

# Linux 系统概论

天津医科大学  
生物医学工程与技术学院

2015-2016 学年下学期（春）  
2014 级生信班

## 第二章 用户和组

伊现富 (Yi Xianfu)

天津医科大学 (TIJMU)  
生物医学工程与技术学院

2016 年 3 月



# 教学提纲

## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

## • 命令管理

## • 账户管理

## • 组管理

## • 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题

## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

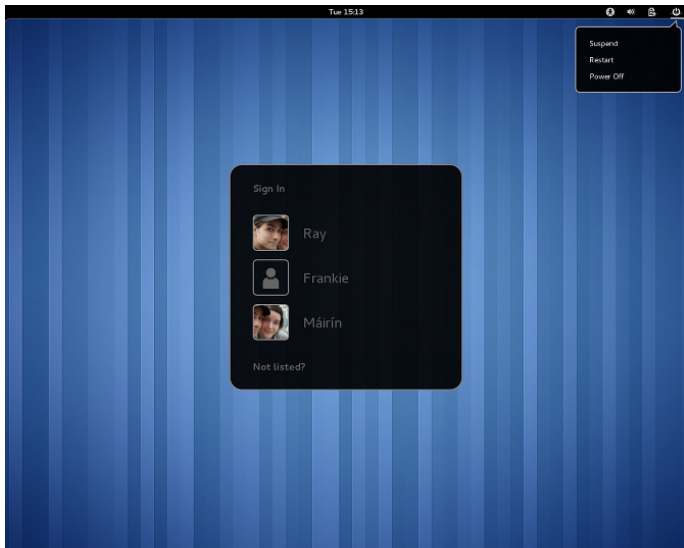
- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题





## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



- ❶ 根账户（根用户/超级用户账户，root，UID=0）
  - 不受任何限制，能够进行任何操作，包括自我毁灭
  - 谨慎使用，仅在必要且用于最重要的任务时使用
- ❷ 系统账户（伪用户，UID：1-499/999）
  - 系统账户用于系统进程，如守护进程、系统服务、网络服务等。
  - 系统账户通常没有密码，且不能登录系统。
  - 系统账户的UID范围通常为1-499，但某些系统可能扩展到999。
- ❸ 用户账户（普通用户账户，UID：500/1000-60000）
  - 用户账户用于普通用户登录系统。
  - 用户账户通常有密码，且可以登录系统。
  - 用户账户的UID范围通常为500/1000-60000，但某些系统可能有所不同。





## ❶ 根账户（根用户/超级用户账户，root，UID=0）

- 不受任何限制，能够进行任何操作，包括自我毁灭
- 谨慎使用，仅在必要且用于最重要的任务时使用

## ❷ 系统账户（伪用户，UID：1-499/999）

- 与系统和程序服务相关
  - bin、daemon、shutdown、halt 等，任何 Linux 系统默认都有这些伪用户
  - mail、news、games、apache、ftp、mysql 及 sshd 等，与 Linux 系统的进程相关
  - 通常不需要或无法登录系统
  - 可以没有家目录
- 由操作系统在安装过程中提供或由软件制造商提供
- 对系统特定组件进行操作，协助用户所需的服务或程序
- 不要轻易修改，否则可能会给系统带来不良影响

## ❸ 用户账户（普通用户账户，UID：500/1000-60000）



## ❶ 根账户（根用户/超级用户账户，root，UID=0）

- 不受任何限制，能够进行任何操作，包括自我毁灭
- 谨慎使用，仅在必要且用于最重要的任务时使用

## ❷ 系统账户（伪用户，UID：1-499/999）

- 与系统和程序服务相关
  - bin、daemon、shutdown、halt 等，任何 Linux 系统默认都有这些伪用户
  - mail、news、games、apache、ftp、mysql 及 sshd 等，与 Linux 系统的进程相关
  - 通常不需要或无法登录系统
  - 可以没有家目录
- 由操作系统在安装过程中提供或由软件制造商提供
- 对系统特定组件进行操作，协助用户所需的服务或程序
- 不要轻易修改，否则可能会给系统带来不良影响

## ❸ 用户账户（普通用户账户，UID：500/1000-60000）

- 为用户和用户组提供对系统的交互式访问
- 对关键系统文件和目录的访问权限是有限的



- ❶ 根账户（根用户/超级用户账户，root，UID=0）
  - 不受任何限制，能够进行任何操作，包括自我毁灭
  - 谨慎使用，仅在必要且用于最重要的任务时使用
- ❷ 系统账户（伪用户，UID：1-499/999）
  - 与系统和程序服务相关
    - bin、daemon、shutdown、halt 等，任何 Linux 系统默认都有这些伪用户
    - mail、news、games、apache、ftp、mysql 及 sshd 等，与 Linux 系统的进程相关
    - 通常不需要或无法登录系统
    - 可以没有家目录
  - 由操作系统在安装过程中提供或由软件制造商提供
  - 对系统特定组件进行操作，协助用户所需的服务或程序
  - 不要轻易修改，否则可能会给系统带来不良影响
- ❸ 用户账户（普通用户账户，UID：500/1000-60000）
  - 为用户和用户组提供对系统的交互式访问
  - 对关键系统文件和目录的访问权限是有限的



