用户用户组权限

- 用户：满足多个人操作电脑的需求。
- 用户组：组内成员拥有共享资源的权限
- 权限：不可能让所有人都能随意操作电脑内容，不安全。（避免入侵）

用户种类以及增删改查操作

操作用户必须要有管理员身份`sudo`。

用户种类：

- **root** 用户拥有至高无上的权限。
- 系统用户，为系统运行提供的用户。
- 个人自己创建的用户。

查——用户信息存放的路径

不同的系统版本路径可能有区别

Ubuntu

```
/etc/passwd # 用户帐户信息目录。
```

解析用户信息文件

例：

```
prophet:x:1000:1000:prophet,,,:/home/prophet:/bin/bash
```

从左至右解析：

- `prophet` 用户名。
- `:`为分割符，分开不同的选项。
- `x` 经过加密处理的用户密码。
- `1000` UID 用户的ID，**系统用户特殊UID<500。**
- `1000` GID 分组的ID，**ubuntu不允许把所有用户纳入一个组，而是每个用户都有一个单独的组。**
- `prophet,,,` 用户的备注。
- `/home/prophet` 用户的目录。
- `/bin/bash` 使用的工具。

`shadow`**影子账户信息**

```
/etc/shadow # 影子户帐户信息。保护用户密码安全
```

```
prophet:$6$DfchRfyt3N9dTNmi$6OXWWik7pAfXnbEfjKotXX1tLpH.1CNz4jULO5u9IEMLprapQR.478h5Ba7YESUh1oh8wUl.icF9pvrjFGZBf/:19183:0:99999:7:::
```

从左至右解析：

```
用户名：加密密码：最后一次修改时间（1970年1月1日到今天的天数）：最小修改时间间隔（0没有限制）：密码有效期（99999默认273年约等于无限制）：密码需要变更前的警告天数（默认7）：密码过期后的宽限时间：账号失效时间（开始计算时间也是1970年）：保留字段
```

users

打印当前主机所有登陆用户的名称。

增——添加账户

相关目录

```
/etc/default/useradd # 帐户创建的默认值。
```

该文件，在新建用户时为用户提供一个默认的用户信息模板。

```
/etc/skel/    #包含默认文件的目录。
```

用来存放新用户配置文件的目录，当我们添加新用户的时候，这个目录下的所有文件会自动被复制到新添加用户的`home`目录下面。默认情况下，`/etc/skel`目录下的所有文件都是隐藏文件（以.开头的文件）：通过修改，添加，删除`etc/skel`目录下的文件，我们可以为新创建的用户提供统一的，标准的初始化环境 。

```
/etc/login.defs # 影子密码套件配置。
```

文件是用来定义创建用户时需要的一些用户配置信息。如创建用户时，是否需要`home`目录，UID和GID的范围，用户及密码的有效期限，家目录的权限，密码加密方式等等。

`useradd` 创建的新的系统用户

用于Linux中创建的新的系统用户。`useradd`可用来建立用户帐号。帐号建好之后，再用`passwd`设定帐号的密码．而可用`userdel`删除帐号。使用`useradd`指令所建立的帐号，实际上是保存在`/etc/passwd`文本文件中。

