Права доступа к файлам

Учетная запись пользователя

Linux – многопользовательская операционная система. Это означает, что компьютером под управлением Linux могут одновременно пользоваться несколько человек. В такой системе должен существовать механизм, позволяющий защищать файлы одного пользователя от несанкционированного доступа или модификации другим пользователем.

В основе системы безопасности Linux лежит понятие учетной записи, которая присваивается каждому пользователю. Учетная запись – это объект системы, при помощи которого Linux ведет учет работы пользователя. Учетная запись содержит данные о пользователе, необходимые для входа в систему и дальнейшей работы с ней.

С каждой учетной записью связывается идентификатор пользователя (User ID) или uid – уникальное число, однозначно идентифицирующее учетную запись пользователя. uid используется для персонального учета действий пользователя и определения прав доступа к другим объектам системы.

В Linux используются специальные файлы и программы для отслеживания и управления учетными записями пользователей в системе. Кратко рассмотрим как ведется обработка учетных записей пользователей в Linux.

Файл /etc/passwd

Для сопоставления входного имени (имя, которое запрашивается при входе в систему) со значением идентификатора пользователя служит файл /etc/passwd, который содержит часть информации о пользователе.

```
user@linux-pc:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
...
user:x:1000:1000:,,,:/home/user:/bin/bash

```

Поля файла /etc/passwd содержат следующую информацию:

1. входное (регистрационное) имя пользователя;
2. пароль пользователя;
3. числовой идентификатор учетной записи;
4. числовой идентификатор группы, к которой относится учетная запись пользователя;
5. текстовое описание учетной записи
6. местоположение домашнего каталога
7. командная оболочка, используемая по умолчанию.

Учетная запись пользователя root принадлежит администратору системы и всегда имеет идентификатор пользователя 0.

В Linux создается много учетных записей, которые не принадлежат реальным пользователям, а используются для выполнения различных функций. Эти учетные записи называются системными. Системная учетная запись — это специальная учетная запись, которую используют службы, работающие в операционной системе, для получения доступа к ресурсам системы. Идентификаторы пользователей с числовыми значениями меньше 500 зарезервированы для системных учетных записей.

В каждом поле пароля в файле /etc/passwd задано значение x. Это не означает, что у всех учетных записей один и тот же пароль. В настоящее время в большинстве Linux пароли пользователей хранятся в отдельном файле (/etc/shadow). Доступ к этому файлу имеют только специальные программы.
Файл /etc/shadow

К файлу /etc/shadow имеет доступ только пользователь root. В файле содержится по одной записи для каждой учетной записи пользователя в системе. Записи выглядят следующим образом:

В каждой записи файла /etc/shadow имеются девять полей с такими данными:

1. входное имя, соответствующее входному имени в файле /etc/passwd;
2. зашифрованный пароль;
3. количество дней, отсчитываемое с 1 января 1970 года, которое позволяет определить дату последнего изменения пароля;
4. минимальное количество дней, по истечении которого может быть изменен пароль;
5. количество дней до того, как должен быть изменен пароль;
6. количество дней до истечения срока действия пароля, после чего пользователь получит предупреждение в связи с необходимостью сменить пароль;
7. количество дней после истечения срока действия пароля, по прошествии которых учетная запись будет отключена;

8. дата (хранимая как количество дней с 1 января 1970 года), после которой учетная запись пользователя была отключена;
9. поле, зарезервированное для дальнейшего использования.

Добавление нового пользователя

Для добавления нового пользователя используется команда useradd. Команда создает новую учетную запись и развертывает домашний каталог пользователя.

В процессе работы команда, с одной стороны, использует системные значения по умолчанию , с другой стороны, параметры, задаваемые через командную строку. Для просмотра системных значений по умолчанию необходимо ввести следующую команду:

```
user@linux-pc:~$ useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

В рассматриваемом примере показаны следующие значения по умолчанию:
новый пользователь добавляется к общей группе с идентификатором группы 100;
для нового пользователя создается домашний каталог /home/loginname;
учетная запись не отключается по истечении срока действия пароля;
новая учетная запись не настраивается на истечение срока действия в заданную дату;
для новой учетной записи в качестве командного интерпретатора, заданного по умолчанию, используется командный интерпретатор sh;
при создании учетной записи пользователя система копирует содержимое каталога /etc/skel в домашний каталог пользователя;
система не настраивает электронную почту.

Удаление пользователя

Для удаления пользователя используется команда userdel. По умолчанию команда userdel удаляет только сведения о пользователе из файла /etc/passwd. Если используется параметр -r, то команда userdel удаляет домашний каталог пользователя.

Изменение информации о пользователе

Команда	**Описание**
usermod	Редактирует поля учетной записи пользователя.

Команда	Описание
passwd	Изменяет пароль для существующего пользователя.
chpasswd	Изменяет пароль для нескольких пользователей.
change	Изменяет дату истечения пароля.
chfn	Изменяет комментарий к учетной записи пользователя.
chsh	Изменяет заданный по умолчанию командную оболочку для пользователя.

Группы

Учетные записи пользователей хорошо подходят для управления безопасностью применительно к отдельным пользователям, но они не удобны, когда требуется обеспечить совместную работу с ресурсами для групп пользователей. Для достижения указанной цели в Linux используются группы.

Для групп назначаются разрешения, которые позволяют нескольким пользователям совместно работать в рамках общих разрешений на такие объекты как файлы, каталоги или устройства.

У группы, так же, как и у пользователя, есть имя и идентификационный номер — Group ID (gid). В Linux пользователь должен принадлежать как минимум к одной группе — группе по умолчанию. При создании учетной записи пользователя обычно создается группа, имя которой совпадает с входным именем. Именно эта группа будет использоваться как группа по умолчанию для этого пользователя. Пользователь может входить более чем в одну группу, но в учетной записи указывается только номер группы по умолчанию.

Общие сведение о правах доступа к файлам

Права доступа к каталогам и файлам определяются в терминах «право на чтение», «право на запись», «право на выполнение».

