

第3章 用户与组管理

本章内容

- 用户与组账号
- 账号管理命令
- 用户与文件系统空间
- 文件权限管理
- 系统安全性

1. 用户与组账号

- 一个用户可以隶属于不同的组
- 一个组可以包含若干用户
- 系统通过帐号对用户与组进行管理

账号

□ Linux系统的账号分为用户账号和组账号

- 用户账号：每个系统的操作者拥有一个用户账号，每个用户账号具有唯一的标识UID和自己所属组的标识GID。
- 组账号：一组用户账号的集合。通过使用组账号，可以设置一组用户对文件具有相同的权限，管理员通常以组为单位分配对资源的访问权限。

用户

- Linux中包括几种不同的用户：
 - 超级用户：root为默认超级用户，属于超级用户组，其UID、GID都固定为0。
 - 普通用户：是由root创建的，每个普通用户在自己的主目录下具有完全权限，普通账号的UID和GID范围通常为500-60000。
 - 伪用户：也称为程序用户，不允许登录系统，只用于某个程序正常运行。例如bin和daemon这些后台程序都有各自的程序用户。其UID和组GID范围通常为1-499。
- 每个用户账号都会有个基本组，默认与账号名称相同，为账号额外加入的组为附加组。

用户账号配置文件

□ 用户账号文件/etc/passwd

- Linux所有的用户账号数据都记录在/etc/passwd文件中，/etc/passwd 文件是一个纯文本文件，该文件的每一行存储一个用户的账号信息，每行采用了相同的格式：

name:password:uid:gid:comment:home:shell

- 每个字段的意义见下页

/etc/passwd解释

域	说明
name 用户登录名	同一系统中用户登录名惟一。有些系统中，该字段被限制在8个字符(字母或数字)的长度之内。
password 口令	系统用口令来验证用户的合法性。如果该字段中的第一个字符是“*”，那么就表示该账号被查封了。
uid 用户标识号	uid 是一个数值，Linux系统中惟一的用户标识，用于区别不同的用户。系统内部管理进程和文件保护时使用 UID 字段。
gid 组标识号	当前用户的缺省工组标识。具有相似属性的多个用户可以被分配到同一个组内，每个组都有自己的组名，。
comment 用户信息	用户的一些相关信息，如用户的真实姓名、办公室地址、联系电话等。
home 用户主目录	定义用户的主目录，或工作目录。 root 用户的工作目录为 /root ，其他用户在 /home 目录下均有自己的主目录。
shell 命令解释程序	shell 是当用户登录系统时运行的程序名称，通常是一个 shell 程序的全路径名，如 /bin/bash 。

示例

- 以下是/etc/passwd文件的一个示例:

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

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

.....

yan:x:500:500:yan:/home/yan:/bin/bash

stu:x:501:501:stu:/home/stu:/bin/bash

用户口令文件/etc/shadow

- ❑ Linux系统中，口令不直接保存在passwd文件中，通常将passwd文件中的口令字段使用一个“x”来代替，将/etc/shadow作为真正的口令文件，用于保存包括个人口令在内的数据。
- ❑ 当然shadow文件不能被普通用户读取，只有超级用户才有权读取。
- ❑ /etc/shadow文件是根据/etc/passwd文件产生的，格式比较相近，一行存储一个用户的信息，包括9个部分，每部分之间用“:”分割，见下页。

/etc/shadow解释

域	说明
用户名	/etc/shadow中用户名和/etc/passwd 是相同的。
密码	如果是“x”，表示这个用户不能登录到系统。
上次修改口令的时间	从1970年1月1日起到最近一次修改间隔（天数）。
两次修改口令间隔最少的天数	如果设置为0，则禁用此功能，即用户必须经过多少天才能修改其口令，此项功能用处不是太大。
两次修改口令间隔最多的天数	用户管理员管理用户口令的时效性，增强了系统的安全性。
提前多少天警告用户口令将过期	当用户登录系统后，系统登录程序提醒用户口令将要作废。
在口令过期之后多少天禁用此用户	表示用户口令作废多少天后，系统会禁用此用户，即系统不再让此用户登录，也不会提示用户过期。
用户过期日期	指定用户作废的天数，空表示永久可用。
保留字段	目前为空，以备将来Linux发展之用。

示例

- ▣ 以下是/etc/shadow文件的一个示例：

```
user1:$1$VE.Mq2Xf$2c9Qi7EQ9JP8GKF8gH7P  
B1:13072:0:99999:7:::
```

```
user2:$1$IPDvUhXP$8R6J/VtPXvLyXxhLWPrn  
t/:13072:0:99999:7::13108:
```

