Lec 13 Linux账号管理与ACL权限设定

Linux的账号与群组

使用者标识符：UID与GID

jasmine <IDs>
账号名称、 IDs

ID与账号的对应在/etc/passwd中

每个用户至少有2个ID，一个是使用者ID（user ID，UID），一个是群组ID（group ID，GID）。

当有显示文件的属性的需求时，系统会依据/etc/passwd与/etc/group找到UID、GID对应的账号名与组名。

实验1：

将用户的ID随便改一个号码（`vim /etc/passwd`），再去看原先该账号拥有的文件，会发现文件的拥有人变成了"数字人"。因为乱改后，找不到对应的账号了。

实验2：

解压缩后，文件的拥有者是"意☆义☆不☆明"的"数字人"，因为Linux找不到原本的号码那个数字对应的用户名。

使用者账号

在终端机登录的时候，在输入账号与密码后，系统会：

1. 先找寻/etc/passwd里是否有你输入的账号，
   如果有，将该账号对应的UID与GID（在/etc/group中）读出来，该账号的家目录与shell设定也一并读出。
2. 核对密码表 /etc/shadow
3. 进入shell

/etc/passwd -rw-r--r--

每一行都代表一个账号，里头很多账号是系统正常运作所必需的，称为系统账号，如bin、daemon等。

```
root@vsa11779357:~# head -n 1 /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

root：账号名称、x：早期Unix的密码，已经改到了/etc/shadow中、0：UID、0：GID（↓/etc/group）、root：用户信息说明栏、/root：家目录、/bin/bash：Shell

UID范围	身份	说明
0	系统管理员	要让其他账号具有root权限，将其UID改为0即可
1～999	系统账号	这些的权限与特性并没有不一样
1000～<与核心有>	可登入账号	给一般用户使用的

/etc/shadow -rw-r-----

```
root@vsa11779357:~# cat /etc/shadow
root:<...>:19629:::::
jasmine:!:19658:1:180:7:180::
```

Q: root的密码忘了怎么办呢?

A: 重启,进入单人维护模式,系统会主动地给予root权限的bash接口,再用passwd修改密码;
或 以Live CD开机后挂载根目录去修改/etc/shadow,将root的密码字段清空,重启后root将不用密码

关于群组: 有效与初始群组、groups、newgrp

/etc/group

```
root@vsa11779357:~# cat /etc/group
flowers:x:485:
```

flowers : x : 485 :
- flowers: 组名
- x: 群组密码,已经移到了/etc/gshadow
- 485: GID
- (空): 此群组支持的账号名称。注:新版Linux中,初始群组的用户群已经不会加入这个字段。

Q: 假如我同时加入多个群组,那么我在作业时,到底以哪个群组为准?

有效群组(effective group)与初始群组(initial group)

GID → initial group

`groups` → 以某个用户的身份登入时,通过此命令知道支持的群组。第一个输出的群组即为effective group。
"通常有效群组的作用是在新建文件"

`newgrp` → 有效群组的切换
想要切换的群组必须是已有的、支持的群组

图。newgrp这个指令会以另外一个shell来提供功能

/etc/gshadow

