**Linux 下/etc/passwd文件详解**

在Linux /etc/passwd文件中每个用户都有一个对应的记录行，它记录了这个用户的一些基本属性。系统管理员经常会接触到这个文件的修改以完成对用户的管理工作。这个文件对所有用户都是可读的。但是Linux /etc/passwd文件中都有些什么内容呢？

　　root:x:0:0:root:/root:/bin/bash

　　bin:x:1:1:bin:/bin:/sbin/nologin

　　daemon:x:2:2:daemon:/sbin:/sbin/nologin

　　desktop:x:80:80:desktop:/var/lib/menu/kde:/sbin/nologin

　　mengqc:x:500:500:mengqc:/home/mengqc:/bin/bash

从上面的例子我们可以看到，/etc/passwd中一行记录对应着一个用户，每行记录又被冒号(:)分隔为7个字段，其格式和具体含义如下：   
　　**用户名**:**口令**:**用户标识号**:**组标识号**:**注释性描述**:**主目录**:**登录Shell**

　　用户名(login\_name):是代表用户账号的字符串。通常长度不超过8个字符，并且由大小写字母和/或数字组成。登录名中不能有冒号(:)，因为冒号在这里是分隔符。为了兼容起见，登录名中最好不要包含点字符(.)，并且不使用连字符(-)和加号(+)打头。

　　口令(passwd):一些系统中，存放着加密后的用户口令字。虽然这个字段存放的只是用户口令的加密串，不是明文，但是由于/etc/passwd文件对所有用户都可读，所以这仍是一个安全隐患。因此，现在许多Linux系统（如SVR4）都使用了shadow技术，把真正的加密后的用户口令字存放到/etc/shadow文件中，而在/etc/passwd文件的口令字段中只存放一个特殊的字符，例如“x”或者“\*”。

　　用户标识号(UID):是一个整数，系统内部用它来标识用户。一般情况下它与用户名是一一对应的。如果几个用户名对应的用户标识号是一样的，系统内部将把它们视为同一个用户，但是它们可以有不同的口令、不同的主目录以及不同的登录Shell等。取值范围是0-65535。0是超级用户root的标识号，1-99由系统保留，作为管理账号，普通用户的标识号从100开始。在Linux系统中，这个界限是500。

　　组标识号(GID):字段记录的是用户所属的用户组。它对应着/etc/group文件中的一条记录。

　　注释性描述(users):字段记录着用户的一些个人情况，例如用户的真实姓名、电话、地址等，这个字段并没有什么实际的用途。在不同的Linux系统中，这个字段的格式并没有统一。在许多Linux系统中，这个字段存放的是一段任意的注释性描述文字，用做finger命令的输出。

　　主目录(home\_directory):也就是用户的起始工作目录，它是用户在登录到系统之后所处的目录。在大多数系统中，各用户的主目录都被组织在同一个特定的目录下，而用户主目录的名称就是该用户的登录名。各用户对自己的主目录有读、写、执行（搜索）权限，其他用户对此目录的访问权限则根据具体情况设置。

　　登录Shell(Shell):用户登录后，要启动一个进程，负责将用户的操作传给内核，这个进程是用户登录到系统后运行的命令解释器或某个特定的程序，即Shell。Shell是用户与Linux系统之间的接口。Linux的Shell有许多种，每种都有不同的特点。常用的有sh(BourneShell),csh(CShell),ksh(KornShell),tcsh(TENEX/TOPS-20typeCShell),bash(BourneAgainShell)等。系统管理员可以根据系统情况和用户习惯为用户指定某个Shell。如果不指定Shell，那么系统使用sh为默认的登录Shell，即这个字段的值为/bin/sh。

　　用户的登录Shell可以指定为某个特定的程序（此程序不是一个命令解释器）。利用这一特点，我们可以限制用户只能运行指定的应用程序，在该应用程序运行结束后，用户就自动退出了系统。有些Linux系统要求只有那些在系统中登记了的程序才能出现在这个字段中。

账号描述：

　　1、

　　系统帐号：系统中还有一些默认的帐号，如daemon、bin等。这些帐号有着特殊的用途，一般用于进行系统管理。这些帐号的口令大部分用（x）号表示，代表它们不能在登录时使用。

　　bin拥有可执行的用户命令文件   
　　sys拥有系统文件   
　　adm拥有帐户文件   
　　uucpUUCP使用   
　　lplp或lpd子系统使用   
　　nobodyNFS使用

　　2、除了上面列出的伪用户外，还有许多标准的伪用户，例如：audit,cron,mail,usenet等，它们也都各自为相关的进程和文件所需要。由于Linux /etc/passwd文件是所有用户都可读的，如果用户的密码太简单或规律比较明显的话，一台普通的计算机就能够很容易地将它破解，因此对安全性要求较高的Linux系统都把加密后的口令字分离出来，单独存放在一个文件中，这个文件是/etc/shadow文件。只有超级用户才拥有该文件读权限，这就保证了用户密码的安全性。

