第04章 用户和组管理

讲师：武永亮

课程目标

- 了解CentOS的账号管理
- 掌握CentOS的用户和组的管理
- 掌握CentOS的权限管理

课程内容

- CentOS账号管理简介
- 用户和组管理
- CentOS的权限管理

账户实质

- 账户实质上就是一个用户在系统上的标识
  - ✓系统依据账户来区分每个用户的文件、进程、任务，给每个用户提供特定的工作环境（如用户的工作目录、shell版本、以及X-Window环境的配置等），使每个用户的工作都能独立不受干扰地进行。
- Linux中的账户包括
  - ✓用户账户
  - ✓组账户

用户

- Linux系统下的用户账户（简称用户）有两种
  - ✓普通用户账户：在系统上的任务是进行普通工作
  - ✓超级用户账户（或管理员账户）：在系统上的任务是对普通用户和整个系统进行管理。
- 每个用户都被分配了一个唯一的用户ID号（UID）
  - ✓超级用户：UID=0，GID=0
  - ✓普通用户：UID>=1000
  - ✓系统用户（伪用户，不可登录）：0<UID<1000

用户（续）

- 用户名和 UID 被保存在 /etc/passwd 这个文件中
- 当用户登录时，他们被分配了一个主目录和一个运行的程序（通常是 shell）
- 若无适当权限，用户无法读取、写入或执行彼此的文件

组

- 组是用户的集合
- 每个组都被分配了一个唯一的组ID号（GID）
- 组和GID 被保存在 /etc/group 文件中
- 每个用户都有他们自己的私有组
- 每个用户都可以被添加到其他组中来获得额外的存取权限
- 组中的所有用户都可以共享属于该组的文件

标准组和私有组

- 标准组
  - ✓标准组可以容纳多个用户
  - ✓若使用标准组，在创建一个新的用户时就应该指定他所属于的组
- 私有组
  - ✓私有组中只有用户自己
  - ✓当在创建一个新用户时， 若没有指定他所属于的组，RHEL/CentOS就建立一个和该用户同名的私有组，且用户被分配到这个私有组中
  - ✓优点：防止新文件归 “公共” 组所有
  - ✓缺点：可能会鼓励创建 “任何人都可以访问” 的文件

用户和组的关系

- 组是用户的集合,一个标准组可以容纳多个用户,同一个用户可以同属于多个组，这些组可以是私有组，也可以是标准组
- 当一个用户同属于多个组时，将这些组分为：
  - ✓主组（初始组）：用户登录系统时的组。
  - ✓附加组：登录后可切换的其他组。

Red Hat 的账户管理

- 默认启用shadow passwords功能。
  - ✓/etc/passwd文件对任何用户均可读，为了增加系统的安全性，用户的口令通常用shadow passwords保护。
  - ✓经过shadow passwords保护的账户密码和相关设置信息保存在/etc/shadow文件里。/etc/shadow只对root用户可读。
  - ✓默认使用sha512哈希算法存储用户的口令。
- 一般不设置组口令。因为绝大多数应用程序不使用它。
- 建议尽量使用私有组来提高系统安全性。
- 管理工具由 shadow-utils 软件包提供。
- 不建议管理员直接编辑修改系统账户文件来维护账户。

账户验证信息文件

- 口令文件 /etc/passwd
  - ✓文件权限 (-rw-r--r--)
- 影子口令文件 /etc/shadow
  - ✓文件权限 (-r--------)
- 组账号文件 /etc/group
  - ✓文件权限 (-rw-r--r--)
- 组口令文件 /etc/gshadow
  - ✓文件权限 (-r--------)

口令文件 /etc/passwd

- 每一个用户一条记录 ,每条记录由用分号间隔的七个字段组成。

字段	说明
name	用户名
password	在此文件中的口令是X，这表示用户的口令是被/etc/shadow文件保护的
uid	用户的识别号，是一个数字。每个用户的UID都是唯一的
gid	用户的组的识别号，也是一个数字。每个用户账户在建立好后都会有一个主组。主组相同的账户其GID相同。
description	用户的个人资料，包括地址、电话等信息
home	用户的主目录，通常在/home下，目录名和账户名相同
shell	用户登录后启动的shell，默认是/bin/bash

