ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8. «УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА»

Теоретическая часть

Разграничение прав доступа в ОС Red Hat Linux обусловлено многозадачностью и многопользовательским режимом ОС и призвано повысить безопасность и надежность системы, а также обеспечить защиту конфиденциальной информации.

Каждый файл характеризуется набором атрибутов, определяющих его принадлежность и права доступа. Отношение принадлежности файла определено для:

владельца файла(user) - пользователя, создавшего этот файл;

группы (group) - в состав которой входит владелец;

прочих (other) пользователей.

К правам доступа относятся: чтение (read), изменение (write), исполнение (execute). Понимание этих прав будет различным и зависеть от содержания файла. Наибольшие различия - между обычными (regular) файлами и каталогами. Эти различия приведены в табл. 1.

	Файлы	**Каталоги**
Чтение	Просмотр содержимого файла (например, текста) в соответствующей программе и возможность его копирования	Обзор списка файлов и возможность копирования каталога (в общем случае, вместе со всем содержимым)
Изменение	Редактирование содержимого файла и его копирование, но не удаление или переименование/перемещение	Обеспечивает возможность записи и удаления файлов
Исполнение	Разрешает запуск программ и сценариев оболочки	Разрешает переход в каталог и перемещение по нему

Атрибуты файла могут быть представлены в символьном

или числовом виде. Символьное представление атрибутов - это строка, где последовательно записаны права доступа в следующем виде:

rwxrwxrwx

где каждая тройка символов определяет права на чтение (**r**), запись (**w**) и исполнение (**x**) для соответствующих пользователей (первая тройка - для владельца (**u**ser), вторая - для группы (**g**roup), третья - для прочих (**o**ther)).

Вот пример отображения списка файлов с правами доступа, представленными в символьном виде:

```
aag@stilo:~> dir -L1
итого 2722316
-rw-r--r-- 1 aag users 498444757 Ноя 27 16:15 aag.asoiu.tar.gz
drwxr-xr-x 2 aag users 4096 Июн 1 2007 bin
-rw-r--r-- 1 aag users 26 Фев 20 10:20 description.txt
drwxr-xr-x 5 aag users 4096 Мар 2 20:01 Desktop
drwx------ 2 aag users 4096 Фев 23 09:50 Documents
drwxr-xr-x 4 aag users 4096 Фев 28 00:03 downloads
-rwxrwxr-x 1 aag users 7523 Окт 20 2006 Dz19.jpg
-rw-r--r-- 1 aag users 8336 Фев 24 01:12 httpd.myconf
-rw-r--r-- 1 aag users 20 Фев 25 16:32 index.html
-rw-r--r-- 1 aag users 30296 Фев 23 10:05 logofish.xcf
drwxr-xr-x 2 aag users 4096 Сен 28 22:53 Music
drwxr-xr-x 3 aag users 4096 Дек 3 13:45 Projects
drwxr-xr-x 4 aag users 4096 Фев 26 00:05 public_html
-rw-r--r-- 1 aag users 1088 Фев 20 10:18 readme.txt
drwxr-xr-x 4 aag users 4096 Фев 27 23:41 scrapbook
-rw------- 1 root root 0 Июн 2 2007 session_mm_cli0.sem
```

Обратите внимание на первые символы в записи прав доступа. В приведенном листинге первый символ **d** указывает, что файл является каталогом. Признаком специального символьного и блочного устройств являются символы **c** и **b**, а для каналов (pipes) соответственно **p**.

Числовое представление прав доступа - это трехзначное число, каждая цифра которого определяет (слева направо) права для владельца, группы и прочих. Права определяются как сумма цифр 4 (чтение), 2 (запись) и 1 (исполнение). Таким образом, например файл, разрешенный для чтения и изменения членам группы и только чтение всем прочим, будет иметь следующие атрибуты:

- в символьном виде: *rw-rw-r—*
- в числовом виде: *664*.