组账号配置文件

- 组账号配置信息保存在两个文件中。
- 组账号文件/etc/group。
- 每一行表示一个组的信息，每行格式：
group_name:password:gid:user_list
- 分别表示：组名、组密码、GID、组成员列表。

root:x:0:root

bin:x:1:root,bin,daemon

daemon:x:2:root,bin,daemon

yan:x:500:yan

组账号配置文件

- 组账号口令文件/etc/gshadow。
- 每一行表示一个组账号的口令信息，每一行表示一个组的信息，每行格式：

group_name:admin,admin,...:user_list

- 分别表示：组名、组密码（一般情况下，没有必要设置）、组管理者、组成员列表。

2. 账号管理命令

- 用户和组账户的管理是Linux系统工作中重要的一部分。
- 在进行账号管理时需要以root身份进行操作。
- 用户和组账号管理包括：
 - 账号的创建
 - 删除
 - 修改
 - 授权

帐号管理命令列表

shell命令	示例	说明
useradd	useradd -d /admin -g dgroup -G root admin	创建辅助管理员账号admin，基本组指定为dgroup，附加组指定为root，工作目录指定为/admin。
passwd	passwd -u yan	解除账户yan的锁。
usermod	usermod -d /home/admin admin	将 admin 用户主目录移到 /home/admin下。
userdel	userdel -r yan	将账号yan的账户和工作目录删除。
su	su root su - root	从普通用户切换到超级用户。加参数，表示改变到root用户的环境。
Groupadd	groupadd stugroup	新建组stugroup
groupdel	groupdel admin	删除组admin。
groups	groups	查询当前登录到主机的组信息。
Users /w/who	users	查询当前登录到主机的用户信息，三个命令列出的信息有所不同

示例

- ❑ `[root@主机名]# su - yan`
- ❑ 解释：当执行这个命令的时候表示切换到yan用户，并且重新读取用户环境相关配置文件，即执行用户主目录下.bash_profile和.bashrc文件，这个也被称为全切换。

示例（续）

- [root@主机名]# su redhat
- 解释：执行这个命令时系统不读取以上两个文件，所以一般被称为半切换，切换之后，yan用户使用的依旧是此前用户的环境配置信息。
 - sudo命令允许系统管理员让普通用户执行一些或全部需要root权限的命令工具。
 - 该工具可以减少root用户的登录和管理时间，提高了系统安全性。因为sudo命令不需要root的密码，只需要用户输入其自身的密码即可临时获得root权限来运行一些外部命令。
 - 该权限是临时的，一般命令执行完之后shell就会回到当前的用户身份。

示例（续）

□ 例：需要给yan用户可以执行useradd命令的权限

- 打开/etc/sudoers配置文件

```
[root@主机名]# vi /etc/sudoers
```

- 在配置文件里添加如下行

```
yan ALL=(root) /usr/sbin/useradd
```

- 切换到yan用户

```
[root@主机名]# su - yan
```

- 普通用户yan执行useradd命令来添加用户stu

```
[yan@主机名]$ sudo /usr/sbin/useradd stu
```

3. 用户与文件系统空间

- ❑ 为了保证用户的独立性，每个用户都有自己的使用空间或目录。
- ❑ 系统可以控制用户对磁盘空间的使用。

主目录

- 用户主目录，有时也称为工作目录，每个用户都有自己的主目录，不同用户的主目录一般互不相同。例如，默认情况下用户yan的主目录就是/home/yan目录。
- 用户刚登录时，其工作目录便是主目录，通常与用户的登录名相同。可以通过“~”字符来引用。
- 修改主目录有方法一：vi /etc/passwd
 - 找到用户所在行，直接修改。此法很暴力，建议慎用。
- 修改主目录有方法二：usermod
 - usermod -d /usr/newfolder -u uid
 - 注意：-u后面一定要接uid，不是用户名。

用户与磁盘空间

- 系统管理员可以控制用户使用的硬盘空间的大小。
- 用户磁盘空间的限制是以文件系统（分区）为单位，而不理会用户文件放在该文件系统中的哪个目录。
- quota（磁盘限额）可以从两个方面来限制用户：
 - 用户所能够支配的索引节点数；
 - 用户可以存取的硬盘分区数。

磁盘限额需要处理的步骤

(1) 修改 /etc/fstab 文件, 在相应的 mount 命令中加入限额选项

```
/dev/hda7 /home Ext3 defaults,usrquota,grpquota 1 2
```

