Лабораторная работа № 15

Тема: " Выполнение администрирования пользователей ОС Linux"

Цель: Изучить возможности Linux при работе с пользователями и управлении правами доступа.

Теоретическая часть

Работа с пользователями

Linux - это многопользовательская операционная система. Каждый пользователь в Linux принадлежит одной основной группе и одной или нескольким дополнительным группам. В Linux, как и в большинстве других операционных системах, работа с пользователями заключается в наборе следующих манипуляций: добавление пользователя/группы, удаление пользователя/группы, модификация настроек пользователя/группы. Данные манипуляции производятся с помощью команд: useradd, groupadd, userdel, groupdel, usermod, groupmod, а так же passwd, gpasswd, id. Существуют так же и графические средства администрирования пользователями, обычно они расположены в оболочке X в разделе Администрирование - Пользователи и группы. Однако, при администрировании Linux использование графических оболочек не приветствуется.

UID, GID

Каждый пользователь в системе имеет свой уникальный идентификационный номер (user-ID, или UID). Также пользователи могут объединяться в группы, которые в свою очередь имеют group-ID, или GID. Чтобы узнать свой UID и GID, т.е. уникальный номер пользователя и номер группы, к которой вы принадлежите, необходимо ввести команду id (рис. 2.1).

```
work@work:~$ id
uid=1000(work) gid=1000(work) группы=4(adm)
,20(dialout),24(cdrom),46(plugdev),105(lpad
min),119(admin),122(sambashare),1000(work)
```

Рис. 2.1. Отобразить UID и GID

Пример добавления пользователя (рис. 2.2.):

```
work@work:~$ sudo groupadd test
work@work:~$ sudo useradd -c "Test Test" -g test -m test
work@work:~$ sudo passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
work@work:~$ sudo it test
sudo: it: command not found
work@work:~$ sudo id test
uid=1001(test) gid=1002(test) groups=1002(test)
work@work:~$ sudo ls -ld /home/test/
drwxr-xr-x 2 test test 4096 2011-12-17 15:13 /home/test/
```

Рис. 2.2. Добавление нового пользователя

В примере мы добавляем группу для нового пользователя (groupadd), далее создаем нового пользователя с полным именем Test Test, имеющего основную группу test и логин test, далее задаем пароль для пользователя test (passwd test) и проверяем параметры созданного пользователя (id и созданный каталог пользователя /home/test/). На рис. 2.2 видно, что UID и GID - более 1000. Данная особенность является признаком обычного пользователя. Значения ниже (меньше) 1000 (а в некоторых версиях - меньше 500) указывают на то, что пользователь является системным пользователем.

В соответствии с соглашением, системные пользователи обычно имеют id меньше, чем 100, а пользователь root имеет id, равный 0. Автоматическая нумерация обычных пользователей начинается со значения UID_MIN, установленного в файле /etc/login.defs. Это значение обычно установлено в 500 или 1000.

Помимо учетных записей обычных пользователей и учетной записи пользователя root, в системе бывает несколько учетных записей специального назначения для демонов, таких как FTP, SSH, mail, news и т.д. Такие учетные записи часто управляют файлами, но к ним невозможно получить доступ путем обычной регистрации в системе. Поэтому обычно они

имеют login shell, определенный как /sbin/nologin или /bin/false, чтобы попытки зарегистрироваться в системе терпели неудачу.

Управление базами данных пользователей и групп в Linux

Основные файлы, содержащие информацию о пользователях и группах, - это четыре файла в каталоге */etc*.

1. /etc/passwd - файл паролей, содержащий основную информацию о пользователях;
2. /etc/shadow - файл теневых шифрованных паролей, содержащий зашифрованные пароли;
3. /etc/group - файл групп, содержащий основную информацию о группах и принадлежащих этим группам пользователях;
4. /etc/gshadow - файл теневых групп, содержащий шифрованные пароли групп.

Данные файлы редактировать обычным текстовым редактором крайне не рекомендуется. Они, обновляются при выполнении вышеуказанных команд, при этом при изменении - блокируются и синхронизируются.

