**基本权限、ACL访问控制、附加权限**

**用户管理和权限管理**

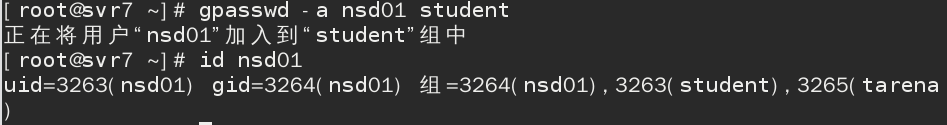
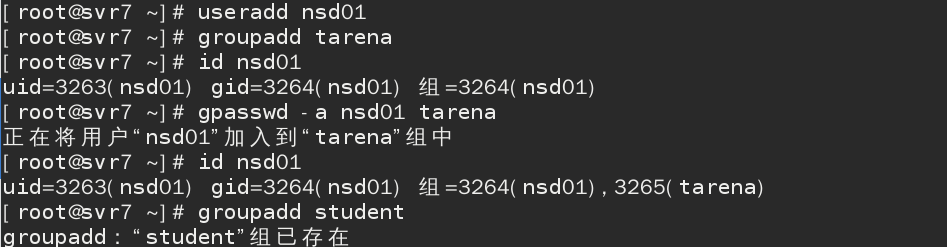
**用户唯一标识：UID**

管理员的用户UID：0

[root@svr7 ~]# man useradd

[root@svr7 ~]# useradd -u 0 -o abc

**组管理**



**#将用户加入组**

**#两个附加组**

**Linux创建一个用户，会修改哪些配置文件：**

/etc/passwd(用户基本信息)

