

SAMS

Unix 系统管理

Unix System Management Primer Plus

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

〔美〕 Jeff Horwitz 著
祁 力 李敬群 王大鹏 译

Unix 系统管理

[美] Jeff Horwitz 著

祁 力 李敬群 王大鹏 译

人民邮电出版社

图书在版编目(CIP)数据

Unix 系统管理/(美)霍维茨(Horwitz, J.)著;祁力,李敬群,王大鹏译.
—北京:人民邮电出版社,2003.4

ISBN 7-115-10874-9

I. U... II. ①霍...②祁...③李...④王... III. UNIX 操作系统—系统管理 IV. TP316.81

中国版本图书馆CIP数据核字(2003)第007271号

版 权 声 明

Jeff Horwitz: Unix System Management Primer Plus(ISBN:0672323729)

Copyright © 2003 by Sams Publishing.

Authorized translation from the English language edition published by Sams.

All rights reserved.

本书中文简体字版由美国 **Sams** 出版公司授权人民邮电出版社出版 未经出版者书面许可,对本书任何部分不得以任何方式复制或抄袭
版权所有,侵权必究

Unix 系统管理

- ◆ 著 [美] Jeff Horwitz
译 祁力 李敬群 王大鹏
责任编辑 李 际
- ◆ 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 电子邮件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本: 787×1092 1/16
印张: 22
字数: 691千字 2003年4月第1版
印数: 1-5 000册 2003年4月北京第1次印刷

著作权合同登记 图字: 01-2002-2766号

ISBN 7-115-10874-9/TP·3193

定价: 36.00元

本书如有印装质量问题,请与本社联系 电话:(010)67129223

内 容 提 要

本书结合来自作者经验的实例,对 Unix 系统管理的基本要素进行全面而深入的阐述,内容涵盖 Unix 系统的设计、部署、维护和升级。全书共分四个部分,第一部分讲述系统规划过程;第二部分讲述系统维护;第三部分讲述系统优化、安全防护和系统自动化;第四部分讲述人的因素在 Unix 系统管理中的影响和作用。

本书是一本关于 Unix 系统管理的教程和参考指南,特别适合已经或准备成为 Unix 系统管理员的读者阅读。由于系统管理的许多基本要素是通用的,因此本书也适合其他系统管理员和科技人员阅读。此外,本书还可以帮助各种机构的管理人员和 IT 部门更好地分析机构内 IT 基础设施上的投资成效或应该如何在 IT 基础设施上投资。对于大专院校的计算机与信息技术专业的学生来说,本书亦可作为将所学知识投入实际应用的指南。

作者介绍

Jeff Horwitz 在过去的 8 年时间里一直从事系统管理员工作，目前他是 TargetRx 医药市场研究公司的生产系统经理。在加入 TargetRx 公司之前，他先后在国家级 Internet 服务提供商、大学以及软件公司工作过，这些经历使得他对各种类型的机构有了深入而独到的见解。他是一名活跃的 SAGE 和 Usenix 成员，已编写了许多得到广泛采用的 Perl 模块。Jeff 在密歇根大学获得了细胞和分子生物学学士学位，此外他还是一名 Sun 认证系统管理员。

本书献给

Mindy——本书的问世可以证明，每个隧道的尽头都会有一线光明。

致谢

首先我要感谢策划编辑 Katie Purdum 和项目编辑 Matt Purcell，感谢他们能够理解一个系统管理员同时作为一个作者所肩负的沉重压力。在本书的整个写作过程中，耐心是一笔宝贵的资产。我要对开发编辑 Lorna Gentry 和技术编辑 Dee-Ann LeBlanc 致以诚挚的谢意，他们为我提供了宝贵的输入工作，没有他们的努力，本书的出版是不可能实现的。我还要感谢如下机构和个人，感谢他们无私地贡献他们的见解和资源：George Broadfoot、Jeremy Eckenroth、Chad Glynn、Kevin Mahlendorf、Scott McMullan、Jason Prigge、Ed Targonski、Eric Weaver、Jeff Wheeler、Don Williams、Geoff Young、密歇根大学、Covad 通信公司、TargetRx 有限公司。最后，感谢我的父母 Larry 和 Fern，是他们不断的鼓励让我渡过了最艰难的时光。

