# 用户和组账户管理

## 用户管理简介

linux操作系统是一个多用户操作系统，它允许多用户同时登录到系统上并使用资源。系统会根据账户来区分每个用户的文件，进程，任务和工作环境，使得每个用户工作都不受干扰。

对安全要求高的服务器，都需要建立合理的用户权限等级制度和服务器操作规范。

在linux中主要是通过用户配置文件来查看和修改用户信息。

## 配置文件

* 保存用户信息的文件：/etc/passwd
* 保存密码的文件：/etc/shadow
* 保存用户组的文件：/etc/group
* 保存用户组密码的文件：/etc/gshadow

## /etc/passwd格式

共7个字段，示例数据为：

root:x:0:0:root:/root:/bin/bash

用户名：密码位：UID(用户标识号)：GID（缺省组标识号）：描述信息：宿主目录：命令解释器（使用的 shell，默认为bash）

使用命令：man 5 passwd

用户名：用户登陆系统的用户名

密码：密码位

UID：用户标识号

GID：默认组ID

描述信息：存放用户的描述信息

宿主目录: 用户登陆系统的默认目录，普通用户默认是在/home/下

命令解析器: 用户使用的Shell，默认是bash

## Linux用户分类

超级用户：（root，UID=0）

普通用户：（UID在500到60000）

伪用户：（UID在1到499）

**伪用户:**

1、伪用户与系统和程序服务相关

    bin、daemon、shutdown、halt等，任何Linux系统默认都有这些伪用户

    mail、news、games、apache、ftp、mysql及sshd等，与Linux 系统的进程相关

2、伪用户通常不需要或无法登录系统

3、可以没有宿主目录

## 用户组

每个用户至少属于一个用户组

每个用户组可以包含多个用户

同一个用户组的用户享有该组共有的权限

## 初始组和附加组

初始组：就是指用户一登录就立刻拥有这个用户组的相关权限，每个用户的初始组只能有一个，一般就是和这个用户的用户名相同的组名作为这个用户的初始组。

初始组有且仅有一个，可以修改，但不建议修改。

附加组：指用户可以加入多个其他的用户组，并拥有这些组的权限，附加组可以有多个。

## /etc/shadow格式

共9个字段，示例数据为：

root:$1$FAKb8T5g$3ni9CM7RlbrwWpDGfWP0:15439:0:99999:7:::

用户名：加密密码：最后一次修改时间：最小时间间隔：最大时间间隔：警告时间：密码过期后宽限天数：失效时间：标志（保留字段）

查看命令：man 5 shadow

**用户名:** 登陆系统的用户名

加密密码：如果密码位是!!或者\*代表没有密码，不能登录

（忘记密码,可在shadow下删除加密密码，不需密码就能登录，然后修改密码）

最后一次修改时间：用户最后一次修改密码的天数，是从1970年1月1日开始计算的天数

最小时间间隔：两次修改密码之间的最小天数

最大时间间隔：密码保持有效的最多天数

警告时间：从系统开始警告到密码失效的天数

密码过期后宽限天数：0表示密码过期后立即失效，-1表示密码永远不会失效

失效时间：密码失效的绝对天数（不用管有效期）

标志：保留字段

## 操作用户命令

### 添加用户命令：useradd

语法：useradd [选项] 用户名

-u 指定组ID（uid）

-g 指定所属的组名（gid）

-G 指定多个组，用逗号“，”分开（Groups）

-c 用户描述（comment）

例子：

useradd -u 888 -G sys,root -c "nvshen" yifei

passwd yifei

用户密码：生产环境中，用户密码长度8位以上，设置大小写加数字加特殊字符，要定期更换密码。

ys^h\_L9t

### 修改密码命令  passwd

语法：passwd [选项] [用户名]

选项：

    -S    查询用户密码的密码状态。仅root用户可用 （即查看某一个用户的shadow记录）

### 修改用户命令：usermod（user modify）

-g 添加组 usermod -g sys tom 指定组必须存在

-G 修改用户附加组 usermod -G sys,root tom

### 删除用户命令：userdel（user delete）

-r 删除账号时同时删除目录（remove）

删除用户时，默认删除同名的组。

如果用户所属组，被其他用户依赖，或者该用户使用了非同名组，则不删除该组，只删除该用户。

### id命令

作用：查看指定用户的id和组id情况

语法：id 用户名

eg:



## /etc/group格式

共4个字段，数据格式为：

root:x:0:root

sys:x:3:root,bin,adm

组名：组密码位：GID：组成员（组内所有用户列表）

**组名：**用户所在的组

**组密码：**密码位，一般不使用

**GID：**主标示号

**组内用户列表:** 属于该组的用户列表

## /etc/gshadow 文件格式

共4个字段，数据格式为：

root:::

bin:::bin,daemon

组名：组密码：组管理员用户名：组中附加用户

## 操作用户组命令

### 添加组：groupadd

-g 指定gid

### 修改组：groupmod

-n 更改组名（new group）

groupmod -n new\_gname old\_gname

### 删除组：groupdel

如果要删除的组归属于某一个用户的所属组，则不能删除该组

# useradd -g hadoop hdfs

# groupdel hadoop

groups

显示用户所属组