

网络管理

必备工具软件精解

(Linux版)

李波 杨红 编著

- 网络服务状态的听诊器
- 网络潜在危机的X光机
- 网络故障排除的手术刀
- 网络传输性能的体温计
- 网络远程管理的工具箱
- 网络应用测试的虚拟机

做 Linux 做不了的事

做 Linux 做不好的事

做 Linux 拒绝做的事

网络管理

必备工具软件精解

(Linux版)

李波 杨红 编著

人民邮电出版社
北京

图书在版编目 (CIP) 数据

网络管理必备工具软件精解: Linux版 / 李波, 杨红编
著. —北京: 人民邮电出版社, 2009.1
ISBN 978-7-115-19156-4

I. 网… II. ①李…②杨… III. ①计算机网络—操作系统 (软件)—系统管理②Linux操作系统—系统管理
IV. TP316.8

中国版本图书馆CIP数据核字 (2008) 第173230号

内 容 提 要

本书精选了运行于 Linux 环境下的多款常用的网络管理工具, 分别详细地介绍了这些软件的功能、特点、适用范围、安装和使用方法。本书涉及的网络工具主要有系统管理、网络地址管理、网络连通性测试、网络性能测试、网络安全性测试、系统日志、服务器监控、远程操作、远程管理、虚拟机工具等, 通过操作实例进行了详细介绍, 使读者能更好地掌握这些工具的使用技巧。

本书内容全面、语言简练、通俗易懂, 可作为网络管理员的即查即用的工具手册, 同时也可作为 Linux 爱好者、学员的学习用书。

网络管理必备工具软件精解 (Linux 版)

- ◆ 编 著 李 波 杨 红
责任编辑 陈 昇
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京昌平百善印刷厂印刷
- ◆ 开本: 787×1092 1/16
印张: 28.75
字数: 854 千字
印数: 1—4 000 册
- 2009 年 1 月第 1 版
2009 年 1 月北京第 1 次印刷

ISBN 978-7-115-19156-4/TP

定价: 45.00 元

读者服务热线: (010)67132692 印装质量热线: (010)67129223
反盗版热线: (010)67171154

前 言

随着计算机网络的发展,计算机已融入了各行各业,而 Linux 操作系统就是目前在服务器领域应用广泛的一种网络操作系统。Linux 操作系统凭借其稳定、安全、功能强大、操作简单等特性越来越受人们的欢迎。

由于使用 Linux 操作系统的用户越来越多,所以 Linux 系统本身的安全性能、网络性能、网络安全等就越受人们的重视。为了提高 Linux 系统和网络的工作效率,本书精心挑选了一些常用的 Linux 系统管理工具、网络测试工具、网络管理工具,并详细地介绍了其功能、特点、使用方法,使读者在学习本书后,能及时地处理各种系统故障和网络故障,有效地降低系统管理和网络管理的难度,提高系统和网络的工作性能、加强其稳定性。

本书具有以下 3 个重要特点。

(1) 本书中的所有工具都是基于 Linux 或 UNIX 操作系统的管理工具,这些网络管理工具体积小、功能强大、安装与配置方法简单、对系统硬件配置要求低,非常适用于 Linux 管理员、Linux 爱好者阅读和使用。

(2) 本书中所介绍的大多数软件都属于开放源代码型的软件,这些软件可在 Linux 操作系统下和 UNIX 操作系统下通用。由于 Linux 操作系统本身就是一款免费的开源性操作系统,所以任何人都可以使用 Linux 操作系统,同时任何人都可以在该平台上使用开源性软件。目前,各计算机用户(包括网络管理员)使用这些开发源代码型的软件就可以拥有一些全功能的系统、网络监视与分析的应用软件工具包。

(3) 本书中的知识点与网络管理实际相结合,除对精选的工具软件做了详细介绍以外,还针对具体应用列举了实例,读者只需按照书中的方法进行操作,即可完成各种系统和网络的管理工具。

本书由李波、杨红编著,同时李海宁、陈志成、田俊乐、许广博、李寅、刘国增、赵卫东、刘淑梅、杨伏龙、李文俊、王同明、石长征、肖丽芳等也参与了部分章节的编写工作。他们在系统管理和网络维护方面有着丰富的经验,曾从事过多年的网络教学和管理,因此具有较高的理论水平和丰富的实践经验,曾编著有 20 余部计算机类图书,均受到了读者的好评。

感谢您选择了本书,希望我们的努力对您的工作和学习带来更多的帮助,也希望您把对本书的意见和建议告诉我们。如果您在阅读本书时遇到什么问题,欢迎与我们联系, E-mail:Helpkj@163.com。