影子口令文件 /etc/shadow

- 每一个用户一条记录,每条记录由用分号间隔的九个字段组成。

字段	说明
用户名	用户登录名
口令	用户的密码，是加密过的（MD5）
最后一次修改的时间	从1970年1月1日起，到用户最后一次更改密码的天数
最小时间间隔	从1970年1月1日起，到用户应该更改密码的天数
最大时间间隔	从1970年1月1日起，到用户必须更改密码的天数
警告时间	在用户密码过期之前多少天提醒用户更新
不活动时间	在用户密码过期之后到禁用账户的天数
失效时间	从1970年1月1日起，到账户被禁用的天数
标志	保留位

组账号文件 /etc/group

- 每一个组一条记录,每条记录由用分号间隔的四个字段组成

字段	说明
组名	这是用户登录系统时的默认组名，它在系统中是唯一的
口令	组口令，由于安全性原因，已不使用该字段保存口令，用“x”占位
组ID	是一个整数，系统内部用它来标识组
组内用户列表	属于该组的所有用户名表，列表中多个用户间用“,”分隔

组口令文件 /etc/gshadow

- 每一个组一条记录,每条记录由用分号间隔的四个字段组成

字段	说明
组名	组名称，该字段与group文件中的组名称对应
加密的组口令	用于保存已加密的口令
组的管理员账号	管理员有权对该组添加删除账号
组内用户列表	属于该组的用户成员列表，列表中多个用户间用“,”分隔

验证账号文件的一致性

- Red Hat 不建议管理员直接编辑修改系统账户文件来维护账户。若用户直接编辑了账户文件，建议使用账号文件的一致性检测命令。
- pwck
  - ✓验证用户账号文件，认证信息的完整性。
  - ✓该命令检测文件“/etc/passwd”和“/etc/shadow”的每行中字段的格式和值是否正确。
- grpck
  - ✓验证组账号文件，认证信息的完整性。
  - ✓该命令检测文件“/etc/group”和“/etc/gshadow”的每行中字段的格式和值是否正确。

用户默认环境配置及模板

- 用户默认配置文件
  - ✓/etc/login.defs
  - ✓/etc/default/useradd
- 新用户基本信息
  - ✓/etc/skel
  - ✓如果手工创建用户，则需复制该目录到用户主目录

课程内容

- CentOS账号管理简介
- 用户和组管理
- CentOS的权限管理

用户和组管理工具

- 用户管理
  - ✓useradd
  - ✓usermod
  - ✓userdel
- 组管理
  - ✓groupadd
  - ✓groupmod
  - ✓groupdel

添加用户账号（useradd）

- 格式：

  ✓# useradd [<选项>] <用户名>

- 常用选项

-g group	指定新用户的主（私有）组。
-G group	指定新用户的附加组。
-d directory	指定新用户的自家目录。
-s shell	指定新用户使用的Shell，默认为bash。
-e expire	指定用户的登录失效时间，例如：08/10/2001
-M	不建立新用户的自家目录。

useradd命令添加用户的过程

- 编辑账户验证信息文件
  - ✓/etc/passwd, /etc/shadow
  - ✓/etc/group, /etc/gshadow
- 创建主目录 /home/<username>
  - ✓根据骨架目录（Skeleton Directory） /etc/skel/ 的内容填充用户主目录
- 设置权限

设置用户口令

- 命令格式
  - ✓passwd [<用户账号名>]
- 使用举例
  - ✓设置用户自己的口令
    - $ passwd
    - # passwd
  - ✓root 用户设置他人的口令
    - # passwd user1

添加用户账号举例

- 例一：
  - ✓# useradd -g group1 -e 12/31/2011 user1
  - ✓# passwd user1
- 例二：
  - ✓# useradd -G staff tom
  - ✓# passwd tom
- 例三：
  - ✓# useradd -G ftpgrp -d /var/ftp2 -M ftp1
  - ✓# passwd ftp1

useradd 命令参数的默认值

- 显示 useradd 命令参数的默认值
  - ✓useradd -D
  - ✓从文件 /etc/default/useradd 中读取
- 更改 useradd 命令参数的默认值
  - ✓格式
  - ✓# useradd -D [-g group] [-b base] [-s shell] [-e expire]
  - ✓举例
  - ✓# useradd -D -s /bin/ksh

修改用户账号（usermod）

- 格式：
  - ✓# usermod [<选项>] <用户名>
  - ✓选项与useradd命令基本相同
- 举例：
  - ✓# usermod -l user2 user1 更改user1的用户名为user2
  - ✓# usermod -G softgroup user1 更改user1的附加组列表
  - ✓# usermod -d /home user1 设置user1的新主目录
  - ✓# usermod -g group1 user1 更改user1的所属组

