

第1天-文件权限管理

一、Linux用户权限解析

我们linux服务器上有严格的权限等级，如果权限过高导致误操作会增加服务器的风险。所以对于我们了解linux系统中的各种权限及要给用户，服务等分配合理的权限十分重要

二、ugo权限讲解

```
u user
g group
o other
```

```
--- --- ---
u   g   o
rwx r-x --x
```

```
r read
w write
x execute
```

```
[root@qfedu.com ~]# chmod 权限 文件
[root@qfedu.com ~]# chmod u-r-w a.txt
[root@qfedu.com ~]# chmod u+r a.txt
[root@qfedu.com ~]# chmod g+w a.txt
[root@qfedu.com ~]# chmod o+x a.txt
[root@qfedu.com ~]# chmod u+w,g-w,o+w a.txt
[root@qfedu.com ~]# chmod a-r a.txt      a表示ugo3个位置
[root@qfedu.com ~]# chmod -r a.txt      (建议少用)
```

```
4=r 2=w 1=x
rwx 4+2+1=7
r-- 4
r-x 4+1=5
745
```

```
[tom@qfedu.com ~]$ chmod 604 a.txt
[tom@qfedu.com ~]$ ll a.txt
-rw----r-- 1 tom tom 44 Nov 25 11:43 a.txt
```

三、文件所有者/所属组讲解

```
[root@qfedu.com ~]#chown 用户 文件
[root@qfedu.com ~]#chown user2 a.txt

[root@qfedu.com ~]#chown {.:}组 文件
[root@qfedu.com ~]#chown .grp2 a.txt

[root@qfedu.com ~]#chown 用户.组 文件
[root@qfedu.com ~]#chown user3:grp3 a.txt
```

-R recursive 递归修改，修改目录的时候连带目录的所有子文件一起修改

四、linux文件类型讲解

linux里面 一切皆文件

查看文件类型

```
[root@qfedu.com ~]#ls -l 文件名
-rwxrwxrwx. 1 root root 819 11月 18 10:14 1考试.txt
```

文件类型种类

- 普通文件 f
- d 目录
- b 块设备 /dev/sda /dev/sda1 /dev/sr0
- c 字符设备 /dev/pts/0 /dev/tty0
- #tty //查看字符设备名称
- l symbolic link 符号链接 软链接（快捷方式）
- s socket 套接字 网络进程间通信的一种方式
- p pipe 管道 本地进程间通信的一种方式

文件数据类型

```
[root@qfedu.com ~]#file 文件
比如：
[root@qfedu.com ~]# file VNC-5.2.0-Linux-x64-RPM.tar.gz
VNC-5.2.0-Linux-x64-RPM.tar.gz: gzip compressed data,
from Unix, last modified: Tue Jun 3 18:07:35 2014
```

查看命令类型

比如：

```
[root@qfedu.com ~]# type ls
ls 是 `ls --color=auto' 的别名
```

五、权限掩码

umask 用户掩码

控制用户创建文件和目录的默认权限

root用户默认权限

目录777 文件666

查看umask

```
[root@qfedu.com ~]#umask
```

0022 root账户默认

0002 普通用户默认

修改umask

```
[root@qfedu.com ~]#umask 0111
```

计算方法：

先把掩码做取反操作，然后在与原始权限做与运算

六、文件属性

又称为隐藏权限

```
[root@qfedu.com ~]# lsattr a.txt
```

```
[root@qfedu.com ~]# chattr +a a.txt
```

```
[root@qfedu.com ~]# chattr -a a.txt
```

```
[root@qfedu.com ~]# chattr +i a.txt
```

```
[root@qfedu.com ~]# chattr -i a.txt
```

+A: Atime, 告诉系统不要修改对这个文件的最后访问时间

+S: Sync, 一旦应用程序对这个文件执行了写操作, 使系统立刻把修改的结果写到磁盘。

+d: No dump, 在进行文件系统备份时, dump程序将忽略这个文件。

chattr命令不能保护/、/dev、/tmp、/var目录

七、sudo提权

```
[root@qfedu.com ~]# visudo
#别名的定义
Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping,
/sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm,
/usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

开放个别命令使用权:
huxulong    ALL=/usr/bin/passwd, /bin/cat, NETWORKING
开放所有命令使用权:
huxulong    ALL=(ALL)        ALL
```

八、文件权限管理实战

- 1、使用命令对Linux文件进行权限的修改操作（`rw` `chmod`）并进行测试
- 2、修改用户的所有者所属组并进行测试
- 3、改系统权限掩码（`umask`）并进行测试
- 4、用命令修改文件属性（`chattr`） 并进行测试
- 5、通过`sudo`给普通用户提权并进行测试
- 6、思考并理解`/tmp`目录权限

干锋云计算学院