## ❶ 根账户（根用户/超级用户账户，root，UID=0）

- 不受任何限制，能够进行任何操作，包括自我毁灭
- 谨慎使用，仅在必要且用于最重要的任务时使用

## ❷ 系统账户（伪用户，UID：1-499/999）

- 与系统和程序服务相关
  - bin、daemon、shutdown、halt 等，任何 Linux 系统默认都有这些伪用户
  - mail、news、games、apache、ftp、mysql 及 sshd 等，与 Linux 系统的进程相关
  - 通常不需要或无法登录系统
  - 可以没有家目录
- 由操作系统在安装过程中提供或由软件制造商提供
- 对系统特定组件进行操作，协助用户所需的服务或程序
- 不要轻易修改，否则可能会给系统带来不良影响

## ❸ 用户账户（普通用户账户，UID：500/1000-60000）

- 为用户和用户组提供对系统的交互式访问
- 对关键系统文件和目录的访问权限是有限的



- ❶ 根账户（根用户/超级用户账户，root，UID=0）
  - 不受任何限制，能够进行任何操作，包括自我毁灭
  - 谨慎使用，仅在必要且用于最重要的任务时使用
- ❷ 系统账户（伪用户，UID：1-499/999）
  - 与系统和程序服务相关
    - bin、daemon、shutdown、halt 等，任何 Linux 系统默认都有这些伪用户
    - mail、news、games、apache、ftp、mysql 及 sshd 等，与 Linux 系统的进程相关
    - 通常不需要或无法登录系统
    - 可以没有家目录
  - 由操作系统在安装过程中提供或由软件制造商提供
  - 对系统特定组件进行操作，协助用户所需的服务或程序
  - 不要轻易修改，否则可能会给系统带来不良影响
- ❸ 用户账户（普通用户账户，UID：500/1000-60000）
  - 为用户和用户组提供对系统的交互式访问
  - 对关键系统文件和目录的访问权限是有限的

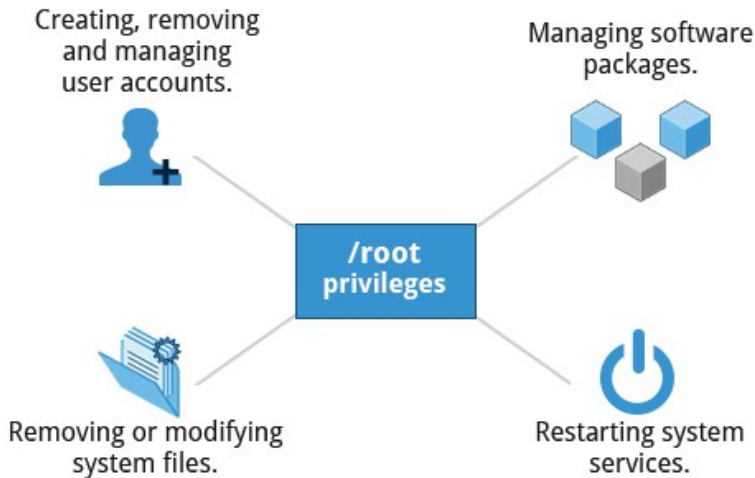


- ❶ 根账户（根用户/超级用户账户，root，UID=0）
  - 不受任何限制，能够进行任何操作，包括自我毁灭
  - 谨慎使用，仅在必要且用于最重要的任务时使用
- ❷ 系统账户（伪用户，UID：1-499/999）
  - 与系统和程序服务相关
    - bin、daemon、shutdown、halt 等，任何 Linux 系统默认都有这些伪用户
    - mail、news、games、apache、ftp、mysql 及 sshd 等，与 Linux 系统的进程相关
    - 通常不需要或无法登录系统
    - 可以没有家目录
  - 由操作系统在安装过程中提供或由软件制造商提供
  - 对系统特定组件进行操作，协助用户所需的服务或程序
  - 不要轻易修改，否则可能会给系统带来不良影响
- ❸ 用户账户（普通用户账户，UID：500/1000-60000）
  - 为用户和用户组提供对系统的交互式访问
  - 对关键系统文件和目录的访问权限是有限的



- ❶ 根账户（根用户/超级用户账户，root，UID=0）
  - 不受任何限制，能够进行任何操作，包括自我毁灭
  - 谨慎使用，仅在必要且用于最重要的任务时使用
- ❷ 系统账户（伪用户，UID：1-499/999）
  - 与系统和程序服务相关
    - bin、daemon、shutdown、halt 等，任何 Linux 系统默认都有这些伪用户
    - mail、news、games、apache、ftp、mysql 及 sshd 等，与 Linux 系统的进程相关
    - 通常不需要或无法登录系统
    - 可以没有家目录
  - 由操作系统在安装过程中提供或由软件制造商提供
  - 对系统特定组件进行操作，协助用户所需的服务或程序
  - 不要轻易修改，否则可能会给系统带来不良影响
- ❸ 用户账户（普通用户账户，UID：500/1000-60000）
  - 为用户和用户组提供对系统的交互式访问
  - 对关键系统文件和目录的访问权限是有限的







Operations that do not require Root privilege	Examples of this operation
Running a network client	Sharing a file over the network
Using devices such as printers	Printing over the network
Operations on files that the user has proper permissions to access	Accessing files that you have access to or sharing data over the network
Running SUID-root applications	Executing programs such as <i>passwd</i> .



