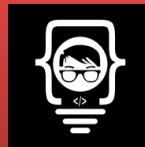




Ubuntu Server 从入门到精通

fanghong.yuan@163.com

第六章：帐号管理





用户帐号

帐号证明你就是你

- 用户帐号管理
 - 为新员工创建帐号
 - 修改帐号密码策略
 - 禁用休假员工帐号
 - 删除离职员工帐号
 - 设置帐号访问权限
- 每个人保管自己的密码
 - 不要将密码泄漏给任何人
 - 保证密码复杂度
 - 不要将密码写在纸条上贴在显示器上



用户帐号

帐号证明你就是你

- Root帐号
 - 能做任何事情（甚至删除操作系统自身）
 - 大部分Linux发行版安装时要求设置root帐号密码
 - Ubuntu 默认禁用Root帐号
 - 可sudo或临时切换为root帐号
 - 可手动启用root帐号
 - 平时以普通员工帐号管理计算机
 - `rm -rf /`
- 安装过程中创建管理员个人帐号
 - 作为日常管理使用



创建、删除帐号

帐号证明你就是你

- `useradd -d /home/user01 -m user01`
 - `-d` 帐号主目录（复制于/etc/skel）
 - `-m` 同时创建主目录（默认首次登陆时创建主目录）
 - `-c` 全名（描述）
 - `-e` 帐号过期YYYY-MM-DD
 - `-N` 不创建同名组帐号
 - `-g` 指定主组（必须已经存在）
 - `-G` 额外组
 - 帐号名最长32个字符
 - 用户主目录拷贝自/etc/skel



帐号数据库

帐号证明你就是你

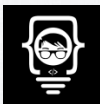
- /etc/passwd
 - 用户名 : 密码 : UID : GID : 全名,房间号,司电,宅电,others : 主目录 : shell
- /etc/shadow
 - 用户名 : 密码
 - 密码为"!"、"*"的帐号不能直接登陆系统（其他帐号登录后可切换为）
 - ! : 密码锁定
 - : 上次修改日期
 - 自1970-01-01起的天数
 - 0 表示用户下次登陆时需要修改密码，空表示关闭密码过期功能



帐号数据库

帐号证明你就是你

- `/etc/shadow`
 - : 密码最小使用期 : 密码最长使用期
 - 后值小于前值时，用户无法更改密码
 - : 密码过期前几天提醒 :
 - : 密码过期几天后帐号会被锁定
 - 帐号过期用户不能登录，密码过期看此设置是否锁帐号
 - : 帐号过期日（距1970-01-01的天数）
 - : 保留



设置帐号密码

帐号证明你就是你

- `passwd user01`
 - `-l` 锁定帐号密码！
 - `-u` 解锁帐号
 - `-d` 删除密码（帐号无密码可登录）
 - `-n / -x` 密码最小 / 最大 使用期
 - `-w` 密码过期前几天发警告
 - `-i` 密码过期几天后锁帐号
 - `-e` 密码立刻过期（下次登录必须修改）
 - `-S` 查看帐号的密码状态（L 锁定、P 活动）
 - `passwd -a -S`



添加帐号

帐号证明你就是你

- adduser user02
 - 基于useradd 的perl脚本
 - 并非所有Linux发行版中都包含
 - 向导方式运行（不需记忆命令参数）
 - /usr/sbin/adduser
- 批量添加帐号
 - sudo newusers users.txt

```
user01:pass1::User01:/home/user01:/bin/bash
user02:pass2::User02:/home/user02:/bin/bash
```





删除帐号

帐号证明你就是你

- `userdel user01`
 - 未同时删除用户主目录
 - 进行文件备份
- `rm -rf /home/user01`
- `userdel -r dscully`

删除用户主目录

删除帐号同时删除其主目录



切换帐号

帐号证明你就是你

- 切换到 root 帐号

- su

需要输入root密码（默认失败）

- sudo su

输入当前帐号密码（当前帐号属于sudo组）

- sudo -i

同上

- sudo -s

同上

- su user01

切换到其他帐号（输入目标帐号密码）

- sudo su user01

切换到其他帐号（输入当前帐号密码）



组帐号管理

分组归类统一管理

- 将用户帐号分组管理和指派权限
- 用户创建时同时生成同名的组帐号
- 每个文件有惟一的所属帐号和所属组（属主、属组）
 - 每个用户可以同属属于多个组，但只有一个主组
- `groups` 查看所有的组帐号
- `cat /etc/group`
 - 组名 : 密码（通常不使用） : GID : 逗号分隔的成员用户帐号



组管理

分组归类统一管理

- `groupadd gname`
- `groupdel gname`
- `gpasswd -a user gname`
- `usermod -aG gname user`
 — `-a`
- `usermod -g gname user`
- `usermod -d /home/u2 u1 -m`
- `usermod -l u2 u1`
- `gpasswd -d uname gname`

添加组

删除组

将用户加入额外组

将用户加入额外组

附件（否则替换）

修改用户主组

将主目录内容移动到新位置

将用户u1修改为u2

将用户从组中删除

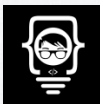




密码策略

使用足够复杂的密码

- Pluggable Authentication Module (PAM)
 - apt install libpam-cracklib
 - vi /etc/pam.d/common-password
 - password required pam_pwhistory.so remember=9 use_authok

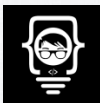


权限

权限决定你能访问哪些资源

- 每个文件和文件夹拥有惟一的属主和属组
 - ls -l
- 权限类型
 - r、w、x 读、写、执行
 - u、g、o 属主、属组、其他

权限	文件	文件夹
R	读取文件内容、拷贝	列出目录内容
W	更改文件内容	创建、 删除 文件及文件夹
X	作为应用程序执行文件	Cd进入；读取文件属性和权限



设置权限

权限决定你能访问哪些资源

- 属主和 root 可以修改权限
- `chmod u+rw a.txt`
- `chmod g-w a.txt`
- `chmod 664 a.txt`
- `chmod 770 -R path/`
- 权限与搜索
 - `find /path/dir/ -type f -perm 644 -user yuanfh -group yuanfh -exec chmod 644 {} \;`
 - `find /path/dir/ -type d -perm 755 -user yuanfh -exec ls -l {} \;`
 - `find /home -nouser -exec rm -rf {} \;` 查无有效属主对象（已删除帐号）





修改属主和属组

权限决定你能访问哪些资源

- `chown yuanfh a.txt`
- `chown -R yuan /path`
- `chown yuanfh:yuanfh a.txt`
- `chgrp users a.txt`



特殊权限

权限决定你能访问哪些资源

- Setuid (4)
 - 主要针对可执行程序
 - 任何用户执行程序时使用属主的权限
 - `chmod u+s a.sh`
- Setgid (2)
 - 主要真对可执行程序 and 目录
 - 应用于目录时可实现共享访问效果 (新建文件的属组继承目录属组)
 - `chmod g+s path/`

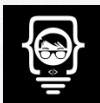




特殊权限

权限决定你能访问哪些资源

- sticky bit (1)
 - 针对目录的受限删除位 (root、属主可以删)
 - /tmp 目录即为典型例子
 - `chmod o+t path/`



掩码

权限决定你能访问哪些资源

- 决定文件和目录的默认权限
 - 文件默认权限：666-掩码
 - 文件夹默认权限：777-掩码
- /etc/login.defs
 - UMASK 022
 - USERGROUPS_ENAB yes
- umask
 - 002 用户名与组名相同、UID与GID相同
- umask 027



...

Questions?

