

Linux权限管理

- 1 作者：牟建波
- 2 时间：2025-01-04
- 3 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

```
1  # 用户和组的主要配置文件
2  /etc/passwd: 用户及其属性信息(名称、UID、主组ID等)
3  /etc/shadow: 用户密码及其相关属性
4  /etc/group: 组及其属性信息
5  /etc/gshadow: 组密码及其相关属性
6
7  # passwd文件格式: jimbo:x:1000:1000:jimbo:/home/jimbo:/bin/bash
8  login name: 登录用名 (jimbo)
9  passwd: 密码 (x)
10 UID: 用户身份编号 (1000)
11 GID: 登录默认所在组编号 (1000)
12 GECOS: 用户全名或注释
13 home directory: 用户主目录 (/home/jimbo)
14 shell: 用户默认使用shell (/bin/bash)
15
16 # shadow文件格式: jimbo:$6$uUUUJh0...:0:99999:7:::
17 登录用名 (jimbo)
18 用户密码:一般用sha512加密 ($6$uUUUJh0...)
19 从1970年1月1日起到密码最近一次被更改的时间 (:)
20 密码再过几天可以被变更 (0表示随时可被变更) (0)
21 密码再过几天必须被变更 (99999表示永不过期) (99999)
22 密码过期前几天系统提醒用户 (默认为一周) (7)
23 密码过期几天后帐号会被锁定 (:)
24 从1970年1月1日算起, 多少天后帐号失效 (:)
25
26 # group文件格式: jimbo:x:1000:
27 群组名称: 就是群组名称 (jimbo)
28 群组密码: 通常不需要设定, 密码是被记录在 /etc/gshadow (x)
29 GID: 就是群组的 ID (1000)
30 以当前组为附加组的用户列表(分隔符为逗号) (:)
31
32 # gshadow文件格式: jimbo:!::
33 群组名称: 就是群组的名称 (jimbo)
34 群组密码: (!)
35 组管理员列表: 组管理员的列表, 更改组密码和成员 (:)
```

3.用户和组管理命令

3.1 用户管理命令

```
1  # 创建用户: useradd
2  useradd常见选项:
3  -m: 创建家目录
4  -d: 指定家目录
5  -s: 指定登录shell
6  -u: 指定UID
7  -g: 指定主组
8  -G: 指定附加组
9
10 sudo useradd username      # 创建用户
11 sudo useradd -m -d /home/path -s /bin/bash -u 1001 username # 自定义选项: 家目录、shell、UID
12
13 # 设置用户密码: passwd
14 sudo passwd useradd
15
16 # 修改用户属性: usermod
17 usermod常见选项:
18 -l: 修改用户名。usermod -l new_name old_name
19 -d: 修改家目录
20 -G: 添加用户到主组
21 -aG: 添加用户到附加组
22 -L: 锁定用户
23 -U: 解锁用户
24
25 sudo usermod -G 组名1,组名2 用户名      # 添加用户到主组
26 sudo usermod -aG 组名 用户名            # 添加用户到附加组
27 sudo gpasswd -d 用户名 组名              # 从组中移除用户
28
29 # 删除用户: userdel
30 sudo userdel username                    # 删除用户但保留家目录
31 sudo userdel -r username                 # 删除用户并移除家目录和邮件文件
32
33 # 查看用户信息: id
34 id username                             # 显示用户UID、GID、所属组
35
```

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

3.2 组管理命令

```
1 # 创建组: groupadd
2 sudo groupadd groupname # 创建组
3 sudo groupadd -g 1005 groupname # 自定义创建组, 指定GID为1005
4
5 # 修改组属性: groupmod
6 常见选项:
7 -n: 修改组名
8 -g: 修改组GID
9
10 sudo groupmod [选项] groupname # 修改组属性
11
12 # 删除组: groupdel
13 sudo groupdel groupname # 删除组
```

3.3 密码策略管理

```
1 # 设置密码过期时间: chage
2 常见选项:
3 -d: 更改密码的时间
4 -M: 密码最大有效期(天)
5 -E: 账户过期日期(YYYY-MM-DD)
6 -W: 密码过期前警告天数
7 -I: 密码过期后账户锁定天数
8
9 sudo chage -d 0 用户名 # 强制用户下次登录修改密码
```