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## 组账户

- 为了简化权限管理，将多个账户集中在一起形成一个组
- 一个组可以包括多个账户，一个账户至少属于一个组
- 同一组的用户享有该组共有的权限

## 权限管理中的三类用户

- 用户：文件的所有者
- 组：指派给文件的组
- 其他：系统中既不是所有者也不属于组的用户



## 组账户

- 为了简化权限管理，将多个账户集中在一起形成一个组
- 一个组可以包括多个账户，一个账户至少属于一个组
- 同一组的用户享有该组共有的权限

## 权限管理中的三类用户

- 用户：文件的所有者
- 组：指派给文件的组
- 其他：系统中既不是所有者也不属于组的用户



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



文件	用途	说明
/etc/passwd	用户信息文件，为系统识别已授权的用户	任何用户都可以查看，只有根用户才能修改
/etc/shadow	密码文件，保存相应账户加密后的口令	普通用户无法查看，根用户能读取但不能直接编辑
/etc/group	用户组文件，存放组账户的信息	同/etc/passwd
/etc/gshadow	用户组密码文件，保存组相应组加密后的口令	同/etc/shadow



文件	用途
/etc/login.defs	用户配置文件
/etc/default/useradd	用户配置文件
/etc/skel	新用户信息文件
/etc/issue	登录信息





## 用户账号相关的配置文件:

这两个配置文件中，每一行对应一个用户账号，不同的配置项之间用冒号“:”进行分隔，直接修改这些文件或者使用用户管理命令都可以对用户账号进行管理

配置文件	说明
/etc/passwd	保存用户名称、主目录、登录Shell等基本信息，这是一个文本文件，任何用户都可以读取文件中的内容
/etc/shadow	保存用户的密码、账号有效期等信息，只有超级用户root才有权限读取shadow文件中的内容，普通用户是无法查看这个文件的，并且即使是root用户也不允许直接编辑该文件中的内容。



## 组账号相关的配置文件:

某一个组账号包含有哪些成员，将会在 /etc/group 文件内每一行的最后一个字段中体现出来，多个组成员之间使用 “,” 分隔

配置文件	说明
/etc/group	保存组账号名称、GID号、组成员等基本信息，
/etc/gshadow	保存组账号的加密密码字符串等信息（但很少使用到）。

IT165.net  
汉云立方



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`
- `/etc/gshadow`
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 `su`
- 安全的 `sudo`
- `su` vs. `sudo`

