

03 用户与组管理

Linux是一个多用户多任务的分时操作系统，任何一个用户要获得系统的使用授权，都必须拥有一个用户账户。用户账户代表登录和使用系统的身份。

分时操作系统将CPU的时间划分成若干个片段，称为时间片，操作系统以时间片为单位，轮流为每个终端用户服务，每个用户轮流使用一个时间片而使每个用户并不感到有别的用户存在。



用户类型

用户账号

- 超级用户(super user)：根账号root，可以执行所有任务，在系统中不受限制地执行任何操作。
- 系统用户(system user)：系统本身或应用程序使用的专门账号。
- 普通用户(regular user)：供实际用户登录使用的普通用户账号,只能对自己目录下的文件进行访问和修改。

用户ID (UID)

- 超级用户 (UID=0)
- 系统用户 (伪用户) (UID=1~499, 65534(nobody))：限制本机登录
- 普通用户 (UID>=1000)：操作权限受到限制

用户组

组是一类特殊账户，是具有相同或者相似特性的用户集合。

组的类别

- 超级组(supersuser group)
- 系统组(system group)
- 自定义组

组ID (GID)

- 超级组，组名为root (GID=0)
- 系统组 (GID=1~499)
- 自定义组 (GID>=1000)

用户与组的对应关系

一个用户可以同时属于多个组，某个组为主要组，其它为次要组。Ubuntu在创建用户时，会为用户自动创建一个同名的组作为主要组（默认组）。

- 一对一：即一个用户可以存在一个组中，也可以是组中的唯一成员。
- 一对多：即一个用户可以存在多个用户组中。那么此用户具有多个组的共同权限。
- 多对一：多个用户可以存在一个组中，这些用户具有和组相同的权限。
- 多对多：多个用户可以存在多个组中。其实就是上面三个对应关系的扩展。

UBUNTU管理员

Ubuntu管理员是具有管理权限的普通用户，有权删除用户、安装软件和驱动程序、修改日期和时间等。


Ubuntu默认禁用root用户，系统安装时创建的第一个用户自动成为管理员（加入到sudo组）。

赋予普通用户管理员权限

```
sudo vim /etc/sudoers
```

在sudoers中添加

```
username ALL=(ALL) ALL
```



```
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL
student ALL=(ALL) ALL
```

暂时切换到ROOT身份

执行sudo -i 暂时切换到root身份登录

```
lei@lei-VirtualBox:~$ sudo -i
root@lei-VirtualBox:~# exit
logout
lei@lei-VirtualBox:~$ sudo su root
root@lei-VirtualBox:/home/lei# exit
exit
lei@lei-VirtualBox:~$
```

使用su命令临时切换用户

格式：su [选项] [用户登录名]

su lei

从root切换到其它账户不需要输入密码，普通用户切换到普通用户需要输入目标账户密码。

暂时切换到ROOT身份

Ubuntu默认不提供root密码，不能直接使用su命令升至root权限，必须使用sudo获得root权限。

```
lei@lei-VirtualBox:~$ sudo su root
[sudo] password for lei:
root@lei-VirtualBox:/home/lei#
```

如果想像其它Linux发行版本一样使用root用户，可以设置root密码

```
lei@lei-VirtualBox:~$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
lei@lei-VirtualBox:~$
```


用户配置文件

Linux系统中，用户账户、用户密码、组信息均存放在不同的配置文件中。

用户配置文件：用于保存系统用户的基本信息

文件位置：/etc/passwd

文件中每一行对应一个系统用户的基本信息

文件中使用冒号（：）分隔各个字段，从左起这些字段的含义如下：

字段1：用户名

字段2：用户登录密码。x表示密码保存在用户密码文件中
([/etc/shadow](#))

