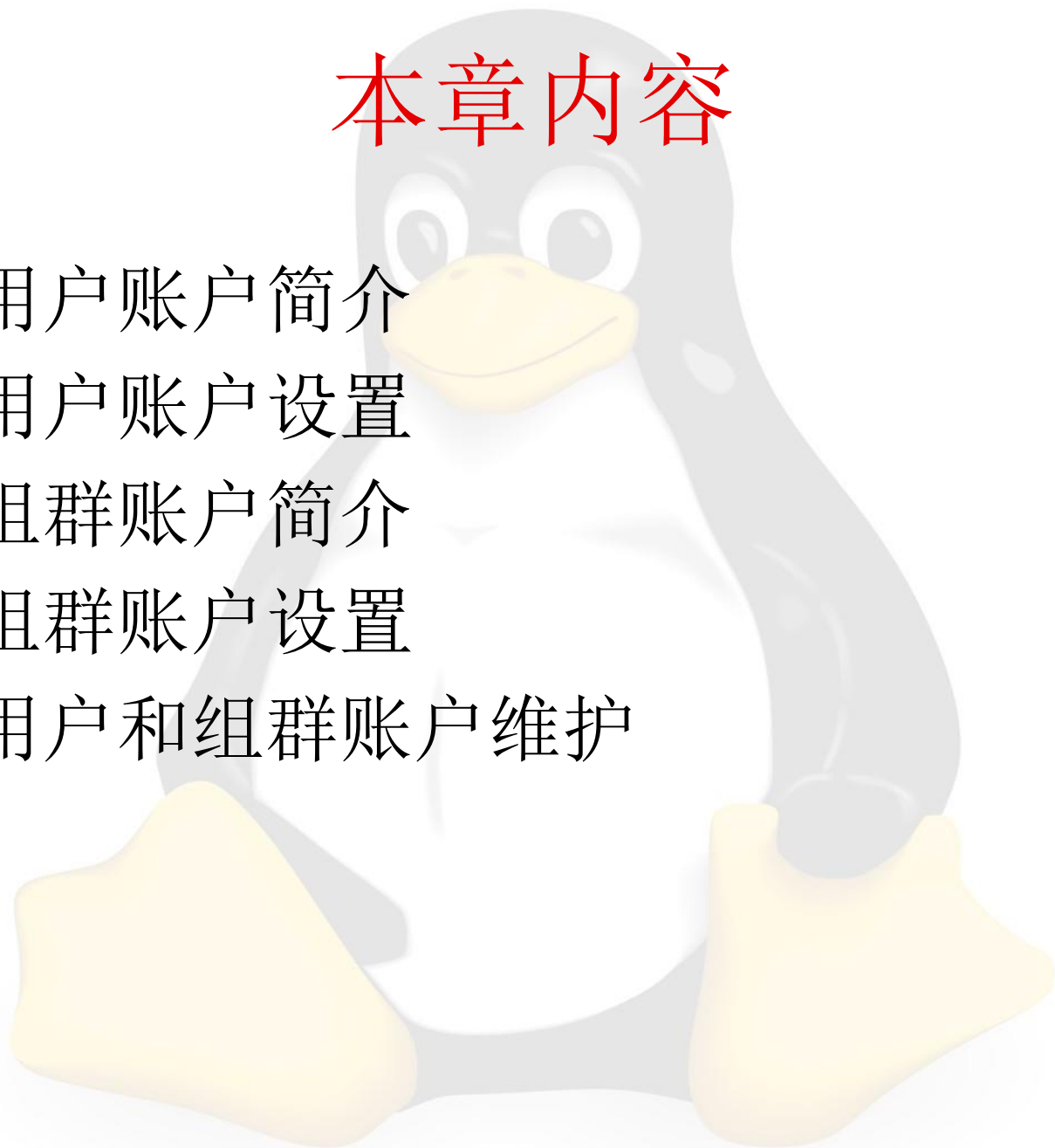


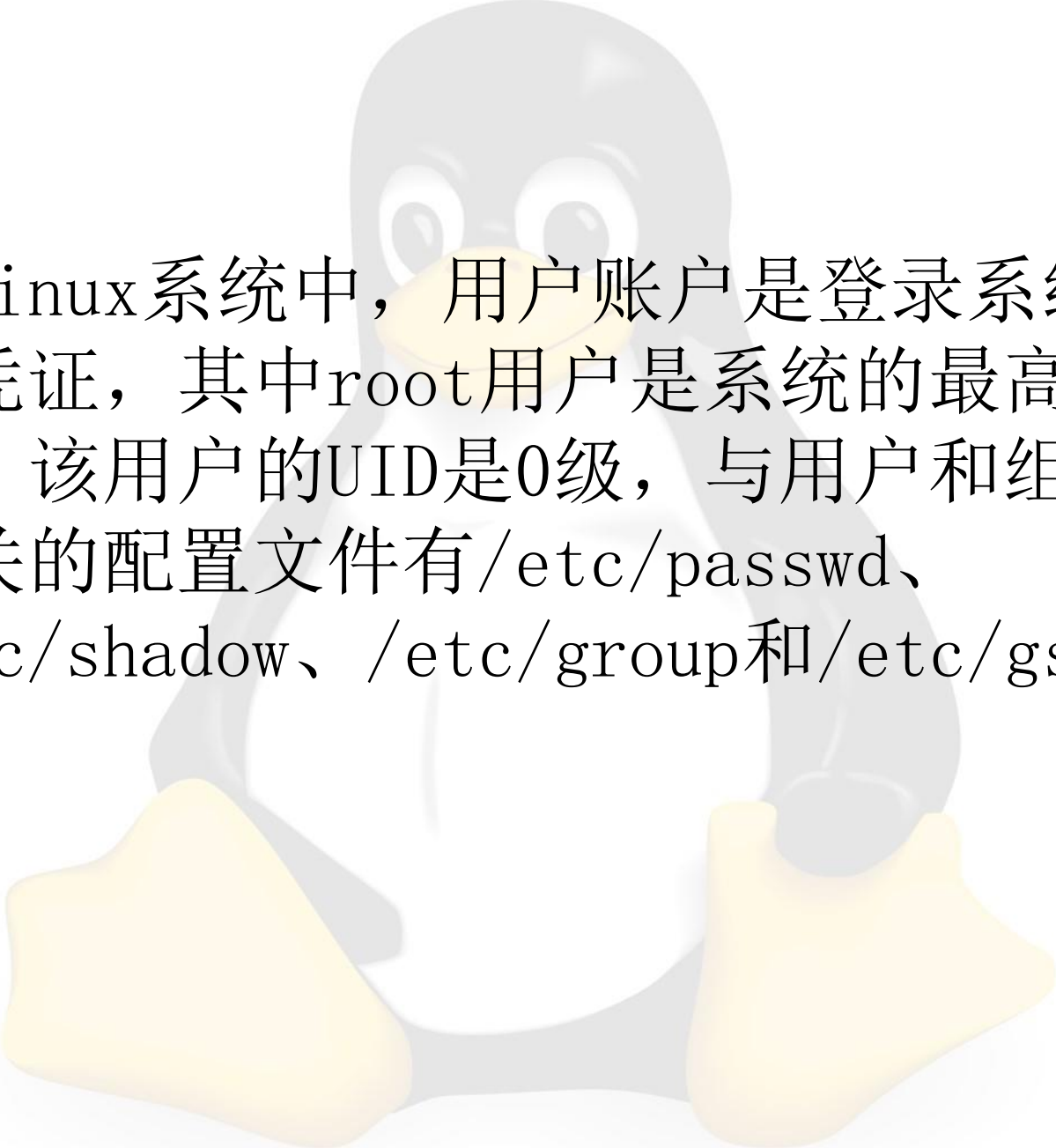
第7章 用户和组群账户管理



本章内容

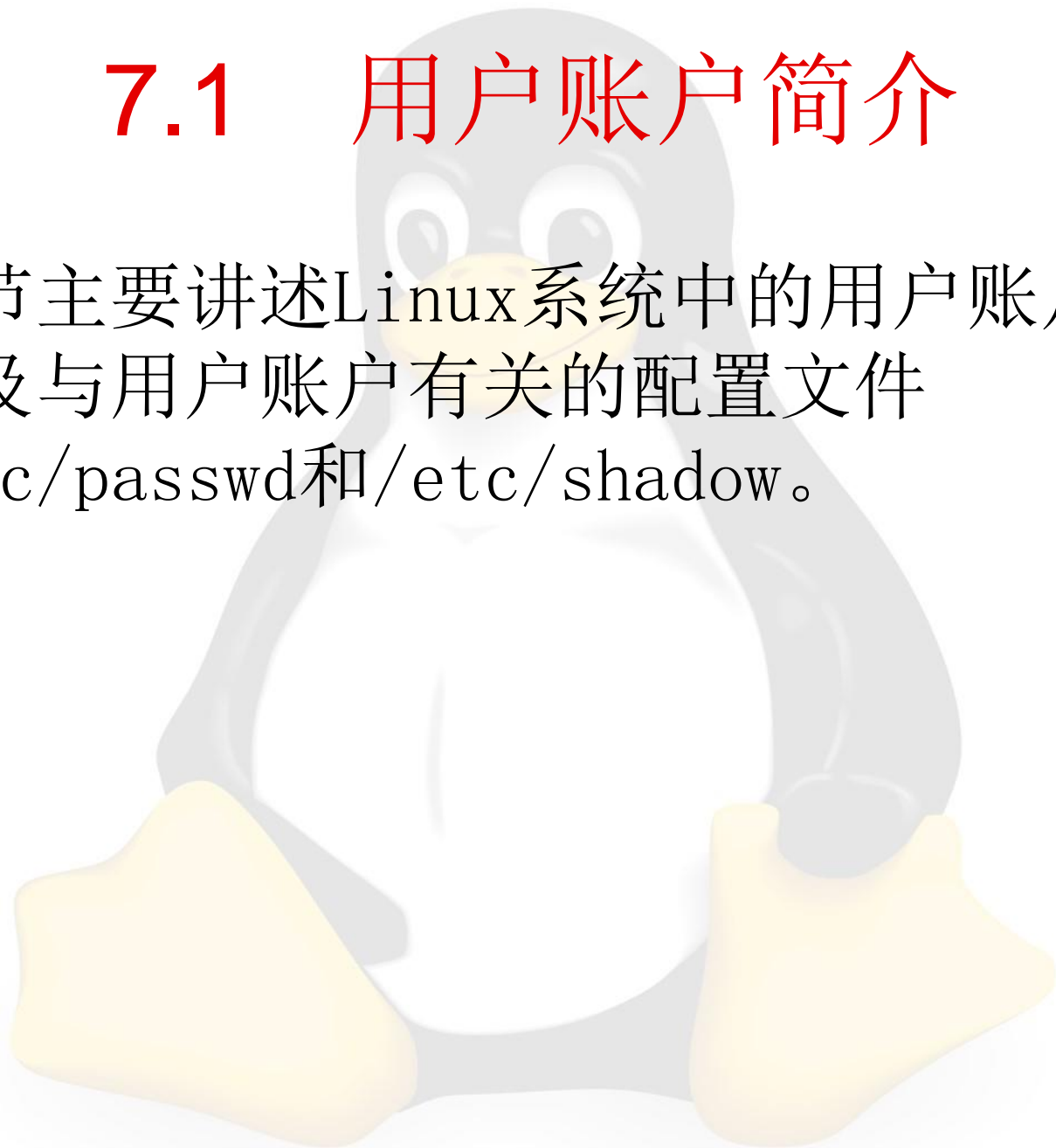
- 7.1 用户账户简介
- 7.2 用户账户设置
- 7.3 组群账户简介
- 7.4 组群账户设置
- 7.5 用户和组群账户维护



