**1. 运行用户空间应用程序**

我们知道Linxu分为内核态和用户态，用户态和内核态交互的桥梁就是shell，用户的应用程序通常运行在用户态，也就是用户空间，默认情况下，root用户拥有系统最高权限，很多时候我们在linux部署应用程序时，程序可能需要取得某些系统权限才能正常运行，比如在所属组为root的目录里新建一个\*.pid文件,普通用户是没有权限的，所以我们一般直接使用root用户来运行应用程序，这样就不用担心权限不足的问题，但是root用户账户下运行应用程序可能存在安全风险，所以这样的做法是不安全的。

在安装一些应用时，比如Mysql，安装运行过程需要我们提供root权限，但是在安装完成并正常运行时，我们通过top命令查看进程信息时发现：

8534 mysql 20 0 1610988 175816 18328 S 0.3 4.3 8:12.66 mysqld

mysql安装程序自动给我们创建了一个用户mysql和相应的用户组mysql，并使用mysql这个特定的用户来运行mysql服务。这样做的好处就是使用特定的用户来运行程序，而不是最高权限的root用户。

很多服务启动需要root权限，但是服务启动后，root账户通常将其转移到服务账户，这里就是mysql账户，linux中的服务账户才是标准的用户账户，主要区别就是服务账户仅仅用来运行一个服务，该账户不需要拥有像登陆用户那样指定shell和类似/home/username的家目录，取而代之的是该用户的初始工作目录可能是应用程序安装目录。

**2.服务账户创建与管理**

linux中每一个用户都有一个用户组，在创建用户时如果不指定用户组，则默认创建一个和用户名同名的用户组，关于用户组、用户信息分别保存在/etc/group /etc/passwd 中，用户口令保存在/etc/shadow中，我们可以打开文件查看，关于每个字段代表什么意思可以自己查阅。 假设我们需要运行一个应用程序，程序安装目录为/usr/local/MyApp

**2.1 首先创建用户组**

sudo addgroup --system test

# --system 参数表示我们创建一个系统组，组ID根据最新的组ID+1

root@ubuntu:/data/document# addgroup --system test

Adding group `test' (GID 127) ...

Done.

我们打开/etc/group查看

ubuntu:x:1000:

sambashare:x:124:ubuntu

mysql:x:125:

activemq:x:126:

test:x:127: # 这是我们刚创建的用户组 组ID为127

2.2 创建用户

adduser --system --ingroup test --no-create-home --disabled-password test

Adding system user `test' (UID 119) ...

Adding new user `test' (UID 119) with group `test' ...

Not creating home directory `/home/test'

我们创建了一个用户test，指定所属组为test，--system表示该用户是系统用户， --ingroup 指定所属组 --no-create-home 表示不为该用户创建家目录 --disabled-password 该用户不用来登录

**2.3 修改用户配置**

我们创建的用户用来运行我们的应用，所以需要指定该用户的工作目录为应用安装目录 /usr/local/MyApp

usermod -c "这里是用户描述" -d /usr/local/MyApp -g test test

使用命令行对用户信息进行修改最终都会写入到配置文件中，这里的配置文件就是/etc/passwd文件

**2.4 修改应用目录的所属组和用户**

sudo chown -R test:test /usr/local/MyApp

# 应用安装目录所属组为test，所属用户为test

sudo chmod u+rwx,g+rxs,o= /usr/local/MyApp

# 修改目录权限

**3. 运行程序**

在运行程序时使用root用户运行，但是在启动脚本里需要将root转移到指定的服务账户test