Linux权限管理

```
作者：牟建波
时间：2025-01-04
描述：日常学习笔记
```

1.Linux安全模型

3A模型：认证、授权、审计

- Authentication：认证，验证用户身份
- Authorization：授权，不同的用户设置不同权限
- Accouting|Audition：审计

当用户登录成功时，系统会自动分配令牌 token，包括：用户标识和组成员等信息

用户：Linux中每个用户是通过 `UID` (User ID)唯一标识

管理员：root，UID为0

普通用户：UID为1-60000

- 系统用户：UID为1-999，给守护进程使用
- 登录用户：UID为1000+，给用户使用

用户组：Linux中用户组通过 `GID` (Group ID)唯一标识

管理员组：root，GID为0

普通组：

- 系统组：GID为1-999，给守护进程使用
- 普通组：GID为1000+，给用户使用

用户和组的关系：一个用户仅有一个主组，可有多个附加组

安全上下文：运行中的程序，即进程 (process)，以进程发起者的身份运行，进程所能够访问资源的权限取决于进程的运行者的身份。即谁做谁负责

比如：分别以 root 和 jimbo 的身份运行 /bin/cat /etc/shadow ，得到的结果是不同的，资源能否能被访问，是由运行者的身份决定，非程序本身

2.用户和组的配置文件

```
# 用户和组的主要配置文件
/etc/passwd：用户及其属性信息(名称、UID、主组ID等)
/etc/shadow：用户密码及其相关属性
/etc/group：组及其属性信息
/etc/gshadow：组密码及其相关属性

# passwd文件格式：jimbo:x:1000:1000:jimbo:/home/jimbo:/bin/bash
login name：登录用名（jimbo）
passwd：密码 （x）
UID：用户身份编号 （1000）
GID：登录默认所在组编号 （1000）
GECOS：用户全名或注释
home directory：用户主目录 （/home/jimbo）
shell：用户默认使用shell （/bin/bash）

# shadow文件格式：jimbo:$6$uUUUJhO...::0:99999:7:::
登录用名（jimbo）
用户密码:一般用sha512加密（$6$uUUUJhO...）
从1970年1月1日起到密码最近一次被更改的时间 （:）
密码再过几天可以被变更（0表示随时可被变更） （0）
密码再过几天必须被变更（99999表示永不过期） （99999）
密码过期前几天系统提醒用户（默认为一周） （7）
密码过期几天后帐号会被锁定 （:）
从1970年1月1日算起，多少天后帐号失效（:）

# group文件格式：jimbo:x:1000:
群组名称：就是群组名称（jimbo）
群组密码：通常不需要设定，密码是被记录在 /etc/gshadow（x）
GID：就是群组的 ID（1000）
以当前组为附加组的用户列表(分隔符为逗号)（:）

# gshadow文件格式：jimbo:!::
群组名称：就是群的名称（jimbo）
群组密码： （!）
组管理员列表：组管理员的列表，更改组密码和成员（:）
```

```
以当前组为附加组的用户列表：多个用户间用逗号分隔（:）
```

3.用户和组管理命令

3.1 用户管理命令

```
# 创建用户：useradd
useradd常见选项：
-m：创建家目录
-d：指定家目录
-s：指定登录shell
-u：指定UID
-g：指定主组
-G：指定附加组

sudo useradd username     # 创建用户
sudo useradd -m -d /home/path -s /bin/bash -u 1001 username # 自定义选项：家目录、shell、UID

# 设置用户密码：passwd
sudo passwd useradd

# 修改用户属性：usermod
usermod常见选项：
-l：修改用户名。usermod -l new_name old_name
-d：修改家目录
-G：添加用户到主组
-aG：添加用户到附加组
-L：锁定用户
-U：解锁用户

sudo usermod -G 组名1,组名2 用户名      # 添加用户到主组
sudo usermod -aG 组名 用户名            # 添加用户到附加组
sudo gpasswd -d 用户名 组名             # 从组中移除用户

# 删除用户：userdel
sudo userdel username      # 删除用户但保留家目录
sudo userdel -r username   # 删除用户并移除家目录和邮件文件

# 查看用户信息：id
id username      # 显示用户UID、GID、所属组

```

```
# 切换用户
su username     # 普通切换，不读取目标用户配置文件
su - username   # 完全切换，读取目标用户配置文件
```

3.2 组管理命令

```
# 创建组：groupadd
sudo groupadd groupname     # 创建组
sudo groupadd -g 1005 groupname    # 自定义创建组，指定GID为1005

# 修改组属性：groupmod
常见选项：
-n：修改组名
-g：修改组GID

sudo groupmod [选项] groupname     # 修改组属性

# 删除组：groupdel
sudo groupdel groupname     # 删除组
```

3.3 密码策略管理

```
# 设置密码过期时间：chage
常见选项：
-d：更改密码的时间
-M：密码最大有效期(天)
-E：账户过期日期(YYYY-MM-DD)
-W：密码过期前警告天数
-I：密码过期后账户锁定天数

sudo chage -d 0 用户名     # 强制用户下次登录修改密码
```