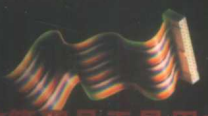

系统管理员工具用书

UNIX 系统故障检测、预防与排除

[美] Brad Stone　Julie Symons 著
王　艺　陈郁虹　马　伟　等译

UNIX Fault Management: A Guide for System Administrators

- 在任意 UNIX 系统平台上使系统的完整性和有效性最大化 —— 包括簇!
- 监视系统、磁盘、网络、应用程序和数据库 —— 为恢复和防御提供帮助
- 为系统管理员提供快速参考诊断和恢复功能

PH PTR

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

UNIX 系统故障检测、预防与排除

系统管理员工具用书

UNIX Fault Management:
A Guide for System Administrators

[美]Brad Stone　Julie Symons　著

王　艺　陈郁虹　马　伟　等译

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 提 要

本书介绍 UNIX 服务器的故障监视技术和监视工具，以及建立系统监视平台的过程，为操作员在客户环境中解决系统的故障问题提供帮助。书中首先概括操作员应完成的任务，并详述了事件的接收和处理方式。之后重点介绍可接收的事件类型、事件检测方式、事件通知方式以及问题的调查和恢复方式。本书根据具体的计算机组件详细描述了各种组件的监视工具和产品，其中包括“系统监视”、“磁盘监视”、“网络监视”、“应用程序监视”、“数据库监视”和“企业管理”。

图书在版编目(CIP)数据

UNIX 系统故障检测、预防与排除：系统管理员工具用书/(美)斯通 (Stone, B.)等著；
王艺等译 . - 北京：电子工业出版社，2000. 10
书名原文：Unix Fault Management：A Guide for System Administrators
ISBN 7-5053-6169-4

Ⅰ. U… Ⅱ. ①斯…②王… Ⅲ. ①UNIX 操作系统-故障检测②UNIX 操作系统-故障修复
Ⅳ. TP316.81

中国版本图书馆 CIP 数据核字(2000)第 69320 号

书　　名：**UNIX 系统故障检测、预防与排除**——系统管理员工具用书
原 书 名：UNIX Fault Management：A Guide for System Administrators
著　　者：[美]Brad Stone　Julie Symons
译　　者：王　艺　陈郁虹　马　伟等
责任编辑：史　平
排版制作：北京东光印刷厂
印 刷 者：三河市金马印装有限公司
出版发行：电子工业出版社　URL：http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787 × 1092　1/16　印张：19.5 字数：499 千字
版　　次：2000 年 10 月第 1 版　2000 年 10 月第 1 次印刷
书　　号：ISBN 7-5053-6169-4 / TP·3309
印　　数：5000 册　　定价：32.00 元
版权贸易合同登记号　图字：01-2000-1146

译者的话

随着 UNIX 系统的广泛应用，其故障检测与维护技术越来越受到广大系统管理员和操作员的关注，《UNIX 系统故障检测、预防与排除》一书集中讨论了 UNIX 系统使用中常见的故障、检测与维护技术。

本书分十章及附录。首先概括了系统操作员应完成的任务，并详细描述了事件的接收和处理方式。而后将重点放在了可以接收到的各种事件类型、事件的检测方式、操作员接收事件通知的方式以及问题的调查和完成恢复的方式，此后进一步介绍了各类必要的管理工具。书中许多章节重点介绍了具体的计算机组件，比如磁盘、数据库等，为系统管理员和操作员诊断故障、排除故障提供了有益的帮助。附录提供了故障管理标准，并归纳了书中重要的术语及定义。

参加本书翻译的还有徐利平、朱强、张景生、王晋东、李维维、杨军、李明、牛波、张汕、陈晓等同志。李芳、于春华、杨晓娟等同志完成了本书的录入工作。

由于时间仓促、水平有限，书中难免有不足和错误之处，恳请广大读者批评指正。

译者

前　言

本书的目的是为系统管理员和操作员维护关键性 UNIX 系统的完整性和有效性提供帮助。书中介绍了 UNIX 服务器的故障监视工具和监视技术，包括配置成高效簇的系统。因此，本书是操作员在客户环境中解决故障问题的便捷参考书。它指出了关键诊断信息的出处，并描述了要采取的恢复操作。