(2) 重新装载Linux分区

```
[root@主机名]# mount -o remount /home
```

(3) 在欲加磁盘限额的文件系统的安装点目录建立 aquota.user和aquota.group文件

- [root@主机名]# cd /home //注意: /home 为单个分区 /dev/hda7 的装载点
- [root@主机名]# touch aquota.user //为用户设置磁盘限额
- [root@主机名]# touch aquota.group //为用户组设置磁盘限额

磁盘限额需要处理的步骤（续）

(4) 生成符合系统要求的 aquota.user 和 aquota.group

- [root@主机名]# quotacheck /home //生成符合系统要求的aquota.user
- [root@主机名]# quotacheck -g /home //生成符合系统要求的aquota.group

磁盘限额需要处理的步骤（续）

(5) 为用户设置磁盘空间限额

- [root@主机名]# edquota [-u] user_name
- [root@主机名]# edquota -g group_name //对于用户组，本命令将开启一个vi窗口。
- [root@主机名]# edquota [-u] -p protuser user1 user2 user3
- [root@主机名]# edquota -g -p protgroup group1 group2 group3
- [root@主机名]# edquota -t //设定soft quota和hard quota之间的时间，本命令将开启一个vi窗口。

4. 文件权限管理

- 文件权限管理是文件管理与用户管理的结合。
- 分为两部分：
 - 常用的文件权限管理
 - 特殊的权限管理

文件权限

- 文件权限是指对文件的访问权限，包括对文件的读、写、删除、执行等。
- 文件的权限分为三组：
 - 文件拥有者权限
 - 文件所属群组权限
 - 其他用户的权限
- 可以设置r、w、x，分别表示读、写、执行权限。

查看文件的权限属性

- ls命令：查看文件以及目录的权限信息。
- 不带任何参数的ls命令只显示文件名称。
- “ls -al”可以显示当前目录下所有文件或者子目录的权限信息。
- 示例：oradata文件的权限

<u>drwxr-xr--</u>	<u>2</u>	<u>oracle</u>	<u>oinstall</u>	<u>4096</u>	<u>Apr 30 10:38</u>	<u>oradata</u>
↓	↓	↓	↓	↓	↓	↓
文件类型以及权限	链接数	文件所属用户和用户组	文件大小	文件最后被修改的日期	文件名称	

文件权限示例

- 第一列显示文档类型与执行权限，由十个字符组成，分为4个部分：
 - 第1部分，“d”表示目录。
 - 第2部分，对文档所有者（oracle）权限的设定，“rwx”表示用户对oradata目录有读、写和执行的所有权限。
 - 第3部分，对文档所属用户组（oinstall）权限的设定，“r-x”表示用户组对oradata目录有读和执行的权限，但是没有写的权限。
 - 第4部分，对文档拥有者之外的其他用户权限的设定，“r--”表示其他用户或用户组对oradata目录只有读的权限。

文件权限示例（续）

- 第二列显示的是文档的链接数，这个链接数就是硬链接的概念，即多少个文件指向同一个i节点。
- 第三列显示了文档所属的用户和用户组，也就是文档是属于哪个用户以及哪个用户组所有。

文件权限示例（续）

- ❑ 第四列显示的是文档的大小，默认显示的是以bytes为单位，但是也可以通过命令的参数修改显示的单位，例如可以通过“ls -sh”组合人性化地显示文档的大小。对于目录，通常只显示文件系统默认block的大小。
- ❑ 第五列显示文档最后一次的修改日期，通常以月、日、时、分的方式显示。
- ❑ 第六列显示的是文档名称，Linux下以“.”开头的文件是隐藏文件，同理以“.”开头的目录是隐藏目录，隐藏文档只有通过ls命令的“-a”选项才能显示。

改变属主和属组

- ❑ 改变属主可以用chown命令，一般语法为：
chown [-R] 用户名称 文件或目录
chown [-R] 用户名称:用户组名称 文件或目录
- ❑ -R：进行递归式的权限更改，也就是将目录下的所有文件、子目录都更新成为指定的用户组权限。通常用于变更某一目录的情况。
- ❑ 注意，在执行操作前，确保指定的用户以及用户组在系统中是存在的。

改变访问权限

- chmod用于改变文件或目录的访问权限。
- 有两种用法：
 - 方法一：字符设定法
 - 方法二：数字设定法

改变访问权限（字符设定法）

□ 语法：

`chmod [who] [+ | - | =] [mode] 文件名`

- Who: 可以是下面字母中的任何一个或者它们的组合。
- u 表示“用户”，即文件或目录的所有者。
- g 表示“用户组”，即文件或目录所属的用户组。
- o 表示“其它用户”。
- a 表示“所有用户”。它是系统默认值。

