Table of Contents

[1，隐藏权限介绍 0](#_Toc455155876)

[2，查看隐藏权限 0](#_Toc455155877)

[3，修改特殊权限 2](#_Toc455155878)

[3.1，对文件 2](#_Toc455155879)

[3.2，对目录 4](#_Toc455155880)

[4，相关网络资料 5](#_Toc455155881)

# 1，隐藏权限介绍

Linux下的隐藏权限，我们用到两个命令，一个是lsattr,也就是list file attributes。用于查看问加你的attr权限，一个是chattr，也就是change file attributes，用于修改文件的attr权限，包括目录的。详情可以查看man手册，man chattr.

隐藏权限的特点：能限制root用户。

语法

chattr [+-=] [acdeijstu] filename

[root@leopard test]# man chattr

append only (a), 只允许追加，不允许删除，移动

com-pressed (c),

no dump (d),

extent format (e),

immutable (i), 免疫的，防止所有用户误删除，修改，移动文件

data journalling (j),

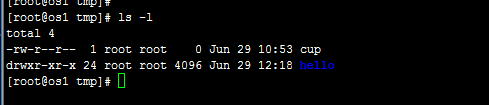
secure deletion (s),

no tail-merging (t),

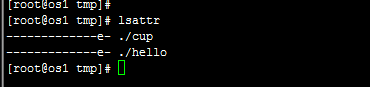
undeletable (u),

# 2，查看隐藏权限

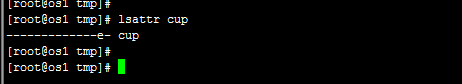
如下图所示，现在我们当前目录下是有一个文件，一个目录。



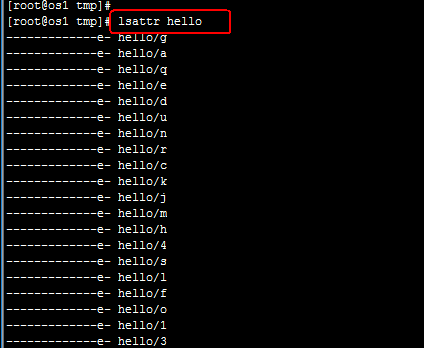
直接执行lsattr，查看当前目录下所有文件和目录的隐藏权限。



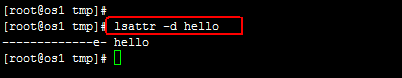
#lsattr cup ，查看文件cup的隐藏权限



# lsattr hello 查看hello目录下所有文件和目录的隐藏权限



# lsattr -d hello --查看hello目录的隐藏权限，-查看指定目录的时候，需要加-d参数。



# 3，修改特殊权限

## 3.1，对文件

修改特殊权限用到的命令是chattr

语法 chattr [+-=] [acdeijstu] filename

append only (a), 只允许追加，不允许删除，移动

com-pressed (c),

no dump (d),

extent format (e),

immutable (i), 免疫的，防止所有用户误删除，修改，移动文件

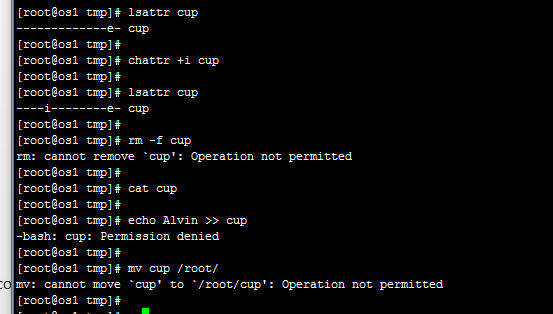
data journalling (j),

secure deletion (s),

no tail-merging (t),

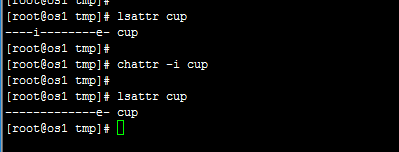
undeletable (u),

一般我们用的比较多的就是特殊权限里的i参数，给文件设置了i的特殊权限之后，就无法删除了，修改和移动也不可以

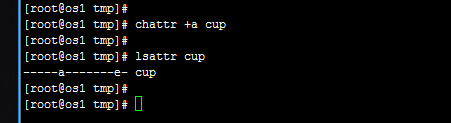
。

还有就是-a参数，用于让文件只能追加新的信息，不能删除原有的内容

这里我们先把刚才添加的-i参数去掉，# chattr -i cup

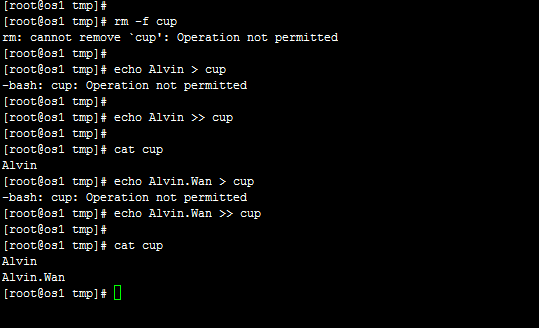


然后执行chattr -a cup,

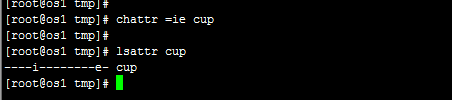


现在我们尝试删除这个cup这个文件，无法删除，尝试写入数据覆盖这个文件，也同样不行，但追加数据到这个文件，执行成功。

所以，在执行-a这个参数之后，该文件变的无法删除无法修改，只能添加新的信息到这个文件，这种属性一般用于日志文件会很合适，因为日志文件就是属于那种只需要添加新的内容，旧的内容不做变更的文件。

