



UNIX Unleashed
Fourth Edition

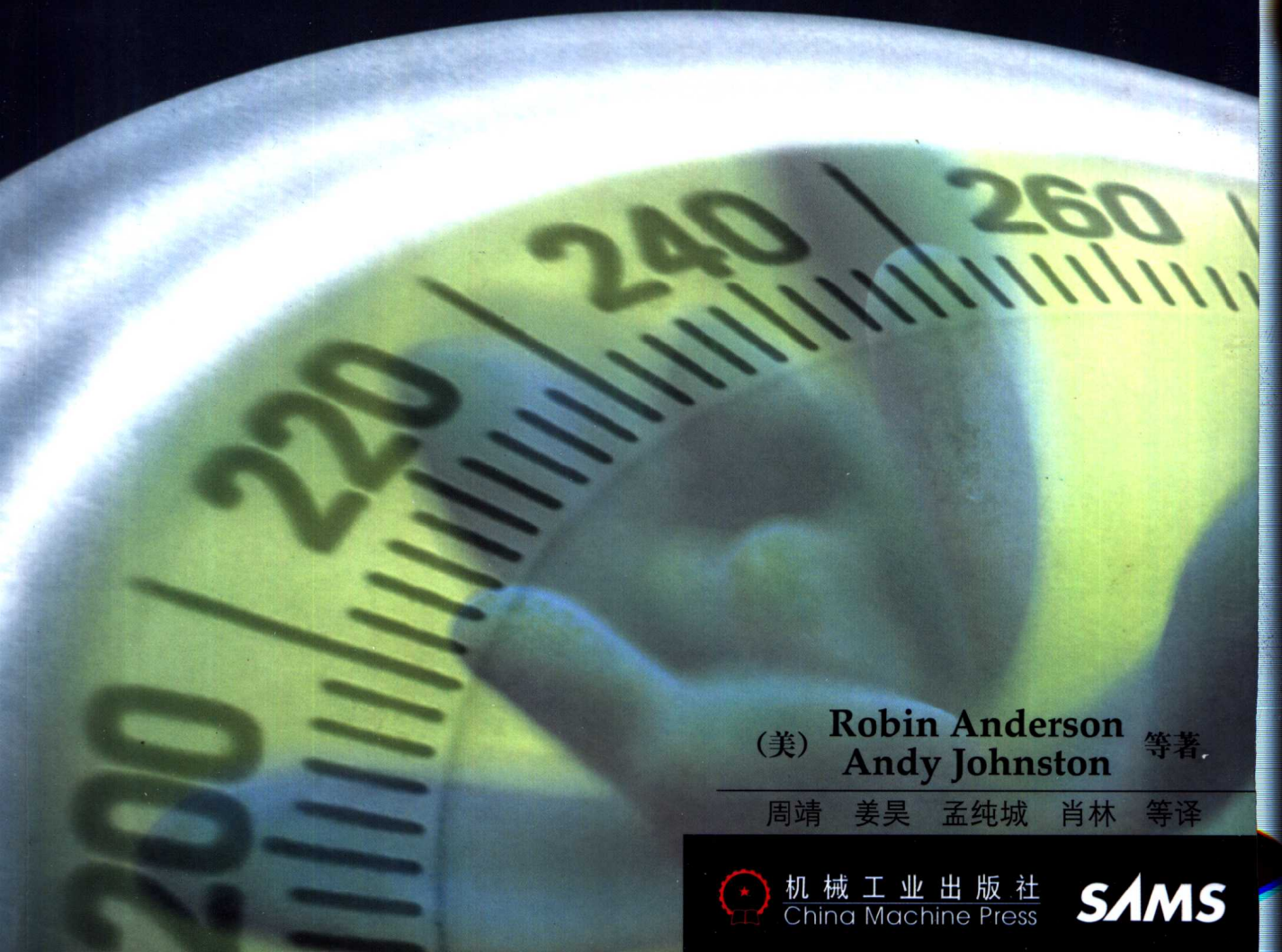


开发人员专业技术丛书

UNIX

技术内幕

(原书第4版)



(美) Robin Anderson 等著
Andy Johnston

周靖 姜昊 孟纯城 肖林 等译



机械工业出版社
China Machine Press

SAMS

开发人员专业技术丛书

UNIX技术内幕

(原书第4版)

(美) Robin Anderson 等著
Andy Johnston

周靖 姜昊 孟纯城 肖林 等译



机械工业出版社
China Machine Press

UNIX已被证明是Internet服务、数据库服务器和其他各种任务信息服务的一种灵活、高效而可靠的平台,随着UNIX系统的广泛部署,越来越急需大量有经验的系统安装、配置和维护人员,本书是该领域的名著,是专为那些想成为系统管理员的读者而写的。

本书是由十几位经验丰富的系统管理员编写的,内容涉及系统管理的方方面面,包括如何构建自己的网络入侵侦测系统、身份验证、加密技术、安全及Web服务的建立和维护等。通过阅读本书,能让一名普通的UNIX用户快速成长为一名初中级系统管理人员。

Robin Anderson, Andy Johnston, et al: UNIX Unleashed, Fourth Edition.

Authorized translation from the English language edition published by Sams, an imprint of Macmillan Computer Publishing U. S. A.

Copyright © 2002 by Sams Publishing.