编 者
2008 年 9 月

目 录

第 1 章 系统管理工具.....1

1.1 系统管理工具.....1

1.1.1 用户账号管理.....1

1.1.2 监视系统.....6

1.1.3 各种服务管理.....14

1.1.4 日志文件管理.....16

1.2 软件管理工具.....20

1.2.1 添加删除应用程序.....20

1.2.2 格式化软盘.....24

1.2.3 挂载文件系统.....24

1.2.4 文件压缩与归档.....26

1.3 文件系统权限管理工具.....37

1.3.1 权限的概述.....37

1.3.2 文件或目录权限的查看.....38

1.3.3 在图形模式下修改文件或目录的 权限.....39

1.3.4 在文本模式下修改文件或目录的 权限.....39

1.3.5 特殊权限的设置.....42

1.4 Linux 命令行工具.....43

1.4.1 free——实时内存监控命令.....43

1.4.2 vmstat——监视虚拟内存使用 情况.....45

1.4.3 shutdown——安全关机命令.....47

1.4.4 halt——最简单的关机命令.....49

1.4.5 reboot——重启动命令.....51

1.4.6 init——操作系统运行控制 命令.....51

1.4.7 ps——进程查看命令.....53

1.4.8 top——系统任务监视工具.....57

1.4.9 pstree——进程树查看命令.....60

1.4.10 pgrep——进程查找命令.....61

1.4.11 fg——将程序或者命令切换到 前台执行.....63

1.4.12 at——在指定的时间执行 命令.....63

1.4.13 kill——终止进程命令.....64

1.4.14 killall——终止进程命令.....66

1.4.15 nice——设置优先级命令.....68

1.4.16 renice——修改优先级命令.....68

1.4.17 procinfo——显示系统状态.....70

1.4.18 crontab——设置计时器.....71

1.4.19 dmesg——显示开机设备 信息.....72

1.4.20 chkconfig——系统服务控制 命令.....73

第 2 章 TCP/IP 工具.....75

2.1 静态 IP 地址管理工具.....75

2.1.1 IP 地址.....75

2.1.2 子网掩码.....75

2.1.3 TCP/IP 配置文件.....76

2.1.4 在图形界面下配置网络.....76

2.2 动态 IP 地址分配工具.....81

2.2.1 获取动态 IP 地址.....81

2.2.2 安装 DHCP 服务.....81

2.2.3 DHCP 服务的启动与停止.....85

2.2.4 DHCP 服务的配置.....86

2.3 Linux 命令行工具.....88

2.3.1 ifconfig——网络接口查看和 配置命令.....88

2.3.2 hostname——查看或设置 主机名.....93

2.3.3 ip——网络配置命令.....95

2.3.4 ip link——配置网络设备的 命令.....97

2.3.5 ip address——协议地址管理 命令.....100

2.3.6 route——显示和修改本地路由 表命令.....106

2.3.7 netcat——网络读写数据 命令.....109

2.3.8 arp——网络地址表管理 工具.....113

2.3.9 IP 计算器——ipcalc.....115

第3章 网络连通性测试工具	118
3.1 Linux 图形界面下测试网络	118
3.1.1 网络设备查询	118
3.1.2 网络连通性测试	119
3.1.3 网络信息统计	120
3.1.4 网络路由跟踪	120
3.1.5 网络端口扫描	121
3.1.6 网络查阅	121
3.1.7 查询登录用户的信息	122
3.1.8 域名查询工具	122
3.2 Linux 命令行工具	123
3.2.1 ping——网络连通性测试命令	123
3.2.2 traceroute——路由跟踪命令	127
3.2.3 netreport——监视网络状态	132
3.2.4 nstat——查看网络状态	132
第4章 网络性能指标	138
4.1 定义网络性能	138
4.1.1 网络可用性	138
4.1.2 网络信息响应时间	140
4.1.3 网络利用率	142
4.1.4 网络吞吐量	142
4.1.5 网络带宽容量	143
4.2 网络性能数据的收集方法	143
4.3 观察网络流量	145
4.3.1 libpcap 库的获取与安装	145
4.3.2 tcpdump 的获取与安装	146
4.3.3 网络接口	146
4.3.4 tcpdump 监视	147
4.3.5 使用 tcpdump 过滤数据包	149
第5章 网络性能测试工具	153
5.1 利用 Netperf 测试网络性能	153
5.1.1 Netperf 的工作方式	153
5.1.2 TCP 网络性能	153
5.1.3 UDP 网络性能	153
5.1.4 Netperf 的获取与安装	154
5.1.5 Netperf 服务器端的启动	155
5.1.6 网络性能测试的指标	156
5.1.7 Netperf 命令行参数	156
5.1.8 Netperf 测试网络性能	157
5.2 利用 Iperf 测试网络性能	161
5.2.1 Iperf 的工作方式	161
5.2.2 Iperf 的获取	161
5.2.3 Iperf 的安装	161
5.2.4 Iperf 的服务器端选项和启动	162
5.2.5 Iperf 客户端的选项	164
5.2.6 Iperf 工具的通用选项	165
5.3 利用 Pathload 测试网络性能	167
5.3.1 Pathload 的工作方式	167
5.3.2 Pathload 的获取	167
5.3.3 Pathload 的安装	167
5.3.4 Pathload 服务器端的启动	169
5.3.5 Pathload 客户端的启动	170
5.3.6 Pathload 客户端的详细输出	171
5.4 利用 Pathrate 测试网络性能	173
5.4.1 Pathrate 的工作方式	173
5.4.2 Pathrate 的获取	173
5.4.3 Pathrate 的安装	173
5.4.4 Pathrate 服务器端的启动	175
5.4.5 Pathrate 客户端的启动	175
5.5 利用 DBS 测试网络性能	177
5.5.1 DBS 的组成	178
5.5.2 安装 NTP 和 Gnuplot	178
5.5.3 获取并安装 DBS	179
5.5.4 dbsd 程序	180
5.5.5 dbsc 配置文件	181
5.5.6 配置 NTP 服务	184
5.5.7 运行测试	186
5.5.8 数据分析	187
5.6 利用 tcptrace 测试网络性能	188
5.6.1 tcptrace 的工作流程	188
5.6.2 tcptrace 的获取与安装	188
5.6.3 以控制台模式使用 tcptrace	189
5.6.4 图形生成工具 xplot	198
5.6.5 输出 tcptrace 图形	199
第6章 网络安全性测试工具	205
6.1 Narrow 安全扫描器	205
6.1.1 NSS 的下载和安装	205
6.1.2 NSS 的用法	206
6.2 Nessus 漏洞扫描器	207
6.2.1 Nessus 的获取	207
6.2.2 Nessus 软件包的安装	207
6.2.3 Nessus 服务的启动与关闭	208
6.2.4 建立 Nessus 用户	209
6.2.5 更改用户密码	211