Если все же есть острая необходимость в редактировании указанный файлов, то при помощи команды vipw можно безопасно редактировать файл /etc/passwd, а при помощи команды vigr безопасно редактировать файл /etc/group. Эти команды заблокируют необходимые файлы на то время, пока при помощи редактора vi будут производиться изменения. Если вы вносите изменения в файл /etc/passwd, команда vipw подскажет, что необходимо проверить, не нужно ли обновить и файл /etc/shadow. Подобным образом, если вы обновляете файл /etc/group при помощи команды vigr, вы получите подсказку, что необходимо обновить и файл /etc/gshadow. Если необходимо удалить администраторов группы, необходимо использовать команду vigr, поскольку команда gpasswd позволяет только добавлять администраторов.

В современных системах, файлы passwd и group не хранят пароли в открытом виде. Это сделано из соображений безопасности. Сами файлы passwd и group должны быть доступными для чтения для всех, а зашифрованные пароли - недоступными для чтения для всех. Поэтому зашифрованные пароли хранятся в теневых файлах, и эти файлы доступны для чтения только пользователю root. Необходимый доступ для изменения аутентификационных данных обеспечивается при помощи suid-программы, которая имеет полномочия пользователя root, но может быть запущена любым пользователем.

Права доступа

Операционная система Linux - это многопользовательская система, которая дает огромные возможности манипулирования доступом к данным для каждого пользователя отдельно. Это позволяет гибко регулировать отношения между пользователями, объединяя их в группы, что позволит защитить данные одного пользователя от нежелательного вмешательства других.

Бессмысленно считать, что файловая система это не самая важная часть операционной системы, поскольку все данные пользователей хранятся именно в файлах.

В UNIX-подобных системах файлы также обеспечивают доступ к периферийным устройствам, дисковым накопителям, принтерам и т.п.

Права доступа к файлам

В свою очередь файлы имеют двух владельцев: пользователя (user owner) и группу пользователей (group owner). Для каждого файла есть индивидуальные права доступа, которые разбиты на три группы:

- Доступ для пользователя-владельца файла (owner).
- Доступ для группы-владельца файла (group).
- Доступ для остальных пользователей (others).

Для каждой категории устанавливаются три вида доступа: (x) - право на запуск файла, (r) - право на чтение файла, (w) - право на изменение (редактирование) файла.

Для того, чтобы увидеть права доступа к файлам необходимо ввести команду ls с ключом –l (рис. 2.3).

```
work@work:~$ ls -l Картинки/Kubuntu_leaflet.jpg
-rw-r--r-- 1 work work 658825 2010-03-26 15:21
Картинки/Kubuntu_leaflet.jpg
```

Рис. 2.3. Просмотр прав доступа к файлу

Для данного примера мы видим, что владелец имеет права на чтение, запись (первые две буквы rw), группа пользователей может лишь читать этот файл (следующая r--), остальные пользователи могут также только читать данный файл (r--).

Изменение прав доступа

Права пользователя могут быть изменены только владельцем файла или пользователем с правами администратора системы. Для изменения прав используется команда:

chmod[u|g|o|a] [+|-|=] [r|w|x] name1 [name2 ...]

В качестве аргументов команда принимает указание классов доступа («u» - владелец-пользователь, «g» - владелец-группа, «o» - остальные пользователи, «a» - все вышеперечисленные группы вместе), права доступа («r» - чтение, «w» - запись, «x» - выполнение) и операцию, которую необходимо произвести («+» - добавить, «-» -убрать, «=» - присвоить).

Таким образом, чтобы разрешить выполнение файла ip, который находиться в директории /home/work/Загрузки всем пользователем необходимо выполнить команду (рис. 2.4):

```
work@work:~$ chmod a+x Загрузки/ip
```

Рис. 2.4. Команда, выдающая права на исполнение файла

Далее, чтобы оставить права записи только для владельца файла необходимо выполнить (рис.2.5):

```
work@work:~$ chmod go-w Загрузки/ip
```

Рис. 2.5. Команда, повзоляющая оставить права записи только для владельца файла

Рассмотрим еще несколько примеров:

- chmod go=w ip - установить право на запись для всех пользователей кроме владельца;
- chmod a+x ip - предоставить право на запись для всех пользователей;
- chmod g+x-w ip - добавить для группы право на выполнения файла, но снять право на запись.

