

Linux中特权帐号与普通帐号的差异Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/607/2021\\_2022\\_Linux\\_E4\\_B8\\_AD\\_E7\\_89\\_c103\\_607073.htm](https://www.100test.com/kao_ti2020/607/2021_2022_Linux_E4_B8_AD_E7_89_c103_607073.htm)

在Linux操作系统中，其帐号大致可以分为特权帐号与普通帐号两类。其实这跟微软操作系统中的角色非常的想象。只是微软操作系统中的预定义角色比较多，而在Linux操作系统中，只有两类用户。作为Linux系统管理员必须要了解这两列帐号的差异。以及在以后的使用过程中需要注意的地方。通常情况下，Linux系统安装完毕之后，系统会自动创建一个特权帐户，即root。如需要在Linux操作系统上部署其他应用的时候，笔者建议大家重新创建一个帐户。如要在Linux操作系统上部署邮箱服务器的话，那么最好建立一个mail的帐户。然后利用这个帐户登陆系统，再进行相关的操作。这个绝对不是多次一举。这主要是因为root帐户与普通的帐户具有很大的差异。这主要体现在以下几个方面。一、磁盘空间上的限制。通常情况下，root帐户对于操作系统具有最高的权限，其往往没有磁盘空间的限制。即使对其他用户设置了磁盘限额，而往往root帐户不会受到这方面的限制。而普通用户的话，其默认情况下只能对自己的主目录有存储文件的权限。为此可以通过磁盘限额等手段来限制其磁盘空间的大小。在有些情况下，实现这个磁盘空间的限制是非常重要的。因为Linux操作系统是一个多用户的操作系统。有可能会在同一个Linux操作系统上同时部署多个应用服务。如可能会同时部署邮件服务器与文件服务器。而他们是分别采用两个不同的帐户名来部署的。那么系统管理员就可以分别为他们设置磁盘限额，防止因为某个应

用由于病毒等原因侵蚀了所有硬盘空间，而导致另外一个服务也当机了。如果两个服务都用root帐户部署，或者其中一个服务采用root帐户运行的话，就不能够对其进行磁盘空间限制了。如对邮件服务器使用root帐户部署，万一邮件服务器中了病毒(或者某些客户端有病毒)而狂发垃圾邮件的话，则很有可能在系统管理未发觉之前，这个硬盘的空间就被消耗殆尽了。从而导致服务器的崩溃。而如果采用了分帐号部署的话，那么最多只是邮箱服务器崩溃，而不会影响文件服务器与root帐户的运行，还有挽救的余地。所以，无论在Linux操作系统上部署多少应用，最好都能够把root帐户与普通帐户分开来。Root帐户一般情况下只用来做管理，而不用作他用。只有如此，才能够实现磁盘限额。

## 二、保证相对独立的环境变量。

Linux操作系统跟Windows操作系统类似，环境变量分为用户环境变量与通用环境变量。用户环境变量就只对当前的用户有效.而通用环境变量则对整个操作系统中的用户有效。有时候在部署网络应用，需要让各个环境变量相对的独立。在某个用户下创建的环境变量(用户环境变量)，到另外一个帐户那边，就是无效的。为此就可以通过创建多个帐户来保证不同帐户之间环境变量的独立性。如在Linux操作系统中需要部署一个ERP应用，其有数据库服务器与ERP应用服务器两个部分组成，这连个部分是相互独立、又相互联系的两个部分。系统管理员往往会分别设置两个普通的帐户来部署这两个应用。通过这个方法，可以为每个应用分别保存个人的环境变量。从而让多个应用部署在同一台计算机上时，可以相对独立的工作，彼此之间不会相互干扰。如果把把这些应用都部署在同一个帐户下，那么就需要设置很多的

环境变量。此时都在一个帐户下进行设置的话，很可能出错，而且也有可能相互冲突。为此为了给某些应用创造一个相对独立的工作环境，笔者建议不要用root帐户在部署这些应用。而且最好为每个应用创建一个普通帐户来管理，以保障环境变量的独立性。