/etc/shadow（用户密码信息）

/etc/group（组的基本信息）

/etc/gshadow（组的密码信息）

**默认用户家目录下，配置文件模板目录**

[root@svr7~]#ls -A /etc/skel/

每创建一个用户，linux系统都会从/etc/skel目录中，把所有内容复制到新建用户的家目录下

#ls -A /etc/skel/

#touch /etc/skel/haha.txt

#ls -A /etc/skel

#useradd nsd03

#ls -A /home/nsd03

**以-开头：表示文本文件；以d开头：表示目录；以l开头：表示快捷方式**

**对于文本文件：r：读取内容 cat head less tail**

**w:修改内容 vim**

**x：执行该文本文件**

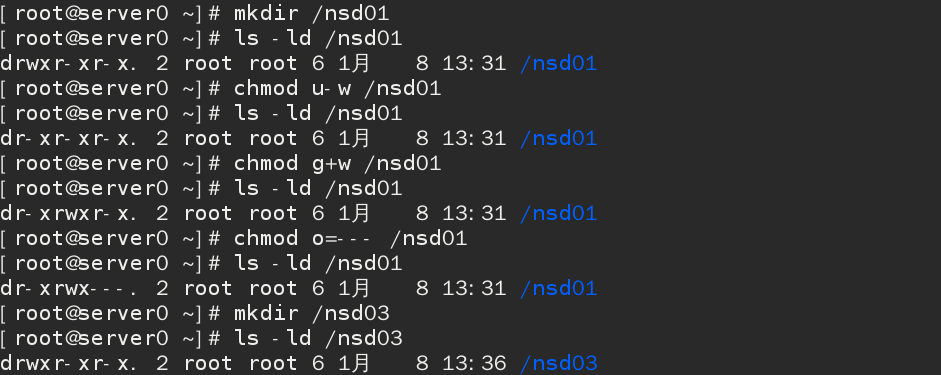
**对于目录：r：浏览此目录内容**

**w：可执行 rm mv cp mkdir touch等更改目录内容的操作**

**x：能cd进入到此目录下**

**用户修改权限命令 chmod**

**chmod** [-R] **归属关系+/-/=权限类别 文档。。。**



**#去除其他人的所有权限**

**#增加所属组的写权限**

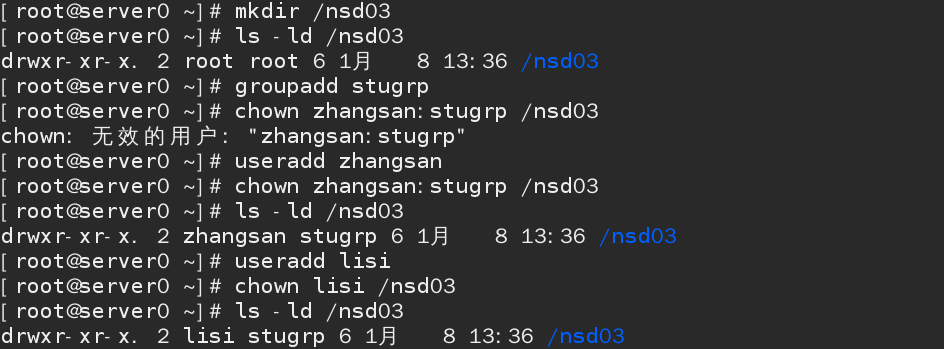
**#去除用户的写权限**

**用户修改归属关系 chown**

**chown** [-R] **属主 文档。。。**

**chown** [-R] **:属组 文档。。。**

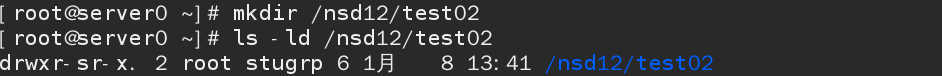
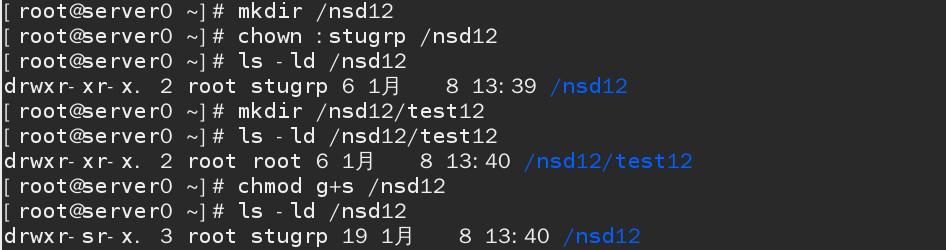
**chown** [-R] **属主：属组 文档。。。**

