Linux 用户管理

用户帐号

用户在使用计算机系统之前，首先要在系统中为该用户建立一个用户账号。建立用户账号时通常需要指定用户名和口令。用户名就是用户账号名，它代表了用户的身份。口令是操作系统用来验证用户身份的凭证。用户名和口令保存在系统的文件中。

一旦为用户建立了用户账号，该用户就成为系统的合法用户，拥有一定的资源和权限。

在 Linux 中增加新用户时，系统为用户建立一个 home 目录，该目录是用户的根目录，用户的程序和数据都存放在此目录下，用户每次登录系统都以此目录作为工作目录。Linux 还在用户 home 目录下建立了一些隐藏的 shell 脚本文件，如.login 和.profile 文件。这些文件在用户登录系统时自动被执行，以建立用户的程序执行环境。

用户的权限是指用户被准许的访问系统资源的能力。

特权用户与普通用户

为了便于管理系统，通常会将用户分为两类：特权用户和普通用户。

特权用户拥有访问系统资源的所有权限，是系统的管理者。他可以访问和修改系统文件，可以执行所有命令和程序，完成系统配置、安装设备和软件、建立和管理用户账号等系统管理功能。

普通用户只拥有访问系统资源的部分权限，是系统的使用者。他可以访问和修改自己的文件，也可以访问权限之内的其他文件，不能访问和修改系统文件，不能执行系统管理命令和程序。

特权用户拥有建立用户账号的权限，在建立用户账号时，指定用户的类型。程序在运行过程中拥有程序执行者的权限，即特权账号下运行的程序拥有特权用户的权限，普通账号下运行的程序拥有普通用户的权限。

通过限制权限，可以保证普通用户的任何操作不会危害系统的正常运行。而特权用户的任何操作都需要小心谨慎，因为一次失误操作可能会造成系统的重大损失。例如，删除了一个重要的系统文件，使系统无法正常运行；安装或执行了一个不安全的软件，造成计算机病毒或攻击者的入侵。

由此可见，特权用户的权限即方便了系统管理，也带来了安全隐患。我们应该遵照一条安全原则：尽量少使用特权账号，不在特权账号下运行任何未经安全认证的程序。

用户管理

Linux 是一个多用户的操作系统，允许多个用户通过本地登录或远程登录同时使用系统。为了在系统中方便地区分不同用户，给每个用户赋予一个唯一的用户标识号 UID。同时，为了便于多个用户共享资源，引入了用户组的概念。系统管理员（特权用户）可以创建多个用户组，每个用户组有唯一的组标识号 GID，每个用户可以属于一个或多个用户组。通过规定用户组的资源访问权限，使一组用户拥有相同的权限。例如，让一个工作小组的成员对本周

的工作计划文档都拥有读权限。Linux 的用户账号信息和用户组信息分别保存在系统文件/etc/passwd 和/etc/group 中。

在 Linux 中，每个运行的程序（进程）都必需拥有一个用户 UID 和用户组 GID，即拥有相应用户和用户组的权限。为了运行操作系统的服务程序，Linux 设置一些虚拟用户。这类用户不具有登录系统的能力，只能用于运行特定的系统服务程序，如 daemon、adm、ftp、mail 等。

1.添加用户

系统管理员使用 useradd 命令创建一个指定用户名（login-name）的新账号：

useradd [options] login-name

这里 option 是 useradd 命令可以使用的选项，主要有：

-u uid 指定新帐号的用户标识号，缺省时系统给它分配一个 UID；

-g group 指定新帐号的用户组标识号，缺省时系统给它分配一个 GID；

-d dir 指定用户的注册目录（即根目录），缺省值为 HOMEDIR/login，其中，HOMEDIR 是所有用户注册目录所处的位置，login 是新的注册名；

