用户和权限管理

1 Linux安全模型

资源分派：

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

在Linux系统中，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。

3A认证：

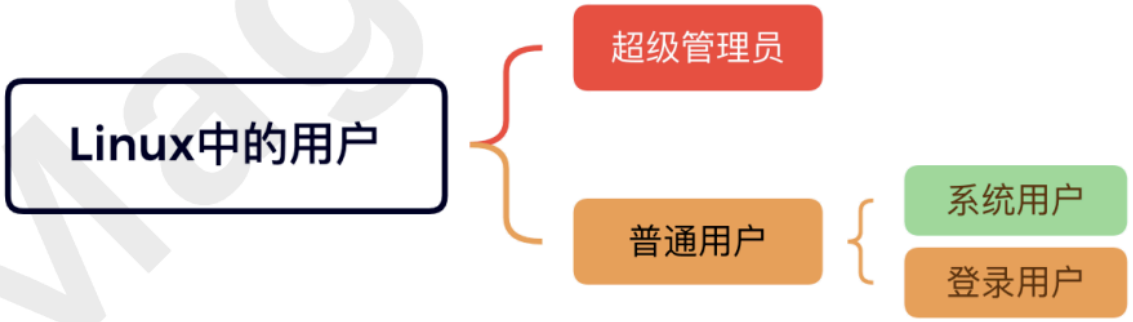
称AAA认证，是一套针对网络设备的网络访问控制策略安全模型。

```
#用于审计的登录日志
#rocky8.6
[root@rocky8 ~]# cat /var/log/secure
Jun 25 07:50:35 rocky8 polkitd[965]: Registered Authentication Agent for
unix•session:c1 (system bus name :1.52 [/usr/bin/gnome-shell], object path
/org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Jun 25 07:51:52 rocky8 sshd[2413]: Accepted password for root from 10.0.0.1 port
53734 ssh2
Jun 25 07:51:52 rocky8 systemd[2420]: pam_unix(systemd-user:session): session
opened for user root by (uid=0)
Jun 25 07:51:52 rocky8 sshd[2413]: pam_unix(sshd:session): session opened for
user root by (uid=0)
[root@ubuntu2204 ~]# tail /var/log/auth.log
May  9 16:34:13 ubuntu2204 passwd[8219]: pam_unix(passwd:chauthtok): password
changed for jose
May  9 17:13:30 ubuntu2204 sshd[1805]: pam_unix(sshd:session): session closed
for user root
May  9 17:13:30 ubuntu2204 systemd-logind[890]: Session 4 logged out. Waiting
for processes to exit.
May  9 17:13:30 ubuntu2204 systemd-logind[890]: Removed session 4.
May  9 17:13:45 ubuntu2204 sshd[8275]: Accepted password for root from 10.0.0.1
port 58443 ssh2
May  9 17:13:45 ubuntu2204 sshd[8275]: pam_unix(sshd:session): session opened
for user root(uid=0) by (uid=0)
May  9 17:13:45 ubuntu2204 systemd-logind[890]: New session 7 of user root.
```

1.1 用户

Linux系统是多用户系统，可以同时存在多个用户，每个用户之间都是互相隔离的。

在Linux系统中，每个用户是通过User Id （UID）来唯一标识的。



- 管理员：root, 0
- 普通用户：1-60000 自动分配
  - 系统用户：1-499 （CentOS 6以前）, 1-999 （CentOS 7以后） 对守护进程获取资源进行权限分配
  - 登录用户：500+ （CentOS6以前）, 1000+（CentOS7以后） 给用户进行交互式登录使用

在Linux中，root以下，都是普能用户，其用户id为1-60000

用户类型	用户名	用户ID （uid）	作用
超级管理员	root(可改)	0	超级管理员
普通用户 -- 系统用户	自定义	1-499(CentOS6及以前)，1-999(CentOS7及以后)	给后台程序使用，像nginx，mysql等
普通用户 -- 登录用户	自定义	500+(CentOS6及以前)，1000+(CentOS7及以后)	给用户进行交互式登录

1.2 用户组

Linux中可以将一个或多个用户加入用户组中，组就是包含0个或多个用户的集合，用户组是通过Group ID（GID） 来唯一标识的。

- 管理员组：root, 0
- 普通组：
  - 系统组：1-499（CentOS 6以前），1-999（CentOS7以后），对守护进程获取资源进行权限分配
  - 普通组：500+（CentOS 6以前），1000+（CentOS7以后），给用户使用