选项

```
-b, --base-dir BASE_DIR  # 如果未指定 -d HOME_DIR，则系统的默认基本目录。如果未指定此选项，useradd 将使用 /etc/default/useradd 中的 HOME 变量指定的基本目录，或默认使用 /home。
-c, --comment COMMENT    # 加上备注文字。任何文本字符串。它通常是对登录名的简短描述，目前用作用户全名的字段。
-d, --home HOME_DIR      # 将使用 HOME_DIR 作为用户登录目录的值来创建新用户。
-D, --defaults           # 变更预设值。
-e, --expiredate EXPIRE_DATE # 用户帐户将被禁用的日期。 日期以 YYYY-MM-DD 格式指定。
-f, --inactive INACTIVE      # 密码过期后到帐户被永久禁用的天数。
-g, --gid GROUP   # 用户初始登录组的组名或编号。组名必须存在。组号必须引用已经存在的组。
-G, --groups GROUP1[,GROUP2,...[,GROUPN]]] # 用户也是其成员的补充组列表。每个组用逗号隔开，中间没有空格。
-h, --help # 显示帮助信息并退出。
-k, --skel SKEL_DIR # 骨架目录，其中包含要在用户的主目录中复制的文件和目录，当主目录由 useradd 创建时。
-K, --key KEY=VALUE # 覆盖 /etc/login.defs 默认值（UID_MIN、UID_MAX、UMASK、PASS_MAX_DAYS 等）。
-l, --no-log-init   # 不要将用户添加到 lastlog 和 faillog 数据库。
-m, --create-home   # 如果用户的主目录不存在，则创建它。
-M                  # 不要创建用户的主目录，即使 /etc/login.defs (CREATE_HOME) 中的系统范围设置设置为 yes。
-N, --no-user-group # 不要创建与用户同名的组，而是将用户添加到由 -g 选项或 /etc/default/useradd 中的 GROUP 变量指定的组中。
-o, --non-unique    # 允许创建具有重复（非唯一）UID 的用户帐户。 此选项仅在与 -o 选项结合使用时有效。
-p, --password PASSWORD # crypt(3) 返回的加密密码。 默认是禁用密码。
-r, --system        # 创建一个系统帐户。
-s, --shell SHELL   # 用户登录 shell 的名称。
-u, --uid UID       # 用户 ID 的数值。
-U, --user-group    # 创建一个与用户同名的组，并将用户添加到该组。
-Z, --selinux-user SEUSER # 用户登录的 SELinux 用户。 默认情况下将此字段留空，这会导致系统选择默认的 SELinux 用户。

# 更改默认值
# 当仅使用 -D 选项调用时，useradd 将显示当前默认值。 当使用 -D 和其他选项调用时，useradd 将更新指定选项的默认值。 有效的默认更改选项是：
参数
```

需要说明的是，设定ID值时尽量要大于500，以免冲突。因为Linux安装后会建立一些特殊用户，一般0到499之间的值留给bin、mail这样的系统账号。

删——删除账户

`userdel` 用于删除给定的用户以及与用户相关的文件

用于删除给定的用户，以及与用户相关的文件。若不加选项，则仅删除用户帐号，而不删除相关文件。

选项

```
-f #强制删除用户，即使用户当前已登录；
-r #删除用户的同时，删除与用户相关的所有文件。
```

请不要轻易用`-r`选项；他会删除用户的同时删除用户所有的文件和目录，切记如果用户目录下有重要的文件，在删除前请备份。

其实也有最简单的办法，但这种办法有点不安全，也就是直接在`/etc/passwd`中删除您想要删除用户的记录；但最好不要这样做，`/etc/passwd`是极为重要的文件，可能您一不小心会操作失误。

改——修改账户

`usermod`用于修改用户的基本信息

`usermod` 命令不允许你改变正在线上的使用者帐号名称。当 `usermod` 命令用来改变user id，必须确认这名user没在电脑上执行任何程序。你需手动更改使用者的 crontab 档。也需手动更改使用者的 at 工作档。采用 NIS server 须在server上更动相关的NIS设定。

选项

```
-c<备注>：修改用户帐号的备注文字；
-d<登入目录>：修改用户登入时的目录，只是修改/etc/passwd中用户的家目录配置信息，不会自动创建新的家目录，通常和-m一起使用；
-m<移动用户家目录>:移动用户家目录到新的位置，不能单独使用，一般与-d一起使用。
-e<有效期限>：修改帐号的有效期限；
-f<缓冲天数>：修改在密码过期后多少天即关闭该帐号；
-g<群组>：修改用户所属的群组；用来制定这个用户默认的用户组
-G<群组>：修改用户所属的附加群组
-l<帐号名称>：修改用户帐号名称；
-L：锁定用户密码，使密码无效；
-s<shell>：修改用户登入后所使用的shell；
-u<uid>：修改用户ID；
-U:解除密码锁定。
-a #--append将用户追加到-G选项提到的补充GROUPS上，而不将用户从其他组中删除
```