-s shell 指明用户注册后使用何种 shell 命令解释程序，缺省值为/bin/sh；

-c comment 指明新帐号的一个简短注释，它将被放入/etc/passwd 文件中相应登记项的注释字段中；

-e expire 指定该帐号的失效日期，其缺省值为 0，表示无失效期；

-f inactive 指定该用户被允许可以不活动的最多天数，一旦用户未登记进入系统的时间超过该值，该帐号将失效，它的缺省值为 0，表示系统不进行有效期检查。

-p passwd 指定新账号的口令，passwd 是加密后的口令值，缺省时新账号不能被使用，直到使用 passwd 命令为该账号设置了口令。

例如，如果使用下列命令：

#useradd -u 200 -g 100 -d /home/monkey monkey

系统将在/etc/passwd 文件中加入 monkey 的登记项，并指定其用户标识号为 200，用户组号为 100，注册目录为/home/monkey。不过此时 monkey 帐号仍被系统封锁，只有等设置了口令后，才能正式使用。

2. 设置或修改口令

系统管理员使用 passwd 命令为指定用户（user-name）设置初始口令或新口令：

#passwd user-name ←#是特权账号的提示符

New passwd: ←输入新口令，不产生回显

Retype new passwd: ←重复输入新口令

由此可以看出 passwd 命令有如下特点：

·口令要输入两次以防止用户敲键盘错误

·口令不显示以防止别人偷看

然后，用户可以登录系统，使用 passwd 命令修改自己（liming）的口令：

$passwd ←$是非特权账号的提示符

Changing password for liming

Old passwd: ←输入旧口令，不产生回显

New passwd: ←输入新口令，不产生回显

Re-enter new passwd: ←重复输入新口令

当用户忘记口令而进不了系统时，只能求助于特权用户，由系统管理员为用户建立新口令。

3. 删除用户

对于不再使用系统的用户，应及时将其删除，以节约系统资源同时维护系统的安全性，防止不良用户利用这些账号。

系统管理员使用 userdel 命令删除一个用户账号（login-name）：

#userdel [-r] login-name

如果 userdel 命令不带任何选项时，只将用户注册名 login-name 在系统文件/etc/passwd 中的登记项删除掉，而用户的注册目录以及其中的文件保存下来；如果 userdel 命令带-r 选项时，则将此用户的登记项、注册目录以及其中的文件一同删除掉，即彻底地将用户从系统中删除。

4. 增加一个用户组

系统管理员使用 groupadd 命令创建一个指定名字（group-name）的用户组：

groupadd [option] group-name

其中 option 是 groupadd 命令可以使用的选项，主要有：

-g GID 指明新增加的用户组标识。但必须注意普通用户组的标识符必须从 500 开始，因为 0～499 是留给系统用户组使用的。如果没有这个选项，那么系统自动赋予一个组标识。

-r 指明创建一个系统用户组。

例如：

#groupadd -g 520 class

该命令建立一个组名为 class 的普通用户组，系统将在/etc/group 文件中加入 class 的登记项，其组标识为 520。

Linux 也提供了采用图形化界面的用户管理器。可以从桌面系统的主菜单中启动用户管理器。用户管理器实现了查看、搜索、修改、添加和删除注册用户和用户组的操作。

用户登录过程

当用户登录系统时，必须给出用户名和口令。系统将用户输入的口令与系统文件中保存的口令进行比较，以此来验证用户的真实身份。只有通过身份验证，用户才被允许进入系统。这时系统将建立起用户环境（桌面环境或程序执行环境），启动用户界面进程。这就是用户的登录过程（如图 1），通常由登录管理系统进程负责完成此过程。

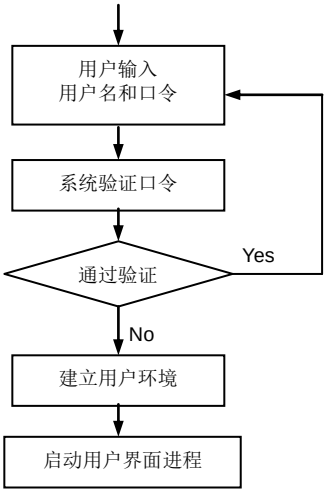

图 1 用户登录过程

用户进入系统后，与用户界面程序（进程）进行交互，或输入命令行，或操作图形界面。

用户界面进程也是系统进程，或者运行命令解释程序，提供命令使用界面；或者运行桌面环境程序，提供图形用户界面。

命令解释程序

命令解释程序负责接收用户从终端设备或窗口中输入的命令字符行，解释执行每条命令，将执行结果显示在终端设备或窗口中。命令解释程序的主要流程如图 2 所示。

用户输入的命令可以是执行操作系统的命令程序，如显示文件目录清单、显示系统时间、或提交一个批处理作业；也可以是执行一个应用程序，如执行 c 语言编译程序、启动文本处理程序、或执行用户的应用程序。

