**第六章 Centos7用户管理**

**本节所讲内容：**

**6.1 用户和组的相关配置文件**

**6.2 管理用户和组**

**6.3实战：进入centos7 紧急模式恢复root密码**

**用户一般来说是指使用计算机的人，计算机对针使用其的每一个人给了一个特定的名称，用户就可以使用这些名称来登录使用计算机，除了人之外，一些系统服务也需要含有部分特权的用户账户运行；因此出于安全考虑，用户管理应运而生，它加以明确限制各个用户账户的权限，root在计算机中用拥有至高特权，所以一般只作管理用，非特权用户可以通过SU或SUDO程序来临时获得特权**

**GNU/Linux 通过用户和用户组实现访问控制----包括对文件访问、设备使用的控**

**个人可以拥有很多账户，只不是彼此名称不同，比如root名称已经占用就不能再用了，此外，任意用户可能从属某个用户组，此用户可以加入某些已经存在的组来获得该组的特权**

**GNU/Linux 系统中的每一个文件都有属一个用户（属主）和一个用户组（属组）。另外，还有三种类型的访问权限：读（read）、写（write）、运行（execute）。我们可以针对文件的属主、属组、而设置相应的访问权限。再次，我们可以通过 ls | stat命令查询文件属主、属组和权限**

**[root@xuegod63 ~]# ll | head -2**

**总用量 8**

**-rw-------. 1 root root 1680 9月 19 2017 anaconda-ks.cfg**

**[root@xuegod63 ~]# stat anaconda-ks.cfg**

**文件："anaconda-ks.cfg"**

**大小：1680 块：8 IO 块：4096 普通文件**

**设备：803h/2051d Inode：16797763 硬链接：1**

**权限：(0600/-rw-------) Uid：( 0/ root) Gid：( 0/ root)**

# 6.1 用户账号

# 6.1.1 用户的分类

**Linux用户三种角色**

**超级用户： root 拥有对系统的最高的管理权限 ID=0**

**普通用户：系统用户 UID:1-999(centos7版本) 1-499(centos6版本)**

**本地用户 UID:1000+ 500+**

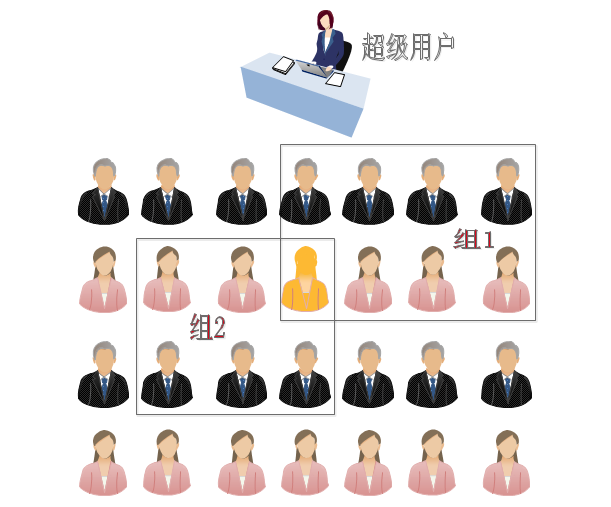
**UID:即每个用户的身份标示,类似于每个人的身份证号码.**

**虚拟用户：伪用户 一般不会用来登录系统的，它主要是用于维持某个服务的正常运行.如：ftp，apache**

**下图是用户和组的关系：**

**一对一：一个用户可以存在一个组中； 一对多：一个用户可以存在多个组中**

**多对一：多个用户可以存在一个组中； 多对多：多个用户可以存在多个组中**

****

## 6.1.2 配置文件

|  |  |  |
| --- | --- | --- |
| **名 称** | **帐号信息** | **说 明** |
| **用户配置文件** | **/etc/passwd** | **记录了每个用户的一些基本属性，并且对所有用户可读，每一行记录对应一个用户，每行记录通过冒号进行分隔** |
| **用户组文件** | **/etc/group** | **用户组的所有信息存放地儿，并且组名不能重复** |
| **用户对应的密码信息** | **/etc/shadow** | **因为passwd文件对所有用户是可读的，为安全起见把密码从passwd中分离出来放入这个单独的文件，该文件只有root用户拥有读权限，从而保证密码安全性** |

