# 管理用户和用户组

这一节详细讨论关于用户和用户组的管理，包括设置密码，设置相关属性，对用户组的相关管理，查看当前用户，切换用户等；

## 用户管理

用户管理实质上是在修改用户的配置文件，而用户管理工具最终也是在操作用户的配置文件；管理工具其实就是一个个的命令，比如添加用户useradd，添加密码passwd等，它的实质其实就是在修改配置文件，直接修改配置文件也可以达到相同的目的

用户配置都放在/etc/shadow和/etc/passwd 这两个文件中，shadow中存放了用户的加密后的密码，passwd存放了用户的基本配置，这两个文件是互补的

### /etc/passwd

这个文件系统用来识别用户，当某个用户登录时，系统首先会在这个文件中寻找相关的用户名，如果找到，则确定他的uid，然后通过UID来确认身份和表示信息，如果存在，则读取/shadow中的密码，用户输入密码，如果正确，则登录系统，读取用户的配置文件；

Passwd内容理解：下图是一个基本的passwd中某一行的内容，每一行的格式都是如此：

|  |  |
| --- | --- |
|  | |
| 第一字段：用户名（登录名） | 这里使用allen作为用户名 |
| 第二字段：密码 | 这里显示x，因为真实密码已经被映射到/etc/shadow中 |
| 第三字段：UID | 下面会讨论 |
| 第四字段：GID | 下面会讨论 |
| 第五字段：用户名全称 | 这个是可选的，可以不设置 |
| 第六字段：用户的根目录所在位置 | Allen这个用户的就是/home/allen； |
| 第七字段：用户所用的shell类型 | Allen使用的是bash，所以是/bin/bash |

|  |  |
| --- | --- |
| UID | |
| 概念 | UID是系统用来标示用户，每个UID都是唯一的，每个用户一个唯一的UID，系统要确保这一规则，UID从0开始，是一个非负整数，root的UID标示为0，表示拥有最高权限，UID的最大值依据系统决定，一般放在/etc/login.defs中，一般的Linux是60000； |
| 唯一性 | 系统要确保用户拥有唯一的UID，这关系到系统安全；试想，如果Allen的UID改为0，那Allen就具有了超级权限 |
| 独立性 | UID是确认用户的标示，系统确认用户是通过UID来实现的，而不是用户名；所以不要让几个用户共用一个UID，这会造成管理的混乱，如果临时想要获取root权限，可以使用su或者sudo来实现；决不能让其他用户和root共享一个UID |
| 虚拟用户UID | 一般，Linux发行版都会给每个系统预留一定的UID和GID，这些被称为虚拟用户，它是系统安装时就创建的，用来完成系统任务所必须的用户，但他们不能用来登录系统，比如ftp,adm,rpm,nobody,bin,shutdown等； |
| 登录用户UID | Centos系统会把前499个UID和GID给虚拟用户占用，登录用户UID和GID是从500开始的，不过有些系统会把999都留出来，取决于etc/login.defs中的UID.min和UID.max； |

### /etc/shadow:

这个文件是/etc/passwd的影子文件，并不是由passwd产生，而是互补关系，它存放了一些passwd中不能存放的东西，比如密码，用户过期时间等安全信息，这个文件只有root可以读取；

不能让其他用户查看这个文件，不要随便更改这个文件的权限给其他用户，一旦发现权限被改，应该立即检查；

下图展示了“shadow”文件中各个字段的含义：

|  |  |
| --- | --- |
|  | |
| 第一字段：用户名 | 和passwd中是相同的，这样就把passwd和shadow中的用户记录联系在一起；非空字段 |
| 第二字段：密码（加密后）， | 如果有些用户在这个字段上是x，表示这个用户不能登录到系统，也可以看做虚拟用户，虚拟用户也可以被管理员修改和操控；非空字段 |
| 第三字段：上次修改密码的时间 | 这个时间是一个时间戳，从1970.1.01开始，到最近一次改密码的时间 |
| 第四字段：两次改密码之间间隔天数 | 如果设置为0，表示禁用此功能；这个功能表示用户必须间隔多少天才能再改密码，默认值是/etc/login/defs中定义的PASS\_MIN\_DAYS中定义的； |
| 第五字段：两次修改密码间隔最多天数 | 这个能增强系统管理用户的时效性，增强了系统安全性。默认值是在添加用户时通过/etc/login.defs中定义的，PASS\_MAX\_DAYS中定义 |
| 第六字段：提前多少天警告用户口令将过期 | 当用户登录系统后，系统会提醒用户口令将作废；如果是默认值，则在添加用户时由/etc/login.defs中的PASS\_WARN\_AGE中定义； |
| 第七字段：在口令过期多少天后禁用此用户 | 此字段表示用户口令作废多少天后，系统会禁用这个用户，系统不会再让这个用户登录，，也不会提示用户过期，是完全禁用； |
| 第八字段：账户过期时间 | 表示用户在何时过期，时间从1970.1.01开始的天数，如果为空，则表示永不过期 |
| 第九字段 | 保留字段 |

## 用户组管理

用户组就是具有共同特征的用户组成的一个组，配合文件存放在/etc/group和/etc/gshadow中，gshadow是存放group的加密文件；

### /etc/group配置分析：

这个文件中存放着用户和用户组，标示了用户属于哪个用户组或者哪几个用户组，因为一个用户可以属于多个用户组，同一用户组之间的用户具有相似的特征，比如把某一个用户加入root组中，它就可以浏览root根目录下的文件。如果root用户把某个文件的读写执行权限开放，则同组的其他用户都可以执行；

Group这个文件是用户组的配置文件，如果某个用户有着对系统最重要的内容，可以让他单独成组，或者把用户下的文件设置为完全私有化；另外，不要把某个用户轻易加到root用户组中

