

系统默认权限、网站比较安全权限、默认权限控制命令umask、文件系统属性（文件属性）、特殊权限

原创

GeorgeKai

2018-01-02 19:28:56

评论(0)

283人阅读

作者：George
归档：学习笔记
2018/1/2

补充：

vimtutor：帮助记忆vim 快捷键

本章正题：linux默认权限、网站比较安全权限、默认权限控制命令、**umask**、文件系统属性（文件属性）、特殊权限、根据权限查找文件

1.1 linux系统默认权限

1.1.1 linux下面文件和目录默认的权限

1. file rw- r-- r-- root root kai.txt
2. dir rwx r-x r-x root root kai.txt

总结：文件644、目录755，属于root和root组，才算比较安全的

1.2 网站比较安全的权限

1.2.1 /app/blog 网站程序存放位置

/app/blog/upload是用户上传的目录（如用户的头像、上传的图片），所以需要有在其中创建文件的权限。

1. blog目录

file 644 root root
dir 755 root root

2. /blog/upload目录

file 644 root root

dir 755 www www

3. 更改upload目录的所有者和属组，网站以www用户运行

测试环境准备：

```
useradd www
```

```
mkdir -p /app/blog/upload
```

```
touch /app/blog/awk.html /app/blog/renyi.jpg /app/blog/li.avi
```

7. LINUX系统默认权限控制命令UMASK

✔ 是什么？ ⊖ 控制linux里面创建文件或目录的默认的权限

通过文件或目录的最大权限 666 777减去umask

✔ 怎么计算？ ⊖

对于文件的默认权限-umask如果有奇数位 奇数位在减完后还要加1

如何修改 ⊖

临时：umask 022

永久：/etc/profile

@51CTO博客

1. 如以上情况会导致www权限不足

解决方法：把upload目录送给www，`chown www.www /app/blog/upload`

网站安全权限设置方法

博客网站blog.oldboyedu.com

一台服务器

blog博客程序（站点目录）



如何让你的网站/博客更安全？

1

1.blog 目录下
文件f 644 目录d 755
文件或目录的所有者 root root

2

2.upload 目录(用户上传 的附件 图片 头像)
文件f 644 目录d 755
文件或目录的所有者 www www

3

1).程序:控制扩展名 .jpg ;.zip
2).挂载参数决定 noexec
3).服务/软件,指定目录禁止解析/执行php。
4).http协议 请求方法控制只能post,禁止get



运行博客 通过 www用户运行(推荐)



运行博客 通过root 用户运行(比较危险)

@51CTO博客

1.3 umask 022 默认反掩码

1.3.1 linux默认的最大权限

file 666

dir 777

作用：控制系统的默认权限

1.3.2 通过umask计算默认权限方法

1) 作用：控制linux中创建文件或目录的默认权限

2) 计算方法：

file最大权限666-umask022=文件默认权限644

dir最大权限777-umask022=目录默认权限755

注： 1. 对于文件修改完后，默认权限=666（文件最大权限）-umask，如果结果有奇数，那么奇数位还要加1

2. 目录修改完后，正常计算即可（777-032=745）

3) 查看系统的反掩码umask：umask

4) 修改umask：

临时修改系统的umask：umask 032（新创建的文件或目录才会生效）

永久修改系统的umask：/etc/profile

1.4 文件扩展属性（隐藏权限）

1.4.1 查看文件扩展属性 lsattr ==> ls attribute

```
[george@georgekai tmp]$ lsattr 123.txt
-----e- 123.txt
```

1.4.2 改变文件扩展属性 chattr ==> changes attribute

1. a === aperm只能追加

1. 只能在尾部追加内容，无法删除，修改

```
[root@georgekai blog]# chattr +a test.sh
```

2. 去掉a权限

```
[root@georgekai blog]# chattr -a test.sh
```

2. i === (immutable无敌)，无法修改，无法删除

1. 锁定文件

```
[root@georgekai blog]# chattr +i test.sh
```

2. 解锁文件

```
[root@georgekai blog]# chattr -i test.sh
```

1.5 特殊权限

1.5.1 s == suid == setuid 4755

作用：运行一个命令时，相当于root

```
[root@georgekai blog]# ls -l awk.html
```

```
-rw-r--r--. 1 root root 0 Jan  2 08:58 awk.html
```

```
[root@georgekai blog]# chmod u+s awk.html == chmod 4644 awk.html
```

```
[root@georgekai blog]# ll awk.html
```

```
-rwSr--r--. 1 root root 0 Jan  2 08:58 awk.html
```

注：S 表示的没有x执行，s 表示s和x权限

1.5.2 t == sticky粘滞位 1777 （目前只有/tmp/ /usr/tmp/有t属性）

t的作用：在/tmp下自己的文件只能自己删除，root除外

```
[www@georgekai tmp]$ touch 123.txt
```

```
[george@georgekai tmp]$ \rm 123.txt
```

```
rm: remove write-protected regular empty file `123.txt'? y
```

```
rm: cannot remove `123.txt': Operation not permitted
```

1.5.3 sgid locate （不常用）

作用：运行某一个命令的时候相当于于这个命令所在家庭（用户组）

1.5.4 find根据权限查找文件

```
[root@georgekai oldboy]# find /usr/ -perm 4755
```

注：-perm ：按权限查找

```
[root@georgekai oldboy]# find / -perm 4755 -or -perm 1755
```

注：-or ：或者

总结：

1. linux权限查看 计算 修改

2. 文件和目录rwx含义

3. 各种权限拒绝错误排查

4. 如何让网站通过权限控制

5. 通过umask计算默认的权限

6. 文件系统的属性（隐藏属性）

7. linux特殊权限 suid sticky locate

请

小伙伴们可以关注我的微信公众号：linux运维菜鸟之旅，更新比51cto慢一些，不过要方便许多



关注“中国电信天津网厅”公众号，首次绑定可免费领2G流量，为你的学习提供流量！



版权声明：原创作品，如需转载，请注明出处。否则将追究法律责任