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



# 用户和组 | 配置文件 | /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101::/var/lib/libuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:103:109::/var/spool/postfix:/bin/false
dovecot:x:104:111:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:106:113::/var/lib/landscape:/bin/false
eric:x:1000:1000:mixeduperic,,,:/home/eric:/bin/bash
jim:x:1001:1001::/home/jim:/bin/bash
bob:x:1002:1002::/home/bob:/bin/bash
tony:x:1003:1003:Tony Smith,,,:/home/tony:/bin/bash
"/etc/passwd" 29L, 1257C
```

29,1

All



# 用户和组 | 配置文件 | /etc/passwd | 7 个字段



字段	含义	说明
1	用户名	用户登录系统时输入的账户；UID 的字符串标记方式，方便阅读
2	密码	x, 密码位，密码放在/etc/shadow 中
3	UID	User ID，用户标识号
4	GID	Group ID，默认组标识号
5	注释	账户的相关信息（全名、电话等）
6	家目录	宿主目录，用户登录系统后默认所处的目录
7	登录 shell	用户登录系统后默认所使用的 shell



# 用户和组 | 配置文件 | /etc/passwd | 7 个字段



字段	含义	说明
1	用户名	用户登录系统时输入的账户；UID 的字符串标记方式，方便阅读
2	密码	x, 密码位，密码放在/etc/shadow 中
3	UID	User ID, 用户标识号
4	GID	Group ID, 默认组标识号
5	注释	账户的相关信息（全名、电话等）
6	家目录	宿主目录，用户登录系统后默认所处的目录
7	登录 shell	用户登录系统后默认所使用的 shell



# 用户和组 | 配置文件 | /etc/passwd | 7 个字段

Field Name	Details	Remarks
Username	User login name	Should be between 1 and 32 characters long
Password	User password (or the character <code>x</code> if the password is stored in the <code>/etc/shadow</code> file) in encrypted format	Is never shown in Linux when it is being typed; this stops prying eyes
User ID (UID)	Every user must have a user id (UID)	<ul style="list-style-type: none"><li>• UID 0 is reserved for root user</li><li>• UID's ranging from 1-99 are reserved for other predefined accounts</li><li>• UID's ranging from 100-999 are reserved for system accounts and groups (except for RHEL, which reserves only up to 499)</li><li>• Normal users have UID's of 1000 or greater, except on RHEL where they start at 500</li></ul>
Group ID (GID)	The primary Group ID (GID); Group Identification Number stored in the <code>/etc/group</code> file	Will be covered in detail in the chapter on Processes
User Info	This field is optional and allows insertion of extra information about the user such as their name	For example: <code>Rufus T. Firefly</code>
Home Directory	The absolute path location of user's home directory	For example: <code>/home/rtfirefly</code>
Shell	The absolute location of a user's default shell	For example: <code>/bin/bash</code>



# 用户和组 | 配置文件 | /etc/passwd | UID

id 范围	该 ID 使用者特性
0 (系统管理员)	当 UID 是 0 时, 代表这个账号是『系统管理员』! 所以当你要让其他的账号名称也具有 root 的权限时, 将该账号的 UID 改为 0 即可。这也就是说, 一部系统上面的系统管理员不见得只有 root 喔! 不过, 很不建议有多个账号的 UID 是 0 啦~
1~499 (系统账号)	<p>保留给系统使用的 ID, 其实除了 0 之外, 其他的 UID 权限与特性并没有不一样。默认 500 以下的数字让给系统作为保留账号只是一个习惯。</p> <p>由于系统上面启动的服务希望使用较小的权限去运行, 因此不希望使用 root 的身份去运行这些服务, 所以我们就得要提供这些运行中程序的拥有者账号才行。这些系统账号通常是不可登陆的, 所以才会有我们在第十一章提到的 /sbin/nologin 这个特殊的 shell 存在。</p> <p>根据系统账号的由来, 通常系统账号又约略被区分为两种:</p> <p>1~99: 由 distributions 自行创建的系统账号;</p> <p>100~499: 若用户有系统账号需求时, 可以使用的账号 UID。</p>
500~65535 (可登陆账号)	给一般使用者用的。事实上, 目前的 linux 核心 (2.6.x 版) 已经可以支持到 4294967295 ( $2^{32}-1$ ) 这么大的 UID 号码喔!





# 用户和组 | 配置文件 | /etc/passwd | UID & GID

用户/组说明	用户/组分类	UID/GID范围	说明
Linux系统中的所有用户账号信息则都存放在/etc/passwd和/etc/shadow文件中，文件中的每一行就代表一个用户。而window所有的本地用户账号的信息都存放在c:\windows\system32\config\sam文件中	root	0	root是Linux系统中默认的超级用户账号，类似于Windows系统中的Administrator用户。
	系统用户	1~499	在安装Linux系统及部分应用程序时，会添加一些特定的低权限用户账号，这些用户一般不允许登录到系统，而仅用于维持系统或某个程序的正常运行。
	普通用户	500~65535	普通用户账号需要由root用户或其他管理员用户创建，拥有的权限受到一定限制，一般只在用户自己的主目录中有完全权限。
Linux系统每创建一个用户账号就会自动创建一个与该账号同名的用户组，该组为用户的基本组。每个用户可以同时加入多个组，用户又另外加入的组称为该用户的附属组（附加组）	Root组	0	类似于windows的administrator组
	系统组	1~499	一般加入一些系统用户
	普通组	500~65535	当创建用户时,如果没有为其指明所属组,则创建一个与用户名同名的组。



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- **/etc/shadow**
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

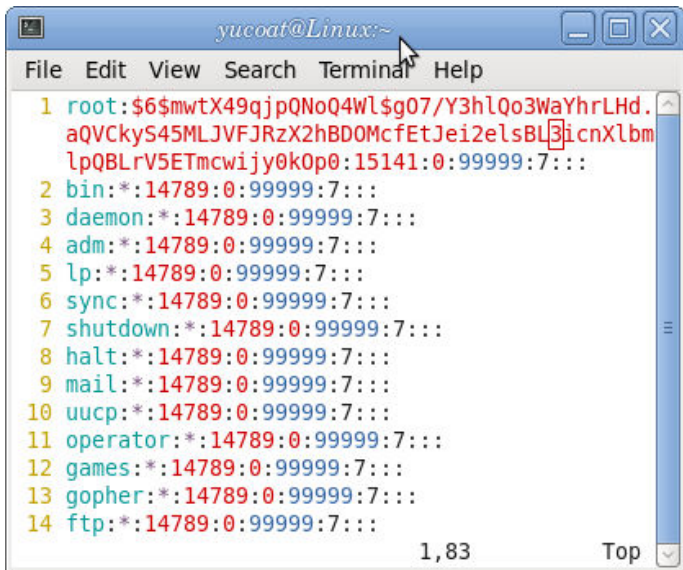
## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



# 用户和组 | 配置文件 | /etc/shadow

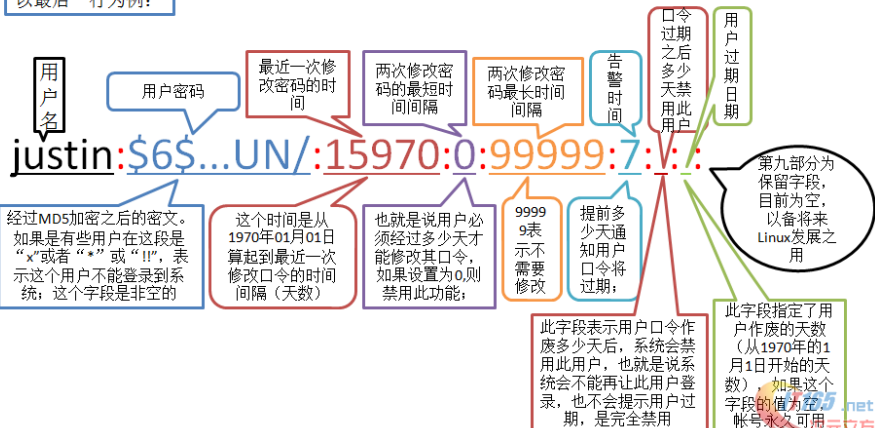