- 
- 在Linux系统中，用户账户是登录系统的唯一凭证，其中root用户是系统的最高管理者，该用户的UID是0级，与用户和组账户相关的配置文件有/etc/passwd、/etc/shadow、/etc/group和/etc/gshadow。

7.1 用户账户简介

- 本节主要讲述Linux系统中的用户账户分类以及与用户账户有关的配置文件 `/etc/passwd` 和 `/etc/shadow`。



用户账户分类

- 用户账户在Linux系统中是分角色的，由于角色不同，每个用户的权限和所能完成的任务也不同。而在实际的管理中，用户的角色是通过**UID**（用户ID号）来标识的，每个用户的**UID**都是不同的。
- 在Linux系统中有三大类用户，分别是root用户、系统用户和普通用户。

1. root用户

- 在Linux系统中，root用户UID为0。root用户的权限是最高的，普通用户无法执行的操作，root用户都能完成，所以也被称之为超级用户。在系统中的每个文件、目录和进程都归属于某一个用户，没有用户许可，其它普通用户无法进行操作的，但对root用户除外。

2. 系统用户


- 系统用户也称为虚拟用户、伪用户或假用户，这类用户不具有登录Linux系统的能力，但却是系统运行不可缺少的用户，比如bin、daemon、adm、ftp、mail等，这类用户都是系统自身拥有的。系统用户的UID为1~999。

3. 普通用户

- 这类用户能登录系统，在Linux系统上进行普通操作，能操作自己目录的内容，其使用系统的权限受限，这类用户都是系统管理员创建的。普通用户的UID为1000~60000。

/etc/passwd文件

- /etc/passwd文件是系统识别用户的一个重要文件，Linux系统中所有的用户都记录在该文件中。假设用户以账户zhangsan登录系统时，系统首先会检查/etc/passwd文件，看是否有zhangsan这个账户，然后确定用户zhangsan的UID，通过UID来确认用户的身份，如果存在则读取/etc/shadow文件中所对应的密码。如果密码核实无误则登录系统，读取用户的配置文件。

- 
- 任何用户都可以读取/etc/passwd文件内容，在/etc/passwd文件中，每一行表示的是一个用户账户的信息，一行有7个段位，每个段位用“:”分隔。

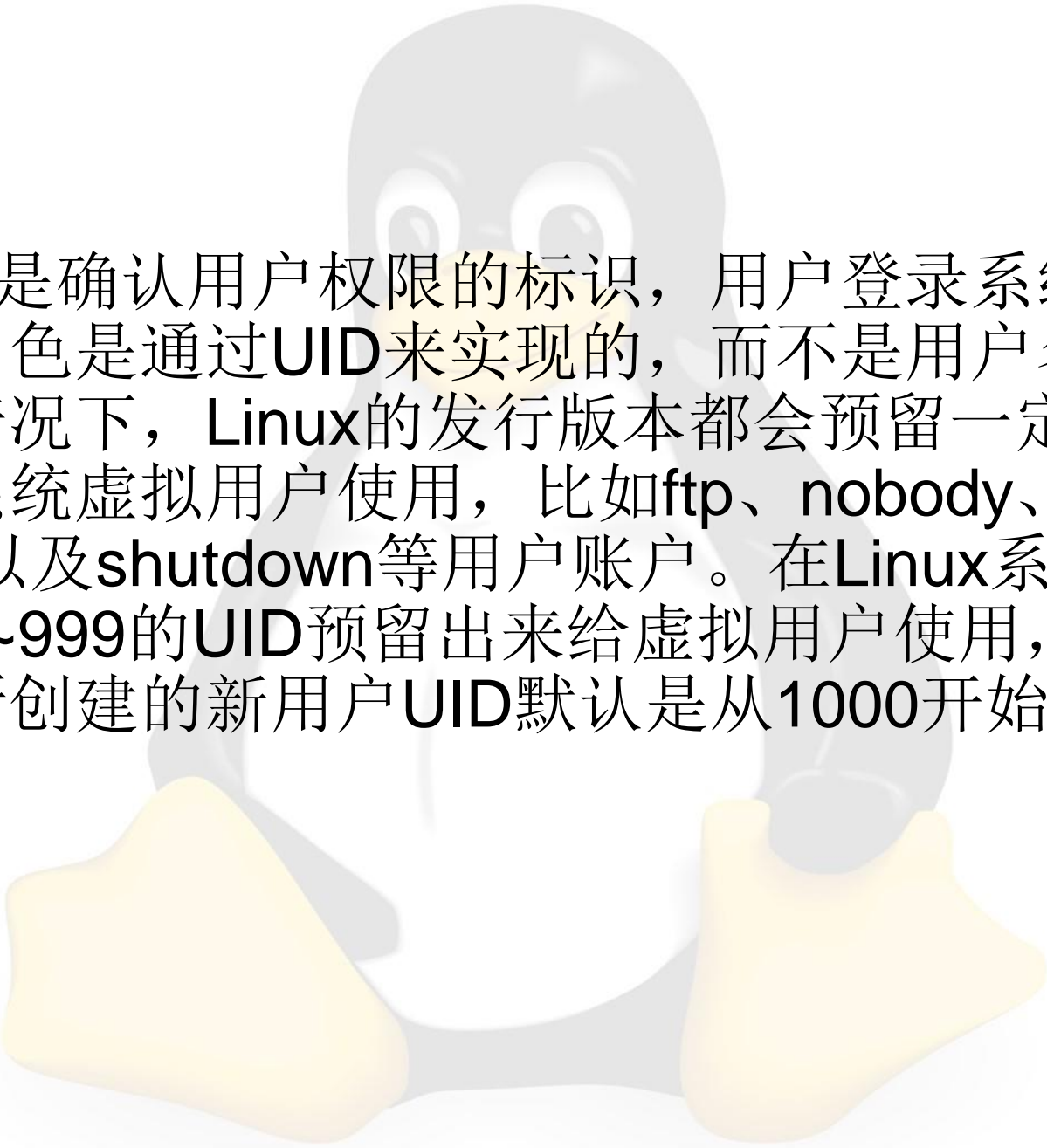
zhangsan:x:1000:1000:张三:/home/zhangsan:/bin/bash

/etc/passwd文件字段含义

字段	字段含义
用户名	也称为登录名，在系统内用户名应该具有惟一性。在本例中，zhangsan就是用户名
密码	存放加密用户的密码，看到的是一个x，其实密码已被映射到/etc/shadow文件中
用户标识号 (UID)	在系统内用一个整数标识用户ID号，每个用户的UID都是惟一的，root用户的UID是0，普通用户的UID默认从1000开始，本例中的用户zhangsan的UID是1000
组群标识号 (GID)	在系统内用一个整数标识用户所属的主要组群ID号，每个组群的GID都是惟一的
用户名全称	用户名描述，可以不设置。在本例中，zhangsan用户的用户名全称是张三
主目录	用户登录系统后首先进入的目录，zhangsan用户的主目录是/home/zhangsan
登录Shell	用户使用的Shell类型，Linux系统默认使用的Shell是/bin/bash

用户UID

- **UID**是用户的ID值，在系统中每一位用户的**UID**值都是惟一的，更确切地说每一位用户都要对应一个惟一的**UID**。**Linux**系统用户的**UID**值是一个正整数，初始值从0开始，在**Linux**系统中默认的最大值是**60000**。
- 在**Linux**系统中，**root**的**UID**是0，拥有系统最高权限。**UID**的唯一性关系到系统的安全，比如在 `/etc/passwd` 文件中把用户 `zhangsan` 的**UID**改为0后，`zhangsan`这个用户会被确认为**root**用户，当用这个账户登录到系统后，可以进行所有**root**用户才能执行的操作。

- 
- **UID**是确认用户权限的标识，用户登录系统所处的角色是通过**UID**来实现的，而不是用户名。一般情况下，**Linux**的发行版本都会预留一定的**UID**给系统虚拟用户使用，比如**ftp**、**nobody**、**adm**、**bin**以及**shutdown**等用户账户。在**Linux**系统中会把**1~999**的**UID**预留出来给虚拟用户使用，管理员所创建的新用户**UID**默认是从**1000**开始的。

/etc/shadow文件

- /etc/shadow文件是/etc/passwd的影子文件，这个文件并不是由/etc/passwd文件产生，这两个文件应该是对应互补的。/etc/shadow文件内容包括用户及被加密的密码以及其它/etc/passwd不能包括的信息，比如用户账户的有效期限等。
- /etc/shadow文件只有root用可以读取和操作，文件的权限不能随便更改为其它用户可读，这样做是非常危险的。如果发现这个文件的权限变成了其它组群或用户可读了，要进行检查，以防系统安全问题的发生。

- **/etc/shadow**文件的内容包括**9**个段位，每个段位之间用“:”分隔。

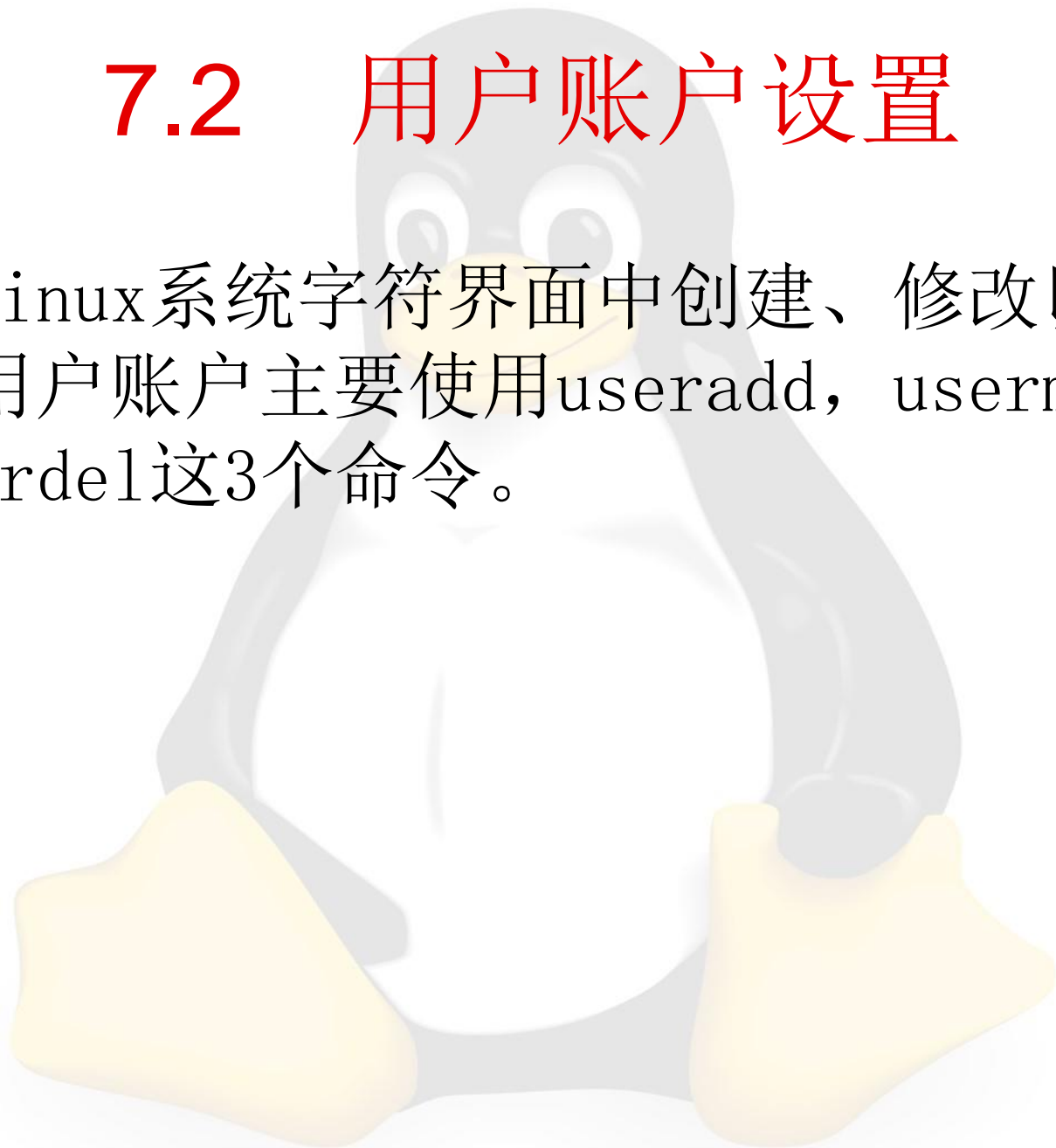
```
zhangsan:$6$E/xvWMmh$rhYLQwwffEqIudVLFzMlvkb0iN4.001  
uk6H.UovEYN0/99dVoHXcaCNGZZkFY1S3QHYgm7e6JPzEew6ybmN  
4e0:16364:0:99999:7:::
```