6.2.6 删除指定用户	211	第 8 章 服务器监控工具	273
6.2.7 测试本机的安全性	212	8.1 系统负荷监测	273
6.2.8 测试网络中主机的安全性	214	8.1.1 uptime 命令	273
6.2.9 安全报告的保存	215	8.1.2 vmstat 命令	274
6.3 Wireshark 网络包分析	216	8.1.3 proc 系统监控	278
6.3.1 Wireshark 的获取与安装	216	8.1.4 xload 和 tload 命令	281
6.3.2 Wireshark 的启动	217	8.1.5 使用 phpsysinfo 监控系统	283
6.3.3 Wireshark 窗口的介绍	219	8.1.6 使用 MRTG 监控系统资源	287
6.3.4 实时捕获数据包	221	8.2 服务器网络流量监控工具	294
6.3.5 处理已捕获的数据包	224	8.2.1 利用 MRTG 监控网络流量	295
6.3.6 文件输入/输出与打印	228	8.2.2 利用 Ntop 监控网络流量	304
6.3.7 文件合并	231	第 9 章 远程操作工具	318
6.3.8 捕获统计	231	9.1 Telnet 远程操作	318
6.4 Snort 网络扫描	234	9.1.1 Telnet 的工作过程和协议	318
6.4.1 Snort 的获取与安装	234	9.1.2 Telnet 服务器端的安装	318
6.4.2 Snort 的命令选项	235	9.1.3 Telnet 服务器端的配置	319
6.4.3 Snort 的 3 种工作模式	236	9.1.4 Telnet 服务的启动与停止	320
6.4.4 snort.conf 规则文件配置	246	9.1.5 Telnet 的使用	321
6.5 Nmap 端口检查扫描	248	9.2 VNC 远程桌面	327
6.5.1 Nmap 的获取	249	9.2.1 VNC 服务的概述	327
6.5.2 Nmap 软件包的安装	249	9.2.2 VNC 服务的安装	327
6.5.3 Nmap 执行类型选项	249	9.2.3 VNC 服务的基本配置	328
6.5.4 nmap 的常规选项	251	9.2.4 VNC 服务的启动与停止	328
6.5.5 nmap 的定时选项	253	9.2.5 访问 VNC 服务	330
6.5.6 扫描目标主机所使用的操作 系统	253	9.3 SSH 远程操作	335
6.5.7 扫描目标主机的服务	254	9.3.1 SSH 服务的概述	335
6.5.8 扫描目标网络的服务	256	9.3.2 SSH 的加密体系	335
6.5.9 nmap 输出清单	257	9.3.3 SSH 服务的安装	336
第 7 章 系统日志分析工具	259	9.3.4 SSH 服务的配置	337
7.1 Linux 系统日志文件	259	9.3.5 SSH 服务的启动与停止	338
7.1.1 常用的 Linux 日志文件	259	9.3.6 Linux 环境下的 SSH 客户端	339
7.1.2 用户登录日志查看	260	9.3.7 Windows 环境下的 SSH 客户端	342
7.1.3 查看进程统计日志	263	第 10 章 远程管理工具	346
7.2 日志分析工具 Logcheck	265	10.1 Webmin 概述	346
7.2.1 Logcheck 的获取与安装	266	10.2 Webmin 的安装与配置	346
7.2.2 配置 Logcheck	266	10.2.1 安装 Apache 服务	346
7.3 日志实时监控工具 Swatch	267	10.2.2 安装 Perl 语言解释器	347
7.3.1 Swatch 的获取与安装	267	10.2.3 安装 OpenSSL 和 Net_SSLeay perl	348
7.3.2 Swatch 的配置	268	10.2.4 安装 Webmin	349
7.3.3 Swatch 的使用	270	10.2.5 配置的 Webmin	350
7.4 架设日志服务器	271	10.3 利用 Webmin 进行系统管理	359
7.4.1 客户端日志配置	271		
7.4.2 日志服务器端的配置	272		

10.3.1 利用 Webmin 进行 用户管理	359	10.5.4 禁止使用 ICMP 协议	409
10.3.2 利用 Webmin 管理开机与 关机	362	10.5.5 强制访问指定网站	410
10.3.3 利用 Webmin 进行进程管理	363	10.5.6 发部内部网络服务器	411
10.3.4 利用 Webmin 进行软件包 管理	364	第 11 章 虚拟机工具	413
10.3.5 利用 Webmin 管理系统日志	367	11.1 VMware 概述	413
10.4 利用 Webmin 进行服务管理	368	11.1.1 VMware 概述	413
10.4.1 利用 Webmin 管理 Samba 服务	368	11.1.2 VMware 的获取	413
10.4.2 利用 Webmin 管理 DHCP 服务	373	11.2 安装 VMware	413
10.4.3 利用 Webmin 管理 DNS 服务	379	11.2.1 安装 VMware	413
10.4.4 利用 Webmin 管理 Web 服务	389	11.2.2 配置 VMware	414
10.4.5 利用 Webmin 管理 Squid 代理服务	398	11.2.3 启动并注册 VMware	417
10.5 利用 Webmin 进行网络安全管理	407	11.3 新建虚拟机	418
10.5.1 禁止用户访问不安全网站	407	11.3.1 建立虚拟机	418
10.5.2 禁止用户上网	408	11.3.2 更改虚拟机配置	425
10.5.3 禁止用户使用指定服务	409	11.4 虚拟光驱	431
		11.4.1 挂载镜像文件	431
		11.4.2 创建光盘镜像文件	432
		附录 A Red Hat Enterprise Linux AS 4 应用软件大全	434
		附录 B Linux 常用命令	440