All rights reserved.

Chinese simplified language edition published by China Machine Press, Copyright © 2002 by China Machine Press.

本书中文简体字版由美国麦克米兰公司授权机械工业出版社独家出版,未经出版者书面许可,不得以任何方式复制或抄袭本书内容。

版权所有,侵权必究。

本书版权登记号:图字:01-2002-0815

图书在版编目(CIP)数据

UNIX技术内幕(原书第4版)/(美)安德森(Anderson, R.)等著;周靖等译. -北京:机械工业出版社,2002.10

(开发人员专业技术丛书)

书名原文:UNIX Unleashed, Fourth Edition

ISBN 7-111-10931-7

I. U… II. ①安…②周… III. UNIX操作系统 IV. TP316.81

中国版本图书馆CIP数据核字(2002)第075673号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑:刘立卿

北京昌平奔腾印刷厂印刷·新华书店北京发行所发行

2002年10月第1版第1次印刷

787mm×1092mm1/16·50印张

印数:0 001-4 000册

定价:89.00元

凡购本书,如有倒页、脱页、缺页,由本社发行部调换

序

新版《UNIX技术内幕》在以前版本的基础上有了大量明显的改动。以前所有“新版”都只是进行一系列更新；但这一次，我们的目的是进行全面改革。面向的读者已从“UNIX用户”转变成了“系统管理员”(sysadmin)。采取的方法已从“什么是shell”转变成了“为什么要分页到交换空间”。本书不再深入讲解软件开发工具，而是全面讲述如何实现主机的安全。

本书并不是一份单纯的故障检测“核对表”。它并不是为那些需要修复一台个人机器的开发者提供的。它讲解的是：作为一名系统管理员，应该怎样以及为什么和在什么时候进行主要的日常工作。它能将一名普通用户提升为初中级系统管理员。和一本教科书不同，本书从头到尾都极具可读性。而且，它既兼具参考手册的功能，还无需像真正的参考手册那样阅读。本书是由UNIX系统管理员为同行撰写的，书中的所有建议和技巧都是由有丰富UNIX使用经验的人提供的。

事实上，本书具备其他许多同类书籍所没有的特点。就我个人的观点来看，那些书籍通常面向课堂教学。如果想查找一个特定的知识项，那些都是很好的参考手册。但是，这本书除了也能做到这一点之外，我觉得本书同那些书的差别在于，它还特别适合自己不时地自学，本书能教会读者如何管理完全使用UNIX机器的站点。

Hal Miller
SAGE前总裁

前 言

自UNIX诞生以来,“UNIX系统管理”领域在近30年的时间里,已有了长足的进展。到20世纪90年代,许多系统管理员还没有注意到自己从事的将是一项至关重要的职业。20世纪90年代初,Internet还是一种前途未卜的用于在各大研究机构之间进行通信的机制。1999年,Internet已成为各种新闻文章和金融投资中的一个热门话题。同时,Internet访问已成为商业和教育的一项基本需求。UNIX很快便证明自己是Internet服务、数据库服务器和其他几乎任何信息服务的一种灵活、高效而可靠的平台。UNIX系统的广泛部署,迫切需要大量有经验的人来安装、配置和维护它们,同时还要保证它们的灵活、高效和可靠。今天,像这样的需要不仅仍然存在,而且还在快速增长着。

与此同时,受过良好培训的、可靠的系统管理员仍然呈短缺现象。极少有大学提供有关这一主题的课程(不管什么级别)。即使提供了这样的课程,也很少由真正有经验的系统管理员来讲授(当然也有一些令人高兴的特例,而我们希望这将演变成一种良好的发展趋势)。人们经常从其他计算机相关领域不经意地“漂流”到我们的领域。例如有的人在自己的PC上安装了一个免费的UNIX(比如Linux),用它取代Microsoft操作系统,然后通过它自学了一些UNIX的东西。有时,负担过重的系统管理员为一名软件开发者提供了root访问权限,让他修复自己的系统,而后这个软件开发者最终变成了一名系统管理员。然而,所有这些都不是正规的方法。正规的方法是先当一名“学徒”,从一个或多个系统管理员那里不断地学一些东西。何时可以结束学徒生涯没有正式的标志。通常一旦学徒获得一份正式工作,而且没有更有经验的系统管理员提供帮助(通常根本没有其他系统管理员),便标志着你的学徒生涯结束了,可以“学成下山”,自己带徒弟了。

本书便主要是为这些“学徒”而设计的。我们假定你作为一名用户,已对UNIX有了一定程度的认识——尽管为了让读者更熟悉这个操作系统,许多章节探讨的都是基础知识。根据“系统管理员协会”(SAGE)的分级系统,我们假定你预备成为一名Level 2级别的系统管理员[注释1]。本书各章在很大程度上反映了作为一名这样的系统管理员所需要担负的不同职责。每一章都试着在理论和实践之间取得一种平衡,既让读者知道如何执行现在的任务,同时又能掌握足够的背景知识,以便进行更深层次的学习和更熟练地解决一些事先难以预料的问题。此外,本书还包括了一些额外的材料,这些材料是一些较有经验的系统管理员所感兴趣的。