/etc/shadow文件字段含义

字段	字段含义
用户名	这里的用户名和/etc/passwd中的用户名是相同的
加密密码	密码已经加密，如果有些用户在这里显示的是“!!”，则表示这个用户还没有设置密码，不能登录到系统
用户最后一次更改密码的日期	从1970年1月1日算起到最后一次修改密码的时间间隔天数
密码允许更换前的天数	如果设置为0，则禁用此功能。该字段是指用户可以更改密码的天数
密码需要更换的天数	如果设置为0，则禁用此功能。该字段是指用户必须更改密码的天数
密码更换前警告的天数	用户登录系统后，系统登录程序提醒用户密码将要过期
账户被取消激活前的天数	表示用户密码过期多少天后，系统会禁用此用户，也就是说系统会不让此用户登录，也不会提示用户过期，是完全禁用的
用户账户过期日期	指定用户账户禁用的天数（从1970年的1月1日开始到账户被禁用的天数），如果这个字段的值为空，账户永久可用
保留字段	目前为空，以备将来Linux系统发展时使用

7.2 用户账户设置

- 在Linux系统字符界面中创建、修改以及删除用户账户主要使用useradd, usermod和userdel这3个命令。



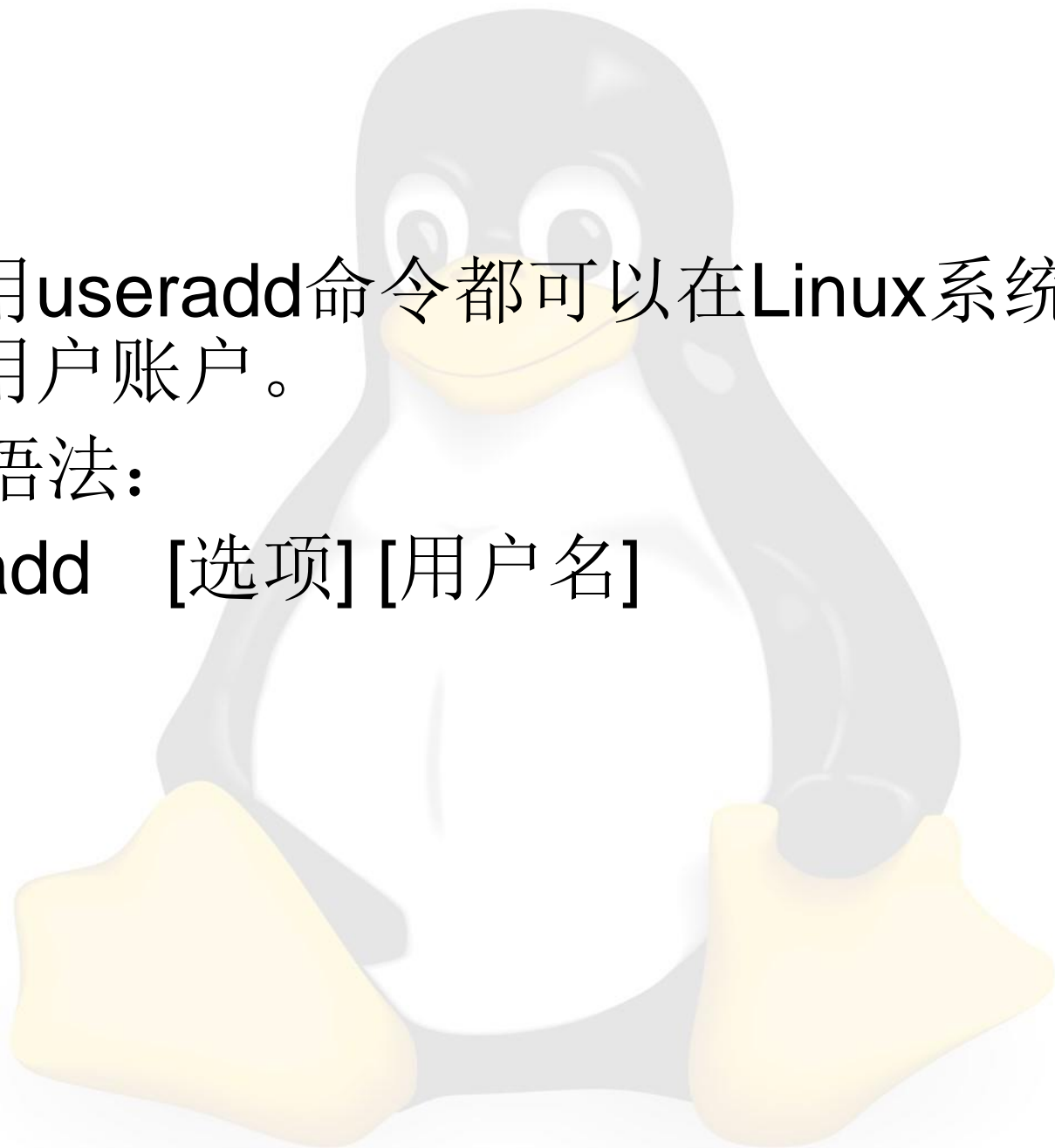
创建用户账户

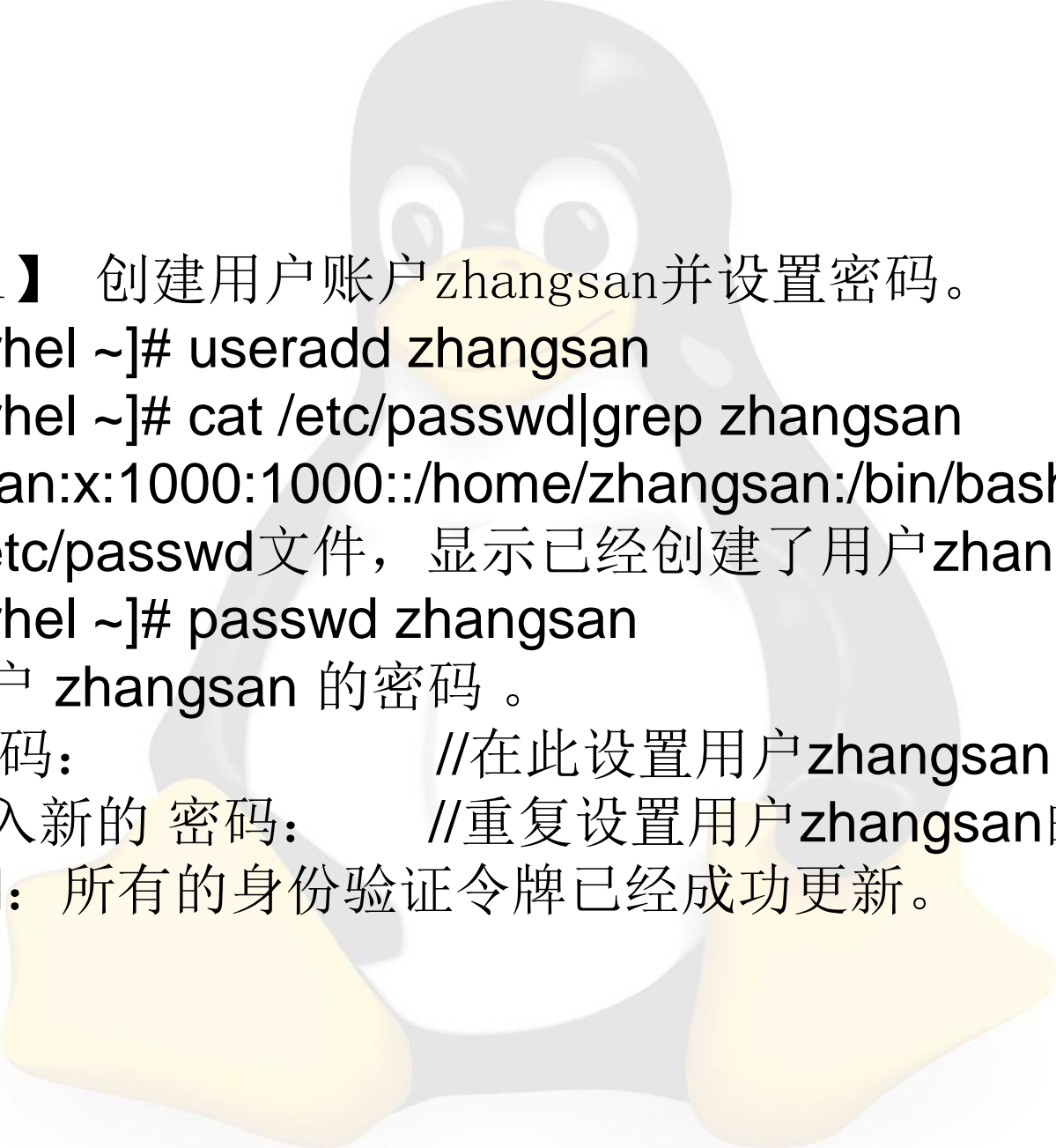
- 创建用户账户就是在系统中创建一个新账户，为新账户分配用户**UID**、组群、主目录和登录**Shell**等资源，新创建的用户账户默认是被锁定的，无法使用，需要使用**passwd**命令设置密码以后才能使用。创建用户账户就是在**/etc/passwd**文件中为新用户增加一条记录，同时更新**/etc/shadow**和**/etc/group**文件。

- 使用**useradd**命令都可以在Linux系统中创建用户账户。

命令语法：

useradd [选项] [用户名]





【例7.1】 创建用户账户zhangsan并设置密码。

```
[root@rhel ~]# useradd zhangsan
```

```
[root@rhel ~]# cat /etc/passwd|grep zhangsan
```

```
zhangsan:x:1000:1000::/home/zhangsan:/bin/bash
```

//查看/etc/passwd文件，显示已经创建了用户zhangsan

```
[root@rhel ~]# passwd zhangsan
```

更改用户 zhangsan 的密码。

新的 密码: //在此设置用户zhangsan的密码

重新输入新的 密码: //重复设置用户zhangsan的密码

passwd: 所有的身份验证令牌已经成功更新。

【例7.2】 对用户账户设置密码和不设置密码的比较。

```
[root@rhel ~]# useradd lisi
```

```
[root@rhel ~]# useradd wangwu
```

//创建用户lisi和wangwu

```
[root@rhel ~]# passwd wangwu
```

更改用户 wangwu 的密码

新的 密码:

//在此设置用户wangwu的密码

重新输入新的 密码:

//重复设置用户wangwu的密码

```
[root@rhel ~]# cat /etc/passwd|grep lisi
```

```
lisi:x:1001:1001::/home/lisi:/bin/bash
```

```
[root@rhel ~]# cat /etc/shadow|grep lisi
```

```
lisi:!!:15493:0:99999:7:::
```