```
yucoat@Linux:~  
File Edit View Search Terminal Help  
1 root:$6$mwtX49qjpQNoQ4Wl$g07/Y3hlQo3WaYhrLHd.  
aQVCkyS45MLJVFJRzX2hBDOMcfEtJei2elsBL3icnXlbn  
lpQBLrV5ETmcwijy0k0p0:15141:0:99999:7:::  
2 bin:!:14789:0:99999:7:::  
3 daemon:!:14789:0:99999:7:::  
4 adm:!:14789:0:99999:7:::  
5 lp:!:14789:0:99999:7:::  
6 sync:!:14789:0:99999:7:::  
7 shutdown:!:14789:0:99999:7:::  
8 halt:!:14789:0:99999:7:::  
9 mail:!:14789:0:99999:7:::  
10 uucp:!:14789:0:99999:7:::  
11 operator:!:14789:0:99999:7:::  
12 games:!:14789:0:99999:7:::  
13 gopher:!:14789:0:99999:7:::  
14 ftp:!:14789:0:99999:7:::  
1,83 Top
```



# 用户和组 | 配置文件 | /etc/shadow | 9 个字段

以最后一行为例：



## 用户和组 | 配置文件 | /etc/shadow | 9 个字段

字段	含义	说明
1	用户名	与/etc/passwd 文件中的第一个字段相对应
2	密码	加密后的密码
3	最后一次修改密码的时间	上一次修改密码的日期与 1970-01-01 相距的天数
4	两次修改密码的最短时间间隔	0 表示禁用，随时可以修改密码
5	两次修改密码的最长时间间隔	99999 表示不需要修改密码
6	告警时间	修改期限前 N 天通知用户密码将过期
7	宽限时间	宽限期一过，账号将被完全禁用
8	账号失效日期	从 1970-01-01 开始；为空时表示账号永久可用
9	保留字段	以备将来使用

## ❶ 奇奇怪怪的字符串：加密过的密码文件

- 以\$1\$ 起始：MD5 加密
- 以\$2a\$ 起始：Blowfish 加密
- 以\$2y\$ 起始：Blowfish (correct handling of 8-bit chars) 加密
- 以\$5\$ 起始：SHA-256 加密
- 以\$6\$ 起始：SHA-512 加密

## ❷ 星号\*, 叹号!, 两个叹号!!：帐号被锁定

- 星号\*, 或\*LK\*：帐号被锁定
- 一个叹号!, 后跟加密的密码：有密码但被锁定，便于日后解锁
- 两个叹号!!：未设置密码且被锁定；密码已经过期

## ❸ 字段为空：没有密码



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



```
swashata@iTgProbook: ~  
swashata@iTgProbook:~$ cat /etc/group  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:swashata  
tty:x:5:  
disk:x:6:  
fax:x:21:  
voice:x:22:  
cdrom:x:24:swashata  
floppy:x:25:  
tape:x:26:  
sudo:x:27:swashata,testuser  
audio:x:29:pulse  
dip:x:30:swashata
```





# 用户和组 | 配置文件 | /etc/group | 4 个字段



字段	含义	说明
1	组名	用户通过它来识别组
2	组密码	空：没有组密码；x：密码位，密码放在/etc/gshadow中
3	GID	Group ID，标识系统中的组
4	组成员	属于组的账户列表，账户之间用逗号隔开

# 用户和组 | 配置文件 | /etc/group | 4 个字段



字段	含义	说明
1	组名	用户通过它来识别组
2	组密码	空：没有组密码；x：密码位，密码放在/etc/gshadow中
3	GID	Group ID，标识系统中的组
4	组成员	属于组的账户列表，账户之间用逗号隔开

## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