本书所有作者,其中包括对每一章进行审阅的技术编辑,都是有经验的系统管理员。我们的希望是,这本书能建立起某种形式的“学徒”体系,这里面包含了由每一位作者提供的大量解释和建议。尽管所有作者在写作时都要遵守一些共同的原则,但我们仍然尽可能地保持了他们个人的见解。

在不同章之间,可能出现不连续的情况;不同的作者相互间也可能产生矛盾。如果这些矛盾是基于个人的意见和经验,那么本书不会尝试化解这些矛盾。在最终成为一名真正的系统管理员的道路上,这会成为你的一种宝贵的经验。

UNIX存在许多变种。但是，我们并不打算讨论每一种（这必定会失败）；我们只选择了其中两种作为例子：Red Hat Linux 7.1和Sun公司的Solaris 8。这两个版本都是在2001年夏天发布的，一个流行于免费世界，另一个则流行于商业世界。对本书讲解的基本概念只需做少量修改，或根本不用修改，即可应用于其他形式的UNIX。本书为了讲解如何进行实际操作，分别利用Red Hat Linux和Solaris的最新版本来提供一个统一的参考平台，所有讨论都是基于它们而展开。

本书对新的系统管理员来说可以作为一个有用的学习工具使用，而对已有大量经验的系统管理员来说可以从中找到一些有价值的参考资料。

注释1 在SAGE分级系统中，Level 2是指“初级”（Junior）系统管理员。要了解这个分级系统的详情可参见<http://www.usenix.org/sage/jobs/jobs-descriptions.html>。

本书原版书书号：ISBN 0-672-32251-X

原出版社联系方式：

传真：317-581-4770

电子邮件：[feedback @ sampublishing.com](mailto:feedback@sampublishing.com)

邮寄地址：

Jeff Koch, Associate Publisher

Sams Publishing

201 West 103rd Street

Indianapolis, IN 46290 USA

目 录

序
前言

第一部分 基本操作

第1章 启动和关机	1
1.1 介绍	1
1.2 五步引导过程概述	1
1.3 第1步：固件——硬件自识别	1
1.3.1 固件的一些实例	2
1.3.2 固件的工作	3
1.3.3 固件设置	3
1.3.4 固件的机制和特点	4
1.4 第2步：bootloader——载入OS	12
1.4.1 bootloader的工作	12
1.4.2 bootloader的机制和特点	12
1.5 第3步：内核——初始化和控制转移	13
1.5.1 内核的工作	14
1.5.2 内核的机制和特点	15
1.6 第4步：init进程和初始化脚本	16
1.6.1 init的工作	17
1.6.2 init的机制和特点：inittab	17
1.6.3 init的机制和特点：init脚本	20
1.7 第5步：交给管理员——其他杂项	22
1.8 系统关闭和更改init级别	23
1.9 dmesg显示的Red Hat引导顺序	23
1.10 dmesg显示的Solaris引导顺序	26
1.11 最佳操作	29
1.12 在线参考	30
1.13 注释	30
第2章 管理磁盘硬件	32
2.1 介绍	32
2.2 物理设备	32

2.3 独立于OS的硬件通信标准	33
2.3.1 串行通信简述	33
2.3.2 FireWire (IEEE 1394) 简述	33
2.3.3 USB简述	34
2.3.4 ATAPI简述	34
2.3.5 并行通信简述	34
2.3.6 IDE / ATA	35
2.3.7 SCSI	37
2.4 了解你的系统	48
2.4.1 命名约定	48
2.4.2 让OS报告它识别到的硬件	49
2.5 添加 / 删除磁盘 (和其他设备)	52
2.5.1 添加设备	53
2.5.2 删除设备	55
2.6 最佳操作	56
2.7 在线参考	57
2.8 注释	59
第3章 文件系统管理	62
3.1 介绍	62
3.2 合理划分磁盘空间	62
3.2.1 虚拟设备：分区	62
3.2.2 逻辑结构：文件系统	66
3.2.3 划分原则	69
3.2.4 分区的技术细节	74
3.3 文件系统的进一步讨论	76
3.3.1 文件系统组成部分管理员须知	77
3.3.2 文件系统类型	85
3.4 管理本地文件系统	90
3.4.1 本地文件系统创建	90
3.4.2 本地文件系统可用性管理	91
3.4.3 空间管理	96
3.5 可移动存储介质	100