//查看/etc/shadow文件，显示在用户lisi的密码字段上显示的是“!!”，表示该用户还没有设置密码，不能登录到Linux系统上

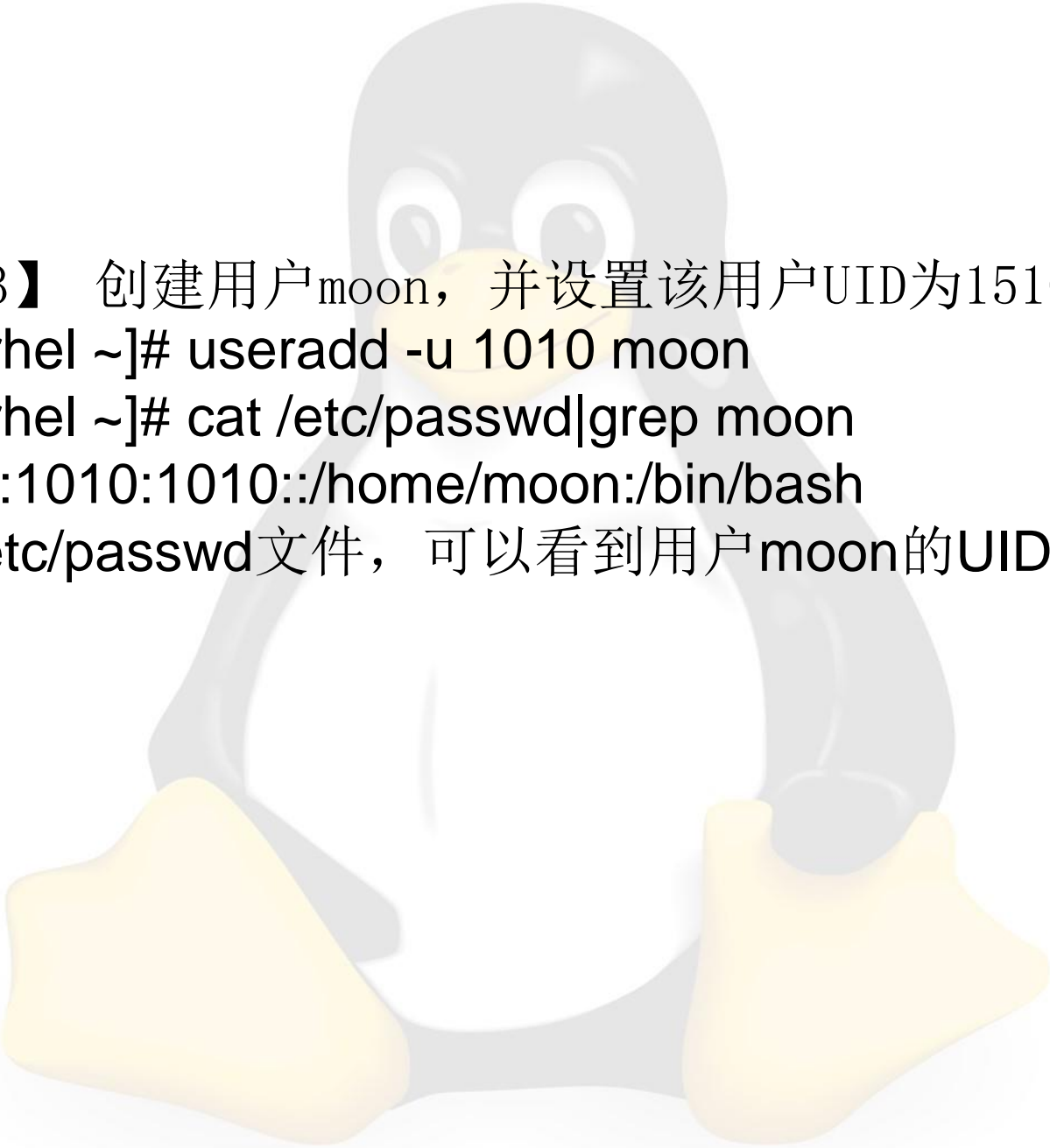
```
[root@rhel ~]# cat /etc/passwd|grep wangwu
```

```
wangwu:x:1002:1002::/home/wangwu:/bin/bash
```

```
[root@rhel ~]# cat /etc/shadow|grep wangwu
```

```
wangwu:$6$KiAl6cl.$p/kEL0heCQBGdEH6/XoSh30Utke6Tx8lJAtVKiBnM1oDIQlwp.Jci  
W1limKz1NmVKP7.0BZ9pF1LcfEzxprpk1:15493:0:99999:7:::
```

//查看/etc/shadow文件，可以看到在用户wangwu的密码字段上显示的是加密的密码，表示该用户已经设置密码，能登录到Linux系统上



【例7.3】 创建用户moon，并设置该用户UID为1510。
[root@rhel ~]# useradd -u 1010 moon
[root@rhel ~]# cat /etc/passwd|grep moon
moon:x:1010:1010::/home/moon:/bin/bash
//查看/etc/passwd文件，可以看到用户moon的UID是1010

【例7.4】 创建用户newuser，并设置该用户主目录为/home/www。

```
[root@rhel ~]# useradd -d /home/www newuser
```

```
[root@rhel ~]# cat /etc/passwd|grep newuser
```

```
newuser:x:1003:1003::/home/www:/bin/bash
```

//查看/etc/passwd文件，可以看到用户newuser的主目录是/home/www

```
[root@rhel ~]# ls -l /home
```

总用量 20

```
drwx-----. 4 lisi    lisi    4096 6月  3 05:42 lisi
```

```
drwx-----. 4 moon    moon    4096 6月  3 05:51 moon
```

```
drwx-----. 4 wangwu   wangwu   4096 6月  3 05:42 wangwu
```

```
drwx-----. 4 newuser  newuser  4096 6月  3 05:49 www
```

```
drwx-----. 4 zhangsan zhangsan 4096 6月  3 05:39 zhangsan
```

//用户newuser的主目录/home/www在创建用户时已经创建了



【例7.5】 创建用户pp，并指定该用户是属于组群root的成员。

```
[root@rhel ~]# useradd -g root pp
```

```
[root@rhel ~]# cat /etc/passwd|grep pp
```

```
pp:x:1004:0::/home/pp:/bin/bash
```

//查看/etc/passwd文件，可以看到pp用户GID字段为0，0为root组群的GID

```
[root@rhel ~]# id pp
```

```
uid=1004(pp) gid=0(root) 组=0(root)
```

//使用id命令，可以看到用户pp的主要组群是root

【例7.6】 创建用户abc，并设置该用户的Shell类型是/bin/ksh。

```
[root@rhel ~]# useradd -s /bin/ksh abc
```

```
[root@rhel ~]# cat /etc/passwd|grep abc
```

```
abc:x:1005:1005::/home/abc:/bin/ksh
```


//查看/etc/passwd文件，可以看到用户abc的Shell类型是/bin/ksh

修改用户账户

- 使用**usermod**命令可以更改用户的**Shell**类型、所属的组群、用户密码的有效期，还能更改用户的登录名。

命令语法：

usermod [选项][用户名]



【例7.7】 修改用户zhangsan的主目录为/home/kkk，并手动创建/home/kkk目录。

```
[root@rhel ~]# usermod -d /home/kkk zhangsan
```

```
[root@rhel ~]# cat /etc/passwd|grep zhangsan
```

```
zhangsan:x:1000:1000::/home/kkk:/bin/bash
```

//查看/etc/passwd文件，可以看到用户zhangsan的主目录已经更改为/home/kkk

```
[root@rhel ~]# mkdir /home/kkk
```

//必须使用mkdir命令创建/home/kkk目录，这样用户zhangsan才能使用该主目录

【例7.8】 修改用户wangwu的主目录为/home/oprof，并自动创建/home/oprof目录。

```
[root@rhel ~]# ls /home
```

```
abc kkk lisi moon pp wangwu www zhangsan
```

```
[root@rhel ~]# cat /etc/passwd|grep wangwu
```

```
wangwu:x:1002:1002::/home/wangwu:/bin/bash
```

//查看/home目录和/etc/passwd文件内容，可以看到用户wangwu的当前主目录是/home/wangwu

```
[root@rhel ~]# usermod -d /home/oprof -m wangwu
```

```
[root@rhel ~]# ls /home
```

```
abc kkk lisi moon opof pp www zhangsan
```

```
[root@rhel ~]# cat /etc/passwd|grep wangwu
```

```
wangwu:x:1002:1002::/home/oprof:/bin/bash
```

//查看/home目录和/etc/passwd文件内容，可以看到用户wangwu的主目录自动由/home/wangwu改为/home/oprof



【例7.9】 修改用户wangwu的登录名为zhaoliu。

```
[root@rhel ~]# usermod -l zhaoliu wangwu
```

```
[root@rhel ~]# cat /etc/passwd|grep zhaoliu
```

```
zhaoliu:x:1002:1002::/home/oprof:/bin/bash
```

//查看/etc/passwd文件，可以看到用户wangwu的新登录名为zhaoliu

【例7.10】 修改用户zhangsan的用户名全称为张三。

```
[root@rhel ~]# usermod -c 张三 zhangsan
```

```
[root@rhel ~]# cat /etc/passwd|grep zhangsan
```

```
zhangsan:x:1000:1000:张三:/home/kkk:/bin/bash
```

//查看/etc/passwd文件，可以看到用户zhangsan的用户名全称为张三

【例7.11】 修改用户zhangsan在密码过期后20天就禁用该账户。

```
[root@rhel ~]# cat /etc/shadow|grep zhangsan
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJD
VnYvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:
15493:0:99999:7:::
```

//用户zhangsan在密码过期后几天禁用该账户默认是没有设置的

```
[root@rhel ~]# usermod -f 20 zhangsan
```

```
[root@rhel ~]# cat /etc/shadow|grep zhangsan
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJD
VnYvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:
15493:0:99999:7:20:::
```

//查看/etc/passwd文件，可以看到用户zhangsan将在密码过期后20天就禁用该账户



【例7.12】 修改用户sun所属的组群为root，该组群必须事先存在。

```
[root@rhel ~]# usermod -g root sun
```

```
[root@rhel ~]# cat /etc/passwd|grep sun
```

```
sun:x:1050:0:太阳:/home/sun:/bin/bash
```

//查看/etc/passwd文件，可以看到用户sun所属的组群是root，组群root的GID是0

【例7.13】 锁住用户zhangsan密码，使密码无效。

```
[root@rhel ~]# usermod -L zhangsan
```

```
[root@rhel ~]# passwd -S zhangsan
```

```
zhangsan LK 2012-06-02 0 99999 7 20 (密码已被锁定。)
```

//查看用户zhangsan密码状态，可以看到该用户密码已经锁住，该用户不能在系统上登录，但是却可以从其他用户账户切换到该账户

【例7. 14】 解除用户zhangsan密码锁住。

```
[root@rhel ~]# usermod -U zhangsan
```

```
[root@rhel ~]# passwd -S zhangsan
```

```
zhangsan PS 2012-06-02 0 99999 7 20 (密码已设置，使用 SHA512 算法。)
```

//查看用户zhangsan密码状态，可以看到该用户密码已经解锁

【例7. 15】 修改用户zhangsan账户的过期日期是2012年12月12号。

```
[root@rhel ~]# cat /etc/shadow|grep zhangsan
```

```
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJDVn  
YvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:15493  
:0:99999:7:20::
```

```
[root@rhel ~]# usermod -e 12/12/2012 zhangsan
```

```
[root@rhel ~]# cat /etc/shadow|grep zhangsan
```

```
zhangsan:$6$faBBno4V$YqUY.YiJV1O4lyu4TXGGt/ikooQlgmnuPdJDVn  
YvyPNRD4CZWcEL0Du7aG71igJhWF5QhXumJgcXYSNzPwvc2/:15493  
:0:99999:7:20:15686:
```