```
[root@s180 etc]# cat gshadow
root:::root
bin:::root,bin,daemon
daemon:::root,bin,daemon
sys:::root,bin,adm
adm:::root,adm,daemon
tty::
disk:::root
lp:::daemon,lp
mem:::
```



# 用户和组 | 配置文件 | /etc/gshadow | 4 个字段



字段	含义	说明
1	组名	用户通过它来识别组
2	组密码	可以是空或! (表示没有密码)
3	组管理员	可以为空; 多个组管理员用逗号隔开
4	组成员	多个组成员用逗号隔开

# 用户和组 | 配置文件 | /etc/gshadow | 4 个字段



字段	含义	说明
1	组名	用户通过它来识别组
2	组密码	可以是空或! (表示没有密码)
3	组管理员	可以为空; 多个组管理员用逗号隔开
4	组成员	多个组成员用逗号隔开

## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

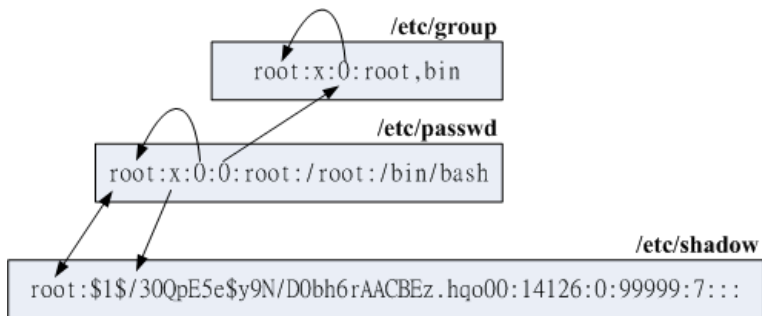
- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题







## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

## • 命令管理

## • 账户管理

## • 组管理

## • 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

## • 总结

## • 思考题



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



- 1 修改/etc/passwd：添加或删除账户行
- 2 修改/etc/shadow：添加或删除账户行
- 3 修改/etc/group：添加或删除账户引用
- 4 添加或删除账户的家目录



- 1 分别在/etc/passwd、/etc/group 和/etc/shadow 文件中添加一笔记  
录
- 2 创建用户家目录
- 3 在用户家目录中设置默认的配置文件
- 4 设置用户初始密码



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## ● 手动管理

## ● 命令管理

## ● 账户管理

## ● 组管理

## ● 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



命令	说明	助记
<b>useradd</b>	向系统中添加账户	Create a new user or update default new user information
usermod	修改账户属性	Modify a user account
userdel	从系统中删除账户	Delete a user account and related files
groupadd	向系统中添加组	Create a new group
groupmod	修改组的属性	Modify a group
groupdel	从系统中删除组	Delete a group



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## ● 手动管理

## ● 命令管理

## ● 账户管理

## ● 组管理

## ● 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



选项	助记	说明	文件及字段
-c	Comment	注释信息	/etc/passwd, 5
-d	Directory	账户的家目录	/etc/passwd, 6
-e	Expire	账号终止日期 (YYYY-MM-DD)	/etc/shadow, 8
-f	—	帐号过期几日后永久停用	/etc/shadow, 7
-g	Gid	初始默认组	/etc/passwd, 4
-G	Groups	附属次要组	/etc/group, 4
-m	—	家目录不存在时自动创建	—
-M	—	强制不创建家目录	—
-s	Shell	默认 shell	/etc/passwd, 7
-u	Uid	指定用户 UID	/etc/passwd, 3

```
1 useradd -c COMMENT -d HOME.DIRECTORY -e
  EXPIRATION.DATE -f INACTIVE.DTAE -g PRIMARY
  .GROUP -G SECONDARY.GROUPS -m -s SHELL -u
  UID ACCOUNTNAME
```





选项	助记	说明	文件及字段
-c	Comment	注释信息	/etc/passwd, 5
-d	Directory	账户的家目录	/etc/passwd, 6
-e	Expire	账号终止日期 (YYYY-MM-DD)	/etc/shadow, 8
-f	—	帐号过期几日后永久停用	/etc/shadow, 7
-g	Gid	初始默认组	/etc/passwd, 4
-G	Groups	附属次要组	/etc/group, 4
-m	—	家目录不存在时自动创建	—
-M	—	强制不创建家目录	—
-s	Shell	默认 shell	/etc/passwd, 7
-u	Uid	指定用户 UID	/etc/passwd, 3

```
1 useradd -c COMMENT -d HOME.DIRECTORY -e
  EXPIRATION.DATE -f INACTIVE.DTAE -g PRIMARY
  .GROUP -G SECONDARY.GROUPS -m -s SHELL -u
  UID ACCOUNTNAME
```



## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer



## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer

```
useradd -d /home/unixnewbie -m unixnewbie
```



## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer

```
useradd -d /home/unixnewbie -g users -m unixnewbie
```



## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer

```
useradd -d /home/unixnewbie -g users -s /bin/sh -m  
unixnewbie
```

## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer

```
useradd -c "Jane Doe" -d /home/unixnewbie -g users -s /bin/sh -m unixnewbie
```

## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer

```
useradd -c "Jane Doe" -d /home/unixnewbie -g users -G  
authors -s /bin/sh -m unixnewbie
```



## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer

```
useradd -c "Jane Doe" -d /home/unixnewbie -e 2006-07-06  
-g users -G authors -s /bin/sh -m unixnewbie
```



## Question

- 账户名：unixnewbie
- 首要组：users
- 默认 shell：Bourne shell
- 真实姓名：Jane Doe
- 次要组：authors
- 有效期：2006 年 7 月 6 日
- 不活动天数：60 天

## Answer