Права доступа можно представить в виде битовой строки, в которой каждые 3 бита определяют права доступа для соответствующей категории пользователей, как представлено в таблице 2.1:

Таблица 2.1

Представление прав доступа в виде битовой строки

rwx	rwx	rwx
421	421	421
user	group	others
владелец	группа	остальные

Таким образом, для команды chmod 666 ip имеем (рис. 2.6):

```
work@work:~$ chmod 666 Загрузки/ip
work@work:~$ ls -l Загрузки/ip
-rw-rw-rw- 1 work work 226568 2010-01-18 11:11 Загрузки/ip
work@work:~$ chmod 644 Загрузки/ip
work@work:~$ ls -l Загрузки/ip
-rw-r--r-- 1 work work 226568 2010-01-18 11:11 Загрузки/ip
```

Рис. 2.6. Пример использования команды chmod

Команда:

chmod 644 имя_файла

устанавливает «обычные» права доступа, т.е. владелец может читать и записывать в файл, а все остальные пользователи - только читать.

Особенности прав доступа для каталогов

Права доступа для каталогов не столь очевидны. Это в первую очередь связано с тем, что система трактует операции чтения и записи для каталогов отлично от остальных файлов. Право чтения каталога позволяет Вам получить имена (и только имена) файлов, находящихся в данном

каталоге. Чтобы получить дополнительную информацию о файлах каталога (например, подробный листинг команды ls -l), системы придется «заглянуть» в метаданные файлов, что требует права на выполнения для каталога. Право на выполнение также потребуется для каталога, в который Вы захотите перейти (т.е. сделать его текущим) с помощью команды cd.

Управление файлами

В ОС Linux следует различать физическую файловую систему, которая отвечает за управление дисковым пространством и размещение файлов в физических адресах диска и логическую файловую систему, которая обеспечивает логическую структуру хранения файлов - пространство имен файлов. ОС Unix и Linux могут работать с различными физическими файловыми системами (Ext2, ext3, ufs), логическое же представление файловой системы в Unix/Linux структурировано. Все файлы в логической файловой системе располагаются в виде дерева, промежуточные вершины которого соответствуют каталогам, и листья - файлам и пустым каталогам. Реально на каждом логическом диске (разделе физического дискового пакета) располагается отдельная иерархия каталогов и файлов. Для получения общего дерева в динамике используется «монтирование» отдельных иерархий к фиксированной корневой файловой системе в качестве ветвей общего дерева. Самым верхом иерархии является корень, который имеет предопределенное имя «/» (слэш). Этот же символ используется как разделитель имен в пути. Далее в корне находятся папки с определенными для каждого дистрибутива именами (etc, home, bin, mnt, proc и т.д.).

Полное имя файла, например, /bin/sh означает, что в корневом каталоге должно содержаться имя каталога bin, а в каталоге bin должно содержаться имя файла sh. Коротким или относительным именем файла называется имя, задающее путь к файлу от текущего рабочего каталога. В каждом каталоге содержатся два специальных имени, имя «.» - ссылка на текущий каталог, и имя «...» - ссылка «родительский» каталог данного текущего каталога, т.е. каталог, непосредственно предшествующий данному в иерархии каталогов. Так, например, для структуры, показанной на рис. 2.7 доступ к файлу file2 из текущего каталога (laba) возможен по полному имени: /home/myvar/file2 или по относительному имени: .../.../.../myvar/file2.

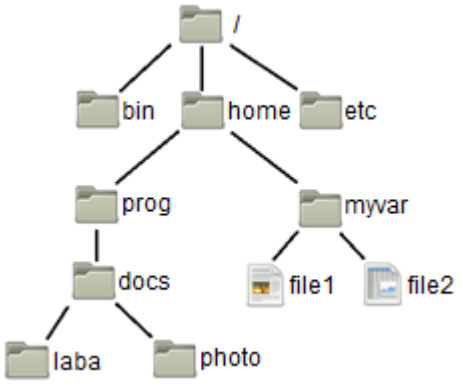

Рис. 2.7. Пример дерева каталогов

Задания к лабораторной работе:

1. Выведите на экран UID и GID своего пользователя; (если его нет, нужно создать)
2. Создайте группу пользователей с именем usersGroup;
3. Создайте пользователя myUser в группе usersGroup;
4. Выведите на экран UID и GID пользователя myUser;

Контрольные вопросы

1. Расскажите про идентификационные номера пользователей и групп в Linux.
2. Расскажите о файлах Linux, содержащих информацию о пользователях и группах системы.
3. Как система Linux хранит пароли пользователей и групп?
4. Как организуется разграничение доступа к файлам в Linux?
5. Какой каталог будет установлен текущим сразу же после входа пользователя в систему?