前 言

很长时间以来，Unix 系统管理一直被很多人视为一种令人费解的技术，但是对于那些精通技术的“奇才”来说，他们是花费了大量的时间来学习 Unix 的复杂特性（包括那些神秘的系统命令、程序和相关的配置文件）才得以施展这些技术的。数不胜数的书籍、Web 站点、课程和参考资料都在试图使人们施展这一技术变得更容易，它们介绍了完成某项任务的各种各样的命令和应用程序。这些大量的 Unix 培训和文档所带来的结果是，很多人的确知道了如何在 Unix 系统上完成某项特定的任务。然而，仅仅靠参加几门课程的学习并不会使一个人成为一名优秀的系统管理员。

一个真正的系统管理员除了做例行的系统维护性工作之外，还必须能做更多的事情：他必须拥有深思熟虑的计划和与人沟通的技巧，并且还同时具有快速而严谨的思考能力。一个好的系统管理员常常探索新技术和评估自己的竞争力，并可以在以往经验的基础上随时适应新的情况。另外别忘了，任何一个成功的系统管理员还必须足够敬业，能够半夜三更开车去数据中心修复一台计算机。这些品质不是能够教会的，只能通过教育和经验的结合来共同培育。

那么如何学习才能够成为一名系统管理员呢？现在有些大学在计算机科学课程中安排了系统管理的科目，但这些课程太少，课程与课程间差别太大，而且还并不成熟。另外，教室里的课程决不会给您足够的实际经验让您能胜任一个实际公司系统的管理。从某种程度上说，系统管理就像一种中世纪的行业：人们在某种手艺人当里从学徒开始渐渐成为大师。学徒观察师傅工作，在旁边协助，这使学徒渐渐学习到该行业的复杂性。因此，一个鞋匠的学徒学的不仅仅是如何修鞋，他还学会了如何成为一个鞋匠。

朝着这样的目标努力，本书将教您如何成为一个真正的系统管理员。本书没有过多地强调系统中完成某些任务的特定命令的使用方法，而是介绍了非常有用的方法和概念，帮助您成为一个有效、有魄力的专业系统管理员，所讨论的主题包括从操作系统选择到有效的电子通信方法、等等。您将学习如何设计、部署、维护和升级 Unix 系统，还将学习如何避免那些导致管理失效和用户受挫的问题，以及引发这些问题的不必要的系统开销和停机时间。

尽管每一章都会讨论到许多重要的工具和方法，并配有实例和示范让您体会它们是如何完成工作的，但本书并不是一本参考手册或者“烹饪书”。本书将作为 Unix 参考手册和烹饪书的补充，向您展示一个业内资深专业人士对真实环境中系统管理员职责的深入见解。

现在市场对系统管理员的需求很大，但我们的工作却比以往任何时候更复杂，要求更为严格，需要更多的责任心。计划、协作和测试现在成了每个系统管理员工作的核心，我们不能只是简单地接手一个项目并在几天内完成它。在阅读本书之前，您可能已经意识到了这个事实，并准备增强自己的技能，以有利于您自己和您所在的机构。本书正是为您所想，全力帮助您成为一个合格的系统管理员！

本书内容结构

第一部分从零开始，循序渐进地介绍了系统规划过程。您将在该部分学习到如何把一系列的业务目标转化成一个个功能完整的系统体系结构，以及如何在这个过程中做出正确的决策。您还将学习到如何把系统应用到生产中并测试它们。

