Table of Contents

[1，普通权限（UGO权限） 0](#_Toc452993632)

[1.1，查看权限 1](#_Toc452993633)

[1.2，增值修改权限 1](#_Toc452993634)

[1.3，减值修改 2](#_Toc452993635)

[1.4，等值修改 2](#_Toc452993636)

[2，ACL 4](#_Toc452993637)

[2.1，针对用户给文件或目录设置ACL 4](#_Toc452993638)

[2.2，针对组给文件设置ACL 5](#_Toc452993639)

# 1，普通权限（UGO权限）

针对文件来说，有三种权限，分别是r，w，x

r -- Read 读权限

w – Write 写权限

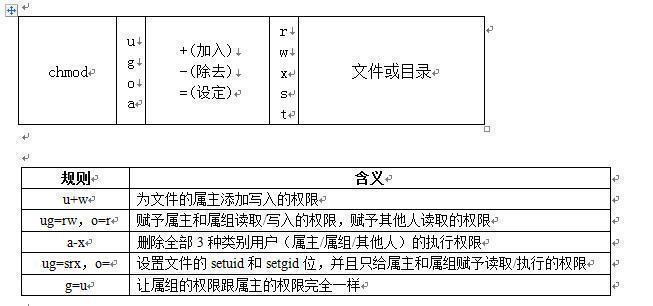
x – eXecute 可执行权限

针对目录来说，也是三种权限，r，w，x

r – 具有读取目录内文件名称的权限

w – 对目录内的文件内容的操作(创建文件)

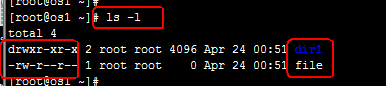
x – 能够cd到目录内的权限



## 1.1，查看权限

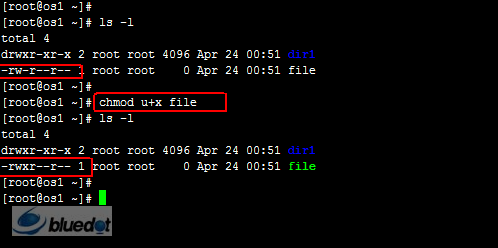
ll是ls -l的间歇，执行ll，可以查看当前目录下的文件和目录的列表，其中列表的信息里也还包括了文件的权限，

下图中的drwxr-xr-x 是dir1的权限，-rw-r—r—是file的权限。其中，第一个字母代表文件类型，比如下图中dir1的权限，d 代表这是文件是一个目录，d后面的3个字母代表该文件所有者对该文件的权限，再后面的三个字母代表该文件所属组对该文件的权限，最后的三个字母代表其他用户对该文件的权限。

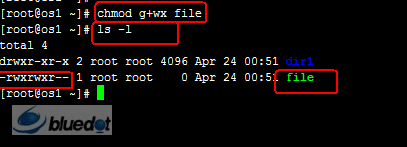


## 1.2，增值修改权限

chmod u+x file ##为文件的所属者添加x权限，也就是可执行权限

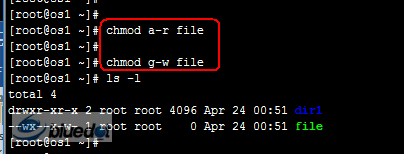


chmod g+wx file # 为文件的所属组添加wx权限，也就可以可写和可执行权限



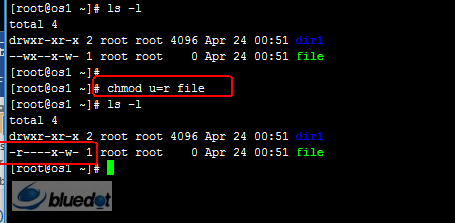
chmod o+w file #为文件的其他用户添加w 权限，也就是可写的权限。

## 1.3，减值修改

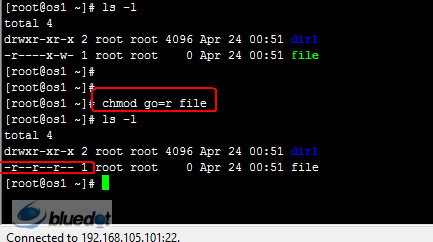


## 1.4，等值修改

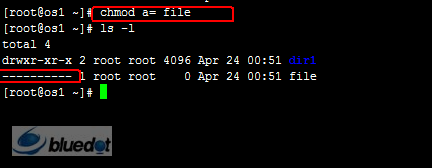
Chmod u=r file #将用户所有者的权限改成只有r、也就是只有读的权限。



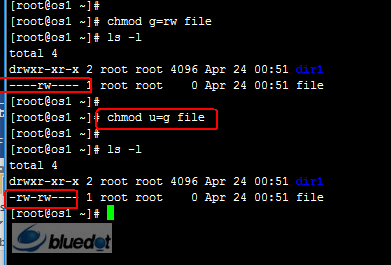
Chmod go=r file # 将file的所属组和其他人的权限改成只读。



Chmod a= file 将file文件设置成任何人没有任何权限。



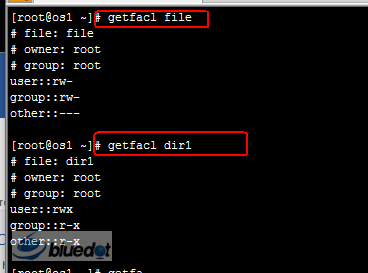
chmod u=g file 将file文件所属组的权限复制给所属者。



# 2，ACL

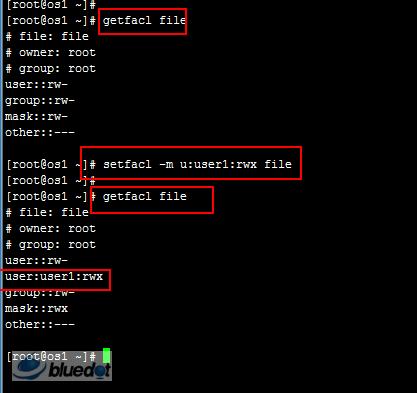
查看ACL

getfacl file ##查看file的ACL设置 。 对查看文件和目录的ACL，都用getfacl

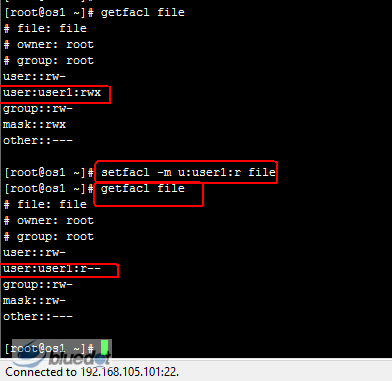


## 2.1，针对用户给文件或目录设置ACL

setfacl -m u:user1:rwx file ##对file 设置ACL，让user1对他拥有rwx权限，也就是全部的权限。

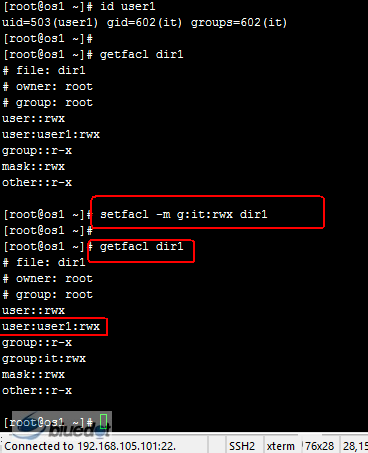


将user1对 file的权限改成只读



## 2.2，针对组给文件设置ACL

setfacl -m g:it:rwx dir1 ## 对dir1 目录设置ACL，让it 组拥有对这个目录的所有权限。



删除上面这条acl

