**实验R3 文件和目录的权限管理**

一、实验目的

1.理解Linux中文件所有者和权限的概念。

2.掌握有关权限操作的常用命令。

二、实验内容

1.文件与目录权限的设置和修改。

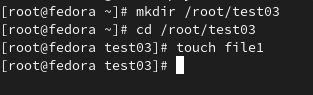
2.改变文件属主和所属组。

3.设置访问控制列表

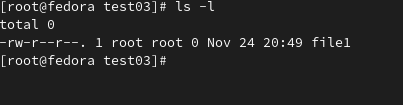
三、实验步骤

1.文件权限操作

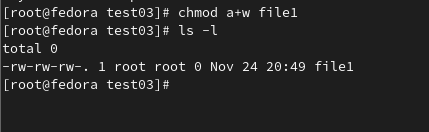
1.1在用户默认工作目录下创建目录test03，进入test03目录，使用touch命令创建空文件file1。



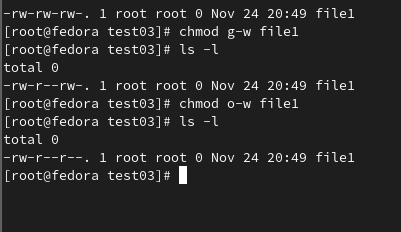
1.2显示file1详细信息，记录文件的权限信息，所属用户和组。



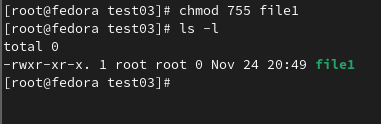
1.3对file1设置权限，使其他用户可以对此文件进行写操作，并查看设置结果。



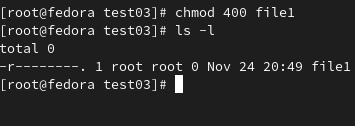
1.4取消同组用户对file1的读取权限，并查看设置结果。



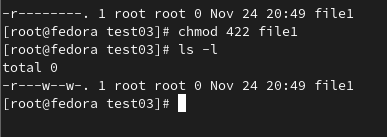
1.5用数字形式来为file1设置权限，使所有者可读、可写、可执行；其他用户和所属组用户只有读和执行的权限，并查看设置结果。