第 1 章 系统管理工具

Linux 操作系统的管理功能非常强大，本章将介绍利用一些 Linux 操作系统的内部功能对系统的管理操作，其中包括系统用户管理、设备管理、系统应用软件管理等操作。

1.1 系统管理工具

在第一次安装操作 Linux，或是向计算机中添加新硬件设备后，都需要利用特殊的用户对这些硬件的设备驱动进行安装，本节就将介绍在 Linux 操作系统环境中管理用户、系统显示设置、服务启动设置，以及打印机的安装设置等。

1.1.1 用户账号管理

在 Linux 操作系统中，为了保证系统的安全，可通过创建多个用户账号，再为每个用户赋予不同的权限，使每个用户都有不同的权限范围，这样各用户之间就会互不干扰，对系统核心也不能直接构成威胁。

1. 管理 root 账号

在 Linux 操作系统中，系统的默认账号是 root，拥有此账号的用户一般是管理员，利用该账号登录的管理可对系统进行完全控制，因为 root 账号拥有对系统控制的最高权利，所以 root 账号在 Linux 操作系统中也必须设置密码。

在 Linux 操作系统安装的过程中，就会提示设置管理员密码，若用户需要对 root 账号的密码进行更改，可执行“应用程序”/“系统设置”/“根口令”菜单命令，将弹出如图 1-1 所示的“根口令”对话框，在该对话框中根据需要输入 root 用户的密码，最后单击“确定”按钮即可完成 root 用户的密码设置。

如果用户设置的根口令过于简单，在单击“确定”按钮后，将会弹出警告对话框，提示用户密码过于简单。

在 Linux 操作系统中，可利用图形界面进行账号管理，也可通过终端命令的方式来实现管理，终端命令可达到 Linux 操作系统中的任何功能，也是 Linux 的一个特点，利用终端命令设置系统根口令的方法如下。

执行“应用程序”/“系统工具”/“终端”菜单命令，将弹出如图 1-2 所示的终端命令窗口。



图 1-1 根口令对话框

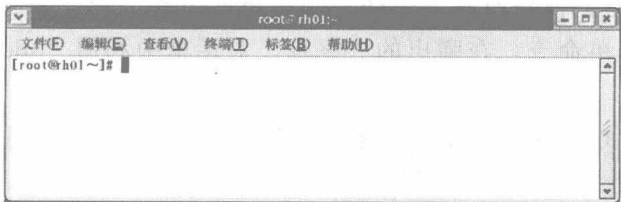


图 1-2 终端命令窗口

由图 1-2 可以看出，终端命令提示符由用户账号、计算机名称、当前工作目录和命令输入区 4 部分构成。“[root@rh01 ~]# █”中，“root”是当前用户账号名称，“rh01”是计算机名称，“~”是当前工作目录（本处为用户宿），“█”为光标，可在光标位置输入如下终端命令：

```
[root@rh01 ~]# passwd           //设置当前用户账号口令
Changing password for user root.
New UNIX password:             //在此输入新的密码
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:      //在此再次重复输入新密码
passwd: all authentication tokens updated successfully.
[root@rh01 ~]#                 //用户账号口令设置完成后返回终端命令提示符下
```

如果在终端命令窗口的命令提示符下输入“userpasswd”命令后按回车键，系统将以对话框的方式提示用户设置新密码。代码设置如下：

```
[root@rh01 ~]# userpasswd
//输入该命令后按回车键将弹出如图 1-3 所示的“查询”对话框
```

在“查询”对话框中输入新的密码后，单击“确定”按钮将弹出如图 1-4 所示的“错误”对话框，在该对话框中再次重复输入新密码。

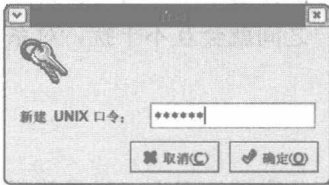


图 1-3 “查询”对话框

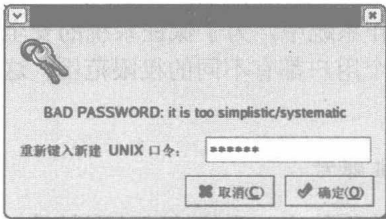


图 1-4 “错误”对话框

完成上述操作后，单击“确定”按钮完成当前用户密码的设置，此时将弹出“信息”对话框，如图 1-5 所示，该对话框提示用户新密码已设置完成，此时单击“关闭”按钮返回终端命令窗口。



图 1-5 “信息”对话框

2. 添加新的用户账号

执行“应用程序”/“系统设置”/“用户和组群”菜单命令，将弹出如图 1-6 所示的“用户管理器”对话框，在该对话框中可向当前系统中添加用户账号和组群，只需单击“添加用户”或“添加组群”按钮，再根据系统的提示即可完成用户账号或组群的增加操作。

