兄弟连教育

www.lampbrother.net

第八讲 权限管理

主讲人：沈超（http://weibo.com/lampsc)

交流论坛：http://bbs.lampbrother.net

课程大纲

8.1 ACL权限

8.2 文件特殊权限

8.3 文件系统属性chattr权限

8.4 系统命令sudo权限

8.2 文件特殊权限

8.2.1 SetUID

8.2.2 SetGID

8.3.3 Sticky BIT

1、SetGID针对文件的作用

- 只有可执行的二进制程序才能设置SGID权限
- 命令执行者要对该程序拥有x（执行）权限
- 命令执行在执行程序的时候，组身份升级为该程序文件的属组
- SetGID权限同样只在该程序执行过程中有效，也就是说组身份改变只在程序执行过程中有效

```
[root@localhost ~]# ll /usr/bin/locate
-rwx--s--x 1 root slocate 35612 8月  24 2010 /usr/bin/locate
```

```
[root@localhost ~]# ll /var/lib/mlocate/mlocate.db
-rw-r----- 1 root slocate 1838850 1月  20 04:29 /var/lib/mlocate/mlocate.db
```

- /usr/bin/locate是可执行二进制程序，可以赋予SGID
- 执行用户lamp对/usr/bin/locate命令拥有执行权限
- 执行/usr/bin/locate命令时，组身份会升级为slocate组，而slocate组对/var/lib/mlocate/mlocate.db数据库拥有r权限，所以普通用户可以使用locate命令查询mlocate.db数据库
- 命令结束，lamp用户的组身份返回为lamp组

2、SetGID针对目录的作用

- 普通用户必须对此目录拥有r和x权限，才能进入此目录
- 普通用户在此目录中的有效组会变成此目录的属组
- 若普通用户对此目录拥有w权限时，新建的文件的默认属组是这个目录的属组

```
[root@localhost ~]# cd /tmp/
[root@localhost tmp]# mkdir dtest
[root@localhost tmp]# chmod g+s dtest
[root@localhost tmp]# ll -d dtest/
[root@localhost tmp]# chmod 777 dtest/
[root@localhost tmp]# su – lamp
[lamp@localhost ~]$ cd /tmp/dtest/
[lamp@localhost dtest]$ touch abc
[lamp@localhost dtest]$ ll
```

3、设定SetGID

- 2代表SGID
  - chmod 2755 文件名
  - chmod g+s 文件名

4、取消SetGID

- chmod 755 文件名
- chmod g-s 文件名

扫描上面的二维码

关注兄弟连官方微信账号

兄弟连官方网址：www.lampbrother.net