//查看/etc/shadow文件，可以看到用户zhangsan的账户过期日期已经更改



【例7. 16】 修改用户zhangsan的Shell类型为/bin/ksh。

```
[root@rhel ~]# cat /etc/passwd|grep zhangsan
zhangsan:x:1000:1000:张三:/home/kkk:/bin/bash
[root@rhel ~]# usermod -s /bin/ksh zhangsan
[root@rhel ~]# cat /etc/passwd|grep zhangsan
zhangsan:x:1000:1000:张三:/home/kkk:/bin/ksh
```

//查看/etc/shadow文件，可以看到用户zhangsan的Shell类型已经更改为/bin/ksh

删除用户账户

- 使用**userdel**命令可以在Linux系统中删除用户账户，甚至连用户的主目录也一起删除。

命令语法：

userdel [选项][用户名]



【例7.17】 删除用户lisi。

```
[root@rhel ~]# userdel lisi
```

```
[root@rhel ~]# cat /etc/passwd|grep lisi
```

//查看/etc/passwd文件，已经查询不到关于用户lisi的数据，说明该账户已经删除

```
[root@rhel ~]# ls /home/
```

```
abc kkk lisi moon opop pp www zhangsan
```

//使用userdel命令删除用户账户并不会删除该用户主目录

【例7.18】 删除用户moon，并且在删除该用户的同时一起删除主目录。

```
[root@rhel ~]# ls /home
```

```
abc kkk lisi moon opop pp www zhangsan
```

//用户moon的主目录为/home/moon

```
[root@rhel ~]# userdel -r moon
```

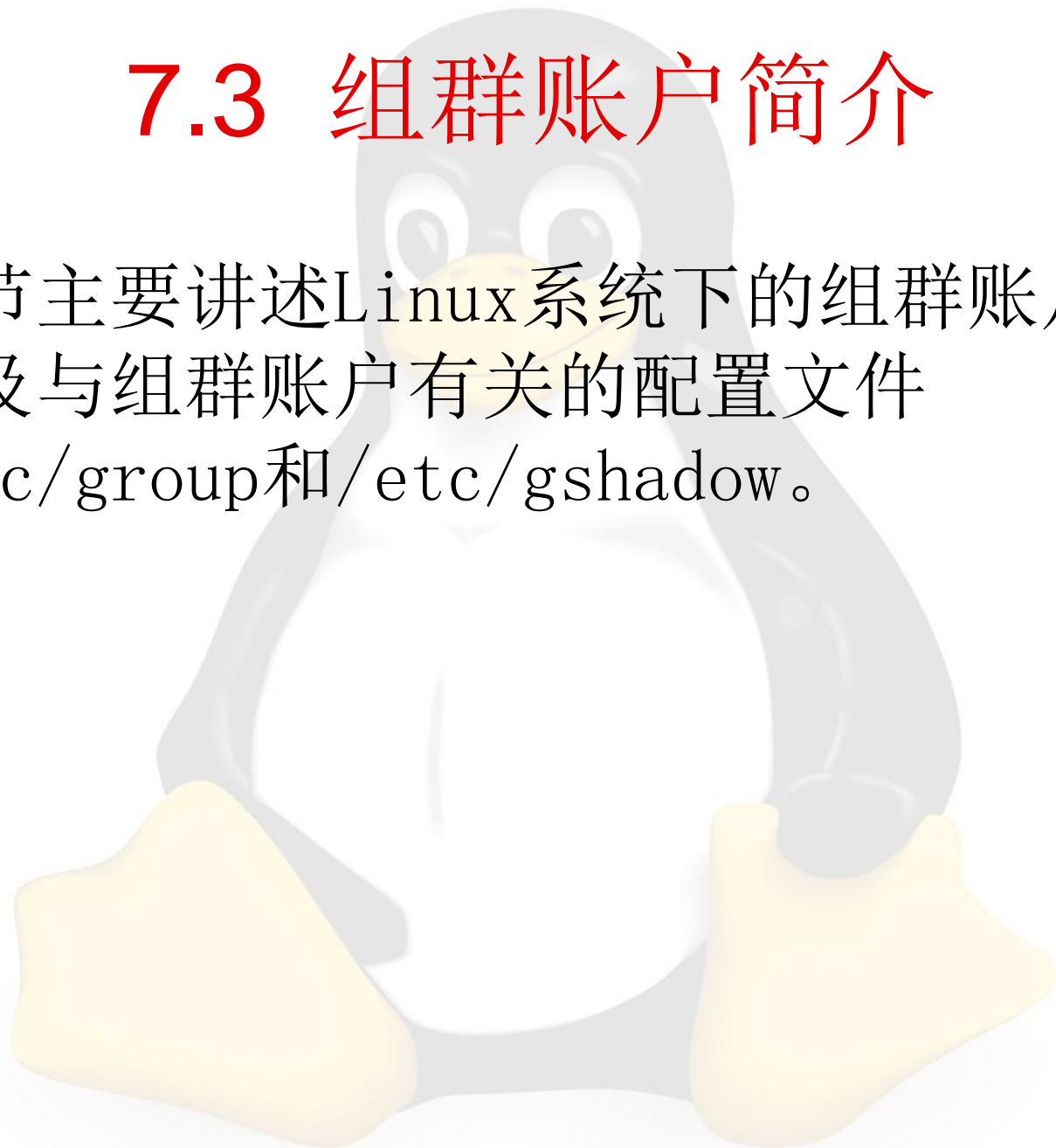
```
[root@rhel ~]# ls /home
```

```
abc kkk lisi opop pp www zhangsan
```

//查看/home目录的内容，可以看到用户moon的主目录随该用户一起删除了

7.3 组群账户简介

- 本节主要讲述Linux系统下的组群账户分类以及与组群账户有关的配置文件 `/etc/group` 和 `/etc/gshadow`。



组群账户分类

- 具有某种共同特征的用户集合就是组群。通过组群可以集中设置访问权限和分配管理任务。
- 在Linux系统中，有两种组群分类方法。
一种方法将组群分为私有组群和标准组群。
 1. 私有组群：当创建一个新的用户账户时，如果没有指定该用户属于哪一个组群，那么Linux就会创建一个和该用户同名的组群，这个组群就是私有组群，在这个私有组群中只包含这个用户。
 2. 标准组群：标准组群也称为普通组群，标准组群可以包含多个用户账户，如果使用标准组群，那么在创建一个新的用户账户时，应该指定该用户属于哪一个组群。



另外一种方法将组群分为主要组群和次要组群。

1. 主要组群：当一个用户账户属于多个组成员时，登陆后所属的组群便是主要群组，其它组群是次要群组，一个用户账户只能属于一个主要组群。
2. 次要组群：次要群组也称附加群组，一个用户账户可以属于多个次要群组。

/etc/group文件

- /etc/group文件是组群的配置文件，内容包括用户和组群，并且能显示出用户是归属哪个组群或哪几个组群。一个用户可以归属一个或多个不同的组群，同一组群的用户之间具有相似的特征。比如把某一用户加入到root组群，那么这个用户就可以浏览root用户主目录的文件，如果root用户把某个文件的读写执行权限开放，root组群的所有用户都可以修改此文件；如果是可执行的文件，root组群的用户也是可以执行的。
- 组群的特性在系统管理中为系统管理员提供了极大的方便，但安全性也是值得关注的，如某个用户有对系统管理有最重要的内容，最好让用户拥有独立的组群，或者把用户的文件的权限设置为完全私有。
- /etc/group文件的内容包括组群名、组群密码、GID及该组群所包含的用户，每个组群一条记录，一行有4个段位，每个段位用“:”分隔。

zhangsan:x:1000:

/etc/group文件字段含义

字段	字段含义
组群名	组群名称，如组群名root
组群密码	存放加密的组群密码，看到一个x，密码已被映射到/etc/gshadow文件中
组群标识号（GID）	在系统内用一个整数标识组群GID，每个组群的GID都是惟一的，默认普通组群的GID从1000开始，root组群GID是0
组群成员	属于这个组群的成员，如root组群的成员有root用户

组群GID

- 组群GID和UID类似，是一个从0开始的正整数，GID为0的组群是root组群。Linux系统会预留GID号1~999给系统虚拟组群使用，创建的新组群GID是从1000开始的，查看系统创建组群默认的GID范围应该查看/etc/login.defs中的GID_MIN和GID_MAX值，可以使用以下命令查看。

/etc/gshadow文件

- /etc/gshadow是/etc/group的加密文件，组群密码就是存放在这个文件中。/etc/gshadow和/etc/group是互补的两个文件；对于大型服务器，针对很多用户和组群，定制一些关系结构比较复杂的权限模型，设置组群密码是很有必要的。比如不想让一些非组群成员永久拥有组群的权限和特性，可以通过密码验证的方式来让某些用户临时拥有一些组群特性，这时就要用到组群密码。
- /etc/gshadow文件中每个组群都有一条记录。一行有4个段位，每个段位用“:”分隔。

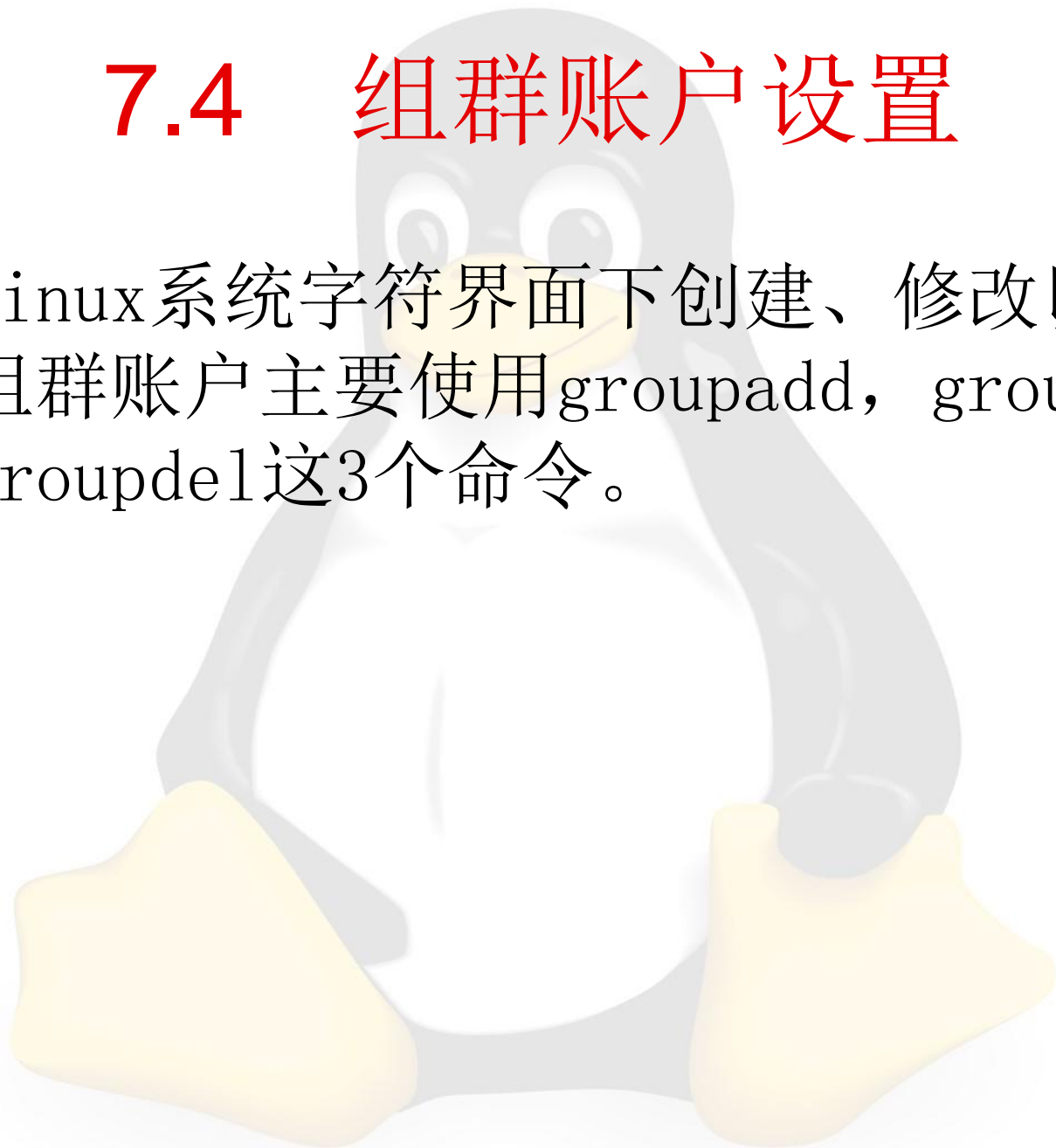
beijing:\$6\$E/xvWMmh\$rhYlQwwffEqIudVLFzMlv1::ou