第二部分将重点放在新系统的维护工作上，因为只有当一个系统具有优秀的技术支持时，它才是一个优秀的系统。该部分的主题包括技术支持基础设施、监控系统的方法、安装补丁和升级系统的操作程序、应付停机事件和从灾难（如洪水或者火灾）中恢复等。

第三部分介绍了系统调优、安全防护和系统自动化的概念，同时也包括为未来扩展做计划的方法。该

部分还介绍了一些工具和技术，您立即就能发现它们对您自己的系统非常有用。这些工具的大多数很少获得媒体的关注，但它们确实在系统管理员工具箱中占有一席之地。

第四部分关注系统管理中的人的因素。该部分的主题也很少在常见的系统管理参考手册中提及，涉及的内容包括：如何与同伴沟通，如何处理与用户之间的关系，以及了解在当今信息技术环境中的标准策略和协定。

本书约定

本书使用一些特殊的段落格式来引起您对特定类型信息的注意。这些信息的类型包括注意、提示和警告；虽然书中没有具体区分某特定信息是属于“注意”、“提示”还是“警告”类型，但是见文知意，您应该一眼就能看出某特定的信息是在引起您的注意、提示某些相关资料还是在向您发出警告。阅读这些信息有助于您更好地理解特定上下文环境中所讨论的问题和方法。

我同时也在本书中加入了大量真实的例子。这些内容有助于您深入理解系统管理员在各种商业企业、ISP 和学术环境中的“前线”经验。仔细研究其他系统管理员在管理 Unix 系统时经历过的成功、挑战和失误，对您来说就是一个从老手那里学习系统管理的机会。基于这些从真实系统管理经验中获得的信息，您可以找到自己的富有创造性的解决方案和最佳方法，使您的 Unix 系统平稳而有效地运行。

目 录

第一部分 从零开始

第 1 章 规划系统体系结构	2
1.1 定义项目范围	2
1.2 系统分类	4
1.2.1 桌面工作站	5
1.2.2 交互式登录服务器	5
1.2.3 应用服务器	5
1.2.4 数据库服务器	5
1.2.5 计算服务器	6
1.2.6 文件服务器	6
1.2.7 管理服务器	6
1.3 收集技术规范	6
1.3.1 将业务目标转化为技术解决方案	7
1.3.2 收集具体业务目标的详细信息	7
1.3.3 定义基本的项目参数	8
1.4 评估兼容性需要	9
1.5 选择软件和硬件	9
1.5.1 选择应用软件	10
1.5.2 选择操作系统软件	11
1.5.3 分析硬件需求	12
1.6 评估供应商技术支持合同	12
1.6.1 硬件支持	13
1.6.2 软件支持	13
1.6.3 供应商的责任	14
1.7 小结	14
1.8 复习题	14
第 2 章 设计数据中心基础设施	15
2.1 是否应该构建自己的数据中心	15
2.2 数据中心的环境控制	16
2.2.1 温度控制	16
2.2.2 湿度控制	17
2.2.3 空气质量维护	18
2.2.4 消防设施	18
2.2.5 噪音限制	19
2.3 选择活动地板还是固定地板	19
2.3.1 固定地板	19
2.3.2 活动地板	19
2.3.3 根据需要进行地板类型	20
2.4 选择和使用机架	20