改变访问权限（字符设定法）

□ 语法：

`chmod [who] [+ | - | =] [mode] 文件名`

□ 操作符号含义如下：

- “+”表示添加某个权限。
- “-”表示取消某个权限。
- “=”表示赋予给定的权限，同时取消文档以前的所有权限。

改变访问权限（字符设定法）

□ 语法：

`chmod [who] [+ | - | =] [mode] 文件名`

- mode表示可以执行的权限，可以是“r”（只读）、“w”（可写）和“x”（可执行），以及它们的组合。
- 文件名可以是以空格分开的文件列表，支持通配符。

□ 例：修改hello.sh文件，使其所有者具有所有权限，用户组和其他用户具有只读权限。

□ # `chmod u=rwx g, o=r hello.sh`

改变访问权限（数字设定法）

- 语法: `chmod abc`文件名

- 数字设定法
 - 0表示没有任何权限;
 - 1表示有可执行权限;
 - 2表示有可写权限;
 - 4表示有可读权限。
- 如果想让文件的属主拥有读和写的权限，可以通过 $4+2=6$ 来实现。

改变访问权限（数字设定法）

- 例：修改hello.sh文件，使其所有者具有读写权限，用户组和其他用户具有只读权限。
□ # chmod 644 hello.sh
- 例：修改hello.sh文件，使其所有者具有所有权限，用户组具有只读和执行权限，其他用户具有执行权限。
□ # chmod 751 hello.sh

文件特殊权限

特殊权限	设置方法与shell命令	解释
setuid	chmod u+s filename	该命令用于文件，当文件具有该权限之后，无论文件被谁执行，该程序都有文件所有者的权限
setgid	chmod g+s dirname	该命令用于目录，当目录具有该权限之后，在该目录内无论哪个用户新建的文件都有和目录相同的组。
stick bit	chmod +t dirname	用于目录，表示目录内的文件只能被root和文件所有者删除，即使目录具有o+w的权限。
文件的不可变属性	chattr +i filename	用于文件，表示即使root用户也不能删除这个文件，直到取消这个属性为止。可用lsattr来查看文件的这个属性。
umask	umask 022 常用的umask值有022、027、002、006、007。	指定哪些权限不应该被授予。umask决定目录和文件被创建时得到的初始权限。一般默认为022，表示新建的目录权限是755(=777-022)，文件的权限是644(=666-022)。

文件特殊权限 (setuid)

- 例: [root@主机名]# ls -l /usr/bin/passwd
-rw-r--r-- 1 root root /etc/passwd
-rwsr-xr-x 1 root root /usr/bin/passwd
 - /etc/passwd文件存放的各个用户的账号与密码信息。
 - /usr/bin/passwd是执行修改和查看此文件的程序，但从权限上看/etc/passwd仅有root权限的写权限，作为普通用户没有权限修改/etc/passwd文件。
 - 给/usr/bin/passwd权限setuid后，普通用户就可以通过执行passwd命令，临时拥有root权限，去修改/etc/passwd文件。

文件特殊权限 (stick bit)

□ 例: [root@主机名]# ls -dl /tmp

drwxrwxrwt 6 root root 4096 08-22 11:37 /tmp

- tmp目录是所有用户共有的临时文件夹，所有用户都拥有读写权限。
- 这就必然出现一个问题，A用户在/tmp里创建了文件a.file，此时B用户看了不爽，在/tmp里把它给删了（因为拥有读写权限），但是执行失败。
- 原因在于，在/tmp目录中，只有文件的拥有者和root才能对其进行修改和删除，其他用户则不行。
- 粘滞位t的用途一般是把一个文件夹的权限都打开，然后来共享文件，就像/tmp目录一样。

5. 系统安全性

- Linux一直以稳定高效且安全著称，但世无完物，其存在于系统内的细小安全隐患同样不可小觑。
 - 帐号安全性
 - 常见漏洞安全性
 - SELinux

帐号安全性

(1) root帐号安全

- ❑ 当管理员在离开时忘了把root注销，这就存在隐患，所以我们希望系统能够自动从shell中注销，以达到保护root帐户的安全。
- ❑ 解决方法为：设置一个特殊的变量“tmout”，即编辑文件/etc/profile，在“histfilesizes=”命令行的下一行增加“tmout=900”，表示所有用户如果在15分钟内无任何操作将自动注销此帐户。
- ❑ 注意，增加了此命令行后，请重新用root登录，更改才能生效。