在“用户管理器”对话框中单击“添加用户”按钮，将弹出“创建新用户”对话框，在该对话框中输入用户名（用户登录账号的名称）、密码等信息，如图 1-7 所示，再单击“确定”按钮完成用户账号的添加操作。

用户也可通过终端命令的方式创建新用户，其方法是执行“应用程序”/“系统工具”/“终端”菜单命令，在弹出的“终端”对话框中利用“adduser”或“useradd”命令创建用户账号。

```
命令格式: adduser [选项] <新用户名>
          useradd [选项] <新用户名>
```

这两个命令的选项如表 1-1 所示。

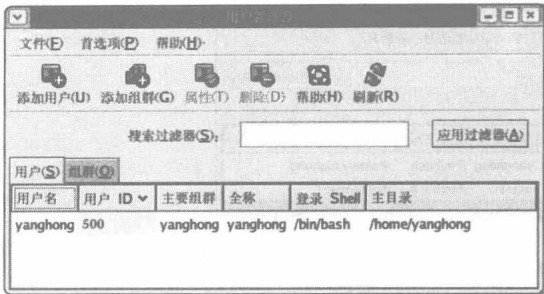


图 1-6 “用户管理器”对话框

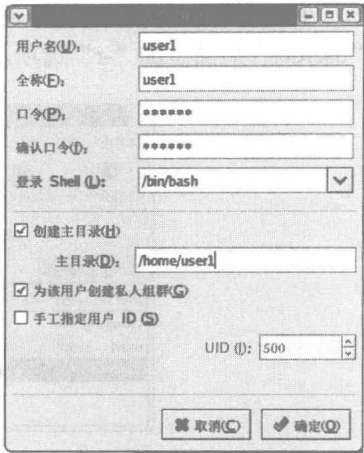


图 1-7 “创建新用户”对话框

表 1-1 “adduser”或“useradd”命令行选项

命令行选项	描 述
-c <备注信息>	用户的注释
-d <用户宿主目录>	设置新建用户的宿主目录
-e <日期>	禁用账号的日期，格式为“YYYY-MM-DD”
-f <天数>	指定用户账号密码过期后，将在几天内禁止用户账号，若指定天数为 0，则表示密码过期后，用户账号立即停用，若指定天数为-1，则任何时候都不停用该用户账号
-g <组群名称>	将当前用户账号加入到指定的组群中，但所指定的组群必须是系统中已有的组群
-G <组群列表>	若一个用户需同时加入多个组群则应选择此选项，各组群名称之间用分号“;”隔开
-m	当指定的用户宿主目录不存在，则创建一宿主目录
-M	不要创建宿主目录
-n	不为用户创建私人组群
-r	创建一个 UID 小于 500 的、不带宿主目录的用户账号
-p <密码>	设置密码
-s	指定用户 Shell 目录，默认为“/bin/bash”
-u uid	指定用户 UID，指定的 UID 值必须大于 499，并且是唯一的

若需要利用终端命令创建用户可在终端命令窗口中添加如下代码：

```
[root@rh01 ~]# adduser user2 //利用 adduser 命令创建一个名为"user2"的用户账号
```

创建的新用户账号名称不能与系统中原有的用户账号名称相同，否则系统将会提示信息，例如下面的代码：

```
[root@rh01 ~]# adduser user1 //利用 adduser 命令创建一个名为"user1"的用户账号
adduser: user user1 exists //已有名为"user1"的用户
[root@rh01 ~]#
```

3. 删除已有的用户账号

删除用户账号的方法也可在“用户管理器”对话框中完成，其操作方法是在该对话框中将需删除的用户账号选中，再在工具栏中单击“删除”按钮，此时被选中的用户将会被删除，如图 1-8 所示。

除通过“用户管理器”对话框完成用户账号的删除操作外，还可直接在终端命令窗口中进行用户账

号删除操作，在终端命令窗口中通过 `userdel` 命令将指定的用户删除，该命令只有一个可选参数 “-r”，若在命令 “`userdel`” 后面添加 “-r” 选项，则可将指定用户的宿主目录和其中的文件一同删除。

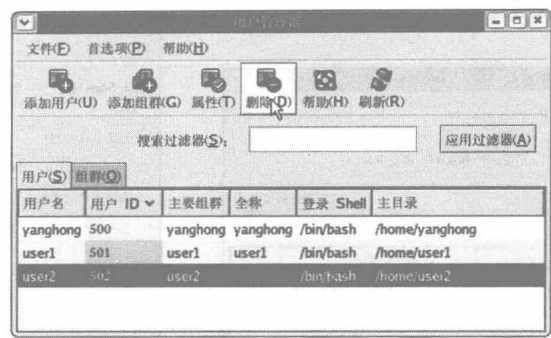


图 1-8 “用户管理器”对话框

命令格式: `userdel [-r] <需删除的用户名>`

例如，需删除当前系统中名为 “user2” 的用户账号名称，其操作方法如下：

```
[root@rh01 ~]# userdel -r user2 //删除名为"user2"的用户账号，同时将其宿主目录删除
```

如果被删除的用户账号名称是系统中没有的，则系统会显示如下的提示信息：

```
[root@rh01 ~]# userdel user2 //删除名为"user2"的用户账号
userdel: user user2 does not exist //没有名为"user2"的用户账号存在
[root@rh01 ~]#
```