# 6.2 用户管理

## 6.2.1 用户命令

**命令：useradd**

**useradd -d -u “UID” -g "初始组" -G "附加组" -s "登陆的shell” 用户**

**-d： -d 用户主目录路径， 可以指定用户家目录**

**-M: 不创建用户的主目录**

**-g：设置用户初始组的名称或数字ID；该组必须是存在的；如果没有设置该选项，useradd会根据/etc/login.defs文件中的USERGROUPS\_ENAB环境变量进行设置。默认USERGROUPS\_ENAB yes 会用和用户名相同的名字创建群组，GID 等于 UID.**

**-G：用户要加入的附加组列表；使用逗号分隔多个组，不要添加空格；如果不设置，用户仅仅加入初始组。(一个用户只允许有一个主组，可以有多个附属组)**

**-s：用户默认登录shell的路径；启动过程结束后，默认启动的登录shell在此处设定；请确保使用的shell已经安装，默认是**[**Bash**](https://wiki.archlinux.org/index.php/Bash)**。有时候需要禁止某些用户执行登录动作，例如用来执行系统服务的用户。将shell设置成 /sbin/nologin 就可以禁止用户登录。**

## 6.2.2 添加登录用户

**例：添加一个名为harry的用户，并使用bash作为登录的shell**

**[root@panda ~]# useradd harry**

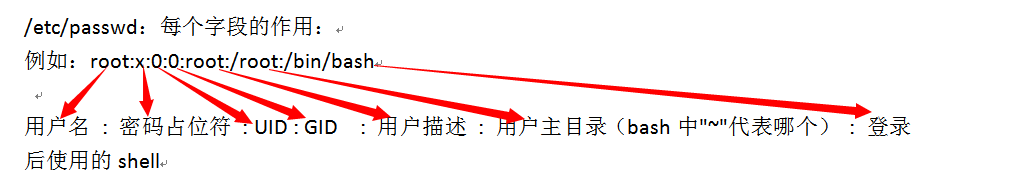
**[root@panda ~]# tail -1 /etc/passwd**

**harry:x:1001:1001::/home/harry:/bin/bash**

**说明：此命令会自动创建harry组，并成为harry用户的默认主组，同时默认的登录shell是bash**

**用户帐户的全部信息被保存在/etc/passwd文件。这个文件以如下格式保存了每一个系统帐户的所有信息 (字段以“:”分割)**

**harry:x:1001:1001::/home/harry:/bin/bash**

**harry：用户名**

**x：密码占位符**

**1001：用户的UID，它都是用数字来表示的**

**1001：用户所属组的GID，它都是用数字来表示的**

**用户描述信息：对用户的功能或其它来进行一个简要的描述**

**/home/harry：用户主目录（shell提示符中“~”代表的那个）**

**/bin/bash：用户登录系统后使用的shell**

**#查看系统中，支持哪些shell**

**[root@xuegod63 ~]# cat /etc/shells #查看系统中，支持哪些shell**

**/bin/sh**

**/bin/bash**

**/sbin/nologin**

**/bin/csh**

### 6.2.3 指定用户UID : -u 用户ID

**[root@xuegod63 ~]# useradd -u 1100 oracle**

**[root@xuegod63 ~]# id oracle**

**uid=1100(oracle) gid=1100(oracle) 组=1100(oracle)**

**[root@xuegod63 ~]# tail -1 /etc/passwd**

**oracle:x:1100:1100::/home/oracle:/bin/bash**

**[root@xuegod63 ~]# ls /home/oracle/ -a**

**. .. .bash\_logout .bash\_profile .bashrc .mozilla**

### 6.2.4 指定用户主目录

**[root@xuegod63 ~]# useradd -d /opt/mk1 mk1**

**[root@xuegod63 ~]# tail -1 /etc/passwd**

**mk1:x:1102:1102::/opt/mk1:/bin/bash**

### 6.2.5 指定用户的主组

**例：**

**[root@xuegod63 ~]# useradd xuegod**

**[root@xuegod63 ~]# id xuegod**

**uid=1103(xuegod) gid=1103(xuegod) 组=1103(xuegod)**

**[root@xuegod63 ~]# useradd -g xuegod xuegod2**

**[root@xuegod63 ~]# id xuegod2**

**uid=1104(xuegod2) gid=1103(xuegod) 组=1103(xuegod)**

### 6.2.6 指定用户的附属组

**我们也可以把这个附属组称为补充组，用户可以有0个或多个附加组的成员**

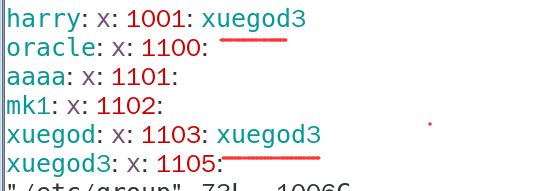
**如果一个组有多个成员，我们是可以在/etc/group文件中最后一个字段看到的**

**[root@xuegod63 ~]# useradd -G xuegod,harry,root xuegod3**

**[root@xuegod63 ~]# id xuegod3**

**uid=1105(xuegod3) gid=1105(xuegod3) 组=1105(xuegod3),0(root),1001(harry),1103(xuegod)**

**[root@xuegod63 ~]# vim /etc/group #在文件的最后**



### 6.2.7 创建用户的另外一个命令

**[root@xuegod63 ~]# adduser xuegod4**

**[root@xuegod63 ~]# id xuegod4**

**uid=1106(xuegod4) gid=1106(xuegod4) 组=1106(xuegod4)**

**[root@xuegod63 ~]# which adduser**

**/usr/sbin/adduser**

**[root@xuegod63 ~]# ll /usr/sbin/adduser**

**lrwxrwxrwx. 1 root root 7 9月 19 2017 /usr/sbin/adduser -> useradd**

**注： adduser是useradd的软链接**

### 6.2.8 删除用户

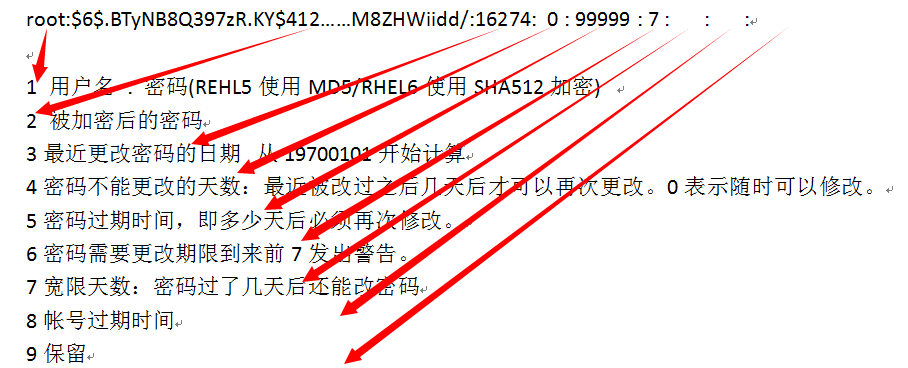
**usage: userdel [options] LOGIN**

**选项：-r 删除的时候，会同时删除用户的家目录和/var/mail下的目录**

## 6.2.9 密码的文件

**[root@xuegod63 ~]# head -3 /etc/shadow**

**root:$6$C88LCVx5ZjfBU7xv$cKcdyNeTFmOYTs9NbRZDTA4hGcbMXc/5hQEWZKCtNyLqlBagrjct.pMfs39iEaF1UbEvcOzWZHMDf9Q5KojXM1::0:99999:7:::**