/etc/gshadow文件字段含义

字段	字段含义
组群名	组群的名称
组群密码	密码已经加密，如果有些组群在这里显示的是“!”，表示这个组群没有密码。本例中组群shanghai没有密码，组群beijing已设置密码
组群管理者	组群的管理者，有权在该组群中添加、删除用户
组群成员	属于该组群的用户成员列表，如有多个用户用逗号分隔。本例中beijing组群的成员是ou

7.4 组群账户设置

- 在Linux系统字符界面下创建、修改以及删除组群账户主要使用groupadd, groupmod和groupdel这3个命令。

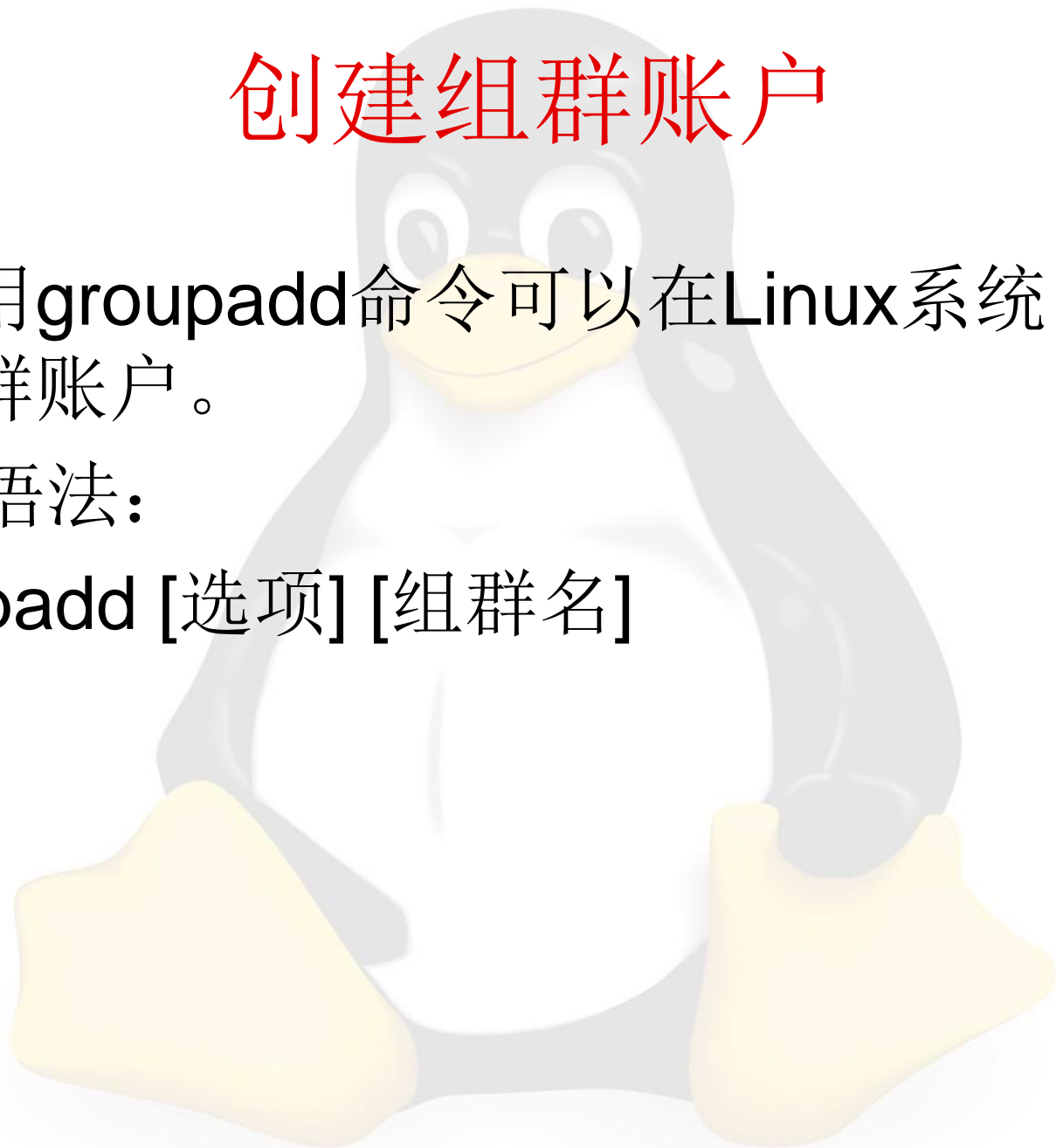



创建组群账户

- 使用groupadd命令可以在Linux系统中创建组群账户。

命令语法：

groupadd [选项] [组群名]





【例7.19】 创建名为china的组群。

```
[root@rhel ~]# groupadd china
```

```
[root@rhel ~]# cat /etc/group|grep china
```

```
china:x:1006:
```

//查看文件/etc/group，可以看到已经创建了组群china，组群GID是1006

【例7.20】 创建名为ou的组群，并且设置该组群GID为1800。

```
[root@rhel ~]# groupadd -g 1800 ou
```

```
[root@rhel ~]# cat /etc/group|grep ou
```

```
ou:x:1800:
```

//查看文件/etc/group，可以看到已经创建了组群ou，组群GID是1800

【例7.21】 创建名为chinese的系统组群。

```
[root@rhel ~]# groupadd -r chinese
```

```
[root@rhel ~]# cat /etc/group|grep chinese
```

```
chinese:x:982:
```

//查看/etc/group文件，可以看到系统组群chinese的GID是982，是小于1000的

修改组群账户

- 使用groupmod命令可以在Linux系统中修改组群账户，比如组群名称、GID等。

命令语法：

groupmod [选项][组群名]



【例7. 22】 将组群ou的GID修改为1900。

```
[root@rhel ~]# groupmod -g 1900 ou
```

```
[root@rhel ~]# cat /etc/group|grep ou
```

```
ou:x:1900:
```

//查看文件/etc/group，可以看到组群ou的GID已经更改为1900

【例7. 23】 修改组群ou的新组群名称为shanghai。

```
[root@rhel ~]# groupmod -n shanghai ou
```

```
[root@rhel ~]# cat /etc/group|grep shanghai
```

```
shanghai:x:1900:
```

//查看/etc/group文件，可以通过原来的GID看到组群ou的名称已经更改为shanghai

删除组群账户

- 使用**groupdel**命令可以在Linux系统中删除组群账户。如果该组群中仍旧包括某些用户，那么必须先删除这些用户后，才能删除组群。

命令语法：

groupdel [组群名]



【例7.24】 删除组群shanghai。

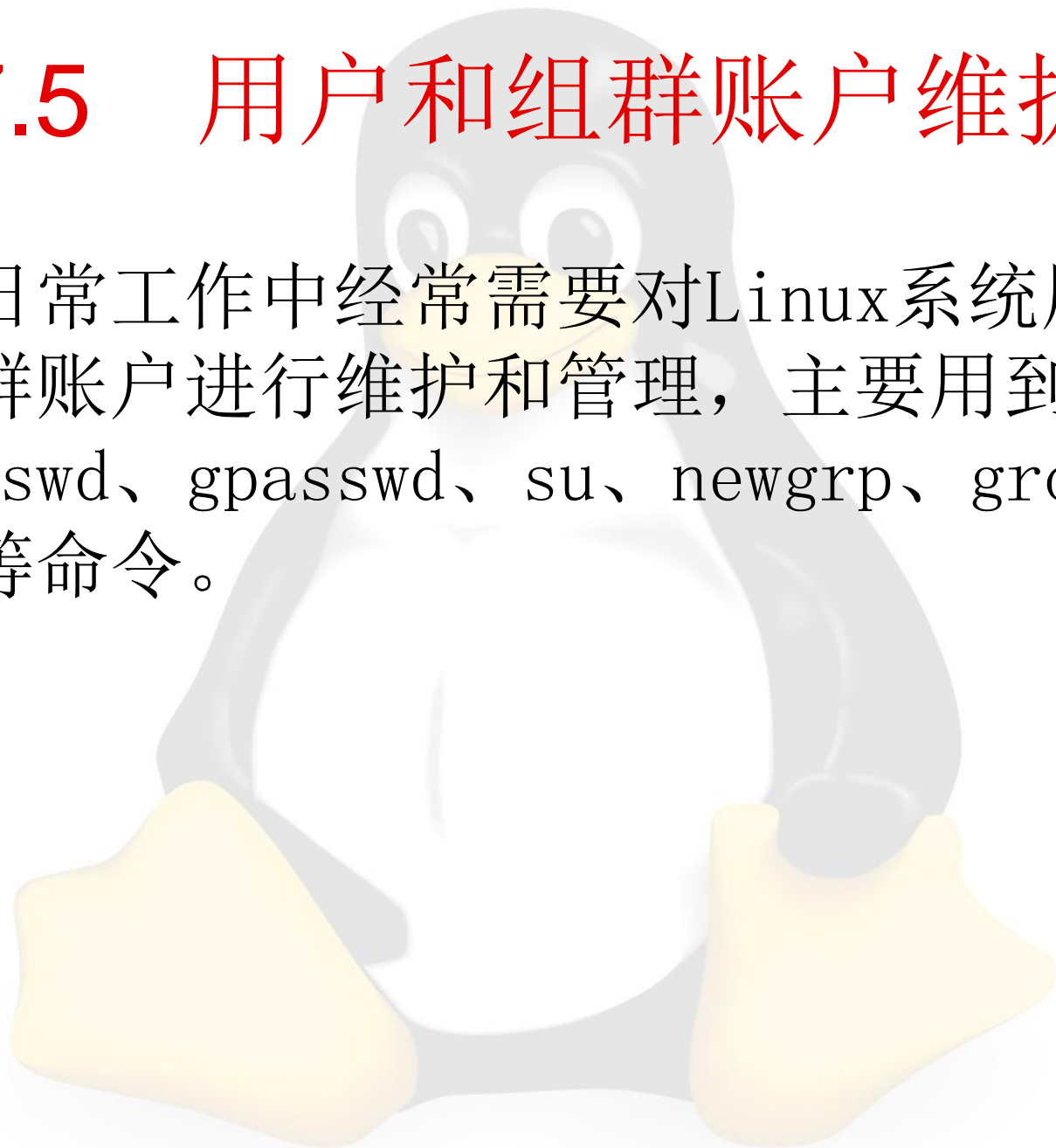
```
[root@rhel ~]# groupdel shanghai
```

```
[root@rhel ~]# cat /etc/group|grep shanghai
```