4. 设置用户密码

通过 `useradd` 或 `adduser` 命令创建的用户账号都是没有密码的，此时可用 Linux 的 `passwd` 命令为用户账号设置密码，也可利用 `passwd` 使用修改已有用户的密码。

命令格式: `passwd [选项] [用户账号]`

该命令的选项如表 1-2 所示。

表 1-2 “passwd” 命令行选项	
命令行选项	描 述
-d	删除密码，本参数仅系统管理员才能使用，即 root 用户账号可以使用
-f	强制修改密码
-k	选择该参数选项后，必需在密码过期后，才能再次修改密码
-l	锁定密码
-S	列出当前用户的密码信息，该选项是大写字母 “S”
-u	将已锁定的用户账号解除锁定

例如，为用户账号名称为 “user1” 的用户设置密码，其操作方法如下：

```
[root@rh01 ~]# passwd -f user1 //强制修改用户账号名称为"user1"的密码
Changing password for user user1.
New UNIX password: //输入"user1"用户的新密码
BAD PASSWORD: it does not contain enough DIFFERENT characters
Retype new UNIX password: //再次重复输入"user1"用户的新密码
passwd: all authentication tokens updated successfully.
[root@rh01 ~]#
```

5. 创建用户组群

执行“应用程序”/“系统设置”/“用户和组群”菜单命令，将弹出“用户管理器”对话框，在该对话框中单击工具栏上的“添加组群”按钮，将弹出“创建新组群”对话框，在该对话框的“组群名”文本框中输入组群的名称，如图 1-9 所示，再单击“确定”按钮即可完成组群的创建。

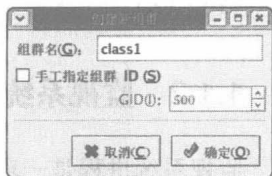


图 1-9 “创建新组群”对话框

6. 删除用户组群

若需将系统中的用户组群删除，可在用户管理器下方面选择“组群”选项卡，此时将显示组群列表，在该列表中显示了当前系统中所有的用户组群，如图 1-10 所示。

在组群列表中选择需删除的组群，再单击“组群”按钮，此时被选中的组群将被删除。

7. 更改用户账号信息

如果需要更改用户信息，可直接在用户管理器中进行操作，其操作方法是执行“应用程序”/“系统设置”/“用户和组群”菜单命令，将弹出“用户管理器”对话框，在该对话框中选中需修改信息的用户账号，再单击工具栏上的“属性”按钮，将弹出“用户属性”对话框，在该对话框中可更改用户账号的名称、用户账号过期设置、口令信息设置等，如图 1-11 所示。

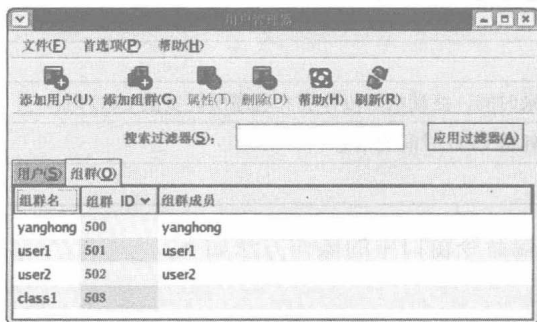


图 1-10 组群列表

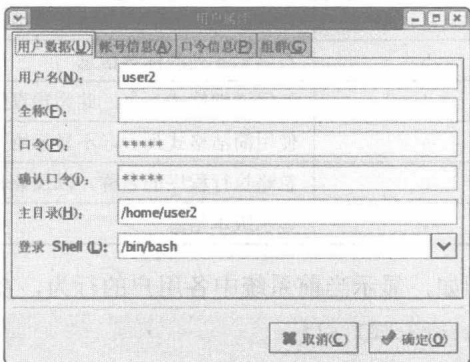


图 1-11 “用户属性”对话框

修改用户账号也可以在终端命令窗口中利用终端命令完成该工作，修改用户信息的命令是“usermod”。

命令格式：usermod [选项] <用户名>

该命令各选项如表 1-3 所示。

表 1-3 “usermod”命令行选项

命令行选项	描 述	命令行选项	描 述
-c <备注信息>	修改用户账号的备注信息	-l <账号名称>	修改用户账号名称
-d <用户宿主目录>	修改用户账号的宿主目录	-L	锁定用户账号密码，使密码无效
-e <有效期限>	修改用户账号的有效期限	-s <Shell>	修改用户账号登录后所使用的 Shell
-f <天数>	当密码过期后，在此天数后将关闭该账号	-u <uid 值>	修改用户账号的 ID 值
-g <组群名称>	修改用户账号所属的组群	-U	解除密码锁定
-G <组群名称>	修改用户账号所属的附加组群		

例如，将当系统中名为“user2”的用户名称改为“hong”，所属组群改为“class1”，其操作方法如下：

```
[root@rh01 ~]# usermod -l hong -g class1 user2
[root@rh01 ~]#
```

1.1.2 监视系统

监视系统进程是一项很重要的工作，一个操作系统不但对系统的安全性要求较高，同时还对系统的稳定性也有一定的要求，这样系统数据才能得到保障。

1. 查看用户行为

在 Linux 操作系统中，每个用户都能执行不同的应用程序，若管理员需要了解当前用户登录系统的情况，以及这些用户执行各种操作，都可利用 Linux 的“w”命令来设置。