本书讲述了建立相应的系统监视平台的过程，所以对负责 UNIX 系统初始化配置和管理任务的系统管理员来说，本书也是十分有用的。对于那些决定为自己的环境购买必要的事件监视工具的客户来说，本书中的产品说明也是很有帮助的。

本书首先概括了操作员应完成的任务，并详细说明了事件的接收和处理方式。之后重点介绍可以接收到的各种事件类型、事件的检测方式、操作员接收事件通知的方式以及问题的调查和完成恢复的方法。其目的是介绍必要的工具，而并非为每个问题提供具体的解决方法。

本书包括故障管理工具和用于解决各类问题的产品。书中许多章节的重点在于介绍具体的计算机组件，比如磁盘或数据库，这对于操作员的具体任务是有帮助的。下面是每章的内容简介：

第 1 章　“系统操作员任务分析”，系统操作员要完成的任务，并就故障管理的内容进行了详细分析。

第 2 章　“可能事件枚举”，监视 UNIX 系统过程中可能发生的各种事件类型。

第 3 章　“使用监视框架”，监视框架及其可以使用之前必须完成的管理任务。

第 4 章　“监视系统”，用于监视 UNIX 服务器的工具和产品。

第 5 章　“监视磁盘”，用于监视外部磁盘设备的工具和产品。

第 6 章　“监视网络”，概述与网络使用相关的多种有效性问题和事件检测工具。

第 7 章　“监视应用程序”，应答时间和关键应用程序有效性的监视方法。

第 8 章　“监视数据库”，重点介绍与数据库使用相关的问题和事件检测的专用工具。

第 9 章　“企业管理”，讨论处理大型企业级客户错误管理的相关问题。

第 10 章　“UNIX 的未来”，讨论一些主要的 UNIX 系统厂商在故障管理方面的发展计划。

附录 A　“标准”，介绍已有的故障管理标准和如何从中受益。

“词汇”包含了书中重要的术语及其定义。

尽管我们认为绝大多数客户关心故障管理问题的目的是为了实现高效的解决方案，但是本书并不讲述如何创建高效的计算环境。需要这方面信息的读者，可以查阅 HP 公司有关高效性内容的外部 Web 站点（http://www.hp.com/go/ha）或阅读 Peter Weygant 所著的《Clusters for High Availability》一书。

总的来说，本书不讨论用户 UNIX 系统的硬件和软件组件的配置与安装问题。有关这方面的信息，用户应查阅相应厂商的产品手册。

本书中的许多实例来自于 HP－UX 服务器。其他 UNIX 平台的性能与此类似，如果某些工具是某种 UNIX 平台特有的，我们会加以注释。

致　谢

在此我们要向为本书做出贡献的许多人表示感谢。

本书涉及的主题很广泛，我们占用了各个领域许多专家的宝贵时间。Peter Weygant 为全书的结构提供了全面的指导。Barb Craig, Scott Rhine, David Miller, John Payne 和 Maria Fisk 为我们提供了磁盘管理和硬件监视方面的素材。Mike Traynor, Pat Mahoney 和 Winson Lau 为网络监视提供了帮助。Bob Sauers 提供了一些性能信息，Tom Murray 提供了一些工具，使 MIB 数据能够呈现在读者的面前。

Sun Microsystems 公司的 Srilakshmi Sitaraman, Mike Grote 和 Ninga Singireddy 花费了大量的时间帮助我们收集了 SyMON 产品的相关信息。

还要感谢 HP 公司的 Stephen Campbell 为我们介绍了 SMART 插件产品，并重写了数据库章节，纠正了许多不确切的内容。

我们还要感谢 BMC 软件公司的 Sara Robinson 为我们提供了 BMC PATROL 应用程序的演示拷贝。另外，IT Masters 的 Judy Posey 也为我们提供了 MasterCell 的帮助信息和屏幕照片。