2.4.1	双支柱机架	21
2.4.2	四支柱机架	22
2.4.3	机柜	22
2.4.4	硬件安装	24
2.4.5	电缆管理	25
2.4.6	配线板	26
2.5	确保数据中心的访问安全	27
2.5.1	周边安全	27
2.5.2	机架安全	27
2.5.3	组件安全	27
2.6	电源管理	28
2.6.1	管理冗余电源	28
2.6.2	使用和管理电源线	28
2.6.3	使用不间断电源	29
2.7	维护和维修的带外管理	31
2.7.1	使用控制台对 Unix 服务器进行带外管理	31
2.7.2	用于带外管理和远程访问的其他硬件	32
2.8	紧急远程访问	33
2.9	小结	33
2.10	复习题	34
第 3 章	系统部署	35
3.1	订购过程	35
3.1.1	确定硬件和软件需求	35
3.1.2	编制所需软件和硬件的目录	36
3.1.3	管理许可证	36
3.1.4	选择供应商	37
3.1.5	索取报价和完成订购单	37
3.2	收货	38
3.2.1	验货	38
3.2.2	设备保管	38
3.2.3	设备的温差适应	39
3.3	记录系统的部署过程	39
3.4	硬件安装	40
3.4.1	开箱	40
3.4.2	为硬件贴标签	41
3.4.3	安装硬件	41
3.4.4	连接电缆和适配器	43
3.4.5	测试硬件	44
3.5	安装软件	44
3.5.1	使用软件安装过程更新日志簿	44
3.5.2	从光盘安装	45
3.5.3	从软盘安装	45
3.5.4	从网络安装	45
3.5.5	安装应用程序	49

3.5.6 管理未打包的软件的安装	49
3.5.7 使用 Solaris 和 Linux 软件包管理器	51
3.5.8 在 Solaris 和 Red Hat Linux 上安装操作系统补丁	53
3.6 将完成部署的系统移交给用户	55
3.6.1 准备程序文档	56
3.6.2 常见问题解答	56
3.6.3 提供联系信息	56
3.7 小结	57
3.8 复习题	57

第二部分 维护

第 4 章 系统测试 59

4.1 测试过程	59
4.1.1 系统测试和产品测试的类型	59
4.1.2 安排测试	60
4.1.3 记录和分析测试结果	60
4.2 单元测试	61
4.2.1 决定需要测试的内容	61
4.2.2 执行单元测试	61
4.2.3 单元测试实例	62
4.3 兼容性测试	65
4.3.1 决定测试内容	65
4.3.2 执行兼容性测试	65
4.3.3 兼容性测试实例	66
4.4 负载测试	66
4.4.1 确定负载测试参数	66
4.4.2 执行负载测试	67
4.4.3 在技术规范要求之内运行	68
4.4.4 判断断点	69
4.4.5 确定负载增长和系统压力之间是线性关系还是几何关系	70
4.5 回归测试	71
4.5.1 执行回归测试	71
4.5.2 评估回归测试结果	71
4.5.3 回归测试实例	71
4.6 Alpha 和 Beta 测试	72
4.6.1 为测试征募用户	72
4.6.2 Alpha 测试	73
4.6.3 Beta 测试	73
4.6.4 测试预发布版	73
4.7 小结	74
4.8 复习题	74

第 5 章 技术支持管理 75

5.1 将技术支持部门与业务规模 and 客户需求相结合	75
------------------------------	----

5.1.1	确定客户	76
5.1.2	提供服务台支持	76
5.1.3	使用其他技术支持人员	77
5.1.4	提供三层技术支持	77
5.1.5	形成灵活的技术支持体系	78
5.2	制定待命程序	78
5.2.1	授权	79
5.2.2	规章制度的制定	79
5.2.3	沟通	80
5.3	问题上报程序	80
5.3.1	使服务台受控于掌握之中	80
5.3.2	凭单分派	81
5.3.3	状态更新	82
5.3.4	提供有关上报的问题的信息	82
5.3.5	做好突发事件计划	83
5.3.6	问题上报流程图	83
5.4	管理不同技术级别之间的沟通	84
5.4.1	使用技术沟通工具	84
5.4.2	在服务台上使用 FAQ (常见问题解答) 列表	85
5.4.3	保持技术支持沟通礼仪	85
5.5	支持工具	86
5.5.1	大型 ISP 使用的支持工具	86
5.5.2	小型市场调查公司使用的支持工具	87
5.6	宣传技术支持部门	88
5.7	小结	88
5.8	复习题	89
第 6 章	监控服务	90
6.1	监控的概念	90
6.1.1	主动监控	90
6.1.2	被动监控	91
6.2	主机监控	91
6.3	网络监控	91
6.3.1	监控链接状态	92
6.3.2	监控网络带宽	93
6.3.3	监控流量内容	95
6.4	服务监控	96
6.4.1	监控端口连接	96
6.4.2	监控 POP Internet 服务	97
6.4.3	监控域名服务	97
6.4.4	超时与重复	98
6.5	系统日志	99
6.5.1	syslog	99
6.5.2	syslog-ng	101
6.5.3	应用程序日志	104