3.6 最佳操作	101	6.3 计时: ntp	178
3.7 在线参考	102	6.3.1 ntp结构	179
3.8 注释	102	6.3.2 在系统中配置ntp	179
第4章 用户管理	105	6.4 配置系统的日志安全	180
4.1 身份、实体、权力的定义	105	6.4.1 保护本地日志配置	181
4.2 在本地存储基本用户信息	107	6.4.2 保护远程日志配置	182
4.2.1 /etc/passwd	107	6.5 使用syslog记录应用程序日志	185
4.2.2 /etc/group	109	6.6 syslog以外的特定应用程序日志	186
4.2.3 /etc/shadow	111	6.7 syslog以外的标准系统日志	186
4.3 在网络上共享用户(或其他人的)信息	115	6.8 跨平台记录syslog的其他方式	190
4.3.1 rsync,rdist,cfengine	115	6.9 日志分析和报告	190
4.3.2 NIS(被NIS+取代)	116	6.9.1 日志分析	192
4.3.3 LDAP	127	6.9.2 实时/准实时警告和通知	194
4.4 创建帐户	129	6.9.3 日志循环和保存	196
4.4.1 策略	129	6.10 最佳操作	198
4.4.2 技术问题	133	6.11 在线参考	199
4.5 删除帐户	136	6.12 注释	200
4.5.1 策略	136	第7章 身份验证	201
4.5.2 技术问题	138	7.1 介绍	201
4.6 最佳操作	140	7.2 身份验证的定义	201
4.7 在线参考	142	7.3 UNIX密码验证概述	201
4.8 注释	143	7.4 好的密码和糟糕的密码	202
第5章 网络应用	147	7.4.1 Linux Red Hat 7.1中的密码检查规则	203
5.1 介绍	147	7.4.2 Solaris 2.8中的密码检查规则	203
5.2 TCP/IP	147	7.4.3 Linux Red Hat 7.1中的密码有效期	205
5.2.1 Internet是网络的网络	147	7.4.4 Solaris 2.8中的密码有效期	206
5.2.2 IP地址	150	7.5 基本UNIX密码实现	206
5.2.3 IP配置与故障排除命令	156	7.5.1 Linux Red Hat 7.1中的密码散列	207
5.2.4 服务与端口	162	7.5.2 Solaris 2.8中的密码散列	208
5.3 最佳操作	166	7.5.3 Linux Red Hat 7.1和Solaris 2.8的 本地密码文件格式	208
5.4 在线参考	167	7.5.4 Linux Red Hat 7.1中的shadow 密码项域	208
第6章 日志	169	7.5.5 Solaris 2.8中的shadow密码项域	208
6.1 介绍	169	7.5.6 在Linux Red Hat 7.1中编辑密码文件	209
6.2 标准UNIX系统日志: syslog	169	7.5.7 在Solaris 2.8中编辑密码文件	209
6.2.1 BSD系统日志	169	7.5.8 Linux Red Hat 7.1中的newusers程序	209
6.2.2 syslog内部模式	173		
6.2.3 syslog.conf	174		

7.6 密码破解	210	8.3.5 第5步: 发布源代码补丁	235
7.7 网络信息系统	211	8.3.6 第6步: 发布二进制形式的 (供应商) 补丁	235
7.7.1 Linux Red Hat 7.1中的nsswitch.conf 文件	213	8.3.7 第7步: 人们应用了补丁	236
7.7.2 Solaris 2.8中的nsswitch.conf文件	213	8.4 审查服务	236
7.8 其他UNIX密码算法	214	8.4.1 第一部分: inetd/xinetd审查	236
7.8.1 Linux Red Hat 7.1中的散列算法	214	8.4.2 第二部分: 使用netstat、lsof和一些 检查工具跟踪其余信息	243
7.8.2 Solaris 2.8中的散列算法	214	8.4.3 定期检查完整性	253
7.9 其他身份验证方案	215	8.5 安全的网络守护进程替代产品	253
7.10 ssh和身份验证	217	8.5.1 TCP Wrappers (tcpd)	253
7.10.1 Linux Red Hat 7.1的OpenSSH	217	8.5.2 Secure Shell (ssh)	254
7.10.2 Solaris 2.8中的ssh选项	218	8.5.3 安全portmapper (portmap/rpcbind)	254
7.10.3 Kerberos	220	8.6 审查密码	255
7.11 集成PAM	220	8.7 使用Bastille Linux实现自动化锁定 Linux/UNIX	256
7.11.1 Linux Red Hat 7.1中的PAM	223	8.7.1 帐户安全 (AccountSecurity.pm)	257
7.11.2 Solaris 2.8中的PAM	224	8.7.2 文件权限 (FilePermissions.pm)	257
7.12 ident服务器和身份验证	224	8.7.3 关闭各种守护进程 (Miscellaneous- Daemons.pm)	258
7.12.1 Linux Red Hat 7.1的identd守护进程	225	8.7.4 引导安全 (BootSecurity.pm)	258
7.12.2 Solaris 2.8的identd守护进程	225	8.7.5 添加功能增强的日志 (logging.pm)	258
7.13 最佳操作	225	8.7.6 配置各种PAM设置 (Configure- MiscPAM.pm)	258
7.14 参考	226	8.7.7 禁用用户工具 (DisableUserTools.pm)	258
第8章 系统安装后的保护措施	228	8.7.8 打印 (printing.pm)	259
8.1 必须加强系统	228	8.7.9 Apache (Apache.pm)	259
8.2 安装补丁: 过程与策略	229	8.7.10 DNS (DNS.pm)	259
8.2.1 安装Solaris时	230	8.7.11 FTP (FTP.pm)	259
8.2.2 在Red Hat Linux系统中安装补丁	231	8.7.12 sendmail (sendmail.pm)	259
8.2.3 Mandrake Linux	232	8.7.13 安全的inetd配置 (SecureInetd.pm)	260
8.2.4 安装补丁的综合考虑	232	8.7.14 tmp目录保护 (TMPDIR.pm)	260
8.3 除了安装补丁以外, 为什么还需要 其他措施	232	8.7.15 防火墙 (firewall.pm)	260
8.3.1 第1步: 有人在程序中发现了一个 bug	232	8.7.16 端口扫描攻击检测程序 (psad.pm)	260
8.3.2 第2步: 有人意识到这个bug是个 安全漏洞	233	8.8 使用其他工具实现自动化锁定 Solaris/UNIX	261
8.3.3 第3步: 有人指出如何利用这个 漏洞	234	8.8.1 Titan	261
8.3.4 第4步: 有人可能会将漏洞的信息 公开	234		