组类型	组名	组ID（gid）	作用
超级管理员组	root	0	给超级管理员使用
普通用户组 -- 系统组	自定义	1-499(CentOS6及以前)，1-999(CentOS7及以后)	给后台用户使用
普通用户组 -- 普通组	自定义	500+(CentOS6及以前)，1000+(CentOS7及以后)	给登录用户使用

1.3 用户和组的关系

- 一个用户至少有一个组，也可以有多个组；
- 一个组至少有0个用户，也可以有多个用户；
- 用户的主要组(primary group)：又称私有组，一个用户必须属于且只有一个主组，创建用户时，默认会创建与其同名的组作为主组；
- 用户的附加组(supplementary group)：又称辅助组，一个用户可以属于0个或多个附加组；
- 使用组，可以对用户进行批量管理，比如对一个组授权，则该组下所有的用户能能继承这个组的权限；

1.4 安全上下文

Linux安全上下文Context：

在Linux系统中，运行中的程序（即进程process），都是以进程发起者的身份运行；

进程所能够访问的资源权限取决于进程的运行者的身份；

首先，什么是程序

一个程序或一个命令，本质上也是一个可执行的二进制文件或一个可执行的脚本文件；

在服务器上有很多文件，只有那些特定的，可以被执行的二进制文件，才能被称为程序；

其次，什么是进程

运行中的程序，就是进程；

第三，程序，进程，用户之间的关系是怎样的

只有可以被执行的文件，才能叫作程序；

对于同一个程序，也不是所有用户都可以运行的，这要取决于当前用户对该程序有没有可执行权限；

用户张三，运行了某个程序，那么，张三就发起了一个进程，该进程的发起者，就是张三，该进程是以张三的身份在运行；

第四，进程的访问资源

一个进程能不能访问某些资源，是由进程发起者决定的（跟进程本身的程序文件无关），比如某进程要读写某个文件，则要看该进程发起者有没有权限读取该文件；

一个旅客能不能坐头等舱，是由旅客自己决定的，跟飞机本身无关；

范例:

```
#reboot命令，只有root用户才有权限执行
[root@ubuntu2204 ~]# reboot
Connection closing...Socket close.

Connection closed by foreign host.

Disconnected from remote host(rocky8.5-2-153) at 11:19:02.
Type `help' to learn how to use Xshell prompt.

#普通用户无权限执行
[root@ubuntu2204 ~]# su - jose
jose@ubuntu2204 reboot
User root is logged in on sshd.
Please retry operation after closing inhibitors and logging out other users.
Alternatively, ignore inhibitors and users with 'systemctl reboot -i'.
```

范例:

```
#root 和普通用户都能执行cat命令，但对于某些文件，只有root 用户才能打开
[root@ubuntu2204 ~]# cat /etc/shadow
root:$6$10pvyo2c4EI8tYh1$PT2yiAT6nrxs9rtjhQFWfDuHyFaV5HARXzn9YZ6wpJKveHccpl5Qolj
t7iIlmHxWuy//::0:99999:7:::
bin:*:18700:0:99999:7:::
daemon:*:18700:0:99999:7:::
adm:*:18700:0:99999:7:::
......

jose@ubuntu2204 cat /etc/shadow
cat: /etc/shadow: Permission denied
```

2 用户和组的配置文件

2.1 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

2.2 passwd文件格式

```
whatis passwd
openssl-passwd (1ssl) - compute password hashes
passwd (1)            - update user's authentication tokens
passwd (5)            - password file

man 5 passwd #查看帮助手册

#文件格式
#login name:password:UID:GID:GECOS:directory:shell

root:x:0:0:root:/root:/bin/bash
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
mage:x:1002:1002::/home/mage:/bin/bash


login name #登录用户名
password #密码位，x只是表示一个占位符，可为空
UID #用户ID，0 表示超级管理员
GID #所属组ID
GECOS #用户全名或注释，描述信息，可为空
directory #用户家目录，在创建用户时，默认会创建在/home 目录下
```

```
shell #用户默认shell，/sbin/nologin 表示不用登录的 shell，一般用 chsh 命令修改 chsh -s
/bin/csh mage
```

修改用户shell

```
[root@ubuntu2204 ~]# getent passwd jose
jose:x:1001:1001::/home/jose:/bin/bash

[root@ubuntu2204 ~]# chsh -s /bin/sh jose

[root@ubuntu2204 ~]# getent passwd jose
jose:x:1001:1001::/home/jose:/bin/sh
```