字段3：用户的ID号（即UID）

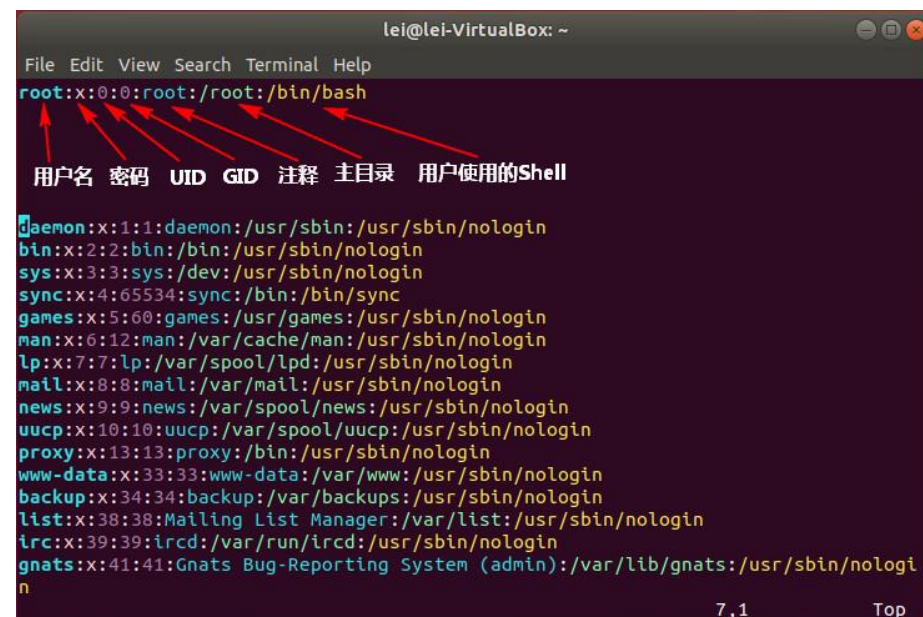
字段4：用户所属（默认）组的ID号（即GID）

字段5：用户全名

字段6：用户主目录。主目录主要用于存放用户的初始化文件

字段7：用户使用的shell

如果要临时禁用某个账户，可以在该账号记录前加*



```
lei@lei-VirtualBox: ~  
File Edit View Search Terminal Help  
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  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

用户名 密码 UID GID 注释 主目录 用户使用的Shell

用户密码文件

文件位置：/etc/shadow

文件中每一行对应一个用户的密码信息，密码采用MD5加密。

文件中使用冒号（：）分隔各个字段，从左起这些字段的含义如下：

字段1：用户名

字段2：加密后的用户密码

字段3：最后一次密码修改的日期（相对1970年1月1日的天数）

字段4：两次密码修改之间的间隔天数，在此期间用户不能修改密码（0表示可以随时修改密码）

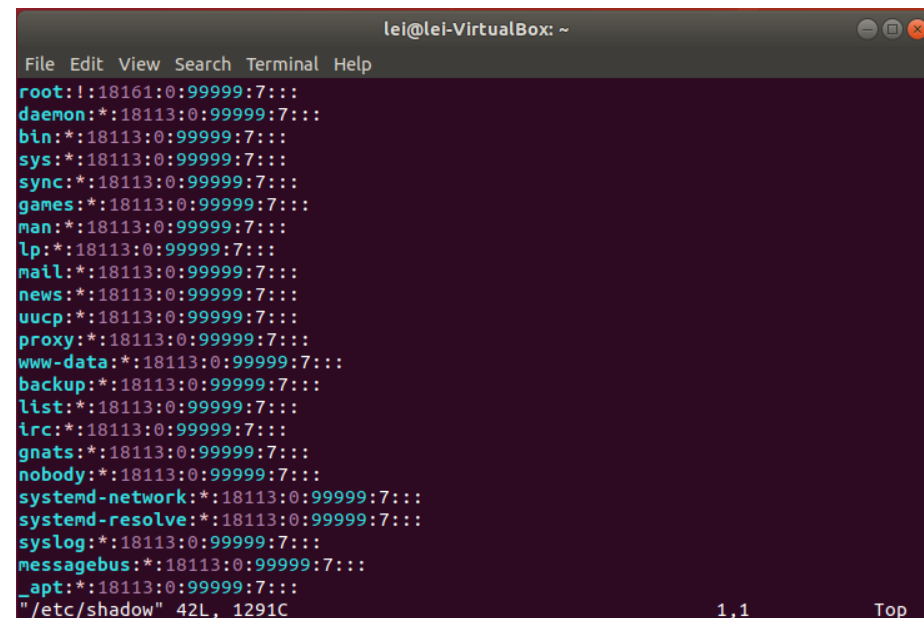
字段5：密码有效天数（1表示用户不能修改密码）

字段6：密码过期之前的警告天数（-1表示没有警告）

字段7：密码过期之后禁止用户登录的天数（1表示不会被禁用）

字段8：保留字段

字段9：保留字段



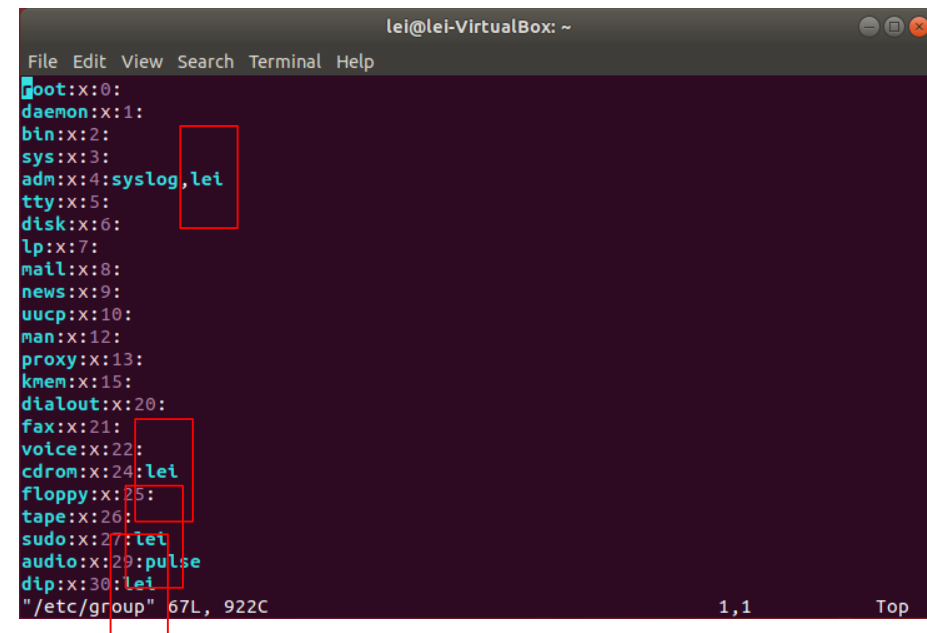
```
lei@lei-VirtualBox: ~  
File Edit View Search Terminal Help  
root:!18161:0:99999:7:::  
daemon*:18113:0:99999:7:::  
bin*:18113:0:99999:7:::  
sys*:18113:0:99999:7:::  
sync*:18113:0:99999:7:::  
games*:18113:0:99999:7:::  
man*:18113:0:99999:7:::  
lp*:18113:0:99999:7:::  
mail*:18113:0:99999:7:::  
news*:18113:0:99999:7:::  
uucp*:18113:0:99999:7:::  
proxy*:18113:0:99999:7:::  
www-data*:18113:0:99999:7:::  
backup*:18113:0:99999:7:::  
list*:18113:0:99999:7:::  
irc*:18113:0:99999:7:::  
gnats*:18113:0:99999:7:::  
nobody*:18113:0:99999:7:::  
systemd-network*:18113:0:99999:7:::  
systemd-resolve*:18113:0:99999:7:::  
syslog*:18113:0:99999:7:::  
messagebus*:18113:0:99999:7:::  
_apt*:18113:0:99999:7:::  
"/etc/shadow" 42L, 1291C 1,1 Top
```

用户组管理

用户组文件：用于保存用户组的基本信息

文件位置：/etc/group

文件中每一行对应一个用户组的基本信息



