GNU/Linux
用户与组管理

Linux 用户与组管理

1. Linux 继承 UNIX 对用户的优秀支持

2. Linux 属于多用户的操作系统

3. 用户管理的种类
   1) 分散式管理方法

   2) 集中式管理方法

Linux 用户与组管理

Linux 用户类型

1. 按建立方式计算
   (1) 内建账户 : 有系统或程序自行建立的账户

   (2) 自定义账户 : 管理员或特权人员手工建立

Linux 用户与组管理

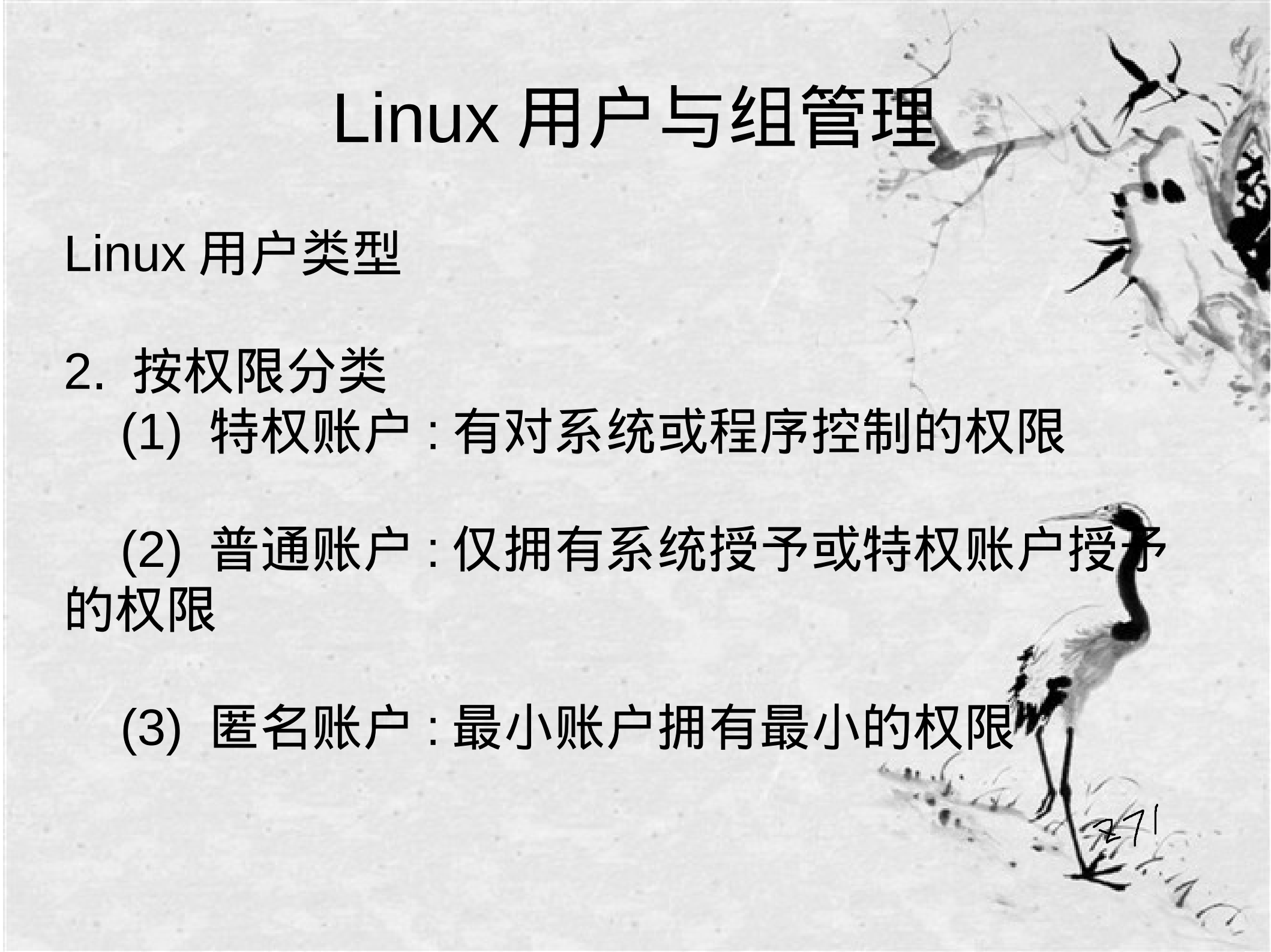
Linux 用户类型

2. 按权限分类

(1) 特权账户 : 有对系统或程序控制的权限

(2) 普通账户 : 仅拥有系统授予或特权账户授予的权限

(3) 匿名账户 : 最小账户拥有最小的权限



Linux 用户与组管理

Linux 用户基本管理方式

1. 对账户进行管理

2. 将权限相同的用户合并至组中，对组进行管理

Linux 用户管理

Linux 用户管理文件

Linux 将用户的信息及密码全部通过文件的方式进行保存 .

