基本权限

r, w, x

（一）

1.文件：

r：可读，可以使用类似cat等命令查看文件内容；

w：可写，可以编辑或删除此文件；

x: 可执行，eXacutable，可以命令提示符下当作命令提交给内核运行；

目录：

r: 可以对此目录执行ls以列出内部的所有文件；

w: 可以在此目录创建文件；

x: 可以使用cd切换进此目录，也可以使用ls -l查看内部文件的详细信息；

2.rwx:

r--:只读

r-x:读和执行

---：无权限

0 000 ---：无权限

1 001 --x: 执行

2 010 -w-: 写

3 011 -wx: 写和执行

4 100 r--: 只读

5 101 r-x: 读和执行

6 110 rw-: 读写

7 111 rwx: 读写执行

755：rwxr-xr-x　111 101 101

rw-r-----: 640

660:rw-rw----

rwxrwxr-x:775

3.三类用户：

u: 属主

g: 属组

o: 其它用户

chown: 改变文件属主(只有管理员可以使用此命令)

chown USERNAME file,...

-R: 修改目录及其内部文件的属主

--reference=/path/to/somefile file,...

参考/path/to/somefile的权限

#chown USERNAME:GRPNAME file,...

#chown USERNAME.GRPNAME file,...

chgrp GRPNAME file,...

-R

--reference=/path/to/somefile file,...

4.修改文件权限

chmod: 修改文件的权限

4.1.修改三类用户的权限：

chmod MODE file,...

-R

--reference=/path/to/somefile file,...

4.2.修改某类用户或某些类用户权限：

u,g,o,a

chmod 用户类别=MODE file,...

4.3.修改某类用户的某位或某些位权限：

u,g,o,a

chmod 用户类别+|-MODE file,...

使用chmod a+[-]x 全部添加或者删除相应权限

5.umask：遮罩码，反向掩码 影响用户新创建的文件和目录的默认权限

666-umask

777-umask

umask 显示

umask 022 设定

普通用户正常为002

文件默认不能具有执行权限，如果算得的结果中有执行权限，则将其权限加1；

umask: 023

文件：666-023=643 X

目录：777-023=754

文件的权限都谁可以修改?

1）root

2）文件的所有者

1.1.4

1、文件的权限

小结：

r单独存在，可查看文件内容

*w单独存在，看不到文件内容，但是可以强制修改文件内容，会覆盖原文件内容，单独存在，意义不大

x单独存在，毫无意义

文件的组合权限

小结：

rx权限：文件可读，可执行，不可修改

rw权限：可读，可写，不可执行

wx：不可读，不可执行，可以覆盖写

ls　r

cp　r

rm　不光考虑文件的权限，还要考虑文件所在的目录的权限

2、目录的权限

小结：

对于目录：

只有r权限时，可以读(有报错)，不能写，也不能进入目录

只有w权限时，毫无意义

只有x权限时，只能进入，不能读，不能写

小结：

目录的rw权限：可以查看内容，不可以进入目录，不能删除目录或它里面的文件

目录的rx权限：可以查看内容，可以进入目录，不可以修改目录的内容

*目录的wx权限：不可以查看目录内容，可以进入目录，可以删除目录下的文件，前提是你需要知道目录下有什么文件