帐号安全性

(2) 删除无用帐号

- Linux提供了多种帐号类型，以下是可以有选择性删除的系统帐号：
 - Sendmail服务器帐号：news、uucp、operator
 - X windows服务器帐号：gopher
 - 具有某些特权的帐号：adm、shutdown、mail、sync
 - 还有某些系统用户、组用户、匿名FTP帐户等
 - 账号删除命令格式为：`[root@主机名]# userdel username`

常见漏洞安全性

(1) 缓冲区溢出

- ❑ 如果用root分区记录数据，就可能因为拒绝服务产生大量日志或垃圾邮件，从而导致系统崩溃。
- ❑ 很多系统专家建议：为/var目录设立单独的分区用于存放日志和邮件，避免root分区被溢出；为特殊的应用程序单独设立分区；以及为/home目录单独设立一个区。
- ❑ 经过这样的单独分区，可以有效避免针对Linux分区溢出的某些恶意攻击。

常见漏洞安全性

(2) 监听服务配置文件/etc/inetd.conf

- ❑ 此文件定制/usr/sbin/inetd将要监听的服务，建议把不用的服务关闭。操作方法：
- ❑ 显示系统开放的所有服务

```
[root@主机名]# grep -v "#" /etc/inetd.conf
```
- ❑ 运行命令关闭不需要的服务

```
[root@主机名]# killall -HUP inetd
```
- ❑ 配置后将其改为“不可更改，只能用root 帐户才能解开”

```
[root@主机名]# chattr -i /etc/inetd.conf
```
- ❑ 最后查看哪些服务在正常运行

```
[root@主机名]# netstat -na --ip
```

常见漏洞安全性

(3) 限制用户资源

- ❑ 对系统上的用户资源作适当限制可以有效防止DoS类型的攻击，如最大进程数等。操作方法为：
- ❑ 如果是对所有用户作限制，先编辑 /etc/pam.d/login文件，检查是否有session required /lib/security/pam_limits.so，然后编辑/etc/security/limits.conf，并加入以下几行：
- ❑ hard core 0----- (禁止core files)
- ❑ hard rss 5000----- (限制内存使用)
- ❑ hard nproc 20 ----- (限制进程数)

SELinux介绍

- ❑ SELinux, 是NSA (美国国家安全局) 和SCC开发的 Linux的一个扩张强制访问控制安全模块。原先是在Fluke上开发的, 2000年以GNU GPL发布。并非所有的 Linux 发行版都支持SELinux。
- ❑ SELinux是一个在内核中执行, 提供MAC能力的子系统, 以弥补传统的DAC架构的不足。
- ❑ SELinux子系统以“类型强制性”读取控制机制为主, 并融合RBAC、MLS与MCS三种MAC读取控制机制的特性。

SELinux安装

- ❑ SELinux 默认安装在Fedora和Red Hat Enterprise Linux上，也可以通过安装包安装在其它发行版上。
- ❑ 判断是否已安装SELinux包的shell命令为：
`[root@主机名]# rpm -qa | grep selinux`

SELinux配置

- ❑ SELinux的配置文件为： `/etc/selinux/config`
- ❑ 其中SELinux参数有三个选项，分别代表：
 - disabled：完全禁止SELinux的功能。
 - permissive：使用 SELinux 的策略文件验证操作，当操作不被允许的时候发出警告，但允许继续执行操作而不阻止操作进行；适合不知道使用SELinux会对系统造成什么影响的人使用。
 - enforcing：使用SELinux的策略文件验证操作，当操作不被允许时直接禁止操作执行。

SELinux安全类型

- SELINUXTYPE参数有两个选项：
 - targeted: 只会对特定的限制级的域下面启动的进程进行策略检查, 而对于无限制的域下面运行的进程则不检查策略文件。
 - strict: 将会对所有进程进行策略检查, 被设计用来对于不同安全级别的域进行更好的策略控制, 可以建立多级分层策略控制。

SELinux安全上下文

- SELinux系统中的每一个进程与对象都会记录一条安全上下文。SELinux的安全上下文的格式为：

USER:ROLE:TYPE:[LEVEL:[CATEGORY]]

- SELinux启动之后，如果要查看文件和进程的安全上下文，可使用以下命令：
 - 查看帐号安全上下文：[root@主机名]# id -Z
 - 查看文件安全上下文：[root@主机名]# ls -Z
 - 查看进程安全上下文：[root@主机名]# ps -Z

本章小结

- Linux系统是一个多用户多任务的操作系统。
- 用户和用户组的管理是系统管理员的重要工作之一。
- 尽管Linux系统一直以稳定安全著称，但是也存在一些隐患。
- SELinux融合RBAC、MLS与MCS三种MAC读取控制机制的特性，以“类型强制性”对文件的读取进行控制，极大地提高了Linux的安全性。