2.3 shadow文件格式

此文件中存储的是用户密码信息，任何用户都无权限

```
[root@rocky ~]# ll /etc/shadow
---------- 1 root root 1344 May 22 10:27 /etc/shadow

#ubuntu 中有权限
[root@ubuntu2204 ~]# ll /etc/shadow
-rw-r----- 1 root shadow 1218 May  9 16:34 /etc/shadow

whatis shadow
shadow (5)           - shadowed password file
shadow (3)           - encrypted password file routines

man 5 shadow

#文件格式
#login name:encrypted password:date of last password change:minimum password
age:maximum password age:password warning period:password inactivity
period:account expiration date:reserved field


root:$6$lwdNTBEpfKFnUipo$Zm4JTG7vVVg6lJaMJ7sPTqmbc/I6GGMIjp7yO.rd6TsKbOlEeRHn4q7
Z/LWJvV/FAWgTJVta9Gd78NPVNfld.1::0:99999:7:::
ftp:*:18700:0:99999:7:::
postfix:!!:19424::::::
jose:$6$Cvfl7WE8khYDd/xb$4pNMm.C46MEOUElWyFbRvO2FcGFv/a.EdD9rtWa0jvZdoThq8spMGw4
rPbcQzqsY99hW3aImVK4SPR/KJaoSh0:19168:0:99999:7:::


login name  #登录用户名
encrypted password  #加密后的密文，一般用sha512加密，可为空，!表示该用户被锁定，不能登录系统
date of last password change  #上次修改密码的时间，自1970年开始，0表示下次登录之后就要改密
码，为空表示密码时效功能无效
minimum password age  #最小时间间隔，当前密码最少能使用多少天，0表示随时可被变更
```

```
maximum password age  #最大时间间隔，当前密码最多能使用多少天，99999表示可以一直使用
password warning period  #警告时间，密码过期前几天开始提醒用户，默认为7
password inactivity period    #不活动时间，密码过期几天后帐号会被锁定，在此期间，用户仍然可以登录，为空表示不使用此规则
account expiration date       #失效时间，从1970年1月1日算起，多少天后帐号失效，为空表示永不过期
reserved field      #保留字段，无意义
```

所有伪用户的密码都是 "!!" 或 "*"，代表没有密码是不能登录的，新建用户还没设密码时为!!，禁用账号，可以直接在密码字段前加！

2.4 group文件格式

```
man group

#文件格式
#group_name:password:GID:user_list

ftp:x:50:
mage:x:1002:

group_name     #组名
password       #组密码，当用户加组时，需要用此密码验证
GID            #组ID
user_list      #用户列表，多个用户用,分隔，此处的用户将当前组作为附加组
```

2.5 gshadow文件格式

```
man gshadow

#文件格式
#group name:encrypted password:administrators:members

ftp:::
mage:!::

group name          #组名
encrypted password #组密码，加密后的密文，!表示还没设密码
administrators     #组管理员
members            #用户列表，多个用户用,分隔，此处的用户将当前组作为附加组
```

3 用户和组管理命令

用户管理命令

- useradd
- usermod
- userdel

组账号维护命令

- groupadd
- groupmod
- groupdel

3.1 用户创建

useradd 命令可以创建新的Linux用户

格式:

```
useradd [options] LOGIN
useradd -D
useradd -D [options]
#常见选项
-u|--uid UID                          #指定UID
-g|--gid GID                          #指定用户组，-g groupname|--gid GID
-c|--comment COMMENT                  #新账户的 GECOS 字段
-d|--home-dir HOME_DIR                #指定家目录，可以是不存在的，指定家目录，并不代表创建家目录
-s|--shell SHELL                      #指定 shell，可用shell在/etc/shells 中可以查看
-r|--system                           #创建系统用户,CentOS 6之前 ID<500，CentOS7 以后ID<1000，不会创建登录用户相关信息
-m|--create-home                      #创建家目录，一般用于登录用户
-M|--no-create-home                   #不创建家目录，一般用于不用登录的用户
-p|--password PASSWORD                #设置密码，这里的密码是以明文的形式存在于/etc/shadow文件中
-G|--groups GROUP1[,GROUP2,...]       #为用户指明附加组，组须事先存在
-D|--defaults                         #显示或更改默认的 useradd 配置，默认配置文件是/etc/default/useradd
-e|--expiredate EXPIRE_DATE           #指定账户的过期日期 YYYY-MM-DD 格式
-f|--inactive INACTIVE                #密码过期之后，账户被彻底禁用之前的天数，0 表示密码过期立即禁用，-1表示不使用此功能
-k|--skel SKEL_DIR                    #指定家目录模板，创建家目录，会生成一些默认文件，如果指定，就从该目录复制文件，默认/etc/skel/，要配合-m
```