`chpasswd` 批量更新用户口令的工具

是批量更新用户口令的工具，是把一个文件内容重新定向添加到`/etc/shadow`中。

选项

```
-e #输入的密码是加密后的密文；
-h #显示帮助信息并退出；
-m #当被支持的密码未被加密时，使用MD5加密代替DES加密。
```

批量更新实例

先创建用户密码对应文件，格式为`username:password`，如`abc:abc123`，必须以这种格式来书写，并且不能有空行，保存成文本文件user.txt，然后执行`chpasswd`命令：

```
chpasswd < user.txt
```

以上是运用`chpasswd`命令来批量修改密码。是`linux`系统管理中的捷径。

`chage` 修改帐号和密码的有效期限

可以编辑`/etc/login.defs`来设定参数,但不要失误

语法:

```
chage 选项 用户名
```

选项

```
-m #密码可更改的最小天数。为零时代表任何时候都可以更改密码。
-M #密码保持有效的最大天数。
-w #用户密码到期前，提前收到警告信息的天数。
-E #帐号到期的日期。过了这天，此帐号将不可用。
-d #上一次更改的日期。
-i #停滞时期。如果一个密码已过期这些天，那么此帐号将不可用。
-l #例出当前的设置。由非特权用户来确定他们的密码或帐号何时过期。
```

`chsh` 用来更换登录系统时使用的shell

若不指定任何参数与用户名称，则`chsh`会以应答的方式进行设置。

选项

```
-s<shell 名称>或--shell<shell 名称> #更改系统预设的shell环境。
-l或--list-shells #列出目前系统可用的shell清单；
-u或--help #在线帮助；
-v或-version #显示版本信息。
```

查看系统安装了哪些shell其他方法：

```
cat /etc/shells
```

其实`chsh -l`也是来查看这个文件。

查看当前正在使用的shell：

```
echo $SHELL
```

`chfn` 提供使用者更改个人资讯

这些信息都存放在`/etc`目录里的`passwd`件里。若不指定任何选项，则`chfn`命令会进入问答式界面。

```
-f<真实姓名>或--full-name<真实姓名>：设置真实姓名；
-h<家中电话>或--home-phone<家中电话>：设置家中的电话号码；
-o<办公地址>或--office<办公地址>：设置办公室的地址；
-p<办公电话>或--office-phone<办公电话>：设置办公室的电话号码；
-u或--help：在线帮助；
-v或-version：显示版本信息。
```

用户组

组目的：组内成员拥有共享资源的权限

操作用户组必须要有管理员身份`sudo`。

查——组信息的存放路径

```
/etc/gourp
```

ubuntu 不允许把所有用户纳入一个组，而是每个用户都有一个单独的组

例：

```
prophet : x : 1000 :
```

解析：

```
组名:组的密码，加密后显示x:组ID:属于该组的列表
```

groups

打印指定用户所在组的名称。

曾——创建组

`groupadd`用于创建一个新的工作组

用于创建一个新的工作组，新工作组的信息将被添加到系统文件中。

选项

```
-g #指定新建工作组的id;
-r #创建系统工作组，系统工作组的组ID小于500;
-K #覆盖配置文件“/ect/login.defs”;
-o #允许添加组ID号不唯一的工作组。
```

删——删除组

`groupdel` 用于删除指定的工作组

本命令要修改的系统文件包括`/ect/group`和`/ect/gshadow`。若该群组中仍包括某些用户，则必须先删除这些用户后，方能删除群组。

语法

```
groupdel(参数)
```

参数

组：要删除的工作组名。

改——修改组信息以及管理组

`groupmod` 更改群组识别码或名称

语法

```
groupmod(选项)(参数)
```

选项

```
-g<群组识别码>：设置欲使用的群组识别码；
-o：重复使用群组识别码；
-n<新群组名称>：设置欲使用的群组名称。
```

参数

组名：指定要修改的工作的组名。

`gpasswd` 工作组文件的管理工具(创建密码、加减组员等操作)

是Linux下工作组文件`/etc/group`和`/etc/gshadow`管理工具。

语法

```
gpasswd (选项)(参数)
```

选项

```
-a：添加用户到组；
-d：从组删除用户；
-A：指定管理员；
-M：指定组成员和-A的用途差不多；
-r：删除密码；
-R：限制用户登入组，只有组中的成员才可以用newgrp加入该组。
```