```
lei@lei-VirtualBox: ~  
File Edit View Search Terminal Help  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:syslog,lei  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mail:x:8:  
news:x:9:  
uucp:x:10:  
man:x:12:  
proxy:x:13:  
kmem:x:15:  
dialout:x:20:  
fax:x:21:  
voice:x:22:  
cdrom:x:24:lei  
floppy:x:25:  
tape:x:26:  
sudo:x:27:lei  
audio:x:29:pulse  
dip:x:30:lei  
"/etc/group" 67L, 922C 1,1 Top
```

文件中使用冒号（：）分隔各个字段，从左起这些字段的含义如下：

字段1：用户组的名称

字段2：组密码

字段3：用户组的ID号（即GID）（跟/etc/passwd中的GID对应）

字段4：用户列表，如果存在多个用户，使用逗号分隔

命令行管理工具

查看用户账户

通过查看用户配置文件/etc/passwd来查看用户信息

```
cat /etc/passwd | grep lei
```

```
lei@lei-VirtualBox:/home$ cat /etc/passwd | grep lei  
lei:x:1000:1000:lei,,,:/home/lei:/bin/bash
```

使用文本分析工具查看全部用户列表

```
awk -F ':' '{print $1}' /etc/passwd
```

```
lei@lei-VirtualBox:/home$ awk -F ':' '{print $1}' /etc/passwd  
root  
daemon  
bin  
sys  
sync  
games
```

添加用户

useradd 用于为系统添加普通用户。

【命令格式】

- useradd [option] username

【常用选项】

- -g：指定用户所属的用户组
- -m：创建用户主目录，默认不创建
- -d：指定用户主目录
- -s：指定用户使用的shell
- -r：指定创建一个系统账号
- -u：指定用户UID

【参数说明】

- 参数表示要创建的用户名称（用户名称不使用中文，最好全使用小写字母）

【用法示例】

- useradd -m leiliu

```
lei@lei-VirtualBox:/home$ sudo useradd -m leiliu
lei@lei-VirtualBox:/home$ ls
lei  leiliu
lei@lei-VirtualBox:/home$ cat /etc/passwd | grep leiliu
leiliu:x:1004:1004::/home/leiliu:/bin/sh
```

设置用户密码

为系统添加用户后，需要使用passwd命令为新用户设置密码，否则新用户无法登录系统。

【命令格式】

- passwd [option] username

【常用选项】

- -d (delete) : 删除用户口令
- -l (lock) : 暂时锁定指定的用户账号
- -u (unlock) : 解除指定用户账号的锁定
- -S (status) : 显示指定用户账号的状态

【参数说明】

- 参数表示要设置密码的用户名称

设置用户密码

【用法示例】

- passwd : 设置当前用户的密码
- passwd leiliu : 设置指定用户的密码

```
lei@lei-VirtualBox:~$ sudo cat /etc/shadow | grep leiliu
leiliu:!:18176:0:99999:7:::
lei@lei-VirtualBox:~$ sudo passwd leiliu
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
lei@lei-VirtualBox:~$ sudo cat /etc/shadow | grep leiliu
leiliu:$6$qW6W6jyk$NnF8XzKZTvYns6I23IrPwnGhZpHWTKASnac/Xdtt8r00U6VCQmXCcN/wmQnoH
BczH9nW4TPU4L.dee7dmShL50:18176:0:99999:7:::
```

root用户可以使用passwd设置所有用户密码

普通用户可以使用passwd设置自身密码

删除用户

该命令用于将系统中不再使用的用户删除。不允许删除正在使用的用户。

【命令格式】

- userdel [option] username

【常用选项】

- -r：删除用户时，连同用户的家目录和邮件文件一并删除

【参数说明】

- 参数表示要删除的用户名称

【用法示例】

- userdel -r leiliu

修改账户

usermod命令用于修改用户的基本信息。

【命令格式】

- usermod [option] username

【常用选项】

- -d : 为用户指定新的家目录
- -m : 为用户指定新的家目录时, 移动原来家目录中的所有文件到新目录(与-d一起使用)
- -s : 修改用户默认的shell
- -l : 修改用户名
- -L : 锁定账号

【参数说明】

- 参数表示要修改的用户名称

【用法示例】

- usermod -md /newdir leiliu (将原来的家目录移动到指定的新目录)
- usermod -s /bin/ksh leiliu

添加用户组

通常将权限相似的用户添加到一个组，然后对组进行管理（例如允许某个用户组访问某个文件）。

【命令格式】

- groupadd groupname

【常用选项】

- -g：指定GID
- -r：创建系统组，不带此选项创建普通组

【参数说明】

- 参数表示要创建的用户组名称

【用法示例】

- groupadd bigdata