用户信息保存文件及位置 :/etc/passwd

用户密码保存文件及位置 :/etc/shadow

Linux 用户管理 -passwd

查看 /etc/passwd

#less /etc/passwd

1. /etc/passwd 内容总共分为 7 个区域

2. 以“ :” 作为区域的分隔符

Linux 用户管理 -passwd

区域 1

账户名 :

1) 区分大小写
2) 账户名可以以字母 , 数字 , 英文句号 '.', 下划线 '_', 连字符 '-' 等连和使用
3) 账户命名最好在 8 个字符之内
4) 账户名必须唯一

Linux 用户管理 -passwd

区域 2

密码区域 :

1) Linux 利用单项散列算法加密密码
2) Linux 将密码存放至 /etc/shadow 文件中
3) 账户的密码再此区域中显示“ X”

Linux 用户管理 -passwd

区域 3

账户 ID(UID):

1) 显示账户的ＵＩＤ号

2) 理论上 UID 号应该唯一

3)UID 号 0-999 为保留 UID

4) 普通账户的ＵＩＤ从 1000-60000

Linux 用户管理 -passwd

区域 4
用户在初始化组的组ＩＤ号 (GID):
1) 显示账户初始化组的ＧＩＤ号

区域 5
账户详细信息 , 其中包含
1) 账户的用户名
2) 办公地点
3) 办公电话
4) 家庭电话

Linux 用户管理 -passwd

区域 6

账户主目录位置

1) 主目录即用户存储私人数据的地方
2) 普通账户主目录默认建立在 /home 下
3) 以账户名作为用户主目录名
4) 默认只有账户才可以进入自己的主目录
5)root 账户主目录在 /root

Linux 用户管理 -passwd

区域 7
账户使用的 shell
1) 指定账户所使用的 shell 及 shell 所在的路径

Linux 用户管理 -shadow

用户的密码被 /etc/shadow 文件所管理，其有 9 个区域，每个区域的作用如下：

区域 1：

账户名 (与 /etc/passwd 一致)

区域 2:

密码

此密码经过散列算法经过加密 ,256bit。如密码忘记，可将此区域情况。即代表密码为空

Linux 用户管理 -shadow

区域 3:

密码自新纪元 (1970-1-1) 起到用户前一次修改密码的天数

区域 4:

密码前次与下一次修改的时间间隔，一般为“0”位不设定，可随时修改

Linux 用户管理 -shadow

区域 5:

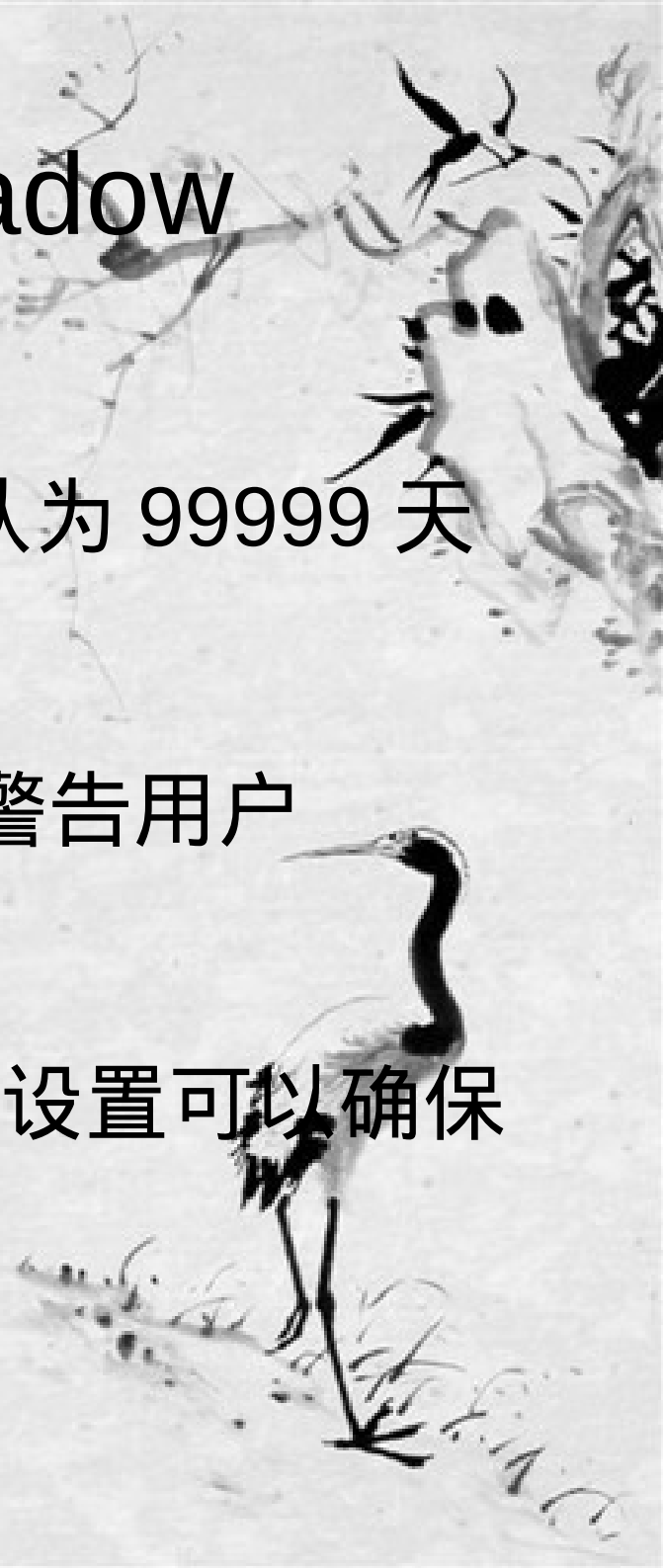
密码最大有效其时间 (天), 默认为 99999 天

区域 6:

密码失效前 , 提前 N(天) 通知警告用户

区域 7:

密码失效后 , 宽限期天数 . 此段设置可以确保密码失效后延长 N 天在将密码失效



Linux 用户管理 -shadow

区域 8:

账号有效期

区域 9:

保留

Linux 用户管理命令 -useradd

命令 :useradd | adduser

功能 : 添加账户

语法格式 :

useradd [选项] <account_name>

Linux 用户管理命令 -useradd

选项

-c: 指定账户的说明信息 (passwd 区域 5)

-d: 指定账户的主目录 (passwd 区域 6)

-e: 指定账号有效期 (shadow 区域 8)

-f: 密码失效宽限期 (shadow 区域 7)

-b: 指定用户主目录的前缀

Linux 用户管理命令 -useradd

选项

-g: 指定账户初始化 (起始) 组 (passwd 区域 4)

-G: 指定账户的其他组资格

-m: 自动复制 shell 环境脚本至新建的用户主目录

-M: 不创建用户主目录

-s: 指定新建账户所使用的 shell(passwd 区域 7)

Linux 用户管理命令 -useradd

选项

-u: 指定新建账户的 UID

-n: 创建与账户同名的组名，并将此组作为账户的初始化组

Linux 用户管理命令 -useradd

示例

1. 添加一个账号员，要求
    1) 账户名为 thomas
    2) 初始组为 root
    3) 账户主目录为 /admin
    4) 密码宽限期为 7 天
    5) 账号有效使用时间为从即日起 3 0 天
    6) 复制 shell 环境脚本
    7)uid 为 614
    8) 所使用的 shell 为 bash

Linux 用户管理命令 -useradd

示例

1. 添加一个临时管理员，要求

#useradd -g root -d /admin -m -e 2222-11-31 -f 7 -s /bin/bash -u 614 thomas

Linux 用户管理命令 -useradd

用户添加涉及的脚本

1. 添加的默认配置文件

   #vim /etc/default/uesradd

   内容

   默认账户加入至 GID100

   GROUP=100

   账户默认主目录前缀为 /home

   HOME=/home

Linux 用户管理命令 -useradd

禁用账号过期功能 (-1)
INACTIVE=-1

账号到期时间 , 不设置即不启用
EXPIRE=

指定用户默认所使用的 shell
SHELL=/bin/bash

Linux 用户管理命令 -useradd

指定用户所使用的 SHELL 环境文件
SKEL=/etc/skel

创建账户名同名的文件作为账户的邮箱
CREATE_MAIL_SPOOL=yes

备注 :