//查看/etc/group文件，可以看到当前组群shanghai已经不存在

7.5 用户和组群账户维护

- 在日常工作中经常需要对Linux系统用户和组群账户进行维护和管理，主要用到passwd、gpaswd、su、newgrp、groups和id等命令。



passwd命令

- 设置或修改用户的密码，普通用户和超级权限用户都可以运行passwd，普通用户只能更改自己的用户密码，root用户可以设置或修改任何用户的密码。如果passwd 命令后面不接任何选项或用户名，则表示修改当前用户的密码。

命令语法：

passwd [选项] [用户名]

【例7.25】 设置用户it的密码。

```
[root@rhel ~]# passwd it
```

更改用户 it 的密码。

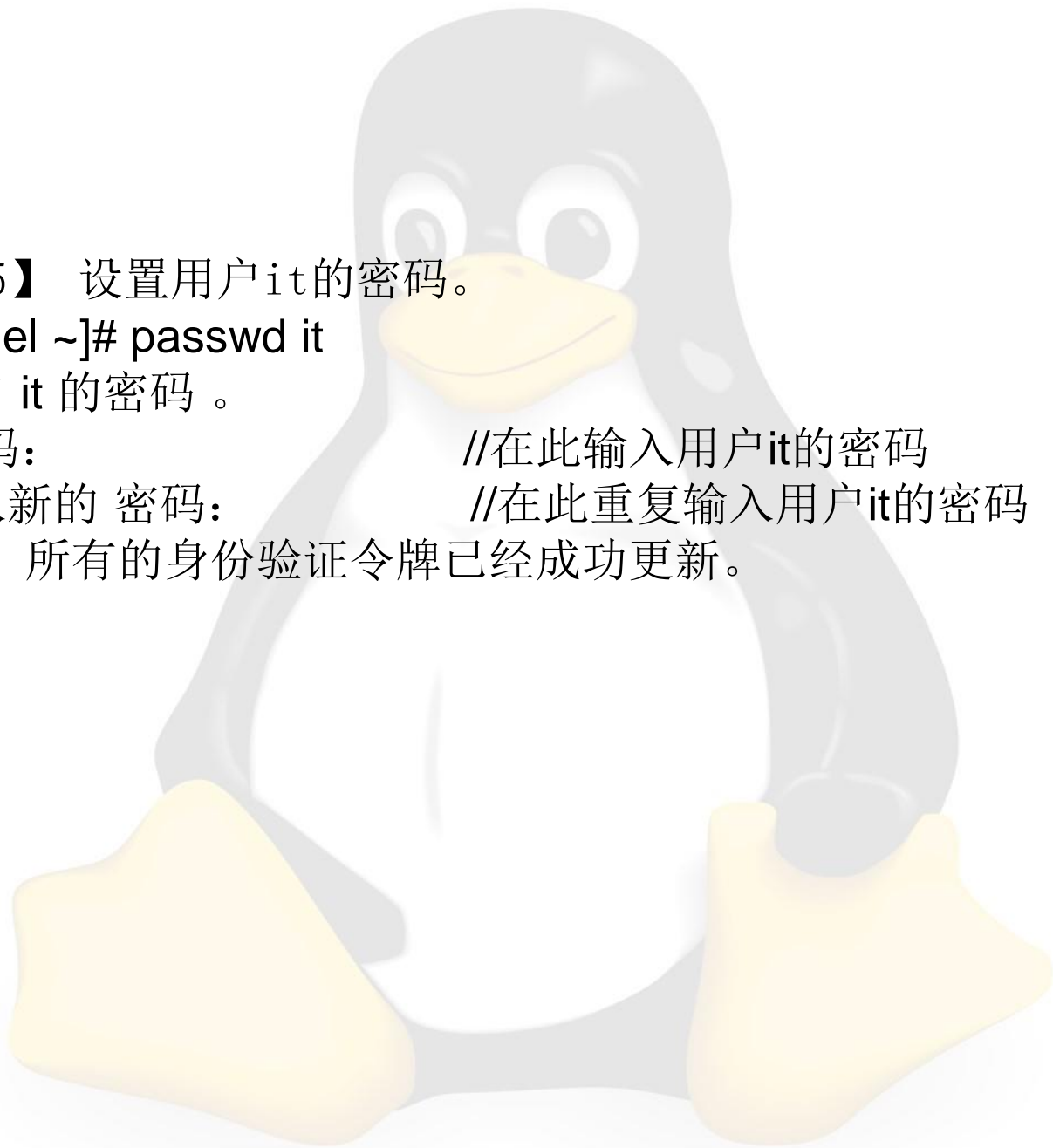
新的 密码:

//在此输入用户it的密码

重新输入新的 密码:

//在此重复输入用户it的密码

passwd: 所有的身份验证令牌已经成功更新。





【例7.26】 锁住用户it的密码。

```
[root@rhel ~]# passwd -l it
```

锁定用户 it 的密码。

passwd: 操作成功

//用户it锁住以后不能登录到系统，但是可以用su命令从其他用户切换到用户it

```
[root@rhel ~]# passwd -S it
```

```
it LK 2012-06-02 0 99999 7 -1 (密码已被锁定。)
```

//查看用户密码状态，可以看到用户it的密码是锁住的

```
[root@rhel ~]# cat /etc/shadow|grep it
```

```
it:!!$6$/4sUM8yo$pRRuww3238PwFCv2o3T7JWMjAN0FA.zkGzhUBW  
shHCK0DX2k1udSXa9w8Y.HQ1hjcvg8laKrmFHGjYZfNZmYm1:15493:  
0:99999:7:::
```

//查看/etc/shadow文件，可以看到用户it密码锁住以后在密码字段前有“!!”



【例7.27】 解锁用户it密码。

```
[root@rhel ~]# passwd -u it
```

解锁用户 it 的密码。

passwd: 操作成功

//已经成功解锁用户it，重新设置用户密码也可以解锁用户

```
[root@rhel ~]# passwd -S it
```

it PS 2012-06-02 0 99999 7 -1 (密码已设置，使用 SHA512 算法。)

//查看用户密码状态，可以看到用户it的密码已经解锁

```
[root@rhel ~]# cat /etc/shadow|grep it
```

```
it:$6$/4sUM8yo$PwRRuww3238PwFCv2o3T7JWMjAN0FA.zkGzhUBW  
shHCK0DX2k1udSxa9w8Y.HQ1hjcvg8laKrmFHGjYZfNZmYm1:15493  
:0:99999:7:::
```

//查看/etc/shadow文件，可以看到用户it密码解锁以后密码字段前的“!!”没有了



【例7.28】 删除用户it的密码。

```
[root@rhel ~]# cat /etc/shadow|grep it
```

```
rtkit:!!:15493::::::
```

```
it:$6$/4sUM8yo$pRRuww3238PwFCv2o3T7JWMjAN0FA.zkGzhUBW  
shHCK0DX2k1udSXa9w8Y.HQ1hjcvg8laKrmFHGjYZfNZmYm1:15493  
:0:99999:7:::
```

//查看/etc/shadow文件，可以看到用户it设置过密码

```
[root@rhel ~]# passwd -d it
```

清除用户的密码 it。

passwd: 操作成功

```
[root@rhel ~]# cat /etc/shadow|grep it
```

```
it::15493:0:99999:7:::
```

//查看/etc/shadow文件，可以看到用户it的密码已经没有了

gpsswd命令

- 设置一个组群的组群密码，或者是在组群中添加、删除用户。

命令语法：

gpsswd [选项] [组群名]



【例7.29】 把用户it添加到kk组群中。

```
[root@rhel ~]# gpasswd -a it kk
```

```
Adding user it to group kk
```

```
[root@rhel ~]# cat /etc/group|grep kk
```

```
kk:x:1002:it
```

//在/etc/group文件中可以看到kk组群中有用户it

【例7.30】 从kk组群中删除用户it。

```
[root@rhel ~]# gpasswd -d it kk
```

```
Removing user it from group kk
```

```
[root@rhel ~]# cat /etc/group|grep kk
```

```
kk:x:1002:
```

//在/etc/group文件中可以看到kk组群中已经没有用户it了



【例7.a】 设置kk组群的密码。

```
[root@rhel ~]# gpasswd kk
```

```
Changing the password for group kk
```

```
New Password:           //在此输入组群kk的密码
```

```
Re-enter new password:   //在此重复输入组群kk的密码
```

```
[root@rhel ~]# cat /etc/gshadow|grep kk
```

```
kk:$6$LyMEB/59ARw/CdN$Gw8ln2/Vi3vUhzdCvbNlnSioUDNcUOWpDu  
kbMleuGq8hjWWnVJWaa6BIFzYa6wdvuBkaVK7Cwkbmq0Vd8./0t1::
```

```
//在/etc/gshadow文件中可以看到组群kk已经设置密码
```

【例7.b】 取消kk组群密码。

```
[root@rhel ~]# gpasswd -r kk
```

```
[root@rhel ~]# cat /etc/gshadow|grep kk
```

```
kk:::
```

```
//在/etc/gshadow文件中可以看到组群kk已经不存在了
```

su命令

- 使用**su**命令可以切换到其它用户账户进行登录。如果**su**命令不加任何选项，默认为切换到**root**用户，并且不改变**Shell**环境。

命令语法：

su [选项] [用户]



【例7.31】 把用户root切换为用户it进行登录，并且连Shell环境也切换。

```
[root@rhel ~]# su - it
```

//从用户root切换到普通用户不需要输入用户it的密码

```
[it@rhel~] $pwd
```

```
/home/it
```

//shel环境已经切换，所以当前工作目录路径为/home/it

【例7.32】 把用户root切换为用户it进行登录，shell环境不需要切。

```
[root@rhel~]#su it
```

```
[it@rhel root] $ pwd
```

```
/root
```

//shell环境没有切换，所以当前工作目录路径为/root

【例7.33】 用户it使用su方式以root用户执行“ls /root”命令。

```
[it@rhel~]$ su - root -c “ls /root”
```