```
lei@lei-VirtualBox:/home$ sudo groupadd bigdata
lei@lei-VirtualBox:/home$ cat /etc/group | grep bigdata
bigdata:x:1005:
```

删除用户组

使用groupdel命令删除用户组

【命令格式】

- groupdel groupname

【常用选项】

没有选项

【参数说明】

- 参数表示要删除的用户组名称

【用法示例】

- groupdel bigdata

用户组管理

使用groupmod命令修改组名和GID

【命令格式】

- groupmod [option] groupname

【常用选项】

- -g : 修改GID
- -n : 修改组名

【参数说明】

- 参数表示要修改的用户名称

【用法示例】

- 修改bigdata的GID为1030
groupmod -g 1030 bigdata
- 修改bigdata的组名为hugedata
groupmod -n hugedata bigdata

```
lei@lei-VirtualBox:/home$ sudo groupadd bigdata
lei@lei-VirtualBox:/home$ cat /etc/group | grep bigdata
bigdata:x:1011:
lei@lei-VirtualBox:/home$ sudo groupmod -g 1030 bigdata
lei@lei-VirtualBox:/home$ sudo groupmod -n hugedata bigdata
lei@lei-VirtualBox:/home$ cat /etc/group | grep hugedata
hugedata:x:1030:
```

查看所属组

groups用于显示某用户所属的全部组。

【命令格式】

- groups username

【常用选项】

没有任何选项

【参数说明】

- 参数表示要查看所属组的用户名，没有参数查看当前用户的所属组。

【用法示例】

- groups leiliu
- groups

添加用户到指定组

【命令格式】

- gpasswd [option] username groupname

【常用选项】

- -a : 向指定组添加用户
- -d : 从指定组中删除用户

【参数说明】

- 参数表示要操作的用户名和组名。

【用法示例】

- gpasswd -a leiliu hugedata
- gpasswd -d leiliu hugedata

```
lei@lei-VirtualBox:/home$ groups leiliu
leiliu : leiliu
lei@lei-VirtualBox:/home$ sudo gpasswd -a leiliu hugedata
Adding user leiliu to group hugedata
lei@lei-VirtualBox:/home$ groups leiliu
leiliu : leiliu hugedata
```

查看用户信息

id命令查看用户的UID，GID和用户所属组的信息。

【命令格式】

- id username

【常用选项】

没有任何选项

【参数说明】

- 参数表示要查看信息的用户名，没有参数查看当前用户的信息。

【用法示例】

- id leiliu

