链滴

tomcat 创建的文件权限和 linux umask、acl

作者：zhaozhizheng
原文链接：https://ld246.com/article/1597032649160
来源网站：链滴

原文**环境**：CentOS7

需求：tomcat里web应用创建的文件，放于指定目录下、提供给其他应用读取（比如ftp、nginx）。

问题：丢到tomcat里的web应用，创建出来的文件或文件夹others没有读权限，比如：

```
drwxr-x--- 2 tomcat tomcat 4096 Jun 16 17:57 temp
-rw-r----- 1 tomcat tomcat    0 Jun 16 17:57 tempfile12
```

解决方法一：

直接在web应用创建文件/文件夹时、通过代码设定权限，比如Java里这个stackoverflow答案提到的Files#setPosixFilePermissions方法。

但是缺点也很明显：一个一个改太麻烦了。

解决方法二：

见识少、google了很久才知道根本原因是tomcat启动脚本catalina.sh里的这一段：

```
#   UMASK           (Optional) Override Tomcat's default UMASK of 0027
# Set UMASK unless it has been overridden
if [ -z "$UMASK" ]; then
    UMASK="0027"
fi
umask $UMASK123456
```

原来是当初看tlcl时一看很简单就忘记的umask……就说怎么tomcat用户直接命令行 touch或 mkdir 文件权限就很宽松。

不想动tomcat的脚本，所以就在tomcat下的.bashrc里加了这个 UMASK变量：

```
export UMASK=0221
```

参考自这个so问题 Tomcat 8 change catalina.out permissions to be readable by all

解决方法三:

Linux 基本的权限控制仅可以对所属用户、所属组、其他用户进行的权限控制，而不能精确地控制每用户的权限。ACL 规则就是用来解决这个问题的。

使用 ACL 规则，我们可以针对单一账户设置文件及目录的访问权限。

实验环境:

操作系统：CentOS Linux release 7.5.1804 (Core)

组：默认用户组

用户：test□x1010:1010::/home/test:/bin/bash

目录： /var/www/web/1.com

已设置acl规则的文件

```
-rw-rwxr--+  1 root root   27 5月   7 08:03 test.
          └──> 已设置 ACL 规则
```

设置ACL规则

命令基本用法

setfacl <选项> [规则] <文件>

-m 新增一条ACL规则

-x 删除一条ACL规则

-b 清空所有ACL规则

给某个目录添加acl规则:

setfacl -m u:qudao:x /var/www/web/1.com

为目录添加默认 ACL 规则

setfacl -m d:u:test1:rwx test_dir

设置好后 再对改用户对 /root目录的访问进行限制

setfacl -m d:u:test1:x test_dir

搜索linux权限相关问题很容易看到有人提到ACL（Access Control List），参考一些使用指南（比如ArchLinux Wiki）、简单使用比如:

setfacl -Rdm "u::rwx,g::rwx,o::rx" upload/1

-m：修改， -d：继承parent目录权限，-R：同样应用到upload的当前所有子文件（夹）

然后在 upload文件夹下尝试创建文件，可以看到:

```
drwxrwxr-x+ 1 root   root       8 Jul  5 16:55 temp
drwxrwxr-x+ 1 docker docker     8 Jul  5 16:55 temp2
```

```
-rw-rw-r--. 1 root   root       0 Jul  5 16:55 tempfile
-rw-rw-r--. 1 docker docker     0 Jul  5 16:55 tempfile21234
```

- 子文件继承了 upload的权限设定

参考这个PDF PosixAccessControlInLinux：

The umask has no effect if a default ACL exists / 设置了默认ACL（-d）、umask就不起效了。

- 新建的子目录也在ACL管理下（有 +标记）
- 文件默认没有execute权限

补充问题：

1. umask是进程相关的参数，linux系统有umask设置（CentOS在/etc/profile里有一段）、但并没有MASK这个变量（这个只是tomcat用到）。

2. ACL只是权限相关，并不能改变文件（夹）的用户和group；后者可以看下 chown的 s bit。

3. 看了前面的PDF和 wikipedia，感觉ACL也是挺复杂/宽泛的概念：比如named user是群组概念不仅file system用还有网络NACL、不限于linux、windows也有……也是挺搞不清的。

参考链接