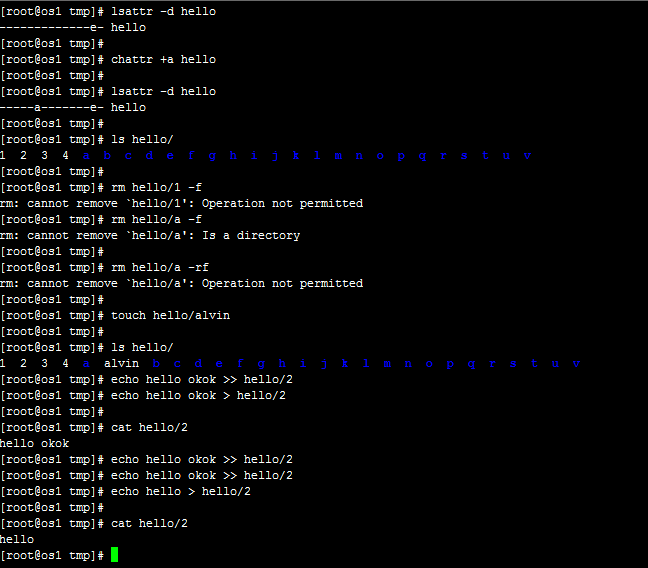


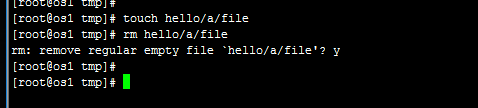
前面我们都是使用的+增加权限，使用-取消权限，实际上我们也可以使用等值修改，就是=



## 3.2，对目录

对目录设置特殊权限，同样的，使用a参数之后，无法删除目录里的文件，但可以修改该目录里的文件，这个时候不只是只能追加新的信息了，也可以覆盖，hello目录的子目录里面，我们也可以新建文件和目录，也可以删除那些文件和目录，但是，我们不能对hello目录的子目录本身进行删除和修改。





# 4，相关网络资料

对于某些有特殊要求的档案(如服务器日志)还可以追加隐藏权限的设定。这些隐藏权限包括：

Append only (a), compressed (c), no dump (d), immutable (i), data journalling (j),secure deletion (s), no tail-merging (t), undeletable (u), no atime updates (A), synchronous directory updates (D), synchronous updates (S), and top of directory hierarchy (T).

大部分属性在文件系统的安全管理方面起很重要的作用。关于以上属性的详细描述请兄弟们查阅chattr的在线帮助man，注意多数属性须要由root来施加。

**通过chattr设置档案的隐藏权限。**

[root]#chattr --help

Usage: chattr [-RV] [-+=AacDdijsSu] [-v version] files...

参数或选项描述：

-R：递归处理，将指定目录下的所有文件及子目录一并处理。

-V：显示详细过程有版本编号。

-v：设定文件或目录版本(version)。

+ ：在原有参数设定基础上，追加参数。

- ：在原有参数设定基础上，移除参数。

= ：更新为指定参数设定。

A：文件或目录的 atime (access time)不可被修改(modified), 可以有效预防例如手提电脑磁盘I/O错误的发生。

S：硬盘I/O同步选项，功能类似sync。

a：即append，设定该参数后，只能向文件中添加数据，而不能删除，多用于服务器日志文 件安全，只有root才能设定这个属性。

c：即compresse，设定文件是否经压缩后再存储。读取时需要经过自动解压操作。

d：即no dump，设定文件不能成为dump程序的备份目标。

i：设定文件不能被删除、改名、设定链接关系，同时不能写入或新增内容。i参数对于文件 系统的安全设置有很大帮助。

j：即journal，设定此参数使得当通过mount参数：data=ordered 或者 data=writeback 挂 载的文件系统，文件在写入时会先被记录(在journal中)。如果filesystem被设定参数为 data=journal，则该参数自动失效。

s：保密性地删除文件或目录，即硬盘空间被全部收回。

u：与s相反，当设定为u时，数据内容其实还存在磁盘中，可以用于undeletion.

各参数选项中常用到的是a和i。a选项强制只可添加不可删除，多用于日志系统的安全设定。而i是更为严格的安全设定，只有superuser (root) 或具有CAP\_LINUX\_IMMUTABLE处理能力（标识）的进程能够施加该选项。我们来举一个例子：

[root]#touch chattr\_test

[root]#chattr +i chattr\_test

[root]#rm chattr\_test

rm: remove write-protected regular empty file `chattr\_test`? y

rm: cannot remove `chattr\_test`: Operation not permitted

呵，此时连root本身都不能直接进行删除操作，必须先去除i设置后再删除。

chattr命令的在线帮助详细描述了各参数选项的适用范围及bug提示，使用时建议兄弟们仔细查阅。由于上述的这些属性是隐藏的，查看时需要使用lsattr命令，以下简述之。

**lsattr命令格式：**

[root]#lsattr [-RVadlv] [files...]

参数或选项说明：

-R：递归列示目录及文件属性。

-V：显示程序版本号。

-a：显示所有文件属性，包括隐藏文件(.)、当时目录(./)及上层目录(../)。

-d：仅列示目录属性。

-l：（此参数目前没有任何作用）。

-v：显示文件或目录版本。

例：

[root]#chattr +aij lsattr\_test

[root]#lsattr

----ia---j--- ./lsattr\_test

关于lsattr的用法，详情请参阅在线帮助man。