```
lei@lei-VirtualBox:~$ id leiliu
uid=1004(leiliu) gid=1010(leiliu) groups=1010(leiliu),1030(hugedata)
```


查看登录用户

who命令查看当前系统的正在登录的用户。

【命令格式】

- who

【常用选项】

没有任何选项

【参数说明】

没有任何参数

【用法示例】

- who

查看历史登录情况

last命令查看系统的历史登录情况。

【命令格式】

- last [option] username

【常用选项】

- n : n为数字，指定查询的次数

【参数说明】

- 参数表示要查看信息的用户名，没有参数查看当前用户的信息。

【用法示例】

- last -5 lei

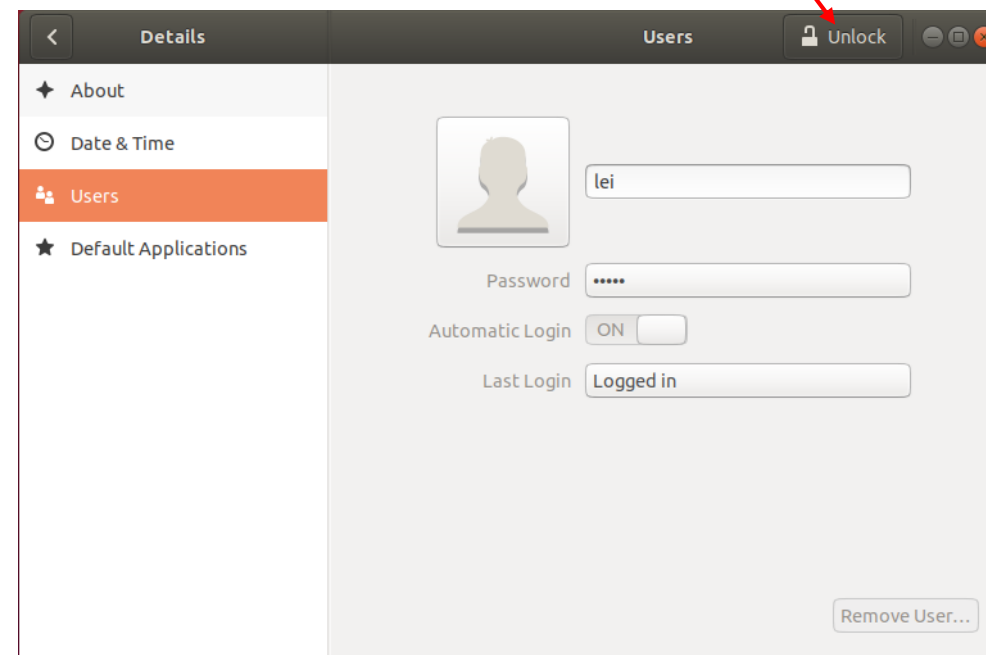