Pam Saverthal 和 Birgitte Ishak 帮助我们处理了给出版社发送的最后邮件。

Informatica 公司的 Lillian Lim 阅读了本书的许多章节并鼓励我们最终完成本书。

我们要感谢 Mark Orvek 以及 Julie 工程组同仁的耐心帮助和支持。

最后，我们还要向 Pam Mujica 和 Joe Green 表示深深的谢意，没有他们在 HP 公司的倡导，就不会有这本书。

目　录

第 1 章　系统操作员任务分析 …… (1)
1.1　系统操作趋势 …… (1)
第 2 章　可能事件枚举 …… (3)
2.1　定义故障管理 …… (3)
2.2　事件类型 …… (4)
2.3　配置事件 …… (4)
2.3.1　应用程序修改 …… (4)
2.3.2　操作系统修改 …… (5)
2.3.3　硬件更换 …… (5)
2.4　故障 …… (5)
2.4.1　系统硬件或软件组件故障 …… (5)
2.4.2　外设故障 …… (6)
2.4.3　外部服务的故障或损失 …… (7)
2.5　资源和性能事件 …… (8)
2.6　安全入侵 …… (8)
2.7　环境变化 …… (9)
第 3 章　使用监视框架 …… (10)
3.1　区分监视框架 …… (11)
3.1.1　监视组件 …… (11)
3.1.2　监视特性 …… (11)
3.1.3　监视器的发现与配置 …… (11)
3.1.4　监视器开发工具箱 …… (11)
3.1.5　通知方法 …… (11)
3.1.6　诊断功能 …… (13)
3.2　IT/O …… (13)
3.2.1　监视组件 …… (13)
3.2.2　监视特性 …… (14)
3.2.3　监视器的发现与配置 …… (15)
3.2.4　监视器开发工具箱 …… (16)
3.2.5　通知方法 …… (16)
3.2.6　诊断功能 …… (17)
3.2.7　附加信息 …… (17)
3.3　Unicenter TNG …… (18)
3.3.1　监视组件 …… (18)
3.3.2　监视特性 …… (18)

3.3.3 监视器的发现与配置 …… (19)
3.3.4 监视器开发工具箱 …… (19)
3.3.5 通知方法 …… (19)
3.3.6 诊断功能 …… (19)
3.3.7 附加信息 …… (20)
3.4 事件监视服务 …… (20)
3.4.1 监视组件 …… (20)
3.4.2 监视特性 …… (21)
3.4.3 监视器的发现与配置 …… (22)
3.4.4 监视器开发工具箱 …… (24)
3.4.5 通知方法 …… (24)
3.4.6 诊断功能 …… (24)
3.4.7 附加信息 …… (25)
3.5 PLATINUM ProVision …… (25)
3.5.1 监视组件 …… (25)
3.5.2 监视特性 …… (26)
3.5.3 监视器的发现与配置 …… (26)
3.5.4 监视器开发工具箱 …… (27)
3.5.5 通知方法 …… (27)
3.5.6 诊断功能 …… (27)
3.5.7 附加信息 …… (28)
3.6 BMC PATROL …… (28)
3.6.1 监视组件 …… (29)
3.6.2 监视特性 …… (29)
3.6.3 监视器的发现与配置 …… (30)
3.6.4 监视器开发工具箱 …… (30)
3.6.5 通知方法 …… (30)
3.6.6 诊断功能 …… (31)
3.6.7 附加信息 …… (31)
3.7 MeasureWare …… (31)
3.7.1 监视组件 …… (32)
3.7.2 监视特性 …… (32)
3.7.3 监视器的发现与配置 …… (33)
3.7.4 监视器开发工具箱 …… (33)
3.7.5 通知方法 …… (33)
3.7.6 诊断功能 …… (34)
3.7.7 附加信息 …… (34)
第4章 监视系统 …… (35)
4.1 识别重要的系统监视类别 …… (35)

