Linux操作系统中超级权限控制的应用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_ti2020/644/2021_2022_Linux_E6_93_8D_E4_BD_c103_644692.htm 在Linux操作系统中，root的权限是最高的，也被称为超级权限的拥有者。普通用户无法执行的操作，root用户都能完成，所以也被称之为超级管理用户。 在系统中，每个文件、目录和进程，都归属于某一个用户，没有用户许可其它普通用户是无法操作的，但对root除外。root用户的特权性还表现在root可以超越任何用户和用户组来对文件或目录进行读取、修改或删除（在系统正常的许可范围内）；对可执行程序的执行、终止；对硬件设备的添加、创建和移除等；也可以对文件和目录进行属主和权限进行修改，以适合系统管理的需要（因为root是系统中权限最高的特权用户）；一、对超级用户和普通用户的理解 1、什么是超级用户；在所有Linux系统中，系统都是通过UID来区分用户权限级别的，而UID为0的用户被系统约定为是具有超级权限。超级用户具有在系统约定的最高权限满园内操作，所以说超级用户可以完成系统管理的所有工具；我们可以通过/etc/passwd 来查得UID为0的用户是root，而且只有root对应的UID为0，从这一点来看，root用户在系统中是无可替代的至高地位和无限制权限。root用户在系统中就是超级用户；2、理解 UID 和用户的对应关系 当系统默认安装时，系统用户和UID 是一对一的对关系，也就是说一个UID 对应一个用户。我们知道用户身份是通过UID 来确认的，我们在《用户（user）和用户组（group）配置文件详解》中的UID 的解说中有谈到“ UID 是确认用户权限的标识，用户登录系统所处

的角色是通过UID 来实现的，而非用户名；把几个用户共用一个UID 是危险的，比如我们把普通用户的UID 改为0，和root共用一个UID，这事实上就造成了系统管理权限的混乱。如果我们想用root权限，可以通过su或sudo来实现；切不可随意让一个用户和root分享同一个UID ；”在系统中，能不能让UID 和用户是一对多的关系？是可以的，比如我们可以把一个UID为0这个值分配给几个用户共同使用，这就是UID 和用户的一对多的关系。但这样做的确有点危险；相同UID的用户具有相同的身份和权限。比如我们在系统中把beinan这个普通用户的UID改为0后，事实上这个普通用户就具有了超级权限，他的能力和权限和root用户一样；用户beinan所有的操作都将被标识为root的操作，因为beinan的UID为0,而UID为0的用户是root，是不是有点扰口？也可以理解为UID为0的用户就是root，root用户的UID就是0；UID和用户的一对一的对应关系，只是要求管理员进行系统管理时，所要坚守的准则，因为系统安全还是第一位的。所以我们还是把超级权限保留给root这唯一的用户是最好的选择；如果我们不把UID的0值的分享给其它用户使用，只有root用户是唯一拥有UID=0的话，root用户就是唯一的超级权限用户；3、普通用户和伪装用户 与超级用户相对的就是普通用户和虚拟（也被称为伪装用户），普通和伪装用户都是受限用户；但为了完成特定的任务，普通用户和伪装用户也是必须的；Linux是一个多用户、多任务的操作系统，多用户主要体现在用户的角色的多样性，不同的用户所分配的权限也不同；这也是Linux系统比Windows系统更为安全的本质所在，即使是现在最新版本的Windows 2003，也无法抹去其

单用户系统的烙印； 二. 超级用户（权限）在系统管理中的作用 超级权限用户（UID为0的用户）到底在系统管理中起什么作用呢？主要表现在以下两点； 1、对任何文件、目录或进程进行操作；但值得注意的是这种操作是在系统最高许可范围内的操作；有些操作就是具有超级权限的root也无法完成；比如/proc 目录，/proc 是用来反应系统运行的实时状态信息的，因此即便是root也无能为力；它的权限如下 [root@localhost ~]# pwd /root [root@localhost ~]# cd / [root@localhost /]# ls -ld /proc/ dr-xr-xr-x 134 root root 0 2005-10-27 /proc/ 