```
root@vsa11779357:~# cat /etc/gshadow
root:::
```

root : : :
- root: 组名
- 密码,开头为!表示无合法密码,所以无群组管理员
- 群组管理员的帐号
- (空): 有加入该群组支持的账号名称(与/etc/group的内容相同)

以系统管理员的角度来说，这个 /etc/gshadow 最大的功能在于建立群组管理员。

先说一下，让一个账号加入另一个的群组有两个方法：①让 root 用 `usermod` ②让群组管理员用 gpasswd

账号管理

新增与移除使用者、相关的配置文件

useradd

useradd [-u UID] [-g <初始群组>] [-G <次要群组>] [-d <家目录绝对路径>] [-s <shell>] <user>

useradd fragrans

① 在 /etc/passwd 中写入一行与帐号相关的数据，包括 UID、GID、家目录、shell 等。

② 在 /etc/shadow 里将此帐号的密码写入（现在没有）。

③ 在 /etc/group 里加入一个与帐号名称一模一样的组名。← CenOS 设定，SuSE 会使用 useradd 的设定

④ 在 /home 底下建立一个与帐号同名的目录作为用户的家目录，且权限为 700。

passwd

给予密码

注：useradd -r

建立一个系统的帐号，由于系统帐号主要是用于进行运作系统所需服务的权限设定，系统帐号默认不会主动建立家目录。

通过 `useradd -D` 可以看到 useradd 的默认值（/etc/default/useradd）

usermod

当然可以直接修改 /etc/passwd 与 /etc/shadow 等文件，但 Linux 也提供了 usermod 这个指令。

userdel

用于删除用户的相关数据，而用户的数据有：

① 用户帐号/密码的相关记录：/etc/passwd、/etc/shadow

② 用户群组的相关记录：/etc/group、/etc/gshadow

③ 用户的个人文件数据：/home/<username>、/var/spool/mail/<username> 等

userdel [-r] <username>

[-r] 连同用户的家目录也一起删除

注：只是"暂时不使用"的话，将 /etc/shadow 里头帐号的失效日某栏设为 0 即可。

用户功能

id UID、GID 等

finger /etc/passwd，新版不支持

chfn change finger

chsh change shell

新增与移除群组 (/etc/group ./etc/gshadow)

groupadd

groupadd [-g <GID>] [-r] <群组名>

[-g] 直接给予 <GID>

[-r] 建立系统群组

groupdel

要确认没有任何/etc/passwd 中的帐号使用该群组作为 initial group

gpasswd

"如果系统管理员 root 太忙了，就可以建立群组管理员帮忙"

使用方法略。

使用外部身份认证系统

除了本机的帐号之外，还可能用到其他外部的身份验证服务器所提供的验证身份的功能。

例如，windows 下的 Active Directory，Linux的 LDAP、NIS 服务器。

主机的细部权限规划：ACL的使用 Access Control List

提供传统的 owner, group, others 的 read, write, execute 权限之外的细部权限设定。

ACL可以针对单一使用者、单一文件或目录来进行 r, w, x 的权限规范。

方向：
- user：可以针对使用者来设定权限
- group：可以针对群组来设定权限
- 默认属性(mask)：在某个目录下建立新文件/目录时，规范新文件/目录的默认权限

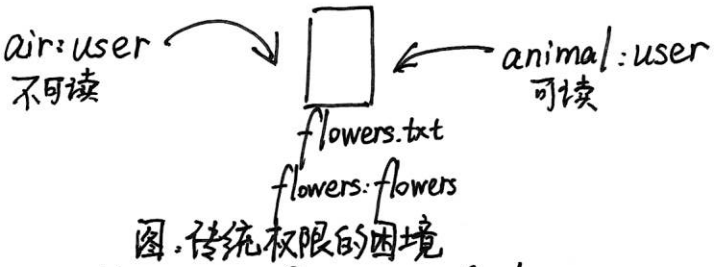

图.传统权限的困境

ACL的设定技巧：getfact、setfacl

详见原书。

使用者身份切换

sudo su	不用密码
su	要密码

su

su 读取变量设定方式为 non-login shell 方式，这种方式很多原本的变量不会改变。

su - 加载root的环境

注：使用 root 切换为其他使用者时，并不需要输入密码。

缺点：当主机是多人共管时，大家都要知道 root 的密码！

sudo

并非所有人都能使用 sudo，而且仅有 /etc/sudoers 内的用户才能够执行 sudo 这个指令。

sudo [-b] [-u <username>]

[-b] background

[-u] 切换到 <username>，没有的话就是 root

需 root 使用 `visudo` 去修改 /etc/sudoers

```
root@vsall779357:~ # visudo
root   ALL=(ALL)   ALL
```

使用者账号　登入者的来源主机名=(可切换的身份)　可下达的指令

Linux 主机上的用户讯息

"对系统上面的用户进行查询"

查询使用者：w，who，last，lastlog

使用者对谈：write，mesg，wall

使用者邮件信箱：mail

CentOS 下大量新增帐号的方法