Linux权限管理：用户与组

由于最近部署服务器的时候在弄nagios监控，并且能够达到系统异常时邮件通知的程度。nagios在网上有很多参考教程，然后就参考多个教程来学习部署，但是中间搞的很痛苦的一点就是其中一段时间弄的nagios用户与发送邮件的用户不是一个用户，然后就遇到了权限管理的问题，最后我决定先把权限管理的这部分内容搞清楚。想想在之前公司的时候这部分就是太随意了，有问题直接把权限搞成777或者直接root了，导致这部分知识的缺陷。

一、用户与组的概念。

1. Linux是多用户多任务的操作系统。比如一台Linux开发服务器，n个开发人员都能够根据自己的用户名登录到服务器开发而且互相无影响。

2. Linux大致可以分为3种角色:

(1)root用户，无所不能的超级用户

(2)普通用户，有自己的HOME目录，并能够对自己目录下的文件进行修改访问，有登录的权限。

(3)伪用户，一般无自己的HOME目录，无登录权限。但是对某些文件具有单独的读写与修改权限，以防止不同用户相互干扰。一般软件进程容易使用这种用户，比如mongodb, hadoop程序，nagios监控程序等等。

3. 用户与组的关系：

可以是1:1, 也可以是1:n, 也可以是n:1, 也可以是n:n。意思就是一个用户可以属于n个组，n个组可以包含多个用户。

二、如何快速找到系统内都有哪些用户哪些组？(配置文件)

(1)查看/etc/passwd文件，系统中所有用户都保存在这里。

known@ubuntu:~/nagios$ cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

下面以root用户为例做详细解释：

root: 用户名，是代表用户账号的字符串。

x：伪口令，由于/etc/passwd是所有用户都可见的，因此如果在这里显示用户密码串会非常不安全，许多linux版本都使用了shadow技术，把真正加密后的用户口令存放到/etc/shadow文件中，而在/etc/passwd文件的口令字段中只存放一个特殊的字符，例如用“x”或者“\*”来表示。

0: 用户标识号,就是用户的UID(user id)，每个用户都有一个UID，通常UID号的取值范围是0～65535，0是超级用户root的标识号，1～99由系统保留，作为管理账号，普通用户的标识号从100开始。UID要尽量保证唯一，以防止权限管理出现问题。

第二个0: 组标识号, 就是组的GID(group id)，表示该用户所属的组。它对应着/etc/group文件中的一条记录。

第二个root: 注释性描述,字段是对用户的描述信息。

/root：也就是用户登录到系统之后默认所处的目录，也可以叫做用户的主目录、家目录、根目录等等。

/bin/bash: 默认shell, 就是用户登录系统后默认使用的命令解释器。

(2)/etc/group文件, 用户的gid所保存的文件

known@ubuntu:~/nagios$ cat /etc/group

root:x:0:nagios

daemon:x:1:

还是以第一行root为例：

root: 用户组名称

x: 用户组的加密口令，一般保存在/etc/gshadow文件里，这里用”x”或者”\*”代替。linux系统默认无用户组口令。

0 : 用户组的组ID(gid, group id)。

nagios ：组内用户列表，用逗号分隔。

(3) /etc/shadow文件

root:$6$wNYcs7SV$R334z4AdMPGwXr1xqEKHHBTfyAAgoAsSOqv0:16973:0:99999:7:::

daemon:\*:16652:0:99999:7:::

bin:\*:16652:0:99999:7:::

还是以第一行为例：

root : 用户名，与/etc/passwd的用户名一致

$6$wNYcs…. : 一串字符口令，用户密码的加密形式。仔细看会发现daemon的这个位置是一个\*，为什么呢？之前已经说了，linux用户存在不能登录的用户，这些用户没有密码，就用”\*”或者”x”代替。

16873 : 最后一次修改的时间，这个一般平时用不到

0: 两次修改密码之间的最小间隔

99999: 两次密码修改之间的最大间隔。一般公司会使用这个，需要经常变更密码，以保证安全。

7 : 警告时间, 从开始警告用户，到用户密码失效之间的天数。

后面还有:::三个冒号，每个冒号后面还可跟字段，

不活动时间：表示口令作废多少天后，该用户就完全禁用了。

失效时间：账户的生存期，超过这个设定时间，帐号失效，用户无法登录。为空表示永久可用。

保留字段：

三、关联

用户创建后的用户id和所属的组id就都已经确定了。那么这个用户能不能访问一个文件，还有一个比对条件我们是需要知道的：文件的权限属性。只有两个权限属性是一致的，访问才会成功。那么下面就是文件的一些关于权限属性的内容。

四、文件相关属性

known@ubuntu:~/wireshark-master/idl$ ls -l

total 36

-rwxr-xr-x 1 known known 710 Aug 18 16:46 coseventcomm.idl

-rwxr-xr-x 1 known known 2360 Aug 18 16:46 cosnaming.idl

drwxr-xr-x 2 known known 4096 Aug 18 16:46 gias

drwxr-xr-x 2 known known 4096 Aug 18 16:46 parlay

-rwxr-xr-x 1 known known 18945 Aug 18 16:46 tango.idl

ls -l的内容

第一列：

-rwxr-xr-x : 这一行数字非常重要，包含了文件属性的精华。

该行可以分为4个部分：

1. - ： 第一个字符，表示文件的类型，’-’表示类型是文件，而d表示类型是目录(directory)，l表示类型是链接.
2. 第234个字符:rwx。表示文件所属用户对该文件的权限，r表示可读，w表示可写，x表示可执行。
3. 第567个字符:r-x ： 表示文件所属组对该文件的权限，r表示可读，-忽略，x表示可执行。
4. 第8910个字符r-x : 表示其他用户对该文件的权限，r表示可读， x表示可执行。

第三列和第四列:

(1)左边的known表示用户为known

(2)右侧的known表示用户组为known。

那么文件的权限就比较清晰了，known用户对文件具有rwx(读写执行)权限。known组对文件具有r-x(读和执行权限)， 其他用户对文件有r-x(读执行)权限。

五：用户管理的命令

1. useradd添加用户命令

创建一个test用户，所属组为root，创建home目录，目录为test.

useradd -d /home/test-g root -m test

2. userdel删除用户命令

删除test用户

userdel test

3.usermod修改用户属性

将用户test添加到用户组users。

sudo usermod -a -G users test

4. id [用户]

显示用户及其所属组。

六、组管理命令

1. 创建组

groupadd [组名]

2. 删除组

groupdel [组名]

3. 将用户添加到组

gpasswd -a [用户名] [组名]

4. 将用户从组中删除

gpasswd -d [用户名] [组名]

|  |  |
| --- | --- |
| 文件 | 作用 |
| /etc/shadow | 保存用户安全信息 |
| /etc/passwd | 用户账户信息 |
| /etc/gshadow | 组帐号的安全信息 |
| /etc/group | 定义用户所属的组 |
| /etc/sudoers | 可以运行sudo的用户 |