8.8.2 Solaris专用的加强工具: YASSP 和jass	264
8.9 最佳操作	264
8.10 资源	265
8.11 注释	265
第9章 日常系统管理	268
9.1 概述	268
9.2 主动的系统管理员	268
9.2.1 成为root的重要性	268
9.2.2 进程管理	269
9.2.3 查看系统日志	273
9.2.4 检查分区使用情况	274
9.2.5 赞成和反对使用配额的理由	274
9.2.6 系统是何时启动的	275
9.2.7 所有程序都在运行吗	275
9.2.8 备份完成了吗	276
9.2.9 成为系统环境专家	277
9.3 反应式管理	277
9.3.1 降低防范	277
9.3.2 排除故障	278
9.3.3 解释用户请求	279
9.3.4 删除的mailspool	281
9.3.5 “新人员需要帐户”的情况	283
9.3.6 “需要为Web页组和邮件组创建 帐户”的情况	283
9.3.7 “<在此插入应用程序名>有问题” 的情况	284
9.3.8 需要新硬件	284
9.3.9 需要新软件/许可证	285
9.4 最佳操作	285
9.5 在线参考	286

第二部分 关键子系统

第10章 X Window系统	287
10.1 介绍	287
10.2 X目录结构	287
10.2.1 XFree86风格	287

10.2.2 Solaris风格	287
10.3 X 发行版导航	287
10.4 非基础性的基础知识	289
10.5 安全性	290
10.5.1 基于主机的授权	290
10.5.2 xauth: 更强的验证方法	291
10.5.3 其他验证方案	293
10.5.4 启动安全验证	293
10.6 自定义环境(以用户身份)	294
10.6.1 .xsession	294
10.6.2 资源	295
10.6.3 键映射	298
10.6.4 实用应用程序: xkeycaps	299
10.6.5 窗口管理器和环境	300
10.7 系统级X环境	301
10.7.1 xdm	301
10.7.2 X字体	304
10.7.3 字体存储方式	306
10.7.4 字体存储位置	307
10.7.5 字体路径	307
10.8 参考	307
第11章 名称服务(DNS)	309
11.1 介绍	309
11.1.1 域和子域	309
11.1.2 BIND	310
11.1.3 名称服务基本原理	310
11.1.4 服务器与客户端的区别	313
11.1.5 FQDN	313
11.2 客户端(即解析程序)	313
11.3 名称服务器	315
11.3.1 主名称服务器和从属名称服务器	315
11.3.2 配置BIND启动	316
11.3.3 配置区	317
11.3.4 维护DNS	324
11.3.5 仅起高速缓存作用的名称服务器	325
11.4 工具和故障排除	325
11.4.1 nslookup	325

11.4.2 dig	326	13.3.1 Samba概述	391
11.5 最佳操作	326	13.3.2 服务器设置	394
11.6 在线参考	326	13.3.3 Samba客户端设置	404
第12章 邮件	328	13.3.4 Samba故障排除和性能调节	405
12.1 UNIX邮件处理	328	13.4 最佳操作	406
12.1.1 UNIX邮件投递代理	329	13.5 在线参考	406
12.1.2 UNIX邮件传输代理	331	第14章 打印	408
12.1.3 UNIX邮件用户代理	334	14.1 介绍	408
12.1.4 SMTP协议	336	14.2 后台打印系统	409
12.2 sendmail MTA包	344	14.2.1 将作业加入队列	409
12.2.1 配置sendmail	345	14.2.2 过滤作业	411
12.2.2 使用m4宏预处理程序	345	14.2.3 命令	412
12.3 UNIX邮件客户端	347	14.3 System V下的打印	412
12.3.1 UNIX工作站邮件配置	347	14.3.1 配置文件	412
12.3.2 使用PINE阅读和发送邮件消息	348	14.3.2 命令	413
12.4 服务器主题	349	14.3.3 添加本地打印机配置	413
12.4.1 专用域邮件集中器	349	14.3.4 在客户端添加远程打印机配置	414
12.4.2 使用procmail作为本地邮件 投递代理	351	14.3.5 删除打印机配置	414
12.4.3 SMTP验证	355	14.3.6 修改默认目标	414
12.4.4 IMAP服务器和POP服务器	358	14.3.7 提交打印作业请求	415
12.4.5 IMAP和POP安全	362	14.3.8 状态信息	415
12.5 最佳操作	363	14.3.9 取消打印作业请求	415
12.6 在线参考	364	14.3.10 终止/启动后台队列	415
第13章 文件共享	365	14.3.11 终止/启动打印	415
13.1 文件共享概述	365	14.3.12 将作业转移到另一个目标	416
13.1.1 文件共享的概念	365	14.3.13 记帐	416
13.1.2 文件共享的历史	366	14.4 BSD系统下的打印	416
13.1.3 文件共享的现状	367	14.4.1 配置文件	416
13.1.4 当网络策略不支持同时使用文件 共享时的共享技术	369	14.4.2 命令	416
13.2 设置NFS	370	14.4.3 添加本地打印机配置	417
13.2.1 NFS概述	370	14.4.4 在客户端添加远程打印机配置	418
13.2.2 服务器设置	374	14.4.5 删除打印机配置	419
13.2.3 客户端设置	381	14.4.6 修改默认目标	419
13.2.4 NFS性能调节和故障排除	386	14.4.7 提交打印作业请求	419
13.3 设置Samba	390	14.4.8 状态信息	419
		14.4.9 取消打印作业请求	419
		14.4.10 终止/启动后台队列	420