****

**格式如下：**

|  |  |
| --- | --- |
| **name** | **登录名称，这个必须是系统中的有效账户名** |
| **password** | **已加密密码，分为三个部分，第一部分是表示使用哪种哈希算法；第二部分是用于加密哈希的salt;第三部分是已加密的哈希**  **哈希算法：$1表示MD5 ; $6 表示SHA-512 ; $5 SHA-256**  **查看帮助说明：**  **man 5 passwd**  **man 5 shadow**  **man 5 group**  **man 3 crypt** |
| **lastchange** | **最近一次更改密码的日期，以距离1970/1/1的天数表示** |
| **min-age** | **不能更改密码的最少天数，最近更改过后几天才可以更改；如果为0表示“最短期限要求”** |
| **maxage** | **密码过期时间，必须更改密码前的最多天数** |
| **warning** | **密码即将到期的警告期，以天数表示，0表示“不提供警告”** |
| **inactive** | **宽限天数，密码到期后** |
| **expire** | **账号过期时间，以距离1970/1/1的天数计算 (千年虫)** |
| **blank** | **预留字段** |

**给用户添加密码：**

**[root@panda home]# passwd oracle 交互**

**Changing password for user oracle.**

**New password:**

**BAD PASSWORD: The password is shorter than 8 characters**

**Retype new password:**

**passwd: all authentication tokens updated successfully.**

**[root@xuegod63 ~]# echo 123456 | passwd --stdin xuegod #不交互**

**[root@xuegod63 ~]# echo 123456 | passwd --stdin harry**

**互动： 两个用户的密码一样？ 那么shadow中加密的hash值一样吗？**

**答： 不一样。 因为salt不一样**

**把2段加密的互换还能登陆吗？salt什么时候指定的？**

## 6.2.10 控制添加用户规则文件的两个文件：/etc/default/useradd 和 /etc/login.defs

**[root@panda home]# egrep -v "^$|^#" /etc/login.defs**

**MAIL\_DIR /var/spool/mail**

**PASS\_MAX\_DAYS 99999**

**PASS\_MIN\_DAYS 0**

**PASS\_MIN\_LEN 5**

**PASS\_WARN\_AGE 7**

**UID\_MIN 1000 #用户ID开始的数字**

**UID\_MAX 60000 # 用户ID结束的数字**

**SYS\_UID\_MIN 201**

**SYS\_UID\_MAX 999**

**GID\_MIN 1000**

**GID\_MAX 60000 #组ID结束的数字**

**SYS\_GID\_MIN 201**

**SYS\_GID\_MAX 999**

**CREATE\_HOME yes #是否为用户建立home目录**

**UMASK 077**

**USERGROUPS\_ENAB yes**

**ENCRYPT\_METHOD SHA512 #shadow文件的加密算法**

**[root@panda home]# cat /etc/default/useradd**

**/etc/default/useradd 文件中的内容如下：**

**GROUP=100 #表示可以创建普通组 。 users组ID为100 。如果没有这一条，或者你把users这个组删除了，当你再创建用户时，将提示：useradd: group '100' does not exist**

**HOME=/home #哪个目录作为用户主目录存放目录。如果你不想让用户家目录在/home下，可以修改这个地方。**

**INACTIVE=-1　　#是否启用帐号过期。passwd文件中第７栏。即：密码过期后是否会失效的设定值 。INACTIVE：无效。-1表示启用**

**EXPIRE=　　　 #帐号终止日期 shadow中第8栏。账号失效的日期 就是 shadow 内的第八字段，你可以直接设定账号在哪个日期后就直接失效，而不理会密码的问题。 通常不会设定此项目，但如果是付费的会员制系统，或许这个字段可以设定！**