4.1.1 监视系统配置的更改 …… (35)
4.1.2 监视系统故障 …… (35)
4.1.3 监视系统资源的使用 …… (36)
4.1.4 监视系统的安全性 …… (36)
4.1.5 监视系统性能 …… (36)
4.2 使用标准命令和工具 …… (36)
4.2.1 bdf 和 df …… (37)
4.2.2 ioscan …… (37)
4.2.3 iostat …… (37)
4.2.4 ipcs …… (38)
4.2.5 mailstats …… (39)
4.2.6 ps …… (39)
4.2.7 sar …… (39)
4.2.8 swapinfo …… (40)
4.2.9 sysdef …… (41)
4.2.10 timex …… (42)
4.2.11 top …… (42)
4.2.12 uname …… (44)
4.2.13 uptime …… (44)
4.2.14 vmstat …… (44)
4.2.15 who …… (45)
4.3 使用系统检测装置 …… (45)
4.3.1 SNMP …… (46)
4.3.2 DMI …… (47)
4.4 使用图形状态监视器 …… (47)
4.4.1 OpenView 网络节点管理器 …… (48)
4.4.2 ClusterView …… (50)
4.4.3 Unicenter TNG …… (52)
4.5 使用事件监视工具 …… (53)
4.5.1 事件监视服务 …… (53)
4.5.2 EMS 高效监视器 …… (53)
4.5.3 EMS 硬件监视器 …… (54)
4.5.4 企业级 SyMON …… (57)
4.5.5 OpenView IT/O …… (59)
4.5.6 GlancePlus Pak 2000 …… (61)
4.6 安全监视 …… (61)
4.6.1 安全综述 …… (61)
4.6.2 安全监视工具 …… (62)
4.7 使用诊断工具 …… (62)

4.7.1 支持工具管理器 …… (63)
4.7.2 HP 预测支持 …… (64)
4.7.3 HA 观察台 …… (65)
4.8 监视系统外设 …… (65)
4.8.1 磁盘 …… (65)
4.8.2 磁带 …… (65)
4.8.3 打印机 …… (65)
4.9 收集系统性能数据 …… (66)
4.9.1 MeasureWare …… (67)
4.9.2 GlancePlus …… (69)
4.9.3 PerfView …… (71)
4.9.4 UNIX 版 BMC PATROL …… (73)
4.9.5 Candle …… (75)
4.10 使用系统性能数据 …… (76)
4.10.1 避免性能问题 …… (76)
4.10.2 检测 CPU 竞争 …… (77)
4.10.3 检查系统资源的使用 …… (77)
4.10.4 检测内存和交换空间的竞争 …… (78)
4.10.5 检测磁盘和文件系统的瓶颈 …… (78)
4.11 避免系统问题 …… (79)
4.12 从系统问题中恢复 …… (79)
4.13 比较系统监视工具 …… (80)
4.14 实例研究:从内存故障中恢复 …… (80)
4.14.1 验证配置 …… (80)
4.14.2 建立监视及重新配置 …… (81)
4.14.3 内存板失效 …… (81)
4.14.4 解决故障并恢复服务 …… (81)
第 5 章 监视磁盘 …… (83)
5.1 区分重要的磁盘监视类 …… (83)
5.2 使用标准命令和工具 …… (84)
5.2.1 bdf 和 df …… (84)
5.2.2 diskinfo …… (84)
5.2.3 fsck …… (85)
5.2.4 ioscan …… (87)
5.2.5 lvdisplay …… (88)
5.2.6 pvdisplay …… (88)
5.2.7 vgdisplay …… (89)
5.3 使用系统检测装置 …… (90)
5.3.1 SNMP …… (90)