Linux口令管理之/etc/passwd文件：

　　/etc/passwd文件是Linux/UNIX安全的关键文件之一.该文件用于用户登录时校验 用户的口令,当然应当仅对root可写.文件中每行的一般格式为:

　　LOGNAME:PASSWORD:UID:GID:USERINFO:HOME:SHELL

　　每行的头两项是登录名和加密后的口令,后面的两个数是UID和GID,接着的 一项是系统管理员想写入的有关该用户的任何信息,最后两项是两个路径名: 一个是分配给用户的HOME目录,第二个是用户登录后将执行的shell(若为空格则 缺省为/bin/sh).

　(1)口令时效

　　/etc/passwd文件的格式使系统管理员能要求用户定期地改变他们的口令. 在口令文件中可以看到,有些加密后的口令有逗号,逗号后有几个字符和一个 冒号.如:

　　steve:xyDfccTrt180x,M.y8:0:0:admin:/:/bin/sh

　　restrict:pomJk109Jky41,.1:0:0:admin:/:/bin/sh

　　pat:xmotTVoyumjls:0:0:admin:/:/bin/sh

　　可以看到,steve的口令逗号后有4个字符,restrict有2个,pat没有逗号.

　　逗号后第一个字符是口令有效期的最大周数,第二个字符决定了用户再次 修改口信之前,原口令应使用的最小周数(这就防止了用户改了新口令后立刻 又改回成老口令).其余字符表明口令最新修改时间.

　　要能读懂口令中逗号后的信息,必须首先知道如何用passwd\_esc计数,计 数的方法是:

　　.=0 /=1 0-9=2-11 A-Z=12-37 a-z=38-63

　　系统管理员必须将前两个字符放进/etc/passwd文件,以要求用户定期的 修改口令,另外两个字符当用户修改口令时,由passwd命令填入.

　　注意:若想让用户修改口令,可在最后一次口令被修改时,放两个”.”,则下 一次用户登录时将被要求修改自己的口令.

　　有两种特殊情况:

　　.最大周数(第一个字符)小于最小周数(第二个字符),则不允许用户修改 口令,仅超级用户可以修改用户的口令.

　　.第一个字符和第二个字符都是”.”,这时用户下次登录时被要求修改口 令,修改口令后,passwd命令将”.”删除,此后再不会要求用户修改口令.

(2)UID和GID

　　/etc/passwd中UID信息很重要,系统使用UID而不是登录名区别用户.一般 来说,用户的UID应当是独一无二的,其他用户不应当有相同的UID数值.根据惯 例,从0到99的UID保留用作系统用户的UID(root,bin,uucp等).

　　如果在/etc/passwd文件中有两个不同的入口项有相同的UID,则这两个用 户对相互的文件具有相同的存取权限.

　　/etc /group文件含有关于小组的信息,/etc/passwd中的每个GID在本文件中 应当有相应的入口项,入口项中列出了小组名和小组中的用户.这样可方便地了 解每个小组的用户,否则必须根据GID在/etc/passwd文件中从头至尾地寻找同组 用户.

　　/etc/group文件对小组的许可权限的控制并不是必要的,因为系统用UID,GID (取自/etc/passwd)决定文件存取权限,即使/etc/group文件不存在于系统中,具 有相同的GID用户也可以小组的存取许可权限共享文件.

　　小组就像登录用户一样可以有口令.如果/etc/group文件入口项的第二个域 为非空,则将被认为是加密口令,newgrp命令将要求用户给出口令,然后将口令加 密,再与该域的加密口令比较.

　　给 小组建立口令一般不是个好作法.第一,如果小组内共享文件,若有某人猜 着小组口令,则该组的所有用户的文件就可能泄漏;其次,管理小组口令很费事, 因为对于小组没有类似的passwd命令.可用/usr/lib/makekey生成一个口令写入 /etc/group.

以下情况必须建立新组:

　　(1)可能要增加新用户,该用户不属于任何一个现有的小组.

　　(2)有的用户可能时常需要独自为一个小组.

　　(3)有的用户可能有一个SGID程序,需要独自为一个小组.

　　(4)有时可能要安装运行SGID的软件系统,该软件系统需要建立一个新组.

　　要 增加一个新组,必须编辑该文件,为新组加一个入口项. 由于用户登录时,系统从/etc/passwd文件中取GID,而不是从/etc/group中 取GID,所以group文件和口令文件应当具有一致性.对于一个用户的小组,UID和 GID应当是相同的.多用户小组的GID应当不同于任何用户的UID,一般为5位数,这 样在查看/etc/passwd文件时,就可根据5位数据的GID识别多用户小组,这将减少 增加新组,新用户时可能产生的混淆.