14.4.11 终止/启动打印	420	15.3.1 Apache须知	432
14.4.12 记帐	420	15.3.2 获取源代码	433
14.5 LPRng下的打印	420	15.3.3 配置源代码	433
14.5.1 配置文件	420	15.3.4 生成Apache	434
14.5.2 命令	421	15.3.5 安装新服务器	434
14.5.3 添加本地打印机配置	422	15.4 配置Apache	436
14.5.4 在客户端添加远程打印机配置	423	15.4.1 配置文件	436
14.5.5 删除打印机配置	423	15.4.2 全局配置指令	437
14.5.6 修改默认目标	423	15.4.3 配置默认服务器	439
14.5.7 提交打印作业请求	423	15.4.4 配置虚拟服务器	443
14.5.8 状态信息	423	15.5 服务器端嵌入	444
14.5.9 取消打印作业请求	424	15.5.1 使用SSI的原因	444
14.5.10 终止/启动后台队列	424	15.5.2 在Apache中配置SSI	444
14.5.11 终止/启动打印	424	15.5.3 测试SSI示例	445
14.5.12 将作业转移到另一个目标	424	15.6 配置MIME	446
14.5.13 记帐	424	15.7 CGI脚本	448
14.6 CUPS下的打印	424	15.7.1 启用CGI	448
14.6.1 配置文件	424	15.7.2 测试配置	449
14.6.2 命令	425	15.8 使用Apache模块添加特性	449
14.6.3 添加本地打印机配置	425	15.8.1 Apache模块的定义	449
14.6.4 在客户端添加远程打印机配置	428	15.8.2 标准模块	450
14.6.5 删除打印机配置	428	15.8.3 附加模块	451
14.6.6 修改默认目标	428	15.8.4 模块配置指令	451
14.6.7 提交打印作业请求	428	15.9 运行改变根目录的 (chrooted) Web 服务器	452
14.6.8 状态信息	429	15.9.1 运行改变根目录服务器的原因	453
14.6.9 取消打印作业请求	429	15.9.2 设置chroot环境	453
14.6.10 终止/启动后台队列	429	15.10 参考	454
14.6.11 终止/启动打印	429	15.11 最佳操作	454
14.6.12 将作业转移到另一个目标	429	第16章 备份	455
14.6.13 记帐	429	16.1 介绍	455
14.6.14 打印机配置	429	16.2 备份的步骤和条件	456
14.7 最佳操作	429	16.2.1 预算	459
14.8 在线参考	430	16.2.2 系统或数据的关键性	459
第15章 基本Web服务	431	16.2.3 了解可能遇到的恢复类型	460
15.1 介绍	431	16.2.4 恢复速度	462
15.2 提供基本Web服务	431	16.2.5 保存	462
15.3 获取并安装Apache	432		

16.2.6 离场存储	462	18.1 介绍	520
16.2.7 中央专用备份服务器	463	18.2 数据库综述	520
16.2.8 完成配置——备份窗口和其他 约束	463	18.2.1 什么是数据库	520
16.2.9 选择备份介质	463	18.2.2 系统结构	523
16.2.10 监视的重要性	464	18.2.3 数据库就是操作系统	524
16.2.11 还原/恢复测试	464	18.2.4 数据库为什么要吞噬如此多的 资源	527
16.2.12 配套的系统配置文档	465	18.3 挑选一家数据库厂商	533
16.2.13 指定备份计划	465	18.3.1 平台选择	533
16.2.14 书写备份策略	466	18.3.2 支持大型系统还是支持小型系统	533
16.2.15 改进系统	467	18.3.3 性能和复杂性	533
16.3 备份与恢复	467	18.3.4 支持和接口	534
16.3.1 常用嵌入工具	467	18.3.5 价格和厂商可用性	534
16.3.2 免费工具	468	18.4 Oracle数据库综述	535
16.3.3 商业化产品	479	18.4.1 机器设置	536
16.4 最佳操作	480	18.4.2 基本结构	539
16.5 在线参考	481	18.4.3 安装过程	542
16.6 总结	481	18.4.4 数据库环境和文件配置	544
		18.4.5 备份	547
		18.4.6 MySQL概述	549
		18.5 总结	552
第三部分 应用程序和工具		第19章 自动化	554
第17章 开放源码软件管理	483	19.1 介绍	554
17.1 介绍	483	19.2 脚本编制	554
17.1.1 有关自由软件的更多话题	483	19.2.1 解释型和编译型语言	554
17.1.2 一些基本的自由软件	484	19.2.2 其他脚本编制语言: Expect、 Perl等	560
17.1.3 在哪里查找自由和开放源码软件	484	19.3 调度和定期执行的进程	563
17.1.4 厂商提供的“自由”软件	485	19.3.1 at: 面向未来事件的一次性调度	563
17.1.5 应当选择源码还是二进制形式	485	19.3.2 cron: 定期调度	564
17.1.6 安装二进制版本	486	19.3.3 anacron: 可拦截的定期调度	565
17.1.7 Solaris包	488	19.3.4 cron的例子	565
17.2 生成源码分发	493	19.4 用cfengine进行自动化配置管理	567
17.2.1 需求	494	19.4.1 工作原理	568
17.2.2 生成一个软件包: OpenSSH	495	19.4.2 用网络分发cfengine的配置文件	569
17.2.3 生成软件	500	19.4.3 一个cfengine命令实例——tidy:	569
17.2.4 高级软件配置	502	19.4.4 示范cfengine.conf文件	571
17.3 管理软件安装	511		
17.4 注释	519		
第18章 数据库	520		