默认创建

```
[root@ubuntu2204 ~]# useradd tom
```

```
#查看
[root@ubuntu2204 ~]# getent passwd tom
tom:x:1002:1002::/home/tom:/bin/sh

[root@ubuntu2204 ~]# getent shadow tom
tom:!:19486:0:99999:7:::

[root@ubuntu2204 ~]# getent group tom
tom:x:1002:

[root@ubuntu2204 ~]# getent gshadow tom
tom:!::

[root@ubuntu2204 ~]# ls /home/tom
ls: cannot access '/home/tom': No such file or directory

#rocky中默认创建
[root@rocky8 ~]# ls -a /home/tom/
. .. .bash_logout .bash_profile .bashrc
```

useradd 命令默认值设定由/etc/default/useradd定义

```
[root@rocky8 ~]# cat /etc/default/useradd
# useradd defaults file
GROUP=100 #useradd不指定组,且/etc/login.defs中的USERGROUPS_ENAB为no或useradd -N时,
group 为100
HOME=/home #默认家目录父目录
INACTIVE=-1    #对应/etc/shadow文件第7列，即用户密码过期后的帐号锁定的宽限期,-1
表示不锁定
EXPIRE=        #对应/etc/shadow文件第8列，即用户帐号的有效期
SHELL=/bin/bash #默认bash
SKEL=/etc/skel #用于生成新建用户家目录的模版文件
CREATE_MAIL_SPOOL=yes #默认创建收件箱
```

显示或更改默认设置

```
#useradd -D
#useradd -D -s SHELL
#useradd -D -b BASE_DIR
#useradd -D -g GROUP


#查看
[root@ubuntu2204 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

```
#更改默认 shell
[root@ubuntu2204 ~]# useradd -D -s /bin/bash

#再次更改
[root@ubuntu2204 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

家目录模板

```
[root@ubuntu2204 ~]# ls -a /etc/skel/
. .. .bash_logout .bash_profile .bashrc

#修改此目录内容后，新创建的用户家目录中的内容会发生改变
```

批量创建用户

```
newusers file
```

范例

```
[root@ubuntu2204 ~]# cat user.txt
u1:123456:1024:1024::/home/u1:/bin/bash
u2:123456:1025:1025::/home/u2:/bin/bash

[root@ubuntu2204 ~]# newusers user.txt
[root@ubuntu2204 ~]# id u1
uid=1024(u1) gid=1024(u1) groups=1024(u1)
[root@ubuntu2204 ~]# id u2
uid=1025(u2) gid=1025(u2) groups=1025(u2)
```

批量修改用户口令

```
chpasswd < file
```

范例

```
root@ubuntu2204 ~]# cat pwd.txt
u1:1234567
u2:1234567

#标准输入重定向
[root@ubuntu2204 ~]# chpasswd < pwd.txt


#多行重定向
[root@ubuntu2204 ~]# chpasswd <<EOF
> u1:1234567
> u2:1234567
> EOF

#管道重定向
[root@ubuntu2204 ~]# echo u1:123456 | chpasswd
```

3.2 用户属性修改

usermod 命令可以修改用户属性

格式:

```
usermod [options] LOGIN

#常见选项
-c|--comment COMMENT          #修改注释
-d|--home HOME_DIR            #修改家目录
-e|--expiredate EXPIRE_DATE   #修改过期的日期，YYYY-MM-DD 格式
-f|--inactive INACTIVE        #密码过期之后，账户被彻底禁用之前的天数，0 表示密码过期立即禁用，-1表示不使用此功能
-g|--gid GROUP                #修改组
-G|--groups GROUPS            #groupName|GID... 新附加组，原来的附加组将会被覆盖；若保留原有，则要同时使用-a选项
-a|--append GROUP             #将用户追加至上边 -G 中提到的附加组中，并不从其它组中删除此用户
-l|--login LOGIN              #新的登录名称
-L|--lock                     #锁定用户帐号，在/etc/shadow 密码栏的增加 !
-m|--move-home                #将家目录内容移至新位置，和 -d 一起使用
-s|--shell SHELL              #修改 shell
-u|--uid UID                  #修改 UID
-U|--unlock                   #解锁用户帐号，将 /etc/shadow 密码栏的!拿掉
```

修改用户信息

```
[root@ubuntu2204 ~]# id tom
uid=1002(tom) gid=1002(tom) groups=1002(tom)

#把tom改成jerry
[root@ubuntu2204 ~]# usermod -c "tom to jerry" -l jerry tom

[root@ubuntu2204 ~]# id jerry
uid=1002(jerry) gid=1002(tom) groups=1002(tom)
```