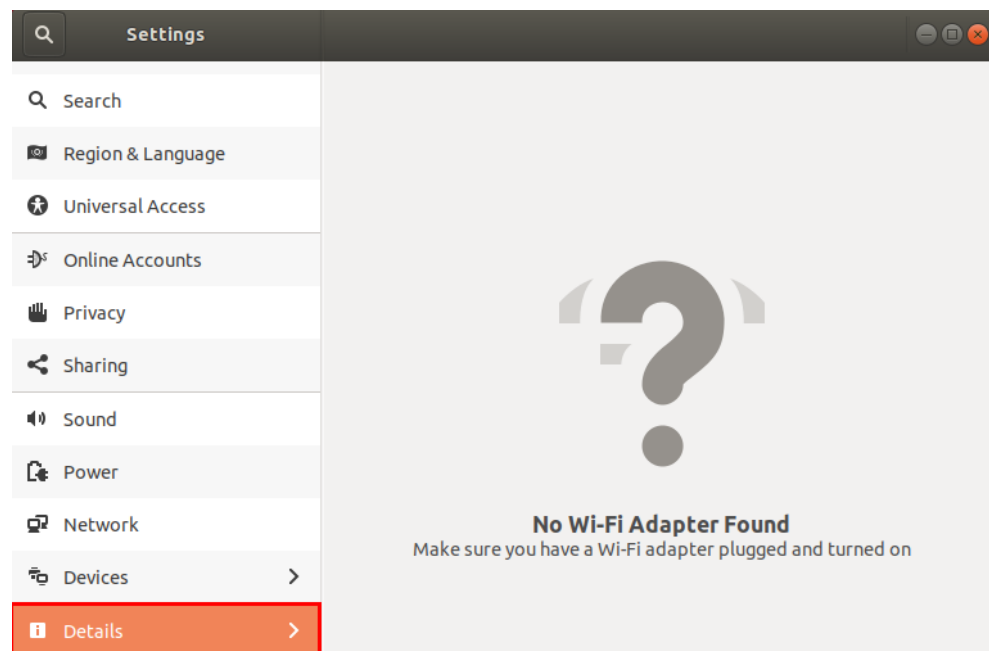
```
lei@lei-VirtualBox:~$ last -5 lei
lei      :0                :0                Sun Oct  6 20:30    still logged in
lei      :0                :0                Sat Oct  5 03:14 - 11:32  (08:18)
lei      :0                :0                Fri Oct  4 22:34 - 03:08  (04:34)
lei      :0                :0                Fri Oct  4 04:20 - down   (18:13)