```
user@linux-pc:~$ touch test.txt
user@linux-pc:~$ ls -l test.txt
-rw-r--r-- 1 user user 0 Aug  1 19:43 test.txt
```

Первые 10 символов — это атрибуты файла. Первый символ определяет тип файла. Остальные девять символов называются режимом доступа к файлу и определяют права на чтение, запись и выполнение для владельца файла, группы владельца файла и всех остальных.

Атрибут	Файл	Каталог
r	Разрешает открывать и читать содержимое файла.	Разрешает читать содержимое каталога, если вместе с этим атрибутом установлен атрибут права на выполнение.

Атрибут	Файл	Каталог
w	Разрешает записывать в файл и изменять его размер. НЕ ДАЕТ право переименовывать и удалять файл.	Разрешает создавать, удалять и переименовывать файлы внутри каталога, если вместе с этим атрибутом установлен атрибут права на выполнение.
x	Разрешает интерпретировать файл как программу и выполнять ее.	Разрешает входить в каталог, т. е. выполнять команду cd для перехода в него.

chmod

Для изменения прав доступа к каталогу или файлу используется команда chmod. Права доступа к каталогу или файлу может изменить только владелец!

Команда chmod поддерживает два разных способа изменения режима: с использованием восьмеричных чисел и символического представления.

Восьмеричное представление

Права доступа к файлу в различных представлениях

Восьмеричное	Двоичное	Права доступа
0	0	—
1	1	–x
2	10	-w-
3	11	-wx
4	100	r–
5	101	r-x
6	110	rw-
7	111	rwx

Рассмотрим пример

```
user@linux-pc:~$ touch test.txt
user@linux-pc:~$ ls -l test.txt
-rw-r--r-- 1 user user 0 Aug  1 20:08 test.txt
user@linux-pc:~$ chmod 600 test.txt
user@linux-pc:~$ ls -l test.txt
-rw------- 1 user user 0 Aug  1 20:08 test.txt
```

С помощью команды chmod мы установили права на чтение и запись файла и отобрали все права у группы и всех остальных.

Символическое представление

Символическая форма записи делится на три части: [ugoa][+-=][rwx].

Первая группа символов определяет к какому объекту относятся новые права:

- u (user) применяется для обозначения пользователя;
- g (group) применяется для обозначения группы;
- o (others) применяется для обозначения всех остальных;
- a (all) применяется для обозначения всех вышеупомянутых объектов.

После этого указывается символ, указывающий следует ли добавить данное право к существующим правам (+), отнять право из существующих прав (-) или задать равным указанному праву (=).

Символическая запись	**Значение**
u+x	Для владельца добавляет право на выполнение
u-x	Для владельца отнимает право на выполнение
+x	Добавляет право на выполнение для владельца, группы и всех остальных. Эквивалентно записи a+x.
o-rw	Для всех остальных отнимает право на чтение и запись.
go=rw	Для группы и всех остальных устанавливает право на чтение и запись. Если прежде файл имел разрешение на выполнение, для группы и всех остальных это право отнимается.
u+x,go=rx	Для владельца добавляет право на выполнение и устанавливает право на чтение и выполнение для группы и остальных.

chown

Иногда возникает необходимость сменить владельца файла. Команда chown используется для изменения владельца или группы каталога или файла. Для использования команды необходимы привилегии суперпользователя.