系统邮箱位置在 /var/spool/mail 目录中

Linux 用户管理命令 -login.defs

用户创建限制文件 --/etc/login.defs, 其内容为 :

指定系统账户的邮箱所在位置
MAIL_DIR　/var/spool/mail

密码最大有效期
PASS_MAX_DAYS 9999

两次密码修改最小间隔
PASS_MIN_DAYS 0

Linux 用户管理命令 -login.defs

密码最小长度
PASS_MIN_LEN 5

密码失效前天前 N 天提示用户
PASS_WARN_AGE 7

本地自定义账户最小 UID
UID_MIN   1000

本地自定义账户最大 UID
UID_MAX 60000

Linux 用户管理命令 -login.defs

本地系统账户最小 UID
SYS_UID_MIN　201

本地系统账户最大 UID
SYS_UID_MAX　999

本地自定义组最小 GID
GID_MIN　1000

本地自定义组最大 GID
GID_MAX　60000

Linux 用户管理命令 -login.defs

本地系统组最小 GID
SYS_GID_MIN　201

本地系统组最大 GID
SYS_GID_MAX　999

默认创建用户主目录
CREATE_HOME　yes

用户主目录 umask 码
UMASK　077

Linux 用户管理命令 -login.defs

当用户删除后同名组没有成员时，同时删除此组 .
USERGROUPS_ENAB　　yes

用 SHA512 算法加密密码
ENCRYPT_METHOD　　SHA512

* 用户 shell 环境使用设置位于 /etc/skel 目录

Linux 用户管理命令 -passwd

命令 :passwd

功能 : 为账户设定 / 更改密码及其他

语法格式 :

passwd [选项] [账户名]

Linux 用户管理命令 -passwd

选项 :

-l: 锁定指定账户

--stdin: 从标准输入中读取密码

-u: 解锁指定账户

-d: 清空指定账户口令

Linux 用户管理命令 -passwd

选项 :

-i: 设置密码宽限期 (shadow 区域 7)

-n: 设置 2 次密码修改间隔时间 (shadow 区域 4)

-x: 设置密码有效期 (shadow 区域 5)

-w: 设置密码过期前警告天数 (shadow 区域 6)

Linux 用户管理命令 -passwd

RHEL7 对密码加密

RHEL7 对密码加密支持 :

md5:128bit 长度加密密码

sha256:256bit 长度加密密码

sha512:512bit 长度加密密码

RHEL7 默认使用 sha512 作为密码加密的算法

可以使用以下命令来替换不同算法加密密码 :

#authconfig --passalgo=sha512 --update

Linux 用户管理命令 -passwd

示例：

1. 通过标准输入更改指定账户密码

   #passwd --stdin thomas

   或

   #echo “test” | passwd --stdin thomas

Linux 用户管理命令 -passwd

示例 :

2. 对 thomas 账户进行密码设定 . 要求

   1) 密码有效期 7 天

   2) 提前 3 天给予警告

   3) 2 次密码修改间隔时间为 2 天

   #passwd -x 7 -w 3 -n 2 thomas

Linux 用户管理命令 -passwd

示例 :

3. 使用管理员改变其他账户密码

   #passwd thomas

4. 账户改变自己的密码

   $passwd

备 : 普通账户无法改变别人的密码

Linux 用户管理命令 -chage

命令 :chage

功能 : 更改账户密码过期信息

语法格式 :

chage [选项] [账户名]

Linux 用户管理命令 -chage

选项：

-m 密码可更改的最小天数。为零时代表任何时候都可以更改密码。

-M 密码保持有效的最大天数。

-W 用户密码到期前，提前收到警告信息的天数

-E 帐号到期的日期。过了这天，此帐号将不可用。

Linux 用户管理命令 -chage

选项：
-d 上一次密码更改的日期

-i 停滞时期。如果一个密码已过期这些天，那么此帐号将不可用。

-l,--list 例出当前的设置。由非特权用户来确定他们的密码或帐号何时过期。

Linux 用户管理命令 -chage

示例 :