锁定用户

用户被锁定之后将无法登录

```
[root@ubuntu2204 ~]# getent shadow jose
jose:$y$j9T$d7EfLYe7v5FrllBSZQ3PH.$LsgwS9XAyBaB.GTGqfiZND6/e8POxrKeXZhpH2IIO.9:1
9486:0:99999:7:::

[root@ubuntu2204 ~]# usermod -L jose

[root@ubuntu2204 ~]# getent shadow jose
jose:!$y$j9T$d7EfLYe7v5FrllBSZQ3PH.$LsgwS9XAyBaB.GTGqfiZND6/e8POxrKeXZhpH2IIO.9:
19486:0:99999:7:::
```

解锁用户

```
[root@rocky8 ~]# usermod -U jose

[root@rocky8 ~]# getent shadow jose
jose:$6$1gfAZcky1hjTfVX0$dcImV6yr9xWzfcfeUIOzXH3pOtOOG71nzUcqD7MoLID8bzsoPKS6OCu
oGbWv.e.qXzzXknAqTfTWvMlZzpp.i/:19158:0:99999:7:::
```

centos 允许空密码用户登录，所以两个 !!，无法用 -U 选项解锁

所谓解锁，只针对于有密码的用户来说，但是，可以直接修改/etc/shadow 文件，将密码栏置空产生空密码用户

```
[root@rocky8 ~]# getent shadow jerry
jerry:!!:19168:0:99999:7:::

[root@rocky8 ~]# usermod -U jerry
usermod: unlocking the user's password would result in a passwordless account.
You should set a password with usermod -p to unlock this user's password.

[root@rocky8 ~]# getent shadow jerry
jerry:!!:19168:0:99999:7:::
```

3.3 删除用户

userdel 可删除 Linux 用户

格式:

```
userdel [options] LOGIN

#常见选项
-f|--force      #强制删除，哪怕用户正在登录状态
-r|--remove     #删除家目录和邮件目录
```

范例:

```
#创建用户并设置密码
[root@ubuntu2204 ~]# useradd -m zhangsan
[root@ubuntu2204 ~]# passwd zhangsan
New password:
Retype new password:
passwd: password updated successfully


#查看相关数据
[root@ubuntu2204 ~]# id zhangsan
uid=1026(zhangsan) gid=1026(zhangsan) groups=1026(zhangsan)


[root@ubuntu2204 ~]# ll -a /home/zhangsan/
total 20
drwxr-x--- 2 zhangsan zhangsan 4096 May  9 20:12 ./
drwxr-xr-x 7 root     root     4096 May  9 20:12 ../
-rw-r--r-- 1 zhangsan zhangsan  220 Jan  7  2022 .bash_logout
-rw-r--r-- 1 zhangsan zhangsan 3771 Jan  7  2022 .bashrc
-rw-r--r-- 1 zhangsan zhangsan  807 Jan  7  2022 .profile

#在另一个终端登录zhangsan
zhangsan@ubuntu2204:~$ id
uid=1026(zhangsan) gid=1026(zhangsan) groups=1026(zhangsan)


#删除登录中的用户失败
[root@ubuntu2204 ~]# userdel zhangsan
userdel: user zhangsan is currently used by process 2454


#强制删除
[root@ubuntu2204 ~]# userdel -f zhangsan
userdel: user zhangsan is currently used by process 2454

[root@ubuntu2204 ~]# id zhangsan
id: ‘zhangsan’: no such user

#报错
```

```
zhangsan@ubuntu2204:~$ whoami
whoami: cannot find name for user ID 1026

zhangsan@ubuntu2204:~$ id
uid=1026 gid=1026 groups=1026
```

用户被删除后，其名下的文件无法显示属主属组，只能显示UID

```
[root@ubuntu2204 ~]# ll /home/zhangsan -d
drwxr-x--- 3 1026 1026 4096 May  9 20:15 /home/zhangsan/
```

如果新建用户，使用了原用户的UID，则可以继承原用户文件

```
[root@ubuntu2204 ~]# useradd -m -u 1026 lisi


[root@ubuntu2204 ~]# ll /home/{lisi,zhangsan} -d
drwxr-x--- 2 lisi lisi 4096 May  9 20:17 /home/lisi/
drwxr-x--- 3 lisi lisi 4096 May  9 20:15 /home/zhangsan/
```

删除用户文件

```
[root@ubuntu2204 ~]# userdel -r lisi
userdel: lisi mail spool (/var/mail/lisi) not found

[root@ubuntu2204 ~]# ll /home/lisi
ls: cannot access '/home/lisi': No such file or directory
```