6.6 日志管理	104
6.6.1 位置	104
6.6.2 文件大小	105
6.6.3 轮替	105
6.6.4 归档	106
6.7 日志监控	106
6.7.1 日志监控软件	106
6.7.2 通知	107
6.8 内部监控与外部监控	109
6.9 监控应用程序	109
6.9.1 Micromuse Netcool®	109
6.9.2 NetSaint	111
6.9.3 Big Brother	112
6.10 小结	112
6.11 复习题	112
第 7 章 补丁、升级和退役	113
7.1 预先在沙箱环境进行测试	113
7.2 对操作系统应用补丁	114
7.2.1 对操作系统应用补丁的最佳方法	114
7.2.2 战胜补丁应用失败	115
7.2.3 从应用补丁后的重启失败中恢复	116
7.2.4 bug 交换	117
7.2.5 撤销补丁	118
7.3 硬件升级	118
7.3.1 确保硬件兼容性	118
7.3.2 确保硬件拥有足够的容量	119
7.3.3 为平稳过渡到升级后的硬件制定计划	120
7.4 操作系统升级	121
7.4.1 决定升级还是从头安装	121
7.4.2 克服共享库的不兼容性	122
7.4.3 避免覆盖配置文件	122
7.4.4 保证升级所需的磁盘空间	123
7.4.5 确保升级后的操作系统有足够的驱动程序支持	124
7.5 固件升级	124
7.6 服务退役	125
7.6.1 确定服务的用户	125
7.6.2 通知用户	127
7.6.3 逐步地进行任何过渡	127
7.6.4 退役，不是销毁	128
7.7 小结	128
7.8 复习题	128
第 8 章 服务停用	130
8.1 服务停用类型	130

8.2 预定的维护	131
8.2.1 计划例行维护性停用	131
8.2.2 预定例行维护性停用	131
8.3 计划外停用	132
8.4 部分服务停用	133
8.5 完全停用及服务降级	134
8.6 分布式服务停用	134
8.7 第三方停用	135
8.8 维护时间段	136
8.8.1 最小使用量时间	136
8.8.2 最长维护时间	137
8.8.3 业务要求	137
8.8.4 在维护时间段内工作	137
8.9 监控对服务等级协议的遵守情况	138
8.9.1 监控对正常运行时间的遵守情况	138
8.9.2 监控对响应时间的遵守情况	139
8.10 注重生产价值	139
8.10.1 适当地使用生产服务器	139
8.10.2 事先宣布所有维护活动	140
8.10.3 日志观察和监控程序	140
8.10.4 迅速响应服务停用事件	141
8.11 停用程序	141
8.11.1 向适当的人员分配解决问题的任务	141
8.11.2 维持对工作进展情况的沟通	142
8.11.3 维护活动日志	142
8.11.4 保持镇定	143
8.12 根源分析	143
8.13 小结	144
8.14 复习题	144

第 9 章 为灾难恢复做准备

145

9.1 什么是 IT 灾难事件	145
9.2 停电	146
9.2.1 停电可能造成的损害	146
9.2.2 提供不间断电源 (UPS)	147
9.2.3 使用发电机作为应急电源	148
9.3 物理灾难和环境灾难	150
9.3.1 火灾	150
9.3.2 洪水和风暴	151
9.3.3 HVAC (暖通空调) 设备故障	151
9.3.4 无法进入数据中心	151
9.4 管理数据丢失	152
9.5 制定灾难恢复计划	153
9.5.1 组建灾难恢复计划小组	154
9.5.2 进行业务影响分析	154