```
useradd -c "Jane Doe" -d /home/unixnewbie -e 2006-07-06  
-f 60 -g users -G authors -s /bin/sh -m unixnewbie
```

## 添加账户

创建账户：`useradd USERNAME`

创建密码：`passwd USERNAME`

## 修改账户

修改账户名：`usermod -l (小写 L) NAME.NEW NAME.OLD`

添加到组：`usermod -G GROUP2 USER`

修改账户属性：`usermod -l NAME.NEW -d DIR -g GROUP NAME.OLD`

## 删除账户

删除账户：`userdel USERNAME`

彻底删除账户：`userdel -r USERNAME`

## 添加账户

创建账户：`useradd USERNAME`

创建密码：`passwd USERNAME`

## 修改账户

修改账户名：`usermod -l (小写 L) NAME.NEW NAME.OLD`

添加到组：`usermod -G GROUP2 USER`

修改账户属性：`usermod -l NAME.NEW -d DIR -g GROUP NAME.OLD`

## 删除账户

删除账户：`userdel USERNAME`

彻底删除账户：`userdel -r USERNAME`

## 添加账户

创建账户：`useradd USERNAME`

创建密码：`passwd USERNAME`

## 修改账户

修改账户名：`usermod -l (小写 L) NAME.NEW NAME.OLD`

添加到组：`usermod -G GROUP2 USER`

修改账户属性：`usermod -l NAME.NEW -d DIR -g GROUP NAME.OLD`

## 删除账户

删除账户：`userdel USERNAME`

彻底删除账户：`userdel -r USERNAME`

## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## ● 手动管理

## ● 命令管理

## ● 账户管理

## ● 组管理

## ● 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## 添加组

创建组：`groupadd -g GID GROUPNAME`

## 修改组

修改组名：`groupmod -n GROUPNAME.N GROUPNAME.O`

修改 GID：`groupmod -g GID GROUPNAME`

## 删除组

删除组：`groupdel GROUPNAME`



## 添加组

创建组：groupadd -g GID GROUPNAME

## 修改组

修改组名：groupmod -n GROUPNAME.N GROUPNAME.O

修改 GID：groupmod -g GID GROUPNAME

## 删除组

删除组：groupdel GROUPNAME



## 添加组

创建组：groupadd -g GID GROUPNAME

## 修改组

修改组名：groupmod -n GROUPNAME.N GROUPNAME.O

修改 GID：groupmod -g GID GROUPNAME

## 删除组

删除组：groupdel GROUPNAME





## gpasswd

### 设置组密码及管理组内成员

选项	作用
-a	添加用户到用户组
-A	设置用户组管理员
-d	从用户组中删除用户
-M	设置组成员列表
-r	删除用户组密码
-R	禁止用户切换为该组



## gpasswd

### 设置组密码及管理组内成员

选项	作用
-a	添加用户到用户组
-A	设置用户组管理员
-d	从用户组中删除用户
-M	设置组成员列表
-r	删除用户组密码
-R	禁止用户切换为该组



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

## • 命令管理

## • 账户管理

## • 组管理

## • 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## 需求

授权用户 jack 和 mary 对目录/software 有写权限。

## 命令

- 1 创建新组：groupadd softadm
- 2 把用户加入组：usermod -G softadm jack ; gpasswd -a mary softadm
- 3 修改目录所属组：chgrp softadm /software
- 4 修改目录权限：chmod g+w /software



## 需求

授权用户 jack 和 mary 对目录/software 有写权限。

## 命令

- ❶ 创建新组：`groupadd softadm`
- ❷ 把用户加入组：`usermod -G softadm jack ; gpasswd -a mary softadm`
- ❸ 修改目录所属组：`chgrp softadm /software`
- ❹ 修改目录权限：`chmod g+w /software`



## 禁用

- `usermod -L USERNAME`
- `passwd -l (小写 L) USERNAME`

## 恢复

- `usermod -U USERNAME`
- `passwd -u USERNAME`

## 删除

- 删除用户家目录中的文件：`userdel -r USERNAME`



## 禁用

- `usermod -L USERNAME`
- `passwd -l (小写 L) USERNAME`

## 恢复

- `usermod -U USERNAME`
- `passwd -u USERNAME`

## 删除

- 删除用户家目录中的文件：`userdel -r USERNAME`



## 禁用

- `usermod -L USERNAME`
- `passwd -l (小写 L) USERNAME`

## 恢复

- `usermod -U USERNAME`
- `passwd -u USERNAME`

## 删除

- 删除用户家目录中的文件：`userdel -r USERNAME`





## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



命令	说明
<b>su</b>	Switch User
su USERNAME	使用 USERNAME 账户登录
su - USERNAME	使用 USERNAME 的用户环境登录
su	登录到根账户



## 密码

- 八位以上，大小写字母、数字、符号组合使用
- 容易记忆
- 定期更换
- 示例：Am@ri31n

## 提示符

- 普通用户为\$
- 超级用户 root 为#



## 密码

- 八位以上，大小写字母、数字、符号组合使用
- 容易记忆
- 定期更换
- 示例：Am@ri31n

## 提示符

- 普通用户为\$
- 超级用户 root 为#



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## sudo (superuser do)

- 在执行 sudo 命令时，临时成为 root。sudo 执行命令的流程是当前用户切换到 root，然后以 root 身份执行命令，执行完成后，直接退回到当前用户。
- 不会泄漏 root 口令。使用 sudo 时，输入的是当前用户的密码。
- 仅向用户提供有限的命令使用权限。通过 sudo，能把某些超级权限有针对性的下放，并且不需要普通用户知道 root 密码。

## sudo 的用法

sudo COMMAND



## sudo (superuser do)

- 在执行 sudo 命令时，临时成为 root。sudo 执行命令的流程是当前用户切换到 root，然后以 root 身份执行命令，执行完成后，直接退回到当前用户。