5.3.2 DMI …… (91)
5.4 使用事件监视工具 …… (92)
5.4.1 EMS磁盘卷监视器 …… (93)
5.4.2 EMS硬件监视器 …… (94)
5.4.3 HARAYMON和ARRAYMOND …… (98)
5.4.4 OpenView IT/O …… (99)
5.4.5 企业级SyMON …… (100)
5.5 使用诊断工具 …… (100)
5.5.1 支持工具管理器 …… (100)
5.5.2 HP预测支持 …… (102)
5.6 收集磁盘性能数据 …… (102)
5.6.1 MeasureWare …… (103)
5.6.2 GlancePlus …… (104)
5.6.3 PerfView …… (104)
5.6.4 BMC PATROL …… (106)
5.7 使用磁盘性能数据 …… (107)
5.8 避免磁盘问题 …… (108)
5.9 从磁盘问题中恢复 …… (109)
5.10 比较磁盘监视产品 …… (109)
5.11 实例研究:镜像磁盘的配置与监视 …… (109)
5.11.1 验证配置 …… (110)
5.11.2 建立监视 …… (110)
5.11.3 镜像失败 …… (111)
5.11.4 恢复镜像 …… (112)
5.11.5 验证配置 …… (112)
第6章 监视网络 …… (113)
6.1 识别要监视的重要网络组件 …… (113)
6.2 使用图形网络状态监视器 …… (113)
6.2.1 NNM …… (114)
6.2.2 IT/O …… (116)
6.2.3 Unicenter TNG …… (117)
6.2.4 企业级SyMON …… (118)
6.3 监视网络接口卡和电缆故障 …… (119)
6.3.1 使用SNMP测试装置 …… (119)
6.3.2 使用标准命令和工具 …… (119)
6.3.3 使用辅助产品监视网络链接 …… (123)
6.3.4 使用链接指定命令 …… (125)
6.4 监视网络和传输协议 …… (127)
6.4.1 使用SNMP检测装置 …… (127)

6.4.2 使用标准命令和工具 …… (127)
6.5 监视网络服务 …… (134)
6.5.1 监视 DHCP/BOOTP 服务器 …… (134)
6.5.2 监视 DNS/NIS 名服务器 …… (135)
6.5.3 监视 FTP …… (136)
6.5.4 监视 NFS …… (136)
6.5.5 监视远程连接 …… (138)
6.5.6 监视 Web 服务器 …… (138)
6.6 监视网络主机 …… (138)
6.6.1 网络节点管理器 …… (138)
6.6.2 互连与路由管理器 …… (140)
6.7 收集网络性能数据 …… (140)
6.7.1 使用 RMON 和 RMON-II 检测装置 …… (141)
6.7.2 NetMetrix 站点管理器 …… (142)
6.7.3 MeasureWare …… (142)
6.7.4 GlancePlus …… (143)
6.7.5 PerfView …… (144)
6.7.6 UNIX 版的 BMC PATROL …… (146)
6.7.7 通用网络公司的 Sniffer Pro …… (146)
6.8 使用网络性能数据 …… (147)
6.8.1 避免性能问题 …… (147)
6.8.2 检测过载网络服务器 …… (147)
6.8.3 检测网络拥挤 …… (148)
6.9 避免网络问题 …… (148)
6.10 从网络问题中恢复 …… (149)
6.10.1 孤立故障 …… (149)
6.10.2 网络层和较低层 …… (149)
6.10.3 传输层和较高层 …… (150)
第 7 章 监视应用程序 …… (151)
7.1 监视重要应用程序组件 …… (151)
7.2 识别应用程序类型 …… (152)
7.3 使用标准命令和工具 …… (152)
7.3.1 ps …… (153)
7.3.2 top …… (153)
7.3.3 vmstat …… (154)
7.4 使用系统测试设备 …… (154)
7.4.1 SNMP …… (155)
7.4.2 DMI …… (155)
7.4.3 pstat …… (156)

7.5 故障检测工具 …… (159)
7.5.1 IT/O …… (159)
7.5.2 MC/ServiceGuard …… (159)
7.5.3 ClusterView …… (160)
7.5.4 事件监视服务 …… (162)
7.5.5 EcoSNAP …… (163)
7.6 ERP 应用程序的监视工具 …… (164)
7.6.1 Envive …… (164)
7.6.2 SMART 插件 …… (165)
7.6.3 BMC PATROL 知识模块 …… (166)
7.6.4 EcoSYSTEMS …… (168)
7.7 资源和性能监视工具 …… (169)
7.7.1 应用程序资源测量 …… (169)
7.7.2 MeasureWare …… (170)
7.7.3 GlancePlus …… (175)
7.7.4 PerfView …… (177)
7.7.5 进程资源管理器 …… (177)
7.8 控制应用程序性能 …… (178)
7.9 应用程序问题的恢复 …… (178)
7.10 应用程序监视产品的比较 …… (179)
第 8 章 监视数据库 …… (180)
8.1 识别重要的数据库监视类 …… (180)
8.1.1 配置数据库 …… (180)
8.1.2 监视数据库错误 …… (181)
8.1.3 监视数据库资源和性能 …… (181)
8.1.4 维护数据库服务器的安全 …… (181)
8.1.5 确保数据库备份成功 …… (182)
8.2 使用标准数据库命令和工具 …… (182)
8.2.1 UNIX 命令 …… (182)
8.2.2 SQL 命令 …… (183)
8.2.3 SNMP MIB 监视 …… (184)
8.2.4 数据库厂商提供的工具 …… (186)
8.3 使用故障检测和恢复工具 …… (190)
8.3.1 MC/ServiceGuard …… (190)
8.3.2 ClusterView …… (191)
8.3.3 EMS HA 监视器 …… (191)
8.4 资源和性能监视工具 …… (193)
8.4.1 应用程序资源测量 …… (193)
8.4.2 Oracle Trace …… (194)