### 三、方便备份用户的文件。

Root帐户与普通帐户的主目录是不同的。特权用户root其主目录是/root，而普通用户的主目录则为/home/帐号名称。Linux操作系统的这个设置非常的有用。如现在Linux操作系统上有两个用户，一个是特权用户，一个是普通的员工。通常情况下，普通帐户只能够把自己的文件、邮件等等保存在自己的主目录中。那么只需要对这个员工帐户的主目录进行备份，就可以备份用户的私有文件。通过备份用户的主目录，即使当操作系统瘫痪或者员工换电脑时，只需要恢复主目录中的文件，那么就可以还用户一个一模一样的工作环境。为此，把特权用户的目录与普通用户的目录分开设置就变得非常的有用。另外，各个用户下的主目录也是相对独立的。如在系统中创建了A与B两个普通帐户。则在操作系统根目录下的/home/目录下就会有A与B两个目录。此时默认情况下，用户A只对目录A具有操纵的权限.而用户B也只有对目录B具有操作的权限。也就是说，各个帐户都只能够操作各自目录下的文件。为此，当多个用户共享同一台主机的时候，每个用户就都有一个私人的文件夹，从而可以防止自己的文件被别人无意中修改或删除。那如果当某个员工离职了，或则遗忘了密码，那么这个员工的文件就无法阅读了吗?这不是会给企业造成很大的损失吗?其实不然。因为特权用户root具有无与伦比的权限，为此root帐户可以访问与修改任何普通帐户的主目录。也就

是说，如果某个员工离职了，而其代理人需要这个员工主目录下的文件，则系统管理员仍然可以凭root帐户登陆系统，并把相关的文件复制给其代理人。从这里也可以看出，root帐户其权限是非常庞大的。默认情况下，最好把root帐户与普通的帐户分开来。以保障各个用户之间能够有一个相对独立的个人主目录。

#### 四、文件相关权限不同。

通常情况下，只有文件的所有者可以更改文件的权限。如用户A(普通帐户)其建立另一个文件，其可以设置其它用户是否对这个文件具有读取、或者修改的权利。因为用户A是这个文件的所有者，所以其有权进行这方面的设置。这是Linux操作系统中权限控制的最基本原则。但是root特权用户会打破这个规则。默认情况下，root帐户可以读取、修改系统中的所有文件以及目录，并可修改所有文件的权限。也就是说，root帐户对文件以及目录进行操作，使不受到所有权这个条件的限制的。即使root帐户不是文件的所有者，其也可以把某些权限授权给其它用户。为此在日常工作中，系统管理员应该限制其它普通用户使用这个账号。俗话说，害人之心不可有，防人之心不可无。如果一些对公司怀有不满的员工，利用root帐号去查看自己无权查看的文件，或者进行修改、删除等等操作，那么就可能会造成比较大的损失。因为root帐户可以对任何用户的文件进行类似的操作。所以在日常工作中，系统管理员要管理好root帐户的口令，不能够泄露。同时在给员工分配帐户的时候，也不要为了省心，而直接把root帐户交给员工使用。不不仅不会省心，而且还会让系统管理员更加的烦心。总之，root帐户与普通帐户是两个根本不同的帐户。或者说，root帐户本来就是为管理员而专门设立的，而不是为

普通用户所创建。为此笔者强烈建议，无论出于什么目的，最好为Linux操作系统设置独立的普通用户。即使是系统管理员在使用Linux操作系统，也最好为其建立一个普通帐户。当他们需要管理员的权利时，可以非常方便的通过su命令转换到特权模式下。另外就是尽量为不同的员工、不同的应用设置不同的帐户。通过不同的帐户给他们提供一个相对独立的工作环境，减少相互之间的干扰。这可以说是Linux操作系统部署中一个约定俗成的原则。更多优质资料尽在百考试题论坛 百考试题在线题库 linux认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问

[www.100test.com](http://www.100test.com)