**Linux**

**权限：**

权限是操作系统用来限制对资源访问的机制，权限一般分为读，写，执行三种。系统中每一个文件都拥有特定的权限，所属的用户及所属组通过这样的机制来限制那些用户，哪些组可以对特定文件进行什么样的操作。

每个进程都是以某个用户的身份运行，所以进程的权限与该用户的权限一样，用户权限越大，该进程拥有的权限就越大。

对于文件目录必须拥有执行权限，否则无法查看其内容。

权限：d rwx r-x r-- :第一个d代表文件类型 第二个rwx代表所属用户对文件的权限 第三个r-x代表所属组对文件的权限， 第四个r--代表其他用户对该文件的权限。

chown命令用于改变文件的所属用户。

chgrp命令用于修改文件所属组。

Chmod命令用以修改文件权限 chmod 模式 文件

u g o 分别代表用户，组，其他

a可以代表ugo

+ -：代表加入或删除权限。

也可以加R表示递归的修改文件夹内的子文件加或文件的权限。

也可以使用数字来修改权限

eg：chmod u +rw linuxcast.net :为这个文件的所属用户加入rw权限

Eg:chmod 660 linuxcast.net 等同于 rw-rw----

**用户扩展权限：**

**默认权限：**

每一个终端都拥有一个umask属性，来确定新建文件。文件夹的默认权限

Umask使用数字权限方式表示，如：022

目录的默认权限是777-umask

文件的默认权限是：666-umask

一般，普通用户默认的umask值是002，root用户的默认umask值是022

也就是说，对于普通用户来讲：

新建文件的权限是666-002 = 664

新建目录的权限是：777-002=775

命令umask用以查看umask值，或者修改umask值

**特殊权限：**

命令其实就是一个可执行文件。

除了普通权限外还有三个特殊权限：

**权限 对文件的影响 对目录的影响**

**Suid 以文件的所属用户身份执行，**

**而非执行文件的用户 无**

**Sgid 以文件所属组身份运行 在该目录中创建的任意新文件的所 属组与该目录的所属组相同**

**Sticky 无 对目录拥有写入权限的用户仅可以 删除其拥有的文件，无法删除其他 用户所拥有的文件**

设置特殊权限范例：

设置suid: chmod u+s linuxcast.net

设置sgid: chmod g+s linuxcast.net

设置sticky： chmod o+t linuxcast.net

与普通权限一样，特殊权限也可以使用数字方式进行表示：

Suid = 4

Sgid = 2

Sticky = 1

所以我们可以通过以下命令设置：

Chmod 4755 linuxcast.net