8.4.3 Oracle V$表 …… (196)
8.4.4 GlancePlus Pak 2000 …… (196)
8.4.5 Oracle Management Pak …… (198)
8.4.6 PerfView …… (199)
8.4.7 数据库的 SMART 插件 …… (201)
8.4.8 BMC PATROL KM …… (202)
8.4.9 PLATINUM DBVision …… (204)
8.5 使用数据库性能数据 …… (205)
8.5.1 避免性能问题 …… (205)
8.5.2 检查系统竞争 …… (206)
8.5.3 检查磁盘瓶颈问题 …… (206)
8.5.4 检查数据库缓冲区和缓冲池的大小 …… (207)
8.6 避免数据库问题 …… (208)
8.7 从数据库问题中恢复 …… (209)
8.8 数据库监视产品对比 …… (209)
第 9 章 企业管理 …… (211)
9.1 企业监视 …… (211)
9.2 识别事件 …… (212)
9.3 使用事件相关工具 …… (213)
9.3.1 OpenView 事件相关服务 …… (213)
9.3.2 Seagate NerveCenter …… (214)
9.3.3 IT Masters 的 MasterCell …… (214)
9.4 监视多个系统 …… (216)
9.4.1 IT/O …… (216)
9.4.2 ClusterView …… (217)
9.5 企业管理框架 …… (217)
9.5.1 ClusterView …… (217)
9.5.2 监视代理 …… (217)
9.6 使用多种工具 …… (217)
9.6.1 IT/O 与网络节点管理器 …… (218)
9.6.2 IT/O 和 PerfView …… (218)
9.6.3 BMC PATROL 和 IT/O …… (218)
9.6.4 PLATINUM ProVision 和 IT/O …… (219)
9.6.5 EMS 和 OpenView NNM 或 IT/O …… (219)
第 10 章 UNIX 的未来 …… (220)
10.1 故障管理的发展趋势 …… (220)
附录 A 标准 …… (222)
A.1 使用 SNMP 和 MIB …… (222)
A.1.1 MIB-II …… (224)

A.1.2 RMON MIB …… (230)
A.1.3 RMON II MIB …… (236)
A.1.4 主机资源 MIB …… (243)
A.1.5 打印机 MIB …… (246)
A.1.6 HP-UNIX MIB …… (252)
A.1.7 HP 簇 MIB …… (256)
A.1.8 HP MC/ServiceGuard MIB …… (257)
A.1.9 网络服务 MIB …… (260)
A.1.10 RDBMS MIB …… (262)
A.1.11 Oracle 私有数据库 MIB …… (264)
A.1.12 Oracle 网络侦听器 MIB …… (268)
A.1.13 Oracle Names MIB …… (270)
A.1.14 Oracle 企业管理器 MIB …… (272)
A.1.15 Oracle 多协议互换 MIB …… (274)
A.1.16 Informix 私有数据库 MIB …… (277)
A.2 使用 DMI 和 MIF …… (282)
A.2.1 系统 MIF …… (283)
A.2.2 软件 MIF …… (286)
词汇 …… (291)

第1章　系统操作员任务分析

系统操作员负责维护公司数据中心内计算机系统的完整性和有效性。操作员职责的涉及面很广，大多数操作员的精力要花费在解决系统故障和用户报告的问题上。其他的基本任务还包括系统状态监视、性能监视及系统备份。有时操作员还要完成一些辅助任务，比如操作系统和应用程序升级、安装修补或完成系统维护等。对于一位操作员而言，在一个操作环境中维护上百个系统的情况并不罕见。