**SHELL=/bin/bash　　#默认shell使用哪个**

**SKEL=/etc/skel　　#模板目录**

**CREATE\_MAIL\_SPOOL=yes　　#是否创建邮箱文件**

**命令：chage**

**-m：密码可更改的最小天数。为0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，为0表示强制在下次登录时更新密码**

**例：修改用户mk密码信息：让这个用户mk首次登录系统时必须更改其密码**

**[root@xuegod63 ~]# chage -d 0 mk**

**[root@xuegod63 ~]# ssh mk@192.168.1.63**

**...**

**Are you sure you want to continue connecting (yes/no)? yes**

**Warning: Permanently added '192.168.1.63' (ECDSA) to the list of known hosts.**

**mk@192.168.1.63's password: 123456**

**You must change your password now and login again! #提示必须改密码**

**更改用户 mk 的密码 。**

**互动： 两个用户的UID可以一样吗？**

**[root@xuegod63 ~]# vim /etc/passwd # 改 mk uid为0**

**mk:x:0:0:mk:/home/mk:/bin/bash**

**[root@xuegod63 ~]# su - mk**

**上一次登录：二 9月 19 22:03:16 CST 2017:0 上**

**[mk@xuegod63 ~]# id mk**

**uid=0(mk) gid=0(root) 组=0(root),10(wheel)**

**查看用户相关命令：**

**#id 用户和组的信息**

**#whoami　　 #查看当前有效用户名**

**#who #显示目前登入系统的用户信息。**

**#w # w命令用于显示已经登陆系统的用户列表**

**#users #用于显示当前登录系统的所有用户的用户列表**

## 6.2.11 修改用户信息

**语法：usermod 【参数】用户名**

**常用参数：**

**-u UID**

**-d 宿主目录**

**-g 起始组 #只能有一个**

**-G 附加组 #可以有多个**

**-s 登录shell**

**-L 锁定**

**例1：修改UID**

**[mk@xuegod63 ~]# id oracle**

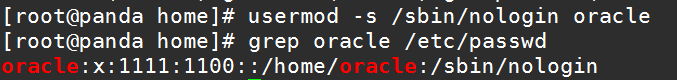
**uid=1100(oracle) gid=1100(oracle) 组=1100(oracle)**