参数

组：指定要管理的工作组。

注意

```
usermod -G 组名 用户名 #其实加 -a 变成 -aG 也能解决
```

这个命令可以添加一个用户到指定的组，但是以前添加的组就会清空掉。

因此想要添加一个用户到一个组，同时保留以前添加的组时，请使用`gpasswd`这个命令来添加操作用户：

```
gpasswd -a 用户名 组名
```

注意：　以上两条命令的名字语法顺序

权限

查看权限认识权限

查看权限我们可以通过`ls -al`命令，查出来的每条内容的开头部分，就是有关权限的信息。

例： 

从左至右解析：

- 开头的第一个字符：是文件的类型。
- 之后每三个字符是一组分别对应三个大类的权限：`user`(本用户：创始人用户)，group（用户组），other（其他用户）。

文件类型

```
- # 普通文件
d # 目录文件
l # 软链接（类似Windows的快捷方式）
# 以下非常见。
b # 块设备文件（例如硬盘、光驱等）
p # 管道文件
c # 字符设备文件（例如猫等串口设备）
s # 套接口文件/数据接口文件（例如启动一个MySql服务器时会产生一个mysql.sock文件）
```

每三个一组的权限字符中每个字符代表

```
r # 可读（read）
w # 可写（write）
x # 可执行（execute）
- # 无权限
```

`chmod` 用来变更文件或目录的权限

选项

```
-c, --changes：当文件的权限更改时输出操作信息。
--no-preserve-root：不将'/'特殊化处理，默认选项。
--preserve-root：不能在根目录下递归操作。
-f, --silent, --quiet：抑制多数错误消息的输出。
-v, --verbose：无论文件是否更改了权限，一律输出操作信息。
--reference=RFILE：使用参考文件或参考目录RFILE的权限来设置目标文件或目录的权限。
-R, --recursive：对目录以及目录下的文件递归执行更改权限操作。
--help：显示帮助信息并退出。
--version：显示版本信息并退出。
```

```
参考man chmod文档的DESCRIPTION段落得知：
u #符号代表当前用户。
g #符号代表和当前用户在同一个组的用户，以下简称组用户。
o #符号代表其他用户。
a #符号代表所有用户。
r #符号代表读权限以及八进制数4。
w #符号代表写权限以及八进制数2。
```

```
x #符号代表执行权限以及八进制数1。
X #符号代表如果目标文件是可执行文件或目录，可给其设置可执行权限。
s #符号代表设置权限suid和sgid，使用权限组合u+s设定文件的用户的ID位，g+s设置组用户ID位。
t #符号代表只有目录或文件的所有者才可以删除目录下的文件。
+ #符号代表添加目标用户相应的权限。
- #符号代表删除目标用户相应的权限。
= #符号代表添加目标用户相应的权限，删除未提到的权限。
```

结合以上信息总结出三种修改权限方式：

三种修改方式命令三种语法

通过符号组合的方式更改目标文件或目录的权限

实例

```
chmod g+w ./test.log # 添加组用户的写权限。

chmod o= ./test.log # 删除其他用户的所有权限。

chmod a-w ./test.log # 使得所有用户都没有写权限。
```

通过八进制数的方式更改目标文件或目录的权限

实例

```
chmod u=rwx, g=rw, o=r ./test.log # 当前用户具有所有权限，组用户有读写权限，其他用户只有读权限。
# 可读是4  可写是2 可执行是1  没权限是 0，u g o 三项每一项都把可开放的权限加起来得出一个数
chmod 764 ./test.log # 等价的八进制数表示：
```

通过参考文件的权限来更改目标文件或目录的权限

实例

```
# 将目录以及目录下的文件都设置为所有用户拥有读写权限。
# 注意，使用'-R'选项一定要保留当前用户的执行和读取权限，否则会报错!
chmod -R a=rw ./testdir/

# 根据其他文件的权限设置文件权限。
chmod --reference=./1.log  ./test.log
```

注意

符号连接的权限无法变更，如果用户对符号连接修改权限，其改变会作用在被连接的原始文件。