删除用户账号（ userdel ）

- 格式：
  - ✓# userdel [<-r>] <用户名>
  - ✓选项-r用于删除用户的宿主目录
- 举例：
  - ✓# userdel ftp1
  - ✓# userdel –r user1

添加组账号（ groupadd ）

- 格式
  - ✓# groupadd [<参数>] <组账号名>
- 常用参数
  - ✓参数-r用于创建系统组账号（ GID小于500 ）
  - ✓参数-g用于指定GID
- 举例
  - ✓# groupadd mygroup
  - ✓# groupadd -r sysgroup
  - ✓# groupadd -g 888 group2

修改组账号（ groupmod ）

- 格式
  - ✓# groupmod [<参数>] <组账号名>
- 常用参数
  - ✓参数-g改变组账号的GID ，组账号名保持不变。
  - ✓参数-n改变组账号名 。
- 举例
  - ✓# groupmod -g 503 mygroup
  - ✓# groupmod –n newgroup mygroup

删除组账号（ groupdel ）

- 格式
  - ✓# groupdel <组账号名>
- 举例
  - ✓# groupdel mygroup
- 注意
  - ✓被删除的组账号必须存在
  - ✓当有用户使用组账号作为私有组时不能删除
  - ✓与用户名同名的私有组账号在使用userdel命令删除用户时被同时删除，无需使用groupdel命令

组成员管理

- 向标准组中添加用户
  - ✓gpasswd -a <用户账号名> <组账号名>
  - ✓# gpasswd -a user1 staff
  - ✓usermod -G <组账号名> <用户账号名>
  - ✓# usermod -G staff user1
- 从标准组中删除用户
  - ✓gpasswd -d <用户账号名> <组账号名>
  - ✓# gpasswd -d user1 staff

用户切换命令

- su
  - ✓直接切换为超级用户
  - ✓普通用户要切换为超级用户必须知道超级用户的口令
  - ✓适用于系统中只有单个系统管理员的情况
- sudo
  - ✓直接使用 sudo 命令前缀执行系统管理命令
  - ✓执行系统管理命令时无需知道超级用户的口令，使用普通用户自己的口令即可
  - ✓由于执行系统管理命令时无需知晓超级用户口令，所以适用于系统中有多个系统管理员的情况，因为这样不会泄露超级用户口令。当然系统只有单个系统管理员时也可以使用。

账户相关命令

id	显示用户当前的uid、gid和用户所属的组列表
groups	显示指定用户所属的组列表
whoami	显示当前用户的名称
w/who	显示登录用户及相关信息
newgrp	用于转换用户的当前组到指定的组账号，用户必须属于该组才可以正确执行该命令

课程内容

- CentOS账号管理简介
- 用户和组管理
- CentOS的权限管理

权限概述

- Linux是多用户操作系统，允许多个用户同时在系统上登录和工作。
- 为了确保系统和用户的安全，采取了如下安全措施
  - ✓通过UID/GID确定每个用户在登录系统后都做了些什么
  - ✓通过UID/GID来区别不同用户所建立的文件或目录
    - 每个文件或目录都属于一个UID和一个GID
  - ✓每个进程都使用一个UID和一个或多个GID来运行
    - 通常由被运行进程的用户决定
  - ✓超级用户具有一切权限，无需特殊说明
  - ✓普通用户只能不受限制的操作主目录及其子目录下的所有文件，对系统中其他目录/文件的访问受到限制

三种基本权限

权限	描述字符	对文件的含义	对目录的含义
读权限	r	可以读取文件的内容	可以列出目录中的文件列表
写权限	w	可以修改或删除文件	可以在该目录中创建或删除文件或子目录
执行权限	x	可以执行该文件	可以使用cd命令进入该目录

三种基本权限（续）

- 目录上只有执行权限:
  - ✓表示可以进入更深层次的子目录
  - ✓要访问该目录下的有读权限的文件，必须知道文件名才可以访问
  - ✓不能列出目录列表也不能删除该目录
- 目录上执行权限和读权限的组合，表示可以进入目录并列出目录列表
- 目录上执行权限和写权限的组合，表示可以在目录中创建、删除和重命名文件