命令格式：w [选项] [用户账号名称]

该命令各选项如表 1-4 所示。

表 1-4 “w” 命令行选项

命令行选项	描 述
-f	开启或关闭显示用户从什么地方进入系统
-h	不显示各列的标题信息
-l	使用详细格式列表，此为预设值
-s	使用简洁格式列表，不显示用户登录时间，终端机阶段作业和程序所耗费的 CPU 时间
-u	忽略执行程序的名称，以及该程序耗费 CPU 时间的信息
-V	显示版本信息

例如，显示当前系统中各用户的行为，在终端命令窗口中的操作方法如下：

```
[root@rh01 ~]# w
12:58:57 up 5:08, 2 users, load average: 0.29, 0.18, 0.14
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU WHAT
root      :0        -          07:58    ?xdm?  30:02  1.40s /usr/bin/gnome-
root      pts/1     :0.0      09:32    0.00s   0.51s   0.02s w
[root@rh01 ~]#
```

由以上返回结果可以看出，系统返回的第 1 组信息中包括 4 个字段：系统当前的时间，如 12:58:57；运行时长，up5:08，系统当前已运行了 5 小时 8 分；登录用户数，2users 表示当前系统中登录用户的总数为两个用户；平均负载指标，load average: 0.29、0.18、0.14，这 3 组数字表示系统在过去 1、5、10 分钟内的平均负载程序，其值越少，表示系统的负载越低，系统的运行就会越流畅。

第 2 组信息共有 8 个字段，用来显示正在进行的各种操作，以及用户占用的系统资源。

USER：该列显示登录的用户账号名，若用户重复登录，则该用户就会重复显示在列表中。

TTY：用户登录的终端代号，所采用的登录方式不同，终端代码也就不同。

FROM：显示用户从什么地方登录，如果是本地登录，将会显示为点“.”，若是从远程登录，则会显示远程主机的 IP 地址或主机名，若显示值为“:0.0”之类的标识，则表示该用户是从 X Window System 以文本模式登录的。

LOGIN：这是 Login At 的意思，表示该用户登录系统的时间。

IDLE：该列表示用户闲置的时间，这是一个计时器，当用户执行任何操作时，计时器就会重置。

JCPU：以终端的代码区分显示所有相关的进程执行时所消耗的 CPU 时间，当系统进程结束时，开始新的进程时则会重新计时。

PCPU：表示 CPU 执行程序消耗的时间。

WHAT：表示用户正在执行的程序名称，如果正在执行文本模式命令，则会显示用户环境的名称。

2. 查看当前已登录系统的用户

执行“应用程序”/“系统工具”/“终端”菜单命令，在弹出的终端命令窗口中使用 who 命令即可查看当前已登录到系统的用户账号名称。

命令格式：who [选项]

该命令各选项如表 1-5 所示。

表 1-5 “who” 令行选项

命令行选项	描 述
-H 或-heading	显示各列的标题栏
-i 或-u	显示闲置时间，若该用户在前一分钟之内有任何动作，将标记成点“.”，如果该用户已超过 24 小时没有任何动作，则标记为“old”字符串
-m	此参数的效果和“am i”字符串相同
-q 或-count	只显示登录系统的账号名称和总人数
-s	选择此参数后，仅负责解决 who 指令其他版本的兼容性问题
-w 或-T 或-mesg 或-writable	显示用户的信息状态栏
-help	显示帮助信息
-version	显示版本信息

例如，显示当前登录到系统中的用户，其操作方法如下：

```
[root@rh01 ~]# who -H
NAME          LINE          TIME          COMMENT
root          :0            Jul  9 07:58
root          pts/1         Jul  9 09:32 (:0.0)
[root@rh01 ~]#
```

3. 查看曾经登录系统的用户

在 Linux 操作系统中，可利用“last”命令显示曾登录到本机用户账号。

命令格式：last [选项]

该命令各选项如表 1-6 所示。

表 1-6 “last” 令行选项

命令行选项	描 述
-a	将登录系统的主机名称或 IP 地址显示在最后一行
-d	将 IP 地址转换成主机名称
-f <记录文件>	指定记录文件
-n <显示列数>	设置显示列数
-R	不显示登录系统的主机名称或 IP 地址
-x	显示系统关机、重新开机，以及执行等级的改变等信息

例如，显示曾登录本机操作系统的用户账号列表，其操作方法如下：

```
[root@rh01 ~]# last
root      pts/1        :0.0          Mon Jul  9 09:32          still logged in
root      pts/1        :0.0          Mon Jul  9 08:39 - 09:19  (00:40)
root      :0          Mon Jul  9 07:58          still logged in
reboot    system boot  2.6.9-42.EL   Mon Jul  9 07:51          (06:46)
root      pts/1        :0.0          Sat Jul  7 09:11 - 09:27  (00:16)
root      :0          Sat Jul  7 08:33 -down    (00:54)
reboot    system boot  2.6.9-42.EL   Sat Jul  7 08:29          (00:58)
root      :0          Fri Jul  6 16:51 - crash   (15:38)
reboot    system boot  2.6.9-42.EL   Fri Jul  6 16:42          (16:45)

wtmp begins Fri Jul  6 16:42:11 2007
[root@rh01 ~]#
```