1. 查看 snow 账户密码设定情况
   #chage -l snow

2. 设置账户 snow 密码有效期 90 天
   #chage -M 90 snow

3. 设置 snow 账户登陆时强制修改口令
   #chage -d 0 snow

Linux 用户管理命令 -chage

示例：

4. 强制 snow 账户登陆时修改口令，且密码可随时更改，但密码最大有效期为 90 天，提前 15 天发送警报消息

```
#chage -d 0 -m 0 -M 90 -W 15 snow
```

5. 设置账号 snow 的有效期至 2100-10-10

```
#chage -E  2100-10-10  snow
```

6. 对账户 snow 的密码更改日期进行设定

```
#chage -d  2009-10-10 snow
```

Linux 用户管理命令 -usermod

命令 :usermod

功能 : 修改已存在的账户

语法格式 :usermod [选项] < 账户名 >

选项 :

与 useradd 命令的大多选项一致

Linux 用户管理命令 -usermod

选项：

-l: 更改账户名

-L: 锁定指定账户

-U: 解锁指定账户

-a: 添加账户到指定组

-d: 指定新的用户主目录

Linux 用户管理命令 -usermod

选项 :
-m: 移动用户主目录到新的位置 , 需和 -d 配合使用

-s: 更改账户 shell

其他选项与 useradd 选项含义一致 , 但功能仅作为修改而非添加

Linux 用户管理命令 -usermod

示例 :

1. 将 thomas 账户名改为 snow
   #usermod -l snow thomas

2. 将 snow 账户锁定
   #usermod -L snow

3. 解锁 snow 账户
   #usermod -U snow

4. 将账户 snow 添加至 wheel 组
   #usermod -aG whell snow

Linux 用户管理命令 -usermod

示例：

4. 将账户 snow 添加至 wheel 组

```
#usermod  -aG  whell snow
```

5. 禁止用户登陆

```
#usermod  -s  /sbin/nologin  student
```

Linux 用户管理命令 -chfn

命令 :chfn

功能 : 修改用户信息 (passwd 区域 5)

语法格式 :chfn [选项] [账户]

示例 :

1. 修改 snow 账户信息

   #chfn snow

Linux 用户管理命令 -chsh

命令 :chsh

功能 : 修改用户信息 (passwd 区域 7)

语法格式 :chsh [选项] [账户]

示例 :

1. 修改 snow 账户的 shell

   #chsh snow

Linux 用户管理命令 -userdel

命令 :userdel

功能 : 删除用户

语法格式 :userdel [选项] [账户]

选项 :
-r: 删除与指定账户相关的主目录及其他信息

Linux 用户管理命令 -id

命令 :id

功能 : 查看当前用户的 UID,GID 及账户、组名

语法格式 :id [选项] [账户]

Linux 用户管理命令 -id

选项 :
-u: 显示账户的 UID
-g: 显示初始组的 GID
-G: 显示附加组的 GID

-un: 显示账户名
-gn: 显示初始组组名
-Gn: 显示附加组组名

Linux 用户管理命令 -w

命令 :w

功能 : 查看当前系统的登陆账户

语法格式 :w [选项] [账户]

Linux 用户管理命令 -w

选项：
-: 只显示头信息

-f: 开启 / 关闭用户从何处登陆至系统的信息

-h: 不显示标题栏

-s: 使用简洁格式显示信息

-u: 忽略执行程序的名称，以及该程序耗费 CPU 时间的信息。

Linux 用户管理命令 -w

示例 :