9.5.3 确定关键功能	154
9.5.4 分配资源	155
9.5.5 确定关键任务	158
9.5.6 生成灾难恢复计划	158
9.5.7 测试恢复程序	160
9.5.8 改动管理——更新恢复计划	160
9.6 灾难演习	161
9.7 小结	161
9.8 复习题	162

第三部分 运行情况良好的机器

第 10 章 在 Unix 系统中提供高可用性

10.1 高可用性	164
10.2 高可用性技术	165
10.2.1 冗余	165
10.2.2 故障恢复	165
10.2.3 负载均衡	166
10.3 用 RAID 实现数据冗余	173
10.3.1 RAID-1	174
10.3.2 RAID-4	174
10.3.3 RAID-5	175
10.3.4 选择适当的 RAID 级别	176
10.3.5 硬件 RAID 和软件 RAID	176
10.3.6 一种典型的 RAID 方案: Solstice DiskSuite	177
10.4 用分离镜像实现数据冗余	178
10.5 用快照实现数据冗余	179
10.6 使用多个网络通路	180
10.6.1 冗余网络提供商	180
10.6.2 本地网络冗余	180
10.7 使用服务器集群	181
10.7.1 具有故障恢复能力的集群	181
10.7.2 并行集群	182
10.8 位置冗余	182
10.8.1 远程镜像	182
10.8.2 内容分布	183
10.9 Internet 服务的高可用性技术	184
10.9.1 使用冗余的域名服务器	184
10.9.2 修改重要的地址	185
10.9.3 使用冗余的邮件集线器	185
10.10 小结	186
10.11 复习题	186

第 11 章 性能调优与容量规划

11.1 测量 CPU 的性能和容量	187
--------------------------	-----

11.1.1	平均负载	187
11.1.2	跟踪用户与系统处理过程	189
11.1.3	分析 CPU 性能的历史数据	192
11.2	CPU 性能调优	193
11.2.1	选择正确的编译选项	193
11.2.2	设置进程优先级	194
11.2.3	使用多个处理器	195
11.2.4	升级处理器	196
11.2.5	跟踪进程	196
11.3	规划 CPU 资源	197
11.3.1	分析 CPU 使用趋势	197
11.3.2	使用可升级的硬件	197
11.4	测量存储设备的性能和容量	198
11.4.1	理解存储设备的容量	198
11.4.2	磁盘结构	199
11.4.3	带宽与等待时间	199
11.4.4	顺序存取与随机存取	199
11.4.5	块 I/O 与字符 I/O	200
11.4.6	索引节 (inode)	200
11.4.7	测量磁盘性能与容量的工具	200
11.4.8	定位大文件和目录	201
11.4.9	使用 iostat 命令测量磁盘活动	202
11.4.10	用 sar 分析磁盘性能的历史数据	203
11.5	磁盘与文件系统性能调优	204
11.5.1	使用高转速的磁盘	204
11.5.2	将文件系统放在最佳的柱面上	204
11.5.3	将数据在多个磁盘上条带化 (RAID-0)	205
11.5.4	优化文件系统的索引节 (inode) 数目	206
11.6	规划存储需求	207
11.6.1	监控磁盘使用趋势	207
11.6.2	为每一个分区分配足够的空间	207
11.6.3	利用基于段优点的卷管理器	207
11.6.4	用配额限制用户占用的空间	208
11.7	测量内存的性能与容量	208
11.7.1	虚拟内存的实现	209
11.7.2	显示交换空间的统计信息	210
11.7.3	用 vmstat 监控内存使用情况	210
11.7.4	用 sar 命令监控页面调度活动	211
11.7.5	监控进程使用内存情况的工具	211
11.8	内存与交换空间性能调优	213
11.8.1	Solaris 的换页优先机制	213
11.8.2	优化访问交换分区的方式	213
11.8.3	利用共享库	214
11.9	规划内存与交换空间容量	214
11.9.1	监控进程使用内存的情况	214