若登录过本机系统的用户过多，用户访问清单也会越多，此时可在“last”命令后面加“|more”参数，此时系统将每显示一屏就暂停下来，按任意键后将显示下一屏。

在使用该命令时，若仅使用“last”命令，将列出所有的用户，若在该命令后边指定用户账号名称，即可列出该用户曾登录本机的记录。

4. 监视系统

在 Linux 系统中的每一个用户都能同时运行多个程序，而每个程序又可能会有多个进程；如果某些进程占用了大量的系统资源，就会因为系统负载过重造成如死机、程序挂起等故障。作为一名系统管理员，需要了解系统中最消耗 CPU 资源的进程，以维持系统的整体性能，因此，随时监视系统的状态也是管理员的一项重要工作。

在 Linux 操作系统下，可在终端命令窗口中利用“top”命令监控系统的资源，如内存、交换分区、CPU 的使用率等。

命令格式: top [选项]

该命令各选项如表 1-7 所示。

表 1-7 “top” 令行选项

命令行选项	描 述
b	使用批处理模式
c	列出程序时，显示每个程序的完整指令，包括指令名称、路径和参数等相关信息
d <间隔秒数>	设置 top 监控程序执行状况的间隔时间，单位为 s
i	执行 top 指令时，忽略闲置或是已成为 Zombie 的程序
n <执行次数>	设置监控信息的更新次数
q	持续监控程序执行的状况
s	使用保密模式，消除互动模式下的潜在危机
S	使用累计模式，其效果类似 ps 指令的“-S”参数

例如，显示本机操作系统资源耗费情况，此时可直接在终端命令窗口中输入“top”命令，按回车键后即可显示出系统中资源的使用情况，因为系统资源是无止境显示的，所以必需按快捷键“Q”终止监视系统，其操作方法如下：

```
[root@rh01 ~]# top
top - 15:22:36 up 7:32, 2 users, load average: 0.45, 0.21, 0.14
```

```
Tasks: 81 total,    2 running,    79 sleeping,    0 stopped,    0 zombie
Cpu(s):  3.8% us,    6.1% sy,    0.3% ni, 89.7% id,  0.0% wa,    0.2% hi,  0.0% si
Mem:      759348k total,  362220k used,  397128k free,    41616k buffers
Swap:     1540088k total,    0k used,  1540088k free,    195232k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3872	root	15	0	41448	18m	6696	S	5.7	2.5	24:19.23	X
4119	root	25	10	30128	16m	9.9m	R	1.9	2.2	14:38.57	rhn-applet-gui
4938	root	15	0	3200	868	692	R	1.9	0.1	0:00.04	top
1	root	16	0	2164	552	472	S	0.0	0.1	0:00.90	init
2	root	34	19	0	0	0	S	0.0	0.0	0:00.01	ksoftirqd/0
3	root	5	-10	0	0	0	S	0.0	0.0	0:00.41	events/0
4	root	5	-10	0	0	0	S	0.0	0.0	0:00.05	khelper
5	root	15	-10	0	0	0	S	0.0	0.0	0:00.00	kacpid
18	root	5	-10	0	0	0	S	0.0	0.0	0:00.23	kblockd/0
36	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pdflush
37	root	15	0	0	0	0	S	0.0	0.0	0:02.68	pdflush
39	root	11	-10	0	0	0	S	0.0	0.0	0:00.00	aio/0
19	root	15	0	0	0	0	S	0.0	0.0	0:00.00	khubd
38	root	25	0	0	0	0	S	0.0	0.0	0:00.00	kswapd0
185	root	25	0	0	0	0	S	0.0	0.0	0:00.00	kseriod
299	root	24	0	0	0	0	S	0.0	0.0	0:00.00	scsi_eh_0
314	root	6	-10	0	0	0	S	0.0	0.0	0:00.00	kmirrord

按快捷键“Q”终上监视系统。

```
[root@rh01 ~]#
```

在 top 命令返回的信息中，第 1 行与“w”命令所返回的结果是相同的，其中包括 4 个字段：系统当前的时间，如 15:22:36；运行时长，up 7:32，系统当前已运行了 7 小时 32 分；登录用户数，2 users 表示当前系统中登录用户的总数为 2 个用户；平均负载指标，load average: 0.45、0.21、0.14，这 3 组数字表示系统在过去 1、5、10 分钟内的平均负载程序，其值越少，表示系统的负载越低，系统的运行就会更流畅。第 2 行显示所有进程的执行情况。第 3 行表示 CPU 的使用情况。第 4 行和第 5 行表示内存和交换分区的使用情况，其他内容就是正在执行的各个进程列表。

(1) 监视指定的用户

若需监视指定的用户账号资源使用情况，则可在 top 命令的执行过程中按快捷键“U”，当系统提示输入用户账号时，再根据需要输入需监视的用户账号名称即可，按回车键将在进程列表中只显示该用户账号所执行的进程。具体代码设置如下：

```
[root@rh01 ~]# top
top - 16:00:00 up 8:09, 2 users, load average: 0.00, 0.07, 0.08
Tasks: 81 total, 1 running, 80 sleeping, 0 stopped, 0 zombie
Cpu(s):  3.7% us,  6.3% sy,  0.0% ni, 90.0% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:      759348k total,  364484k used,  394864k free,  42392k buffers
Swap:     1540088k total,    0k used,  1540088k free,  195240k cached
Which user (blank for all): root //按快捷键"U"后，在此处输入需监视的用户账号名
PID USER  PR    NI  VIRT  RES  SHR  S   %CPU  %MEM  TIME+  COMMAND
3872 root   15     0 41448  18m 6700  S   5.7  2.5 26:17.45 X
```