | - | - | - | - | - | - |
| d-w- (200) | -wx (300) | - | - | - | - | - | - | - | - |
| d-w- (200) | r– (400) | - | - | - | - | - | - | - | - |
| d-w- (200) | r-x (500) | - | - | - | - | - | - | - | - |
| d-w- (200) | rw- (600) | - | - | - | - | - | - | - | - |
| d-w- (200) | rwx (700) | - | - | - | - | - | - | - | - |
| d-wx (300) | — (000) | + | + | - | - | + | - | + | + |
| d-wx (300) | –x (100) | + | + | - | - | + | - | + | + |
| d-wx (300) | -w- (200) | + | + | + | - | + | - | + | + |
| d-wx (300) | -wx (300) | + | + | + | - | + | - | + | + |
| d-wx (300) | r– (400) | + | + | - | + | + | - | + | + |
| d-wx (300) | r-x (500) | + | + | - | + | + | - | + | + |
| d-wx (300) | rw- (600) | + | + | + | + | + | - | + | + |
| d-wx (300) | rwx (700) | + | + | + | + | + | - | + | + |
| dr– (400) | — (000) | - | - | - | - | - | + | - | - |
| dr– (400) | –x (100) | - | - | - | - | - | + | - | - |
| dr– (400) | -w- (200) | - | - | - | - | - | + | - | - |
| dr– (400) | -wx (300) | - | - | - | - | - | + | - | - |
| dr– (400) | r– (400) | - | - | - | - | - | + | - | - |
| dr– (400) | r-x (500) | - | - | - | - | - | + | - | - |
| dr– (400) | rw- (600) | - | - | - | - | - | + | - | - |
| dr– (400) | rwx (700) | - | - | - | - | - | + | - | - |
| dr-x (500) | — (000) | - | - | - | - | + | + | - | + |
| dr-x (500) | –x (100) | - | - | - | - | + | + | - | + |
| dr-x (500) | -w- (200) | - | - | + | - | + | + | - | + |
| dr-x (500) | -wx (300) | - | - | + | - | + | + | - | + |
| dr-x (500) | r– (400) | - | - | - | + | + | + | - | + |
| dr-x (500) | r-x (500) | - | - | - | + | + | + | - | + |
| dr-x (500) | rw- (600) | - | - | + | + | + | + | - | + |
| dr-x (500) | rwx (700) | - | - | + | + | + | + | - | + |
| drw- (600) | — (000) | - | - | - | - | - | + | - | - |
| drw- (600) | –x (100) | - | - | - | - | - | + | - | - |
| drw- (600) | -w- (200) | - | - | - | - | - | + | - | - |
| drw- (600) | -wx (300) | - | - | - | - | - | + | - | - |
| drw- (600) | r– (400) | - | - | - | - | - | + | - | - |
| drw- (600) | r-x (500) | - | - | - | - | - | + | - | - |
| drw- (600) | rw- (600) | - | - | - | - | - | + | - | - |
| drw- (600) | rwx (700) | - | - | - | - | - | + | - | - |
| drwx (700) | — (000) | + | + | - | - | + | + | + | + |
| drwx (700) | –x (100) | + | + | - | - | + | + | + | + |
| drwx (700) | -w- (200) | + | + | + | - | + | + | + | + |
| drwx (700) | -wx (300) | + | + | + | - | + | + | + | + |
| drwx (700) | r– (400) | + | + | - | + | + | + | + | + |
| drwx (700) | r-x (500) | + | + | - | + | + | + | + | + |
| drwx (700) | rw- (600) | + | + | + | + | + | + | + | + |
| drwx (700) | rwx (700) | + | + | + | + | + | + | + | + |

Table 2: Минимальные права для совершения операций

|  |  |  |
| --- | --- | --- |
| Операция | Минимальные права на директорию | Минимальные права на файл |
| Создание файла | (300) | (000) |
| Удаление файла | (300) | (000) |
| Чтение файла | (100) | (400) |
| Запись в файл | (100) | (200) |
| Переименование файла | (300) | (000) |
| Создание поддиректории | (300) | (000) |
| Удаление поддиректории | (300) | (000) |

# Выводы

Получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Список литературы

1. Атрибуты файлов в Linux // URL: https://itproffi.ru/atributy-fajlov-v-linux/ (дата обращения: 01.10.2021).