文件格式详解：

|  |  |
| --- | --- |
|  | |
| 第一字段：用户组名称 |  |
| 第二字段：用户组密码 | x表示没有设置密码 |
| 第三字段：GID | 用户组id，下面讨论 |
| 第四字段：用户列表 | 每个用户之间逗号分隔，本字段可以为空，如果为空，表示用户组为GID的用户名 |

|  |  |
| --- | --- |
| GID | |
| 概念 | 是一个非负整数，从0开始，0表示root用户组，预留了一些GID给虚拟用户，所以centos从500开始分配用户组，默认的GID范围在/etc/login.defs中的GID\_MIN和GID\_MAX中 |
| 在判断用户的访问权限时，默认的GID不是最重要的，只要一个目录让同组用户可以访问的权限，那同组用户就可以拥有该目录的访问权，不管默认的GID是什么； | |

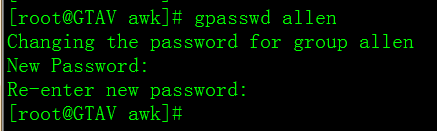
### /etc/gshadow配置分析

这个文件是/group的加密密码文件，用户组的密码就放在这个文件中；设置用户组密码对于大型服务器是非常必要的：比如不想让一些非用户组成员永久性的拥有用户组的权限，可以通过密码验证的方式，临时让他们拥有权限，设置密码过期时间，即可收回权限；

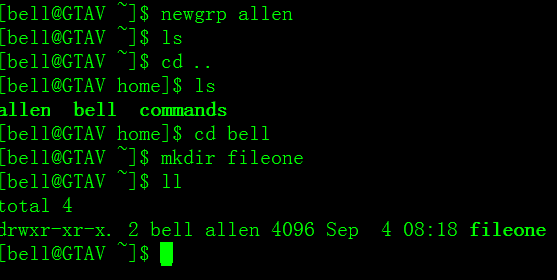
文本格式如下图：

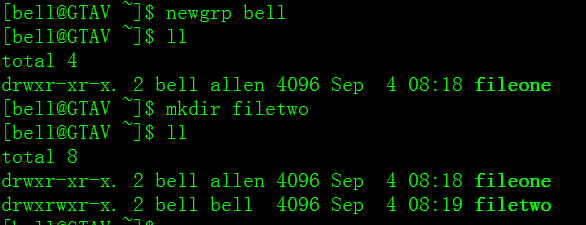
|  |  |
| --- | --- |
|  | |
| 第一字段：用户组名称 |  |
| 第二字段：用户组密码 | 空或者！表示空密码 |
| 第三字段：用户组管理者 | 这里是空 |
| 第四字段： | 表示本组里拥有的成员 |

使用gpasswd命令来设置用户组密码，下面展示了这种用法



使用newgrp来切换用户组，下面展示了这种用法

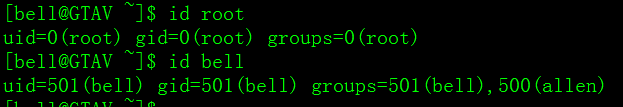




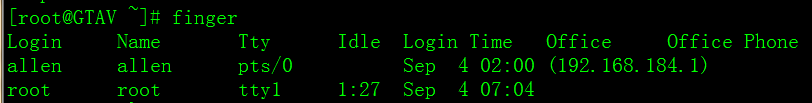
## 查询用户和用户组

### 通过查看用户的配置文件来查看用户信息

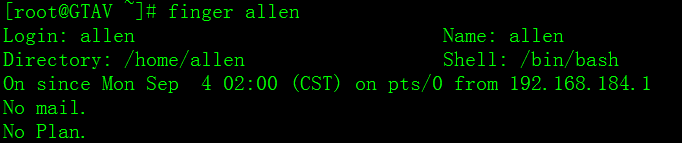
1. 我们可以通过more或者less或者cat命令来查看上面所描述的文件；
2. 通过id或者finger工具查看，ID工具侧重用户，组，uid，gid的查看，finger侧重于用户信息的查询，比如登录名，电话，登录shell类型等；下图演示了这两种方法：（这里不研究id和finger方法，专门的文档来写）

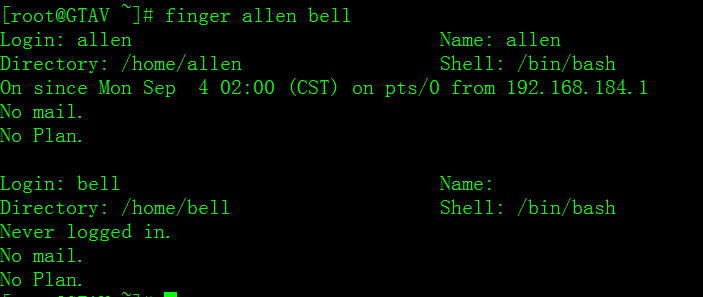


使用finger不带参数和使用w命令是一样的



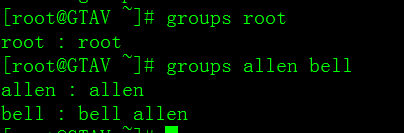
如果finger后加用户名，则会打印更详细的内容





### 用户组的查询

1. 使用groups来查询用户所归属的组



### 修改配置文件来实现对用户组和用户的添加，修改，删除

1. 添加用户（通过修改用户和用户组的配置文件）
2. 修改用户信息
3. 删除用户及用户组办法

只要删除/etc/passwd和/etc/group中的相应记录即可，也可以通过用userdel和groupdel来实现；不想保留根目录，删除即可

来源：http://www.cnblogs.com/zhoug2020/#undefined