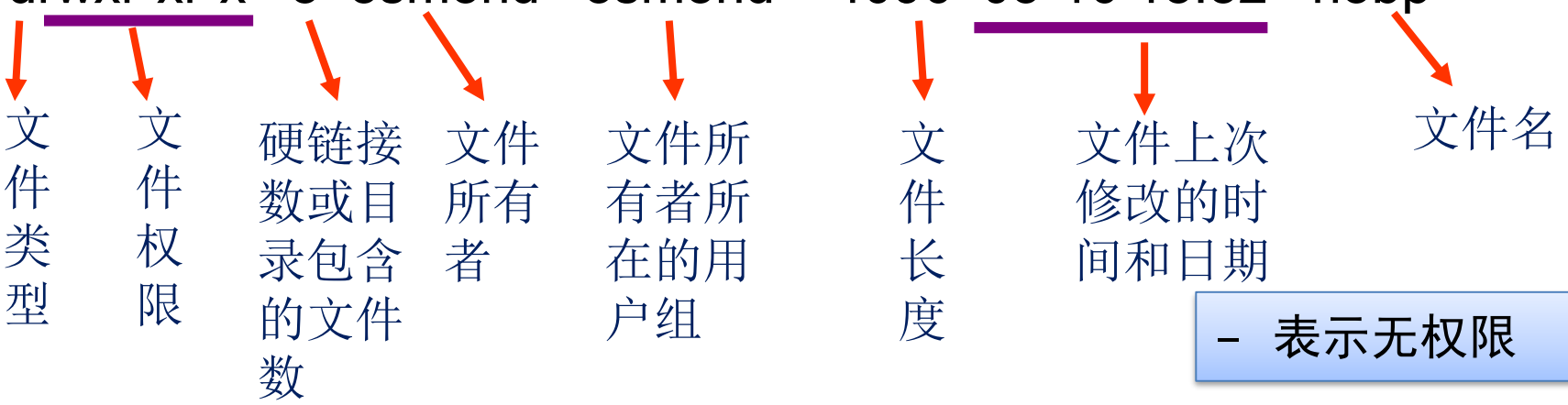
分配三种基本权限

- 文件和目录的创建者可以进行目录权限的分配
- 权限分配
  - ✓属主的权限：用于限制文件或目录的创建者
  - ✓属组的权限：用于限制文件或目录所属组的成员
  - ✓其他用户的权限：用于限制既不是属主又不是所属组的能访问该文件或目录的其他人员
- 权限的优先顺序
  - ✓如果UID匹配，就应用用户属主（user）权限
  - ✓否则，如果GID匹配，就应用组（group）权限
  - ✓如果都不匹配，就应用其它用户（other）权限

查看文件/目录的权限

- 通过给三类用户分配三种基本权限，就产生了文件或目录的9个基本权限位

```
[osmond@soho ~]$ ls  -l
总计 12
-rw-rw-r--   1  osmond     family        0 06-16 20:43   abc
drwxr-xr-x   2  osmond     family     4096  06-16 20:43   docs
-rw-rw-r--   1  osmond    osmond     1155  06-16 20:44   mylist.txt
drwxr-xr-x   3  osmond    osmond     4096  05-16 13:32   nobp
```



文件/目录的权限

```
[osmond@soho ~]$ ls  -l  docs
drwxr-xr-x   2  osmond     family    4096  06-16 20:43   docs
```

- 在显示的结果中，第一个字段的第 2～10 个字符是用来表示权限。
- 这 9 个字符每 3 个一组，组成 3 套 权限控制
  - 第一套控制文件所有者的访问权限
  - 第二套控制所有者所在用户组的其他成员的访问权限
  - 第三套控制系统其他用户的访问权限

常见的权限字符串及其含义

字符串	八进制数值	说明
-rw-------	600	只有属主才有读取和写入的权限。
-rw-r--r--	644	只有属主才有读取和写入的权限；同组人和其他人只有读取的权限。
-rwx------	700	只有属主才有读取、写入、和执行的权限。
-rwxr-xr-x	755	属主有读取、写入、和执行的权限；同组人和其他人只有读取和执行的权限。
-rwx--x--x	711	属主有读取、写入、和执行权限；同组人和其他人只有执行权限。
-rw-rw-rw-	666	每个人都能够读取和写入文件。
-rwxrwxrwx	777	每个人都能够读取、写入、和执行。
drwx------	700	只有属主能在目录中读取、写入。
drwxr-xr-x	755	每个人都能够读取目录，但是其中的内容却只能被属主改变。