19.5 改进自动化技术的提示	573
19.5.1 再教育	573
19.5.2 良好工程	574
19.6 对自动化价值的解释	574
19.7 最佳操作	575
19.8 在线参考	575
第20章 高级Web服务	576
20.1 提供高级Web服务	576
20.1.1 动态与静态站点	576
20.1.2 站点所用软件	578
20.1.3 运行时间、可靠性和风险	582
20.1.4 把用户看成测试者	582
20.1.5 集成和系统级设置	583
20.1.6 成本(以及由管理层决定的事情)	583
20.1.7 不便共享时:专用服务器的情况	588
20.2 脚本语言	588
20.3 数据库	592
20.4 语言	594
20.4.1 PHP	594
20.4.2 Perl	597
20.4.3 Java	599
20.4.4 JSP	600
20.4.5 ASP	600
20.4.6 JavaScript	601
20.4.7 身份验证、状态保存和Cookie	603
20.4.8 服务器身份验证	605
20.4.9 状态变量	607
20.5 安全性	607
20.5.1 系统安全性	608
20.5.2 访问:谁有权用它和在哪里使用	608
20.5.3 污染	609
20.6 后期工作	610
20.6.1 人/页	611
20.6.2 趋势分析	612
20.6.3 负载问题	612
20.6.4 重新设计和报酬	613
20.6.5 干扰和准确的用户数据	613

20.6.6 可视化和使用情况	614
20.6.7 Web广告	615

第四部分 改善系统管理

第21章 安全性	617
21.1 介绍	617
21.2 为什么要担心	617
21.3 复杂系统的危险性	618
21.4 构建一个威胁模型	619
21.5 安全哲学	621
21.5.1 我们完了	621
21.5.2 两种安全哲学	621
21.6 安全就是麻烦	623
21.6.1 备份	623
21.6.2 系统加固	623
21.6.3 系统补丁	625
21.6.4 阅读日志	626
21.6.5 侦测问题	627
21.7 配置管理	629
21.8 策略	630
21.8.1 策略理论	630
21.8.2 规程	631
21.8.3 管理层要买帐	632
21.9 道德	632
21.10 总结	634
21.11 最佳操作	634
21.12 资源	634
第22章 入侵侦测	636
22.1 介绍	636
22.2 网络的危险性	636
22.3 网络协议概念	637
22.3.1 封装	637
22.3.2 分层	638
22.4 堆栈	639
22.4.1 ISO OSI七层模型	639
22.4.2 TCP/IP模型	640
22.5 探索TCP/IP协议	656

22.5.1 缓冲区溢出	656
22.5.2 端口扫描	656
22.6 正签名	657
22.7 负签名	657
22.8 Snort	659
22.8.1 安装Snort	659
22.8.2 测试Snort	661
22.9 NIDS	665
22.10 最佳操作	674
22.11 在线参考	675
第23章 需求分析和性能监视	676
23.1 需求分析	676
23.1.1 资源	677
23.1.2 工作目标	677
23.1.3 需求分析驱动设计	678
23.1.4 需求分析中的注意事项	678
23.2 性能监视	679
23.2.1 找出瓶颈	679
23.2.2 系统整体性能状态	680
23.3 容量展望与计划	693
23.3.1 建立计划表	694
23.3.2 指定替换部件	694
23.3.3 维持灵活性	694
23.4 最佳操作	695
23.5 在线参考	695
第24章 与人相处	696
24.1 赢得尊重	696
24.2 用户想要什么	696
24.3 做一名有远见的管理员	697

24.3.1	如何教用户	698
24.3.2	让他人更能干	698
24.3.3	如何教老板	700
24.3.4	提前维护	701
24.4	成功的仪表	701
24.5	与其他管理员相处	702
24.5.1	指导	703
24.5.2	新上岗的管理员须知	705
24.6	研讨会和协会	705
24.6.1	加入Usenix和SAGE	706
24.6.2	和志同道合者聊一聊	708
24.7	编写文件的好处	709
24.8	管理性策略	711
24.8.1	领导能力	712
24.8.2	制定章程	714
24.9	获取所需资源	715
24.10	好的系统管理员同时也是好人	718
24.11	你不可能取悦每个人	718

第五部分 附 录

附录A	高级安装步骤	721
附录B	从磁盘到文件系统	726
附录C	用户创建核对表	737
附录D	二进制、十六进制小结	739
附录E	UNIX密码系统	747
附录F	方便的命令	758
附录G	参考资料	765
附图	SCSI故障诊断流程图	