1. 显示当前系统登陆的账户

   #w

输出结果

第 1 行

当前时间

uptime 时间

总计账户数

系统负载 :1 分钟 ,5 分钟 ,15 分钟

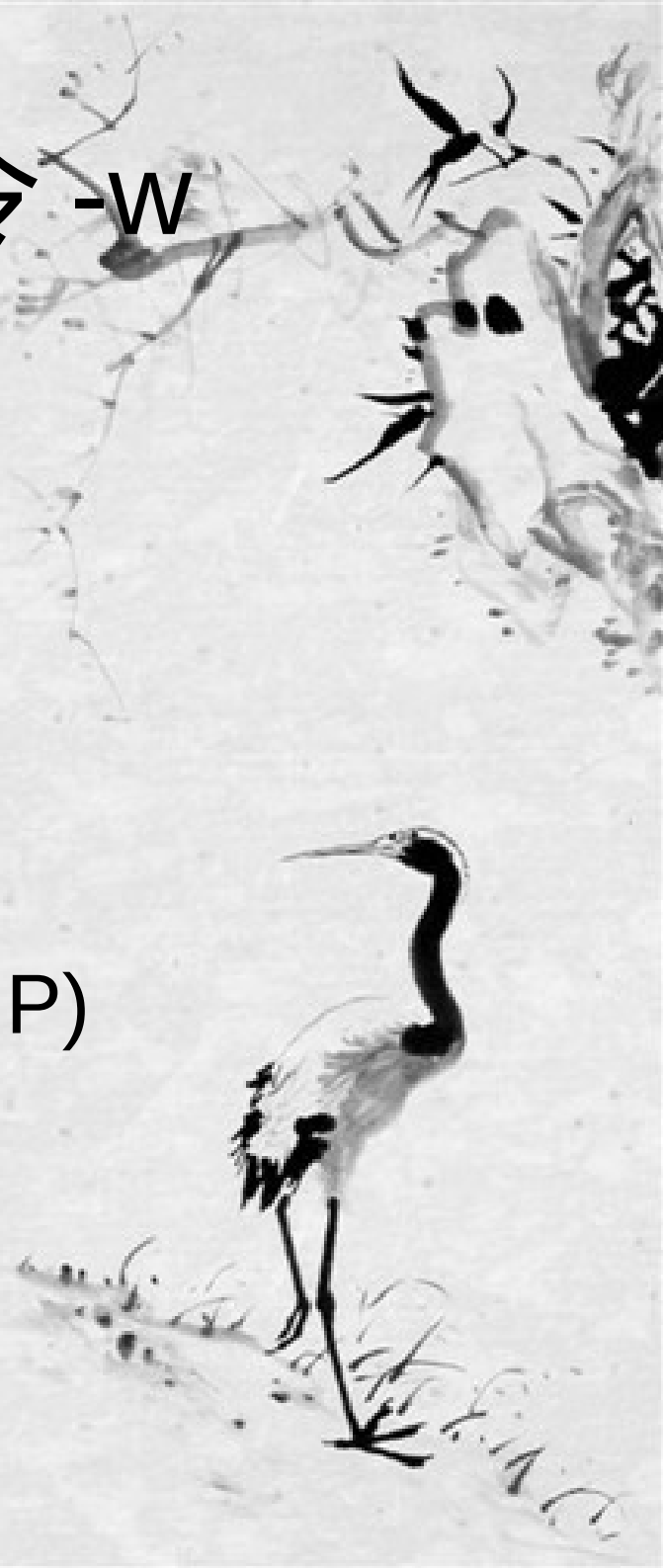
Linux 用户管理命令 -w

示例 :
第 2 行
USER: 账户名

TTY: 此账户所登陆的终端

FROM: 从本地还是远程 (显示远程 IP)

LOGIN@: 登陆时间



Linux 用户管理命令 -w

示例 :
第 2 行
IDEL: 账户不活动时间 (闲置时间)

JCPU: 所登陆在对应的 TTY 终端所有进程使用 CPU 的时间

PCPU: 在 WHAT 显示的进程的 CPU 时间

WHAT: 当前所指定的进程

Linux 用户管理命令 -who

命令 :who

功能 : 显示当前登陆账户及信息

语法格式 :who [选项] [目标]

示例 :

1. 查看当前所有登陆信息

   #who

Linux 用户管理命令 -whoami

命令 :whoami

功能： 显示账户

语法格式 :whoami [选项]

Linux 用户管理命令 -last

命令 :last

功能： 显示账户最后登陆时间

语法格式 :last [选项]

Linux 用户管理命令 -lastlog

命令 :lastlog

功能： 显示最近所有账户最后登陆时间

语法格式 :lastlog [选项]

Linux 组管理 -group

Linux 组的信息保存在 /etc/group, 其总共为四个区域 . 其信息如下 :

区域 1 :

组名

1) 组名必须唯一

2) 组名只可以包含小写字母和数字

Linux 组管理 -group

区域 2:

组密码

1) 组密码亦为散列算法加密

2) 组密码保存在 /etc/gshadow 文件中

3) 组密码在此文件中为“ x ”

Linux 组管理 -group

区域 3:

组 ID(GID)

1)GID 理论唯一

区域 4:

组成员

1) 组成员可账户组成

2) 多成员之间用“，”分割

3) 一个账户可以隶属多个组 , 但不可超过 16 个

4) 用户默认为初始化组 (passwd 中区域 4)

Linux 组管理 -gshadow

Linux 组密码存放再 /etc/gshadow 中，此文件总计有 4 个区域，其信息如下：

区域 1:
组名

区域 2:
组密码 (被散列算法加密的口令)

Linux 组管理 -gshadow

区域 3:

组管理员

可对所管理的组进行账户的添加 / 删除

区域 4:

组成员资格，多成员之间用“，”分割

Linux 组管理命令 -groupadd

命令 :groupadd

功能 : 创建组

语法格式 :groupadd [选项] < 组名 >

选项 :
-g: 指定新建组的 GID

Linux 组管理命令 -groupmod

命令 :groupmod

功能 : 修改现有组

语法格式 :groupmod [选项] < 组名 >

选项 :
-g: 更改指定组的 GID

-n: 更改指定组组名

Linux 组管理命令 -groupmod

示例：

1. 更改 thomas 组的 GID 为 888 及组名为 snow

   #groupmod -g 888 -n snow thomas

Linux 组管理命令 -groupdel

命令 :groupdel

功能 : 删除指定组

语法格式 :groupdel [选项] < 组名 >

Linux 组管理命令 -gpasswd

命令 :gpasswd

功能 : 设定指定组的组密码

语法格式 :gpasswd [选项] < 组名 >

Linux 组管理命令 -gpasswd

命令 :gpasswd

功能 : 设定指定组的组密码

语法格式 :gpasswd [选项] < 组名 >

选项 :
-A: 设定组管理员

-M: 设定组成员

Linux 组管理命令 -gpasswd

示例：

1. 将 lisa 设定为 thomas 组管理员，并添加 snow,arisa 两个账户作为 thomas 组成员

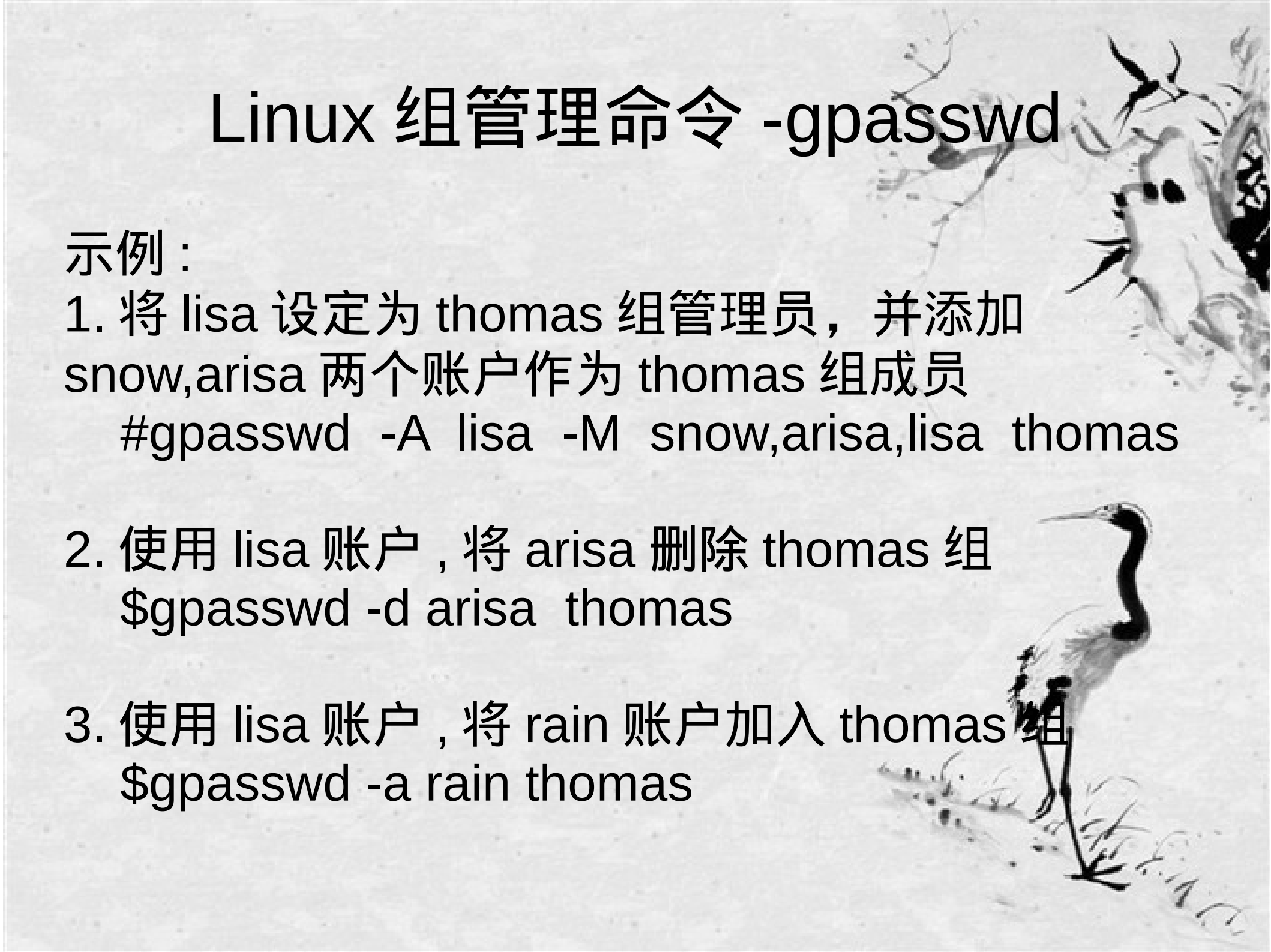
```
#gpasswd  -A  lisa  -M  snow,arisa,lisa  thomas
```

