**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。

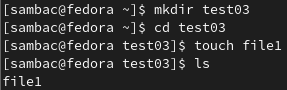
2.改变文件属主和所属组。

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。



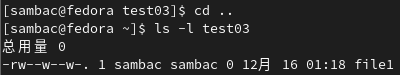
1.6用数字形式更改file1权限，使所有者只能读取此文件，其他任何用户都没有权限，并查看设置结果。



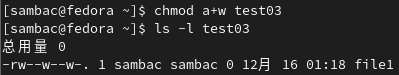
1.7为其他用户添加写权限，并查看设置结果。



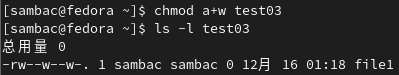
1.8回到上层目录，查看test03的权限。



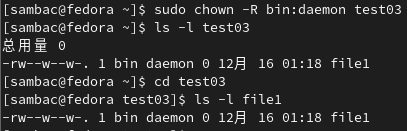
1.9为其他用户添加对此目录的写权限，查看设置结果。



1.10查看并记录目录test03及其中文件的所属用户和组。

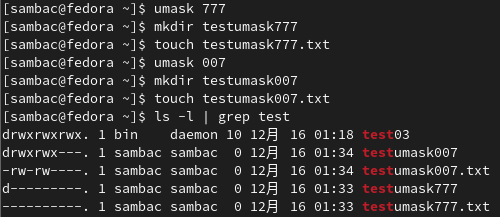


1.11把目录test03及其下的所有文件的所有者改成bin，所属组改成daemon，并查看设置结果。



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。

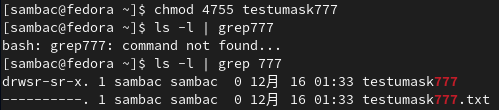
分别将umask设置为777和007进行尝试，设置为777时，所有者、同组者和其他人均没有读、写和执行的权限，设置为007时，仅其他人没有读、写和执行的权限



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。

使用8进制设置：

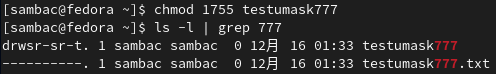
suid：



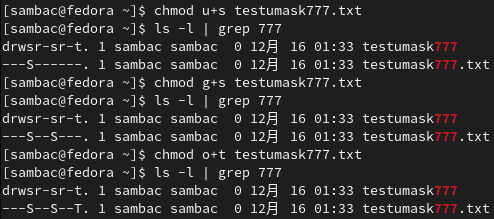
sgid：



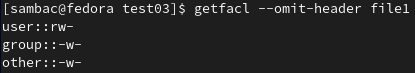
sbid：



使用文字模式设置：



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.列举ls命令不同选项的功能。

-a （all）

列出所有文件 包括隐藏文件

-l （long）

列出所有信息

-1

一行显示一个文件（目录）

-h （human-readable）

使用KB，MB，GB作为大小单位

-S （size）

按照大小排序（从小到大）

-t （time）

按照m时间排序（最新到最旧）

-r （revert）

排序反转

2.说明文件和目录不同权限及其相关含义。

r 可读

w 可写

x 可执行

special permission：

suid：使用命令的所属用户的权限来运行，而不是命令执行者的权限

sgid：使用命令的组权限来运行

sticky-bit：在带有粘滞位的目录中的文件只能被文件的所属用户和root用户删除，不管该目录的写入权限是如何设置的

3.举例说明umask命令的功能。

初始化创建文件或目录时的权限设置，如root用户默认的umask为022，则创建文件默认权限为777-022=755