权限	对应数字
r	4
w	2
x	1
-	0

每个用户都拥有自己的专属目录（主目录），通常放置在 /home 目录下，这些专属目录的默认权限通常为

drwx------

与权限相关的命令

- chmod
  - ✓改变文件或目录的权限
- chown
  - ✓改变文件或目录的属主（所有者）
- chgrp
  - ✓改变文件或目录所属的组
- umask
  - ✓设置文件的缺省生成掩码

修改文件/目录的权限

- 更改已有文件或目录的访问权限
  - ✓使用chmod命令
- chmod命令有两种设置方法
  - ✓文字设定法
    - 使用字母和操作符表达式来修改或设定文件的访问权限
    - chmod [-R] <文字模式> <文件或目录名>
  - ✓数值设定法
    - 使用八进制数字来设定文件的访问权限
    - chmod [-R] <八进制模式> <文件或目录名>

-R 选项表示对目录中的所有文件或子目录进行递归操作

chmod 的文字设定法

操作对象		操作方法		访问权限	
u	属主（user）	+	添加某权限	r	读
g	同组（group）	-	删除某权限	w	写
o	其他（others）	=	直接赋予某权限并取消其他所有权限	x	执行
a	所有（all）			-	无权限

在一个命令行中可给出多个权限模式，其间用逗号间隔

chmod 的文字设定法举例

- chmod u+rw myfile
- chmod a+rx,u+w myfile
- chmod u+rwx,g+rx,o+rx myfile
- chmod a+rwx ,g-w,o-w myfile
- chmod a=rwx myfile
- chmod go=rx myfile
- chmod u-wx,go-x myfile
- chmod a+x myfile

chmod 的数字设定法

- 使用三个数字模式来表示，分别代表用户（n1）、同组用户（n2）和其它用户（n3 ）的访问权限。
- 每个数字模式（n1|n2|n3）由不同权限所对应的数字相加得到一个表示访问权限的八进制数字。

```
chmod n1n2n3 文件或目录名
```

权限	对应数字
r	4
w	2
x	1
-	0

-rw-r--r-- ⟷ 644

drwx--x--x ⟷ 711

drwx------ ⟷ 700

-rwxr-xr-x ⟷ 755

chmod 的数字设定法举例

```
chmod 644 myname.txt
```

设定文件 myname.txt 的权限属性为：-rw-r--r--

```
chmod 750 myname.txt
```

设定文件 myname.txt 的权限属性为：-rwxr-x---

```
chmod 700 mydata/
```

设定目录 mydata 的权限属性为：drwx------

改变文件/目录属主或组

- 只有root用户才能改变文件的所有者
- 只有root用户或所有者才能改变文件所属的组
- 用 chown 命令改变属主 和/或 组
  - ✓chown [-R] <用户名[<.|:>组名]> <文件｜目录>
- chgrp 被用来改变所属组
  - ✓chgrp [-R] <组名> <文件｜目录>

改变属主或组举例

- chown soft myfile
- chgrp softgrp myfile
- chown .softgrp myfile
- chown -R soft mydir
- chgrp softgrp mydir
- chown -R :softgrp mydir
- chown -R soft.softgrp mydir

文件权限的设置准则

- 尽量使用私有组，保护用户各自的文件或目录。
- 把权限设置为 777或666 的世界可读写的权限是不明智的，应该尽量避免使用。
- 应随时了解指定给文件和目录的权限，定期检查文件和目录以确保指定了正确的权限。
  - ✓如果在目录下发现陌生的文件请向系统管理员或安全人员报告。
- 为文件和目录指定权限时请慎重考虑只有在具有充分的理由时再将访问权限授予他人。
  - ✓例如处理小组项目时组员可能需要访问特定的文件或目录需要让他人访问

课程总结

- CentOS账号管理简介
- 用户和组管理
- CentOS的权限管理

本章思考题

- Linux系统是如何标识用户和组的？
- 简述Linux的4个账户系统文件及其各个字段的含义。
- 举例说明创建一个用户账号的详细过程。
- 举例说明如何将一个用户账号添加到一个当前还不存在的组中。
- Linux文件系统的三种特殊权限是什么？何时使用它们？
- 简述chmod命令的两种设置权限的方法。
- 如何更改文件或目录的属主和/或同组人？

本章实验

- 学会管理用户和组账号
- 学会设置文件和目录的操作权限

THANK YOU!