较大型的机构内一般都有许多系统操作员，大约平均每十台 UNIX 服务器就要有一位操作员。系统管理员的职责可以根据区域、应用程序、问题范围(性能、备份等)或时间带来划分。有些情况下，一名操作员需要将职责传递给公司中位于另一国家的数据中心的某个操作员。系统、应用程序、数据库和网络管理可能涉及不同部门的不同人员。在处理故障问题时，操作员可能需要得到更有经验的系统管理员的帮助。大型公司可能会有许多专业技术人员，包括数据库管理员和网络管理员，他们在某些领域有自己的专长。

本书有助于简化操作员解决用户故障问题的基本任务。故障的解决涉及检查系统当前的运行状态、研究近期事件及其相关的错误信息，其目的是找出问题产生的根源。多数系统停机是由于操作员在解决问题时的错误操作造成的。实际上，根据 HP 公司和其他工业咨询公司(如 Gartner Group)的研究表明，操作员所犯的错误是最常见的系统意外故障的根源。以下章节的目的是为了简化监视操作和恢复操作。

本书的监视章节根据系统组成分类，而且每章自成体系，所以应该不必翻来覆去查看多个章节就能解决问题。但是，由于每个问题都有多种形式，所以我们不可能为所有用户可能遇到的问题一一列出解决方法。本书将解释一些有代表性而又有效的监视工具，以及用它们解决问题的方法。读者应阅读一下每章结尾恢复操作的内容，掌握问题解决方法的一般性技术概念，并获取一些工具应用的感性认识。

1.1　系统操作趋势

随着计算机技术的不断变化和 Internet 的迅速发展，系统操作员的职责变得越来越复杂了。新的硬件平台、软件产品和大量的系统和网络平台的管理工作，使系统操作员仅仅靠手工工具完成工作越来越困难了。显然需要实现自动化，目前针对多任务操作员已经有了自动化软件。例如，过去常要使用一些原始的命令进行系统备份，现在一些复杂的软件包(诸如 HP 的 OmniBack Ⅱ 和 Legato 的 NetWorker)都常用于系统及系统集备份任务的简化和自动化。

计算机系统的多种发展趋势使系统的监视任务变得更重要了。对于一些公司来说，整体数据必须一周 7 天，一天 24 小时持续有效，任何系统故障都会导致经济损失。在这样的情况下，操作员不仅需要检测出当前的问题，还必须能预测将来可能出现的错误。本书的一些工具能识别导致系统故障的事件或趋势。

另一种行业趋势是人们根据系统运行的时间比率、系统性能以及操作员解决用户问题的

速度作为衡量 IT(信息技术部门)的标准。管理软件不仅需要指出问题是什么,还要说明应如何解决问题。目前,系统管理已经成为所有相关因素中 UNIX 服务器总成本的最大占有者。

在客户对操作员的需求快速增长的同时,管理工具的开发也正在同步发展。曾经是基于文本和用户触发的工具,现在已发展成为图形和文件驱动的工具。操作员可以从一个中心控制台上观察多个系统;系统可以显示成用颜色表明状态的图标;操作员可以迅速查看数据中心的状态;能够检测和报告到控制台上的问题数目也增加了。

但是,问题报告工具也足以使一般的操作员喘不过气来。有些帮助工具是由企业管理产品提供的,这些内容将在第 3 章"使用监视框架"中介绍,在全书的其余部分加以引用。如果许多系统共享的一个组件失效,那么结果可能是在管理站点上产生大量的事件。另外,组件失效可能会产生级联效果,使其他组件和产品也失效。同时将有大量的事件到达系统或中心控制台。操作员必须能够通过这些事件,找出问题的根源。第 9 章"企业管理"介绍处理这个问题的一些技术。

介绍故障管理工具之前,必须首先定义什么是"管理",我们在下一章完成这项任务。另外,还将介绍用户需要准备接收的事件类型,以充分保护自己的 UNIX 服务器。