11.9.2 分配更多的交换空间	214
11.10 测量网络的性能和容量	215
11.10.1 带宽与时延	215
11.10.2 计算跳数	216
11.10.3 检测数据包丢失	217
11.10.4 检测网络错误	218
11.10.5 检测冲突	219
11.10.6 双工问题	219
11.11 网络性能调优	220
11.11.1 用硬编码设置双工模式	220
11.11.2 提高重要网络流量的优先级	221
11.11.3 调整 TCP 定时器	222
11.12 规划未来的网络容量	223
11.12.1 观察网络流量的长期变化趋势	223
11.12.2 使用可变带宽的电路	224
11.13 小结	224
11.14 复习题	224
第 12 章 过程自动化	225
12.1 调度工具	225
12.1.1 at: 一次性调度	225
12.1.2 cron: 周期性调度	226
12.1.3 重定向 at 与 cron 的输出	227
12.1.4 at 与 cron 的访问控制	227
12.2 root 登录自动化	227
12.2.1 不需要密码的 Berkeley r-命令	228
12.2.2 r-命令的安全隐患	228
12.2.3 用 SSH 代替 r-命令	229
12.3 文件同步自动化	230
12.3.1 用 rcp 和 scp 拷贝文件	230
12.3.2 用 rsync 实现文件同步	231
12.3.3 用 rdist 分发文件	232
12.3.4 运行 rdist 命令	233
12.4 用 cfengine 实现本地配置自动化	234
12.4.1 多种形式的 cfengine	234
12.4.2 配置 cfengine	235
12.5 临时空间管理自动化	237
12.5.1 用 find 管理临时空间	237
12.5.2 用 cfengine 管理临时存储空间	237
12.6 日志维护自动化	238
12.7 将 logrotate 作为通用日志轮替工具	239
12.8 小结	240
12.9 复习题	241

第 13 章 实现系统安全性	242
13.1 认证、授权和记帐	242
13.2 Unix 系统中的安全性	243
13.2.1 物理安全性	243
13.2.2 网络安全性	244
13.2.3 主机安全性	244
13.3 理解最小特权	244
13.4 分离服务	245
13.5 管理 root 帐户	245
13.5.1 限制对 root 密码的使用	245
13.5.2 选择安全的 root 密码	245
13.5.3 永远都不要使用明文通道传送 root 密码	246
13.5.4 将 UID (用户标识) 0 保留用于 root 帐户	246
13.5.5 限制远程访问 root 帐户	246
13.6 权限委托	246
13.6.1 使用 sudo 命令以其他用户的身份运行命令	247
13.6.2 Solaris 8 基于角色的访问控制	249
13.6.3 使用 Unix 组许可权限来编辑文件	250
13.7 盗用和攻击	251
13.7.1 检测可疑行为	251
13.7.2 配置错误	252
13.7.3 使用 Shell 特殊字符	252
13.7.4 Shell 出口	253
13.7.5 缓冲区溢出	253
13.7.6 路径验证错误	254
13.7.7 IP 欺骗	255
13.7.8 拒绝服务攻击	255
13.7.9 消除系统的威胁	256
13.8 给数据加密	258
13.8.1 公钥加密与对称密钥加密	258
13.8.2 单向 hash 算法	259
13.8.3 用 crypt 命令加密工具	259
13.8.4 使用 PGP 加密	260
13.8.5 在 SSH 中选择加密算法和端口转发	264
13.8.6 使用虚拟专用网	265
13.9 选择认证方法	266
13.9.1 一次性密码	266
13.9.2 基于时间的密码	266
13.9.3 证书	266
13.9.4 Kerberos	267
13.10 提高安全性的简单方法	267
13.10.1 尽量少使用 setuid 程序	268
13.10.2 删除全局可写权限 (find 命令)	268
13.10.3 安装 TCP Wrapper	269