第一部分 基本操作

第1章 启动和关机

1.1 介绍

写作本书时，我假定读者会在桌子上摆好这本书，附近有一台刚安装好了操作系统的机器，而且脸上露出了期待的神情（也可能是一种受到挫败的神情——有时这是很难辨别的）。当然，如果面前摆的是一台裸机，也不要绝望。附录A“高级安装步骤”提供了简明的安装指南，可以指导读者一步一步安装Red Hat和Solaris。完成安装后，再回到这里接着往下阅读。

现在你肯定已经有了一台安装好的机器了，惟一关心的便是如何操作它。我们将从最基本的引导过程讲起。没有它，做其他一切都是不可能的。更重要的是，引导过程就是简单意义上的UNIX；通过它能看到各种不同的组件和设计模式（它们构成了UNIX的全部）。本书剩下的部分则集中探讨操作系统（OS）的管理。但在这里，我们打算看一看OS本身，以及每次按下电源按钮之后，它是如何启动的。

1.2 五步引导过程概述

可将引导（启动）过程划分为5个主要步骤：

- 1) 固件：硬件自识别（PROM / BIOS）。
- 2) bootloader（自举操作系统载入器）：载入OS（LILO / bootblk）。
- 3) 内核：初始化和控制转移。
- 4) init和初始化脚本。
- 5) 交给管理员：其他杂项。

本章后面会详细讲解每一个步骤。为理解这个过程，关键在于要认识到，它其实是对功能的一种分层。换言之，每个步骤都在系统的当前状态上，添加了一个附加的功能层。

第一步是完全基于硬件的：打开电源，让机器进行自查和自检。然后添加逻辑层，包括内核、系统进程等等。这个过程也可想像成是将系统控制权从硬件转交给软件。

所以，让我们先来看看最低的一层——硬件。这里是插接电源线，开关电源的地方。因此，电力和电源、插头和接触点等等，才是你在此应当关注的重点。为了让后续步骤正常进行，先让它们工作起来是绝对必要的先决条件。

1.3 第1步：固件——硬件自识别

假定已成功地接好了电源，并打开了电源开关。现在，机器已经打开，并正确地将电力分布到了各个部件，这样便进入了第1步，即固件阶段。

固件是一系列特殊的指令，介于硬件和软件层之间，负责这两者之间的相互传译。尽管听起来似乎是一件微不足道的工作，但它实际起着举足轻重的作用：固件传译的不仅仅是语言，它还要传译核心元素。硬件理解电子脉冲；软件（在其最基本的级别）理解1和0的数据流；固件是两者的一种合成，在硬件中永久（或半永久）地嵌入了软件形式的例程。它代表了用户同计算机进行交互的最基本的级别（原始的硬件插拔动作除外）。

1.3.1 固件的一些实例

在同固件打交道的过程中，可能会遇到以下术语：

- BIOS。
- PROM / EPROM / EEPROM。
- NVRAM。
- CMOS。

在详细讲解它们之前，先来看看它们的共同特点：

- 所有实例都是非易失性的内存芯片，PC和Sun系统均采用。
- 所有都采取与OS无关的技术。它们的设计和运行独立于其中所存放的内容。
- 所有都具有类似的功能：维持基本的、简单的软件和驱动程序，以及它们相关的一套参数。还提供了对键盘、显示器和硬盘的基本访问。
- 所有都采取了专门的设计，在出现磁盘 / 外设故障时，保证本身仍然可用，且不会被破坏；即便不访问硬盘或移动式磁盘，它们存储的程序也能运行。
- 所有都容纳着bootloader程序（参见后面的1.4节）。

1. BIOS

BIOS表示“基本输入 / 输出系统”（Basic Input/Output System），通常集成到PC主板和PC扩展卡上（比如显卡和SCSI卡）。要查看和修改BIOS设置，通常要使用一系列基于文本的菜单屏幕，而且只能在引导时才能访问。

2. PROM

PROM表示“可编程只读存储器”（Programmable Read-Only Memory），并具有以下三种形式：

WORM（一次写，多次读）：这是一种标准设备，即使在重新引导或关闭电源后，信息仍可保留。任何能像这样保留信息的设备都称做是“非易失性”的。

EPROM（可擦除可编程只读存储器）：这是改进版的PROM。暴露在紫光灯下，即可擦除重写。Sun和其他许多公司一度曾大量使用这种类型的固件设备。它首次允许用户在升级固件的同时，不用抛弃存储过它的硬件。

EEPROM（电可擦除可编程只读存储器）：这是另一种改进版的PROM，可用低压充电器（而不是紫光灯）进行删除和重写。Sun目前采用的是这种芯片；不管删除错误设置还是在新版本固件发布后进行升级，都容易许多。另外，利用它可以方便地更改和保存设置；敲入命令后，系统会发送一个弱电流，对固件状态进行相应的更改。

3. NVRAM

NVRAM表示“非易失性随机存取存储器”（Non-Volatile Random-Access Memory）。它实际是一种复合设备，同时由EEPROM和普通RAM构成。加电时，PROM保存的内容会拷贝或映射（shadowed）到RAM中，以便更快地访问。对设置进行的任何修改都会写回EEPROM（所以需要那种特殊类型的PROM）。