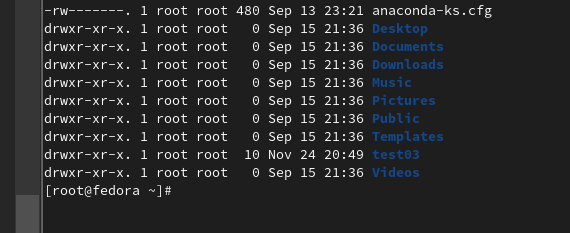


1.6用数字形式更改file1权限，使所有者只能读取此文件，其他任何用户都没有权限，并查看设置结果。

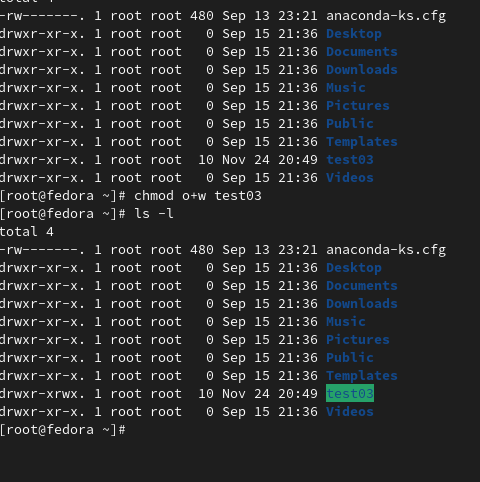


1.7为其他用户添加写权限，并查看设置结果。



1.8回到上层目录，查看test03的权限。  


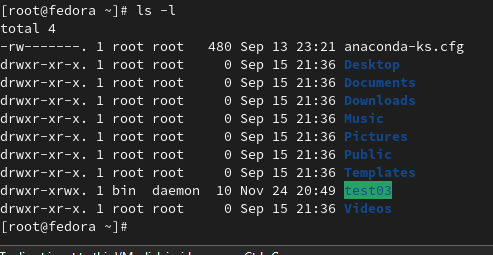
1.9为其他用户添加对此目录的写权限，查看设置结果。



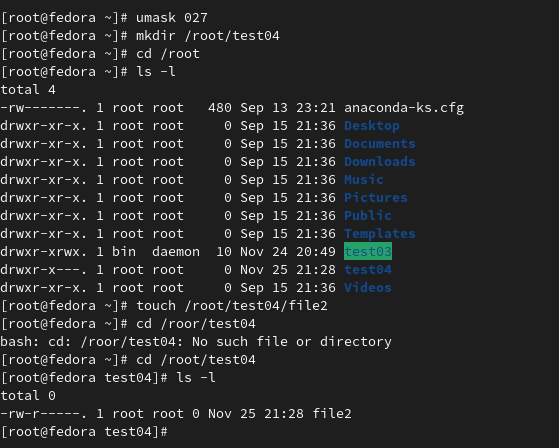
1.10查看并记录目录test03及其中文件的所属用户和组。



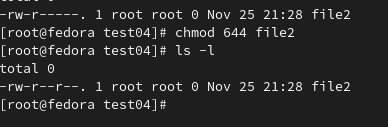
1.11把目录test03及其下的所有文件的所有者改成bin，所属组改成daemon，并查看设置结果。

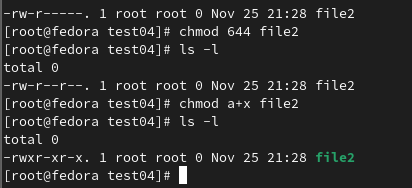


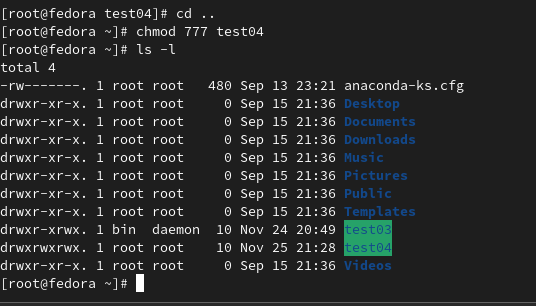
1.12设定umask为不同的值，并分别创建目录和文件，观察其权限。

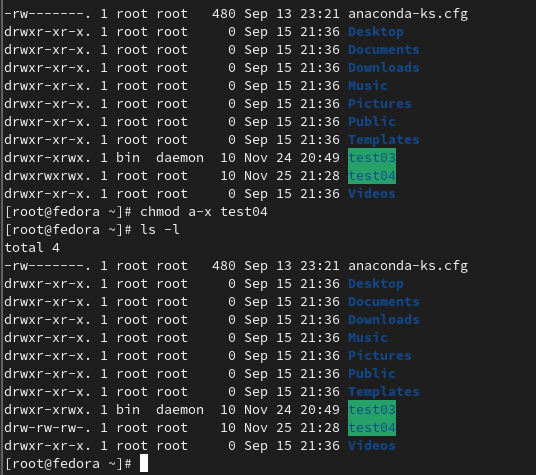


1.13 使用文字设定法和数字设定法，分别设置三种不同的特殊权限，并通过切换不同的用户，来实际验证不同特殊权限分别对文件和目录的不同作用。

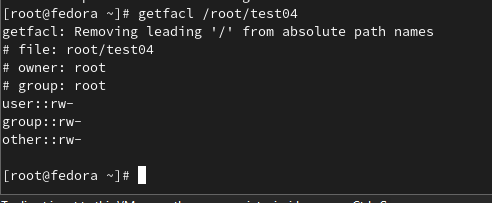








1.14 设置FACL权限，分别设置存取ACL和默认ACL。再设置有效的访问掩码。观察设定的结果，并实际验证设置对不同用户是否有效。





四、实验思考题

1.说明文件和目录不同权限及其相关含义。

文件和目录的不同权限标志着对于不同的用户，他们的读取，修改和执行某个文件的能力是不一样的。设置正确的权限可以更好的保护计算机安全以及个人和组织的隐私。在linux中，对于所有者用户，同组用户以及其它用户分别有着读取写入和执行权限，这九个权限构成了Linux权限的基础。

2.举例说明umask命令的功能。

Umask命令用来指定创建新文件和目录的默认文件权限掩码。权限掩码用三个八进制数字构成。全部权限减去权限掩码既是目标的权限。 Umask045 即是732的目录权限和622的新建文件权限。