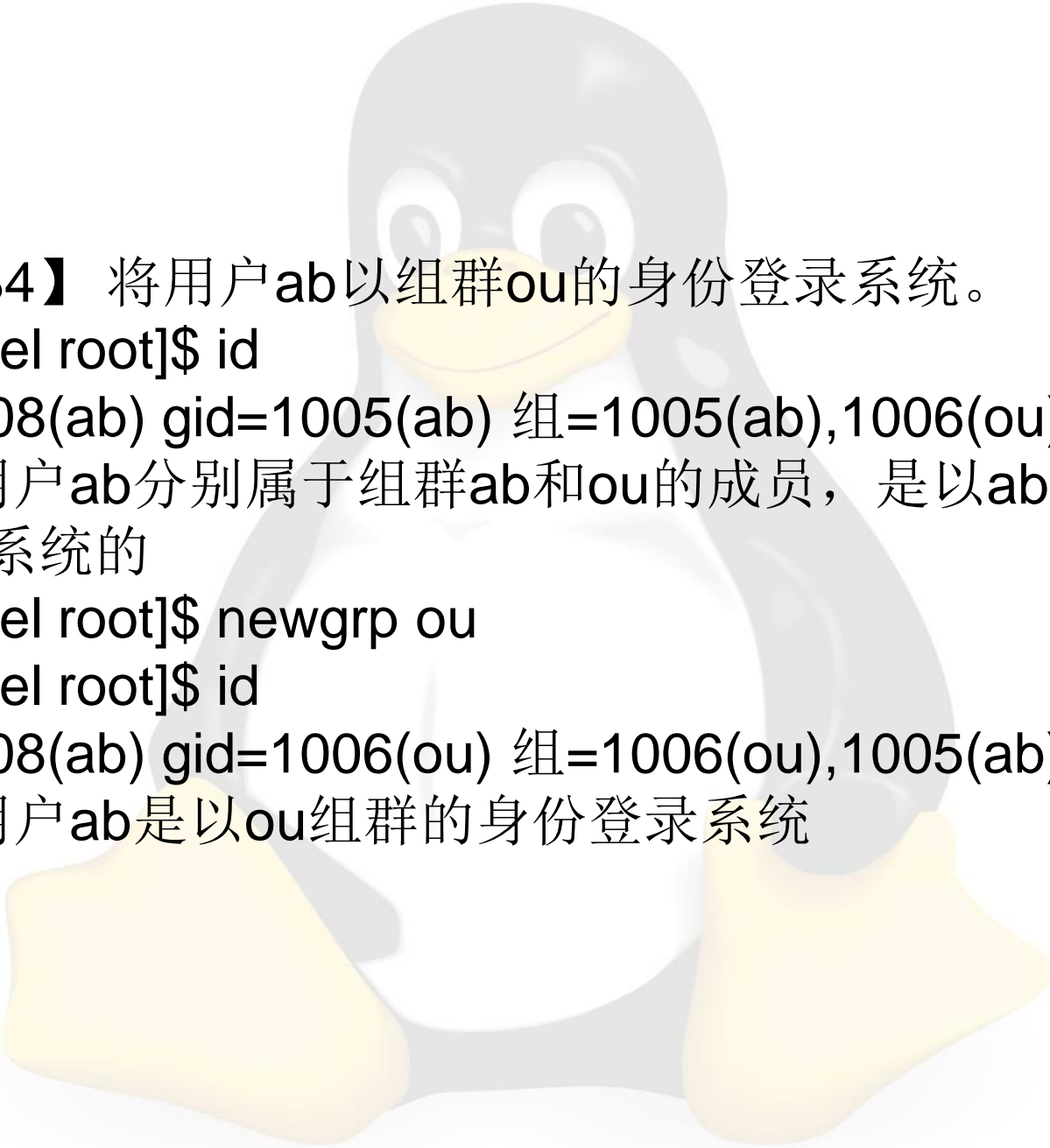
密码: //在此输入用户root密码

newgrp命令

- 让用户账户以另一个组群的身份进行登录。
newgrp命令是以相同的账户名，不同的组群身份登录系统。如果要使用**newgrp**命令切换组群，用户必须是该组群的用户，否则将无法登录指定的组群。单一用户如果要同时隶属多个组群，需要利用交替用户的设置。如果不指定组群名称，则**newgrp**命令会登录该用户名称的预设组群。

命令语法：

newgrp [组群名]



【例7.34】 将用户ab以组群ou的身份登录系统。

```
[ab@rhel root]$ id
```

```
uid=1008(ab) gid=1005(ab) 组=1005(ab),1006(ou)
```

//当前用户ab分别属于组群ab和ou的成员，是以ab组群的身份登录系统的

```
[ab@rhel root]$ newgrp ou
```

```
[ab@rhel root]$ id
```

```
uid=1008(ab) gid=1006(ou) 组=1006(ou),1005(ab)
```

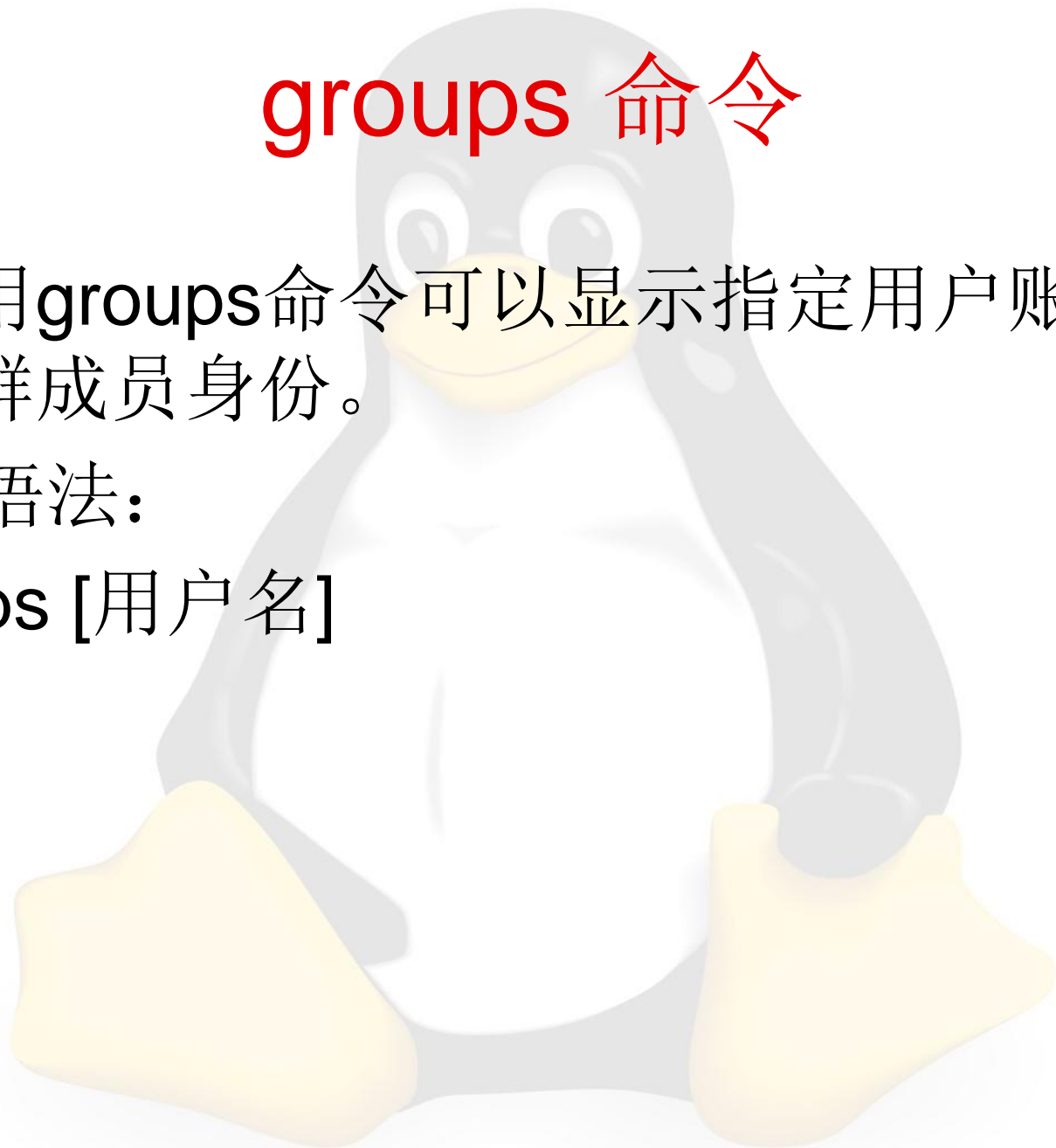
//现在用户ab是以ou组群的身份登录系统

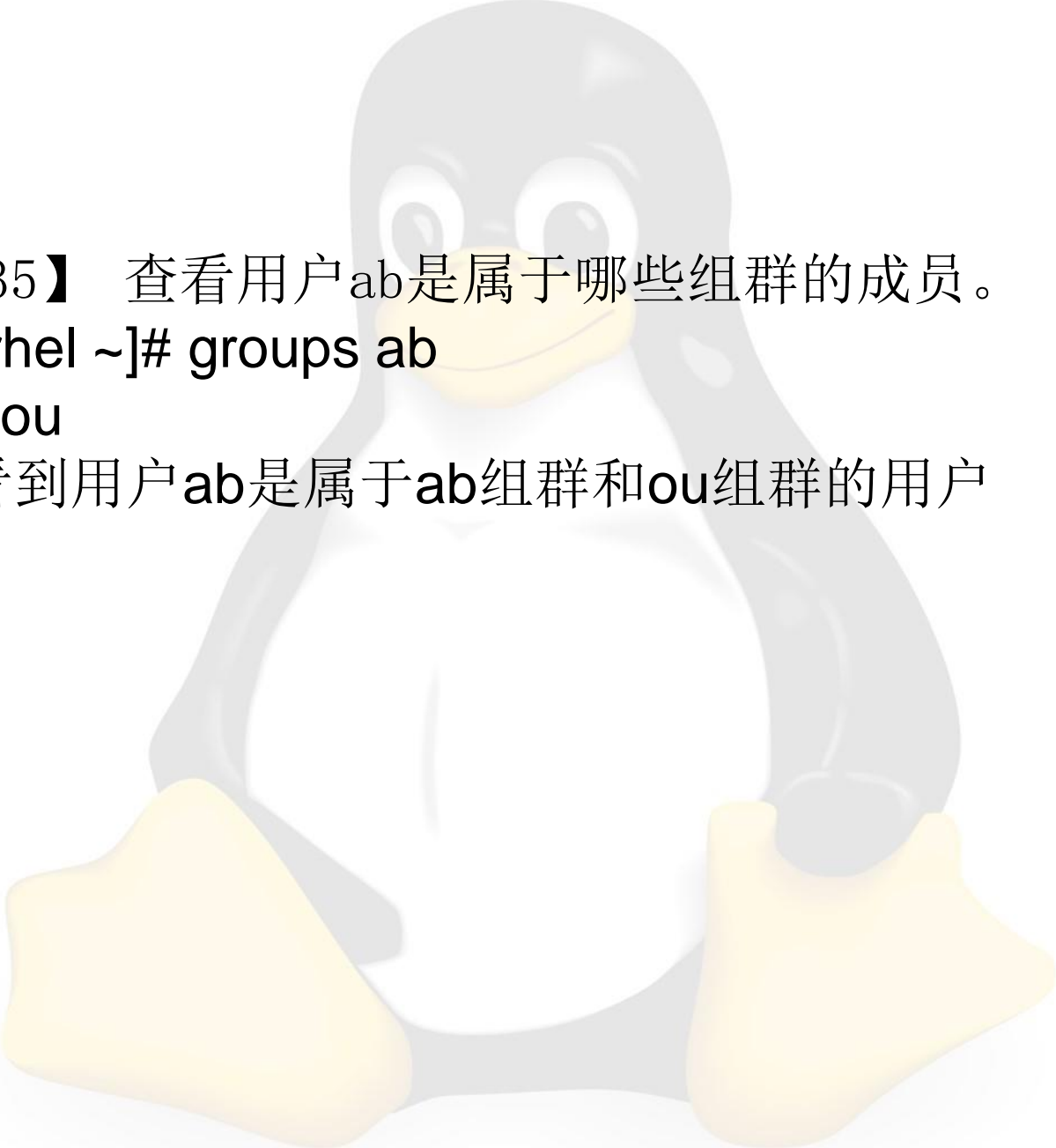
groups 命令

- 使用**groups**命令可以显示指定用户账户的组群成员身份。

命令语法：

groups [用户名]





【例7.35】 查看用户ab是属于哪些组群的成员。
[root@rhel ~]# groups ab
ab : ab ou
//可以看到用户ab是属于ab组群和ou组群的用户

id命令

- 使用id命令可以显示用户的**UID**以及该用户所属组群的**GID**。

命令语法：

id [选项] [用户名]



【例7.36】 查询用户ab的UID、GID 以及归属组群的情况。

```
[root@rhel ~]# id ab
```

```
uid=1008(ab) gid=1005(ab) 组=1005(ab),1006(ou)
```

//用户ab的UID是1008，默认组群是ab，默认用户组群的GID是1005，
归属于ab和ou组群

【例7.37】 显示用户ab所属主组群的GID。

```
[root@rhel ~]# id -g ab
```

```
1005
```

//可以看到用户ab所属主组群的GID是1005

【例7.38】 显示用户ab所属组群的GID。

```
[root@rhel ~]# id -G ab
```

```
1005 1006
```

//可以看到用户ab所属组群的GID是1005和1006

【例7.39】 显示用户ab的UID。

```
[root@rhel ~]# id -u ab
```

```
1008
```

//可以看到用户ab的UID是1008