- 不会泄漏 root 口令。使用 sudo 时，输入的是当前用户的密码。
- 仅向用户提供有限的命令使用权限。通过 sudo，能把某些超级权限有针对性的下放，并且不需要普通用户知道 root 密码。

## sudo 的用法

sudo COMMAND





## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

- 手动管理
- 命令管理
- 账户管理
- 组管理
- 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- **su vs. sudo**

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## su 的缺点

- 不安全：su 只适用于一两个人参与管理的系统，毕竟 su 并不能让普通用户受限的使用；超级用户 root 密码应该掌握在少数用户手中
- 麻烦：需要把 root 密码告知每个需要 root 权限的人

## sudo 的特性

- sudo：受限制的 su，授权许可的 su
- sudo 能够限制用户只在某台主机上运行某些命令
- sudo 提供了丰富的日志，详细地记录了每个用户干了什么
- sudo 使用时间戳文件来执行类似的“检票”系统。当用户调用 sudo 并且输入它的密码时，用户获得了一张存活期为 5 分钟的票
- sudo 的配置文件是 sudoers 文件 (/etc/sudoers, 属性为 0411, 编辑配置文件命令 visudo)，它允许系统管理员集中的管理用户的使用权限和使用的主机

## su 的缺点

- 不安全：su 只适用于一两个人参与管理的系统，毕竟 su 并不能让普通用户受限的使用；超级用户 root 密码应该掌握在少数用户手中
- 麻烦：需要把 root 密码告知每个需要 root 权限的人

## sudo 的特性

- sudo：受限制的 su，授权许可的 su
- sudo 能够限制用户只在某台主机上运行某些命令
- sudo 提供了丰富的日志，详细地记录了每个用户干了什么
- sudo 使用时间戳文件来执行类似的“检票”系统。当用户调用 sudo 并且输入它的密码时，用户获得了一张存活期为 5 分钟的票
- sudo 的配置文件是 sudoers 文件 (/etc/sudoers, 属性为 0411, 编辑配置文件命令 visudo)，它允许系统管理员集中的管理用户的使用权限和使用的主机

# 用户和组 | 身份变换 | su vs. sudo

su	sudo
When elevating privilege, you need to enter the <b>root</b> password. Giving the root password to a normal user should <b>never, ever</b> be done.	When elevating privilege, you need to enter the user's password and not the <b>root</b> password.
Once a user elevates to the <b>root</b> account using <b>su</b> , the user can do <b>anything</b> that the <b>root</b> user can do for as long as the user wants, without being asked again for a password.	Offers more features and is considered more secure and more configurable. Exactly what the user is allowed to do can be precisely controlled and limited. By default the user will either always have to keep giving their password to do further operations with <b>sudo</b> , or can avoid doing so for a configurable time interval.
The command has limited logging features.	The command has detailed logging features.



命令	说明
su	切换到 root 用户
su -	完全切换到 root 用户（环境变量，家目录都会切换过去）
sudo	普通用户执行只有管理员才能运行的命令（环境还是普通账户的）



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

## • 命令管理

## • 账户管理

## • 组管理

## • 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



命令	说明
who	列出当前在线的用户
w	显示登录的用户（进程信息）
whoami	当前作为什么用户登录
who am i	最初作为什么用户登录
id	显示登录的用户以及用户的组的相关信息
groups	显示用户所属的组
finger	显示用户的相关详细信息
last	显示用户最近登录信息
passwd -S	查看用户密码状态



命令	说明
newgrp	切换用户组
chgrp	修改文件所属组
chage	更改用户密码过期信息
pwck	检测/etc/passwd 文件（锁定文件）
grpck	用户组配置文件检测
vipw	编辑/etc/passwd 文件
vigr	编辑/etc/group 文件（锁定文件）





## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

## • 命令管理

## • 账户管理

## • 组管理

## • 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

- 总结
- 思考题



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

## • 命令管理

## • 账户管理

## • 组管理

## • 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

## • 总结

## • 思考题



## 知识点

- Linux 系统中的三类账户
- 用户和组的配置文件
- 管理账户和组的常用命令
- 变换用户身份的方法
- 用户和组管理的辅助命令

## 技能

- 管理用户（创建、修改、删除）
- 管理组（创建、修改、删除）



## 1 引言

## 2 账户

- 三类账户
- 组账户

## 3 用户管理文件

- 配置文件
- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- 配置文件的关系

## 4 管理账户和组

## • 手动管理

## • 命令管理

## • 账户管理

## • 组管理

## • 实例和补充

## 5 身份变换

- 万能的 su
- 安全的 sudo
- su vs. sudo

## 6 辅助命令

## 7 回顾与总结

## • 总结

## • 思考题



- 1 Linux 系统中主要有哪三种类型的账户？
- 2 用户和组管理相关的文件主要有哪些？
- 3 解释/etc/passwd 中各个字段的含义。
- 4 根据要求，使用 useradd 创建一个新账户。
- 5 改变用户身份的方法有哪些？
- 6 列举几个用户和组管理的辅助命令。



# 下节预告

- 安装 Windows 系统时的分区过程
- Windows 系统的目录结构、路径写法
- 日常使用中基本的目录和文件操作
- Windows 系统中的快捷方式





TEX

LATEX

X<sub>Y</sub>TEX

Beamer