Вновь создаваемый файл обычно получает права rw-r--r-- (зависит от установок системы и значения umask). Для изменения атрибутов используется команда chmod, которая может принимать как символьное, так и числовое представление атрибутов в качестве параметра. Ниже приведены примеры использования команды:

aag@stilo:~> dir hello.txt

-rw-r--r-- 1 aag users 17 Map 2 22:32 hello.txt

aag@stilo:~> chmod **go+w** hello.txt // *разрешить запись для группы и прочих*

aag@stilo:~> dir hello.txt

-rw-rw-rw- 1 aag users 17 Map 2 22:32 hello.txt

aag@stilo:~> chmod **ug+x** hello.txt // *разрешить выполнение для владельца и группы*

aag@stilo:~> dir hello.txt

-rwxrwxrw- 1 aag users 17 Map 2 22:32 hello.txt

aag@stilo:~> chmod **a-x** hello.txt // *запретить выполнение для всех (**a** == ugo)*

aag@stilo:~> dir hello.txt

-rw-rw-rw- 1 aag users 17 Map 2 22:32 hello.txt

aag@stilo:~> chmod **go-w** hello.txt // *запретить запись для группы и прочих*

aag@stilo:~> dir hello.txt

-rw-r--r-- 1 aag users 17 Map 2 22:32 hello.txt

aag@stilo:~> chmod **755** hello.txt // *разрешить чтение и выполнение всем и запись владельцу*

aag@stilo:~> dir hello.txt

-rwxr-xr-x 1 aag users 17 Map 2 22:32 hello.txt

aag@stilo:~> chmod **644** hello.txt // *запретить выполнение всем*

aag@stilo:~> dir hello.txt

-rw-r--r-- 1 aag users 17 Map 2 22:32 hello.txt

aag@stilo:~> chmod **711** hello.txt // *разрешить только выполнение для группы и прочих*

aag@stilo:~> dir hello.txt

-rwx--x--x 1 aag users 17 Map 2 22:32 hello.txt

Для смены владельца файла и группы используется команда chown, а для смены группы - команда chgrp.

Задания для самостоятельной работы

1. Войти в систему с собственной учетной записью.

2. Создать в домашнем каталоге 2-3 файла произвольного содержания (имена файлов - u1, u2, u3).

3. Получить развернутый список файлов домашнего каталога и сохранить его в файле listing1.

4. Просмотреть файл listing1, обратив внимание на поля прав доступа, владельца и группы.

5. Повторить п. 2 от имени пользователя root в новом сеансе или по команде su (имена файлов - r1, r2, r3). Завершить сеанс root.

6. Повторить п.3, результат дописать в файл listing1.

7. Открыть файл listing1 и сравнить права доступа для файлов, созданных от вашего имени и от имени суперпользователя.

8. Изменить содержимое файлов, созданных вами и суперпользователем. Сохранить изменения.

9. В tty2 открыть сеанс root.

10. Перейти в каталог /home/ваша_учетная_запись.

11. Изменить права доступа к файлам u1 и r1 следующим образом:

u1: запретить запись для владельца и группы;

r1: разрешить запись для всех.

12. Переключиться в tty1 и изменить содержимое файлов u1 и r1. Сохранить изменения.

13. Перейти в tty2 и изменить владельца файлов u1 и u2 на root,а группу на stud.

14. Из tty1 попробовать изменить файл u2.

15. В tty1 создать файл hello следующего содержания

```
#! /bin/sh
echo Hello, World!
echo -n "I'm "
whoami.
```

16. Выполнить следующие действия и проанализировать результаты:

набрать в командной строке имя файла hello и нажать Enter;

набрать в командной строке sh hello и нажать Enter;

установить для файла hello права на исполнение (x), ввести имя файла в командной строке (./hello) и нажать Enter.

17. Из tty2 создать каталоги /home/shared, home/shared/pub, /home/shared/upload, /home/shared/temp. Установить на них следующие права:

каталог	владелец	группа	права
pub	root	users	775
upload	nobody	users	130
temp	stud	users	777

18. Выполнить копирование, чтение, удаление файлов u1, u2, u3, r1, r2, r3 в каталоги, созданные в п. 17 из сеансов root, stud и вашего. Сравнить и проанализировать результаты.

19. Завершить все сеансы.

Контрольные вопросы

1. Что относят к права доступа?
2. В каком виде могут быть представлены атрибуты файла?
3. Какая команда используется для смены владельца файла и группы?