命令行通常包括命令名和命令参数两部分。命令名是实现命令功能的程序文件名，命令参数是命令程序或应用程序的输入数据。当用户输入一条命令后，命令解释程序首先分析命令行的语法结构，根据命令名查找需要执行的程序文件；创建进程执行该程序，并将命令参数传递给它；等待程序运行结束后，显示执行结果；等待用户输入下一条命令。

命令程序或应用程序在执行过程中也可以利用终端设备或窗口与用户交换信息，但是，交换的信息仅限于字符信息。即用户可以从终端输入数据给程序，程序也可以输出数据显示在终端上。

由此可见，在命令用户界面下，用户与系统以及用户与程序之间的交互活动都是在终端设备上完成的。为了不发生混乱，每个程序在执行时都需要与一个终端设备绑定。在早期，终端设备由字符显示器和键盘组成，通过在计算机系统中连接多个物理终端设备，让每个用户使用一个终端设备，用户运行的程序都与其使用的终端设备绑定。后来，随着图形显示器的出现和图形显示技术的发展，操作系统实现了虚拟终端设备机制，将虚拟终端映射到图形界面下的一个窗口，每个窗口对应一个命令解释进程，用户在窗口中输入命令。用户可以打开多个终端窗口，同时运行多个应用程序。

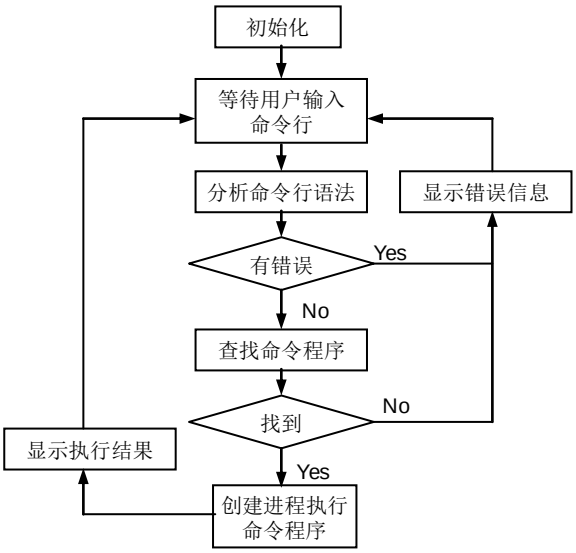

图 2 命令解释程序流程图

同样，如果将计算机 A 的虚拟终端映射到网络连接的另一台计算机 B 上，用户就可以在计算机 B 上远程使用系统 A 的命令界面，用户在计算机 B 上输入的命令将传送到计算机 A 上执行，而执行的结果将送回到计算机 B 的屏幕上。就好像用户在直接使用计算机 A 一样。Telnet 就是实现 Unix 或 Linux 的远程虚拟终端的常用软件之一。

命令界面是操作系统最基本的用户界面，它虽然没有图形界面方便，但具有以下不可替

代的优点：

（1）使用灵活，执行效率高；

每条命令可以带多个命令参数或选项。使用不同的参数或选项，就可以让命令灵活地、有选择地实现功能。命令的执行不需要复杂的图形显示过程，当然执行效率高。

（2）扩展性好

命令是由程序直接实现的，因此易于增加新功能和新命令。也可以将多个命令组合起来实现复杂的功能。

（3）适用范围广

命令界面对硬件设备要求不高，能适应各种应用场合，特别是那些没有图形设备的应用系统。由于命令界面传输的是字符数据，更适合对速度性能有特殊要求的网络应用。