```
chown [владелец][:[группа]] файл...
```

chown может изменить владельца и/или группу в зависимости от первого аргумента.

Аргумент	Результат
alex	Изменит принадлежность файла, назначив владельцем пользователя alex.
alex:users	Изменит принадлежность файла, назначив владельцем пользователя alex и группу users.
:admins	Изменит принадлежность файла, назначив группу admins.
alex:	Изменит принадлежность файла, назначив владельцем пользователя alex и группу этого пользователя.

Изменение идентичности

Суперпользователь - единственный пользователь в Linux, на которого не распространяются ограничения прав доступа.

Входное имя его учетной записи – root, а домашний каталог находится в /root. Этот пользователь предназначен для администрирования системы, поэтому ему разрешен доступ на чтение и запись любого каталога и файла, установку программного обеспечения, создание и удаление других пользователей, предоставление им различных доступов и многое другое.

В некоторых дистрибутивах Linux и сейчас при установке операционной системы, кроме создания обычного пользователя, нужно задать пароль для суперпользователя. После этого войти в систему можно как под обычным пользователем, так и под администратором (root-ом).

Иногда нужно получить привилегии суперпользователя, чтобы выполнить некоторые административные задачи, или «стать» другим пользователем, чтобы, например, проверить настройки учетной записи. Существует три способа приобрести права другого пользователя:

- выйти из системы и войти вновь с учетными данными другого пользователя;
- воспользоваться командой su;
- воспользоваться командой sudo.

В рамках сеанса работы с командной оболочкой команда su позволяет либо начать новый сеанс командной оболочки с идентификатором этого пользователя, либо запустить одиночную команду от его имени.

Команда sudo используется в качестве префикса к командам Linux, позволяя вошедшему в систему пользователю выполнять команды, требующие привилегий root. В отличие от su, команда sudo требует ввода пароля текущего пользователя (выполняющего эту команду). Чтобы пользователь мог выполнить команду, для которой требуется sudo, ему необходимо быть частью группы sudoers. Кроме того, пользователь root может отредактировать конфигурационный файл с именем /etc/sudoers и определить конкретные команды, которые сможет выполнять тот или иной пользователь, используя команду sudo.

Выбор между su и sudo в значительной степени определяется используемым дистрибутивом Linux. Большинство дистрибутивов включают обе команды, но в настройках предпочтение отдается той или иной.

su

Команда su используется для запуска нового сеанса работы с командной оболочкой от имени другого пользователя.

Рассмотрим пример авторизации в качестве суперпользователя:

```
user@linux-pc:~$ su
Введите пароль суперпользователя:
Неудачная попытка!
Введите пароль суперпользователя:
root@linux-pc:/home/user#
```

Отметим несколько важных моментов:

1. При вводе пароля так же, как при авторизации через интерфейс без GUI, в целях безопасности на экране не отображается ни сам пароль, ни даже звёздочки, по которым можно угадать количество символов. При этом все управляющие символы доступны - если Вы уверены, что набрали случайно на одну лишнюю букву больше, можно нажать Backspace. Попытка взаимодействовать таким образом с паролем на кириллице скорее завершится неудачей.
2. После авторизации папка, которая была домашней для user, для root домашней не является, поэтому вместо символа тильды будет виден полный путь. Чтобы перейти в домашнюю папку суперпользователя, достаточно после авторизации за него вызвать cd.

```
su [-[l]] [пользователь]
```

Если указан параметр -l, запущенная командная оболочка станет оболочкой входа для указанного пользователя: будет загружено окружение пользователя и текущим рабочим каталогом станет домашний каталог пользователя. Параметр -l на практике можно сократить до -.

Если пользователь не указан, подразумевается суперпользователь.

С помощью su можно так же просто выполнить единственную команду, не запуская командную оболочку.

```
su -c ‘команда’
```

В этом случае команде su передается единственная команда. Эту команду нужно заключить в кавычки.

sudo

Команда sudo похожа на команду su, но имеет несколько особенностей.

Администратор может определить порядок использования команды sudo обычными пользователями: пользователю может быть разрешен доступ к одним командам и запрещен к другим. Другое важное отличие sudo от su состоит в том, что sudo не требует ввода пароля суперпользователя. Для аутентификации в команде sudo пользователь должен ввести свой пароль. Иначе говоря, концепция sudoers может напомнить Вам систему администрирования Windows - остаётся суперпользователь, который управляет всем без исключений, есть обычные администраторы и пользователи.

```
user@linux-pc:~$ sudo
Введите пароль суперпользователя:
Неудачная попытка!
Введите пароль суперпользователя:
root@linux-pc:/home/user#
```

Кроме того, команда sudo не запускает новую командную оболочку и не загружает окружение другого пользователя.

Обратите внимание, что наличие у Вас прав sudo на своей машине не должно приводить к привычке всё запускать с помощью sudo. Если Вы не планировали изменять какие-то настройки или изменять состояние компьютера для всех, то окошко с запросом пароля учётной записи от sudo должно вызывать у Вас желание, в первую очередь, перепроверить введённую команду.

На новых машинах с установленными дружелюбными ОС зачастую запись суперпользователя “отключена”. При попытке авторизоваться через su без пароля, которого ещё нет, будет выдана ошибка. В таком случае можно совершить одну хитрость - сначала вызвать su из sudo:

```
user@linux-pc:~$ su
Учётная запись суперпользователя деактивирована.
user@linux-pc:~$ sudo su
root@linux-pc:/home/user# passwd
Введите новый пароль:
Повторите пароль:
Пароль успешно изменён!
root@linux-pc:/home/user# exit
user@linux-pc:~$ su
Введите пароль суперпользователя:
```