**[mk@xuegod63 ~]# usermod -u 1111 oracle**

**[mk@xuegod63 ~]# id oracle**

**uid=1111(oracle) gid=1100(oracle) 组=1100(oracle)**

**例2：修改shell**

****

**例3：更改用户主目录**

**[root@panda home]# usermod -m -d /mnt/market market**

**-m选项会自动创建新目录并且移到内容到新目录里面**

**例4：添加说明信息**

**[root@panda mnt]# usermod -c "hello world" market**

**总结：如果你记不住命令， 那么直接改vim /etc/passwd 一样的。**

### 6.2.12解决模板文件被删之后显示不正常的问题

**[mk@xuegod63 ~]# rm -rf /home/xuegod/.bash\***

**[mk@xuegod63 ~]# su - xuegod**

**-bash-4.2$ exit #出现这个不完整的shell提示符，如何处理？**

**[mk@xuegod63 ~]# cp /etc/skel/.bash\* /home/xuegod/**

**[mk@xuegod63 ~]# chown xuegod:xuegod /home/xuegod/.bash\***

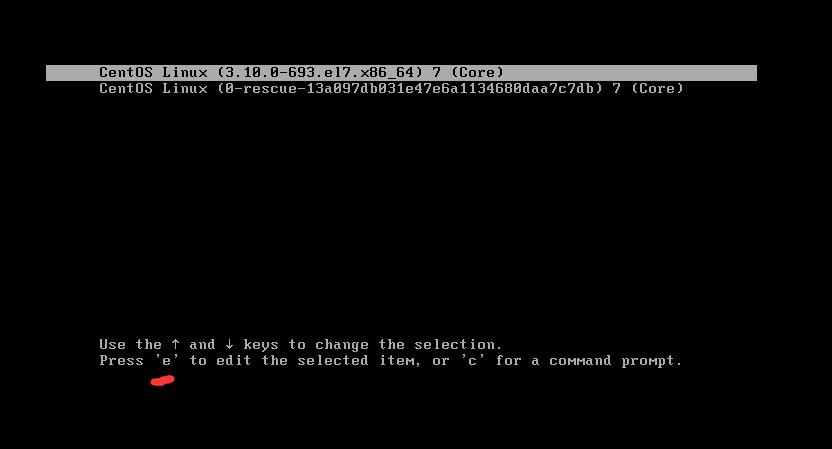
**[mk@xuegod63 ~]# su - xuegod**

**[xuegod@xuegod63 ~]$**

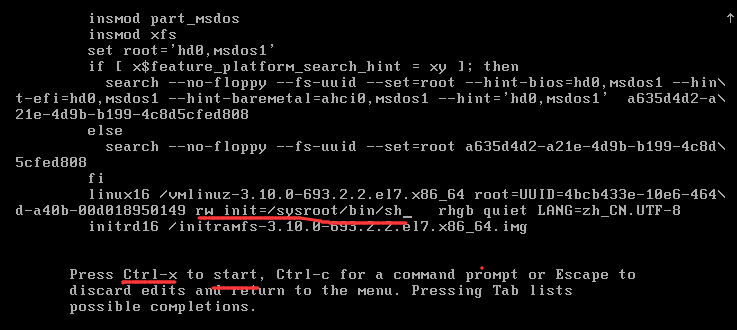
# 6.3实战：进入centos7 紧急模式恢复root密码

**实战场景：公司一台centos7系统，忘记root密码了，需要你快速把root密码修改为xuegod，找回root身份。**

**首先重启，按↑↓键，进入如下界面，选择第一项，按下e键进行编辑**

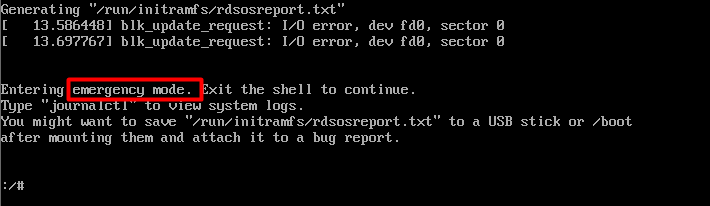
****

**在此界面找到ro这一项，改为rw init=/sysroot/bin/sh**



**改完之后，按下Ctrl+X进入紧急模式**

**原理：启动一个shell环境，系统并没有真正的启动**

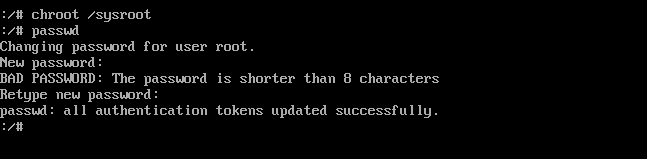
****

**emergency [iˈmɜ:dʒənsi] 紧急**

**换根，修改密码**

**chroot命令用来在指定的根目录下运行指令**

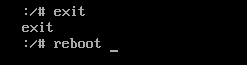
**。chroot，即 change root directory （更改 root 目录）。在 linux 系统中，系统默认的目录结构都是以/，即是以根 (root) 开始的。而在使用 chroot 之后，系统的目录结构将以指定的位置作为/位置**

**在经过 chroot 命令之后，系统读取到的目录和文件将不在是旧系统根下的而是新根下（即被指定的新的位置）的目录结构和文件，  
**

**注：如果系统的selinux开启着，则需要执行命令： touch /.autorelabel**

**以更新系统信息,否则重启之后密码修改不会生效**

**先退出当前根，reboot重启系统**



**总结：**

**6.1 用户和组的相关配置文件**

**6.2 管理用户和组**

**6.3实战：进入centos7 紧急模式恢复root密码**