**附加权限 SGID** 适用于目录，让新增的子目录，自动继承父目录的所属组身份（使目录下新增的文档自动设置与父目录相同的属组）

**#改变/nsd03的属主**

**#改变/nsd03的属主和属组**

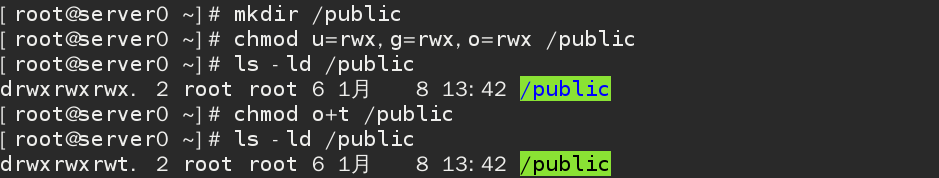
附加在**属组的x位**上；**属组的权限标识会变为s**



**Sticky Bit**

适用于开放w权限的目录，可以阻止用户滥用w写入权限（禁止操作别人的文档）

附加在**其他人的x位**上；**其他人的权限标识会变为t**

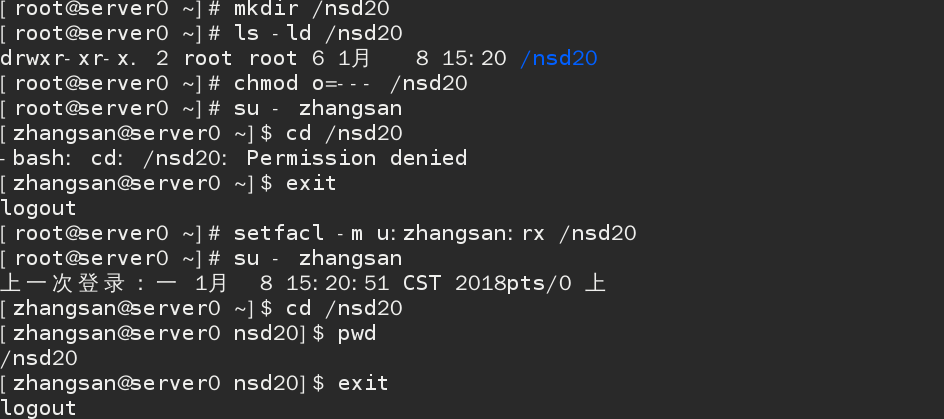


**Acl策略的作用**

**setfacl -m u:用户：权限 文件路径**

**文档归属的局限性：任何人只属于三种角色：属主、属组、其他人，无法实现更精细的控制**

**能够对个别用户、个别组设置独立的权限**



**#设置张三用户对/nsd20只有读和执行权限**

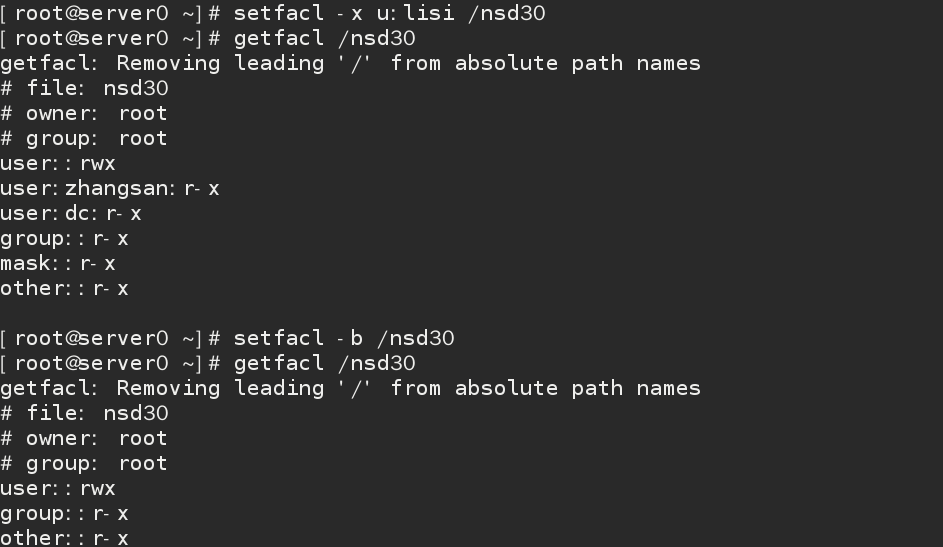
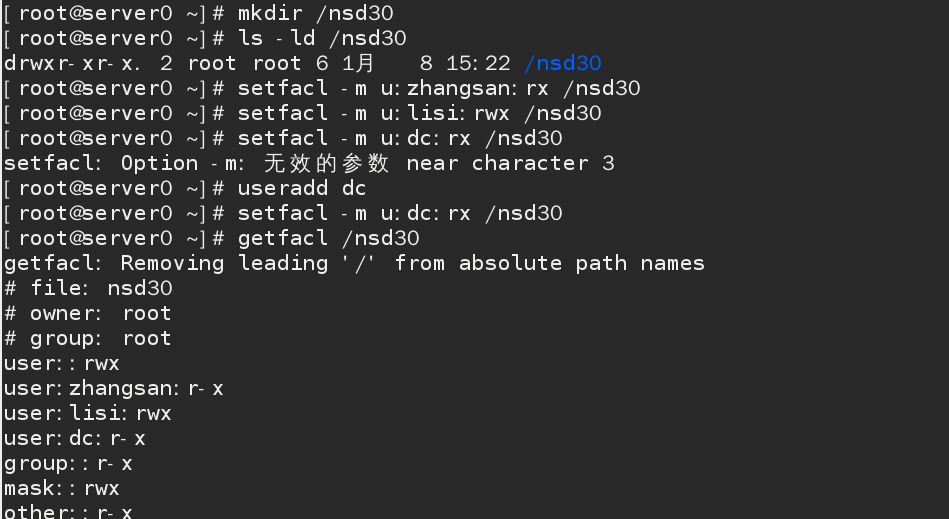
**getfacl 文档。。。 （查看）**

**Setfacl [-R] -m u:用户名：权限类别 文档。。。**

**Setfacl [-R] -m g:组名：权限类别 文档。。。**

**Setfacl -x u:用户名 文档 （删除指定用户的ACL权限）**

**Setfacl [-R] -b 文档。。。 （清除所有）**



**#查看**

**#删除所有的ACL**

**#删除指定的ACL**

**路由器与交换机的区别**

1. 作用：交换机作为组建局域网用的；路由器解决不同网段或者不同局域网之间通信的
2. 识别的地址：交换机识别MAC地址表 识别MAC地址；路由器识别路由表 识别IP地址
3. 工作的层次：交换机在数据链路层；路由器在网络层
4. 未知数据的判断：交换机 广播未知数据帧；路由器 直接丢弃

路由器天生隔离所有广播包