7 用户和用户组管理

7.1 用户配置文件

7.1.1 用户信息配置文件/etc/passwd

1. 用户管理简介

- 越是对服务器安全性要求高的服务器，越需要建立合理的用户权限等级制度和服务器操作规范。
- 在Linux中主要是通过用户配置文件来查看和修改用户信息

2. /etc/passwd(7个字段)

- 第1字段：用户名称
- 第2字段：密码标志
- 第3字段：UID(用户ID)
  - 0：超级用户
  - 1-499:系统用户(伪用户)
  - 500-65535:普通用户
- 第4字段：GID(用户初始组ID)
- 第5字段：用户说明(可以省略)
- 第6字段：家目录
  - 普通用户：/home/用户名/
  - 超级用户：/root/
- 第7字段：登录之后的Shell

3. 初始组和附加组

- 初始组：就是指用户一登录就立刻拥有这个用户组的相关权限，每个用户的初始组只能有一个，一般就是和这个用户的用户名相同的组名作为这个用户的初始组
- 附加组：指用户可以加入多个其他的用户组，并拥有这些组的权限，附加组可以有多个

4. Shell

- Shell就是Linux的命令解释器
- 在/etc/passwd当中，除了标准Shell是/bin/bash之外，还可以写如/sbin/nologin

7.1.2 影子配置文件/etc/shadow

1. 9个字段

- 第1字段：用户名称
- 第2字段：加密密码
  - 加密算法升级为SHA512散列加密算法
  - 如果密码位是"!!"或"*"代表没有密码，不能登录
- 第3字段：密码最后一次修改日期
  - 使用1970年1月1日作为标准时间，每过一天时间戳加1
- 第4字段：两次密码的修改时间间隔(和第3字段相比)
- 第5字段：密码有效期(和第3字段相比)
- 第6字段：密码修改到期前的警告天数(和第5字段相比)
- 第7字段：密码到期之后的宽限天数(和第5字段相比)
  - 0：代表密码过期之后立即失效
  - -1:代表密码永远不会失效
- 第8字段：账号失效时间
  - 要用时间戳表示
- 第9字段：保留字段

2. **时间戳换算**

- 把时间戳换算成日期
  - date -d "1970-01-01 16066 days"
- 把日期换算成时间戳
  - echo \$(($(date --date="2020/02/13" +%s)/86400 + 1))

7.1.3 组信息文件/etc/group

1. 四个字段

- 第1字段：组名
- 第2字段：组密码标志
- 第3字段：GID
- 第4字段：组中附加用户

7.1.4 组密码文件/etc/gshadow

1. 四个字段

- 第1字段：组名
- 第2字段：组密码
- 第3字段：组管理员用户名
- 第4字段：组中附加用户

7.2 用户管理相关文件

1. 用户的家目录

- 普通用户：home/用户名/，所有者和所属者都是此用户，权限是700
- 超级用户：/root/，所有者和所属者都是root用户，权限是550

2. 用户的邮箱 /var/spool/mail/用户名/
3. 用户模版目录 /etc/skel

7.3 用户管理命令

1. **添加用户命令useradd**

- useradd [选项] 用户名
- 选项：
  - -u UID：手动指定用户的UID号
  - -d 家目录：手动指定用户的家目录
  - -c 用户说明：手动指定用户的说明
  - -g 组名：手动指定用户组的初始组
  - -G 组名：指定用户的附加组
  - -s shell：手动指定用户的登录shell。默认是/bin/bash
- 添加默认用户(**useradd sc**)之后会变化的地方：
  - grep sc /etc/passwd
  - grep sc /etc/shadow
  - grep sc /etc/group
  - grep sc /etc/gshadow
  - ll -d /home/sc/ (ll是ls -l的别名)
  - ll /var/spool/mail/sc
- 用户默认值文件：
  - /etc/default/useradd
  - GROUP=100 #用户默认组
  - HOME=/home #用户家目录
  - INACTIVE=-1 #密码过期宽限天数(shadow文件7字段)
  - EXPIRE= #密码失效时间(8)
  - SHELL=/bin/bash #默认shell
  - SKEL=/etc/skel #模版目录
  - CREATE_MAIL_SPOOL=yes #是否建立邮箱
  - /etc/login.defs
  - PASS_MAX_DAYS 9999 #密码有效期(5)
  - PASS_MIN_DAYS 0 #密码修改间隔(4)
  - PASS _MIN_LEN 5 #密码最小5位(PAM)
  - PASS_WARN_AGE 7 #密码到期警告(6)
  - UID_MIN 500 #最小和最大UID范围
  - GID_MAX 60000
  - ENCRYPT_METHOD SHA512 #加密模式

2. **修改用户密码命令passwd**

- passwd [选项] 用户名

- 选项：
  - -S 查询用户密码的密码状态。仅root用户可用。
  - -l 暂时锁定用户。仅root用户可用。
  - -u 解锁用户。仅root用户可用。
  - --stdin 可可以通过管道符输出的数据作为用户的密码
  - 示例：echo“123”丨passwd --stdin lamp

3. **修改用户信息命令usermod**

- usermod [选项] 用户名
- 选项：
  - -u UID：修改用户的UID号
  - -c 用户说明：修改用户的用户说明
  - -G 组名：修改用户的附加组
  - -L：临时锁定用户(Lock)
  - -U：解锁用户(Unlock)

4. **修改用户密码状态命令chage**

- chage [选项] 用户名
- 选项：
  - -l：列出用户的详细密码状态
  - -d 日期：修改密码最后一次更改日期(shadow3字段)
  - -m 天数：两次密码修改间隔(4)
  - -M 天数：密码有效期(5)
  - -W 天数：密码过期前警告天数(6)
  - -I 天数：密码过期后宽限天数(7)
  - -E 日期：账号失效时间(8)
- **chage -d 0 用户名** #把密码修改日期归零，这样用户一登录就要修改密码

5. **删除用户命令userdel**

- userdel [-r] 用户名
- 选项：
  - -r 删除用户的同时删除用户家目录
- 手动删除用户：
  - vi /etc/passwd
  - vi /etc/shadow
  - vi /etc/group
  - vi /etc/gshadow
  - rm -rf /var/spool/mail/sc
  - rm -rf /home/sc/

6. **查看用户ID命令id**

- id 用户名

7. **切换用户身份命令su -**

- su [-选项] 用户名
- 选项：
  - -：选项只使用“-”代表连带用户的**环境变量**一起切换
  - -c：仅执行一次命令，而不切换用户身份；如：
  - su -root -c “useradd user3” #不切换成root，但是执行useradd命令添加user3用户
- 超级用户切换成普通用户不需要密码，而普通用户切换成其他用户需要密码

7.4 用户组管理命令

1. **添加用户组命令groupadd**

- groupadd [选项] 组名
- 选项：
  - -g GID：指定组ID

2. **修改用户组命令groupmod**

- 选项：
  - -g GID：修改组ID

    - -n 新组名：修改组名

3. **删除用户组命令groupdel**

- groupdel 组名

4. **把用户添加入组或从组中删除**

- gpasswd [选项] 组名
- 选项：
    - -a 用户名：把用户加入组
    - -d 用户名：把用户从组中删除
- 也可以直接修改配置文件