lei      :0                :0                Thu Oct  3 11:00 - down   (00:26)
```

图形化管理工具

图形化管理工具

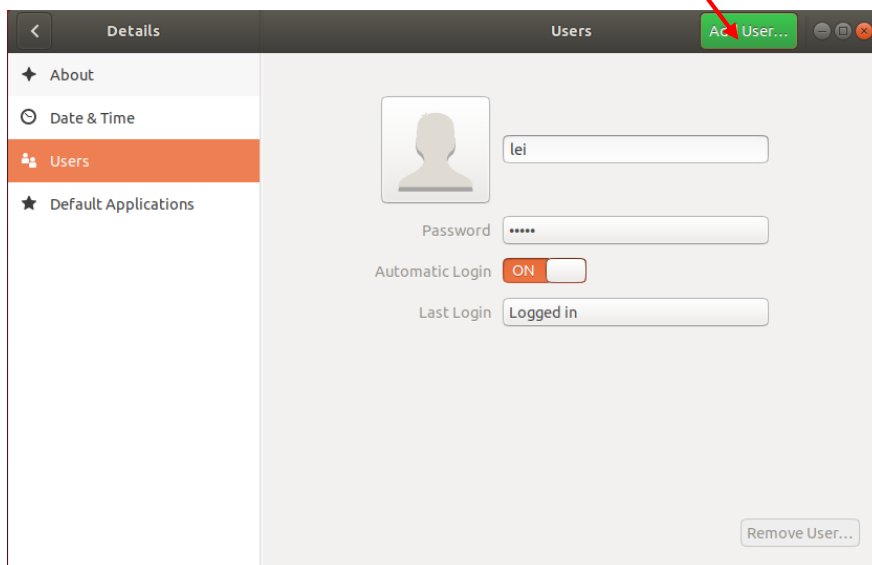
在系统设置中setting=>Details=>Users，可以打开用户管理工具。

解锁

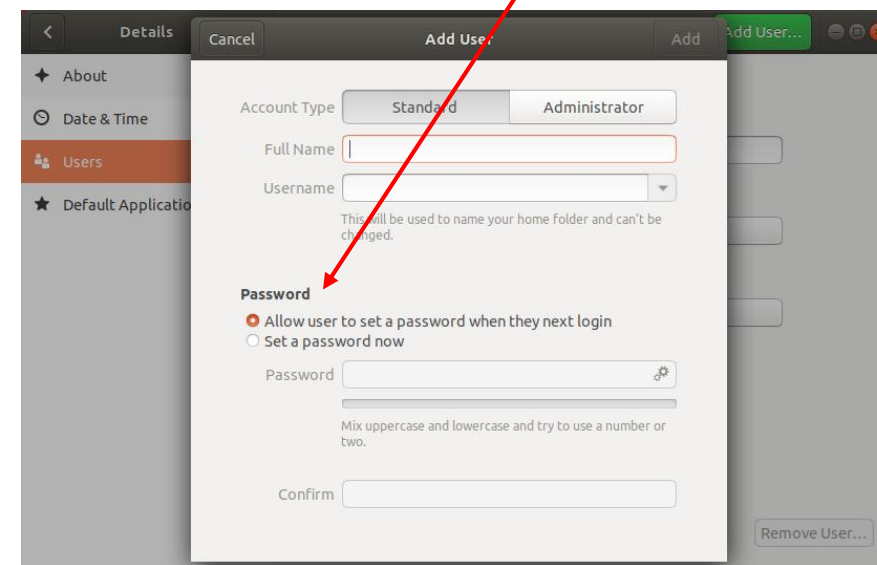


图形化工具

添加用户



现在为用户设置密码
还是用户登录时设置

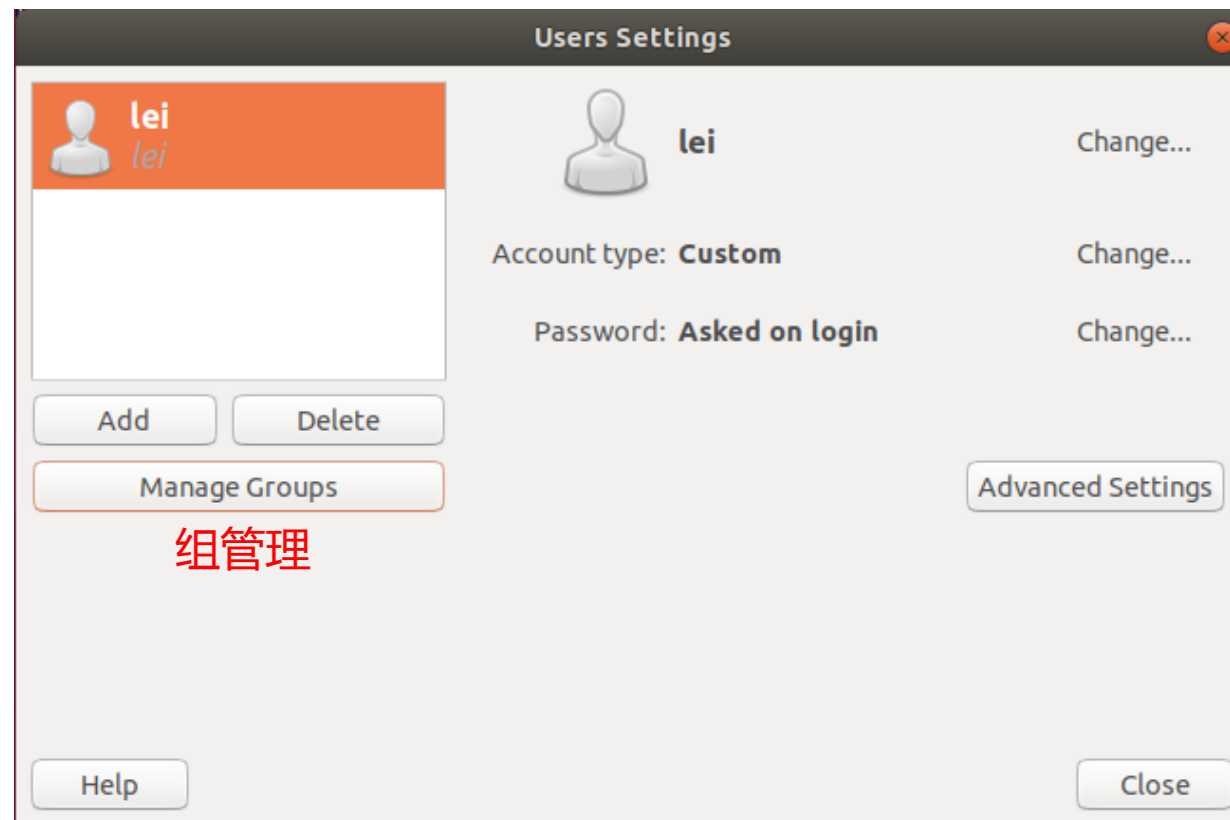


组管理工具

安装gnome-system-tools

```
sudo apt-get install gnome-system-tools
```

在dash中搜索user



组管理工具