2. 使用 lisa 账户，将 arisa 删除 thomas 组

```
$gpasswd -d arisa  thomas
```

3. 使用 lisa 账户，将 rain 账户加入 thomas 组

```
$gpasswd -a rain thomas
```



Linux 组管理命令 -newgrp

命令 :newgrp

功能 : 切换组

语法结构 :newgrp 新组组名

Linux 组管理命令 -newgrp

示例 :

1. 将当前账户切换至附加组 users 组

   #newgrp users

2. 将当前账户切换至 lisa 组 (lisa 组不属于当前用户初始组、附加组)

   #newgrp lisa

   password:　　<- 输入 lisa 组的组密码

Linux 用户和组管理方法 - 文件管理

对于用户和组除了命令之外，亦可以通过对相应的管理文件的编辑可以完成

1. 对用户管理

   #vim /etc/passwd

   或

   #vipw

2. 对组管理

   #vim /etc/group

   或

   #vigp

Linux 用户和组管理方法

对于 Linux 下使用批量添加账户的方法可以按照以下步骤实现 :

步骤 1: 按照 /etc/passwd 格式创建一个模板文件 , 为 addusers.txt
内容如下 :

```
user01::601:2000:user:/home/user01:/bin/bash
user02::602:2000:user:/home/user02:/bin/bash
user03::603:2000:user:/home/user03:/bin/bash
user04::604:2000:user:/home/user04:/bin/bash
```

Linux 用户和组管理方法

对于 Linux 下使用批量添加账户的方法可以按照以下步骤实现 :

步骤 1: 按照 /etc/passwd 格式创建一个模板文件

注意：用户名、 UID 、 $HOME 都必须要唯一，密码段可以设置为小写的 x, 也可以空着。

Linux 用户和组管理方法

对于 Linux 下使用批量添加账户的方法可以按照以下步骤实现 :

步骤 2: 将内容导入至 /etc/passwd 中

#newusers < addusers.txt

用 less 等程序查看 /etc/passwd 中有无这些用户

Linux 用户和组管理方法

对于 Linux 下使用批量添加账户的方法可以按照以下步骤实现 :

步骤 3: 将 /etc/shadow 密码还原至 /etc/passwd

#pwunconv

Linux 用户和组管理方法

对于 Linux 下使用批量添加账户的方法可以按照以下步骤实现 :

步骤 4: 编写密码文件 . 其文件名为 newpasswd.txt

```
#vi  newpasswd.txt
user1:123456
user2:123456
user3:123456
user4:123456
```

Linux 用户和组管理方法

对于 Linux 下使用批量添加账户的方法可以按照以下步骤实现 :

步骤 5: 将 newpasswd.txt 内容导入之 /etc/passwd

#chpasswd < newpasswd.txt

步骤 6: 将密码写回至 /etc/shadow

#pwconv