《Unix系统管理》

图书基本信息

书名：《Unix系统管理》

13位ISBN编号：9787115108746

10位ISBN编号：7115108749

出版时间：2003-4

出版社：人民邮电出版社

作者：霍维茨(Horwitz Jeff)

页数：332

译者：祁力

《Unix系统管理》

内容概要

《Unix系统管理》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《Unix系统管理》也适合其他系统管理员和科技人员阅读。此外，《Unix系统管理》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，《Unix系统管理》亦可作为将所学知识投入实际应用的指南。

《Unix系统管理》

书籍目录

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 根据需要选择地板类型 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和客户需求相结合 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(r) 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 监控对服务等级协定的遵守情况 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 164
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 187
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
13.10.4 删除inetd中不必要的服务 271
13.10.5 使用安全的密码 271
13.10.6 监控文件系统的完整性 272
13.11 及时了解安全性论谈中的相应内容 272
13.12 小结 273
13.13 复习题 273
第四部分 人的因素
第14章 内部沟通 275
14.1 编写系统文档 275
14.1.1 以文档用户的知识水平和需求为导向编写文档 275

14.1.2 网络图 276
14.1.3 主机功能 278
14.1.4 程序性文档 279
14.1.5 使文档易于获取 279
14.2 改动管理 280
14.2.1 改动认可 280
14.2.2 改动通知 281
14.2.3 将改动记入日志 282
14.3 使用控制工具进行配置管理 283
14.3.1 检查登入文件 284
14.3.2 检查登出文件 285
14.3.3 解锁 286
14.3.4 查看RCS日志 286
14.3.5 查看不同版本间的变化 287
14.4 系统活动时间表 288
14.5 命名约定 288
14.6 小结 289
14.7 复习题 289
第15章 与用户互动 290
15.1 用户类型 290
15.1.1 新手 290
15.1.2 权威用户 291
15.1.3 通天晓 291
15.1.4 安静的用户 291
15.1.5 恶意用户 292
15.2 与用户沟通 292
15.2.1 主动的沟通手段 293
15.2.2 被动的沟通手段 294
15.3 应对问题用户 297
15.3.1 对资源的不当使用 297
15.3.2 骚扰其他用户 298
15.3.3 对系统发起攻击 299
15.3.4 黑客利用您的系统攻击其他系统 299
15.4 预防用户问题 299
15.4.1 强制实施策略 300
15.4.2 像一个偏执狂一样对待安全破坏活动 300
15.5 处理远程用户问题 300
15.5.1 确定远程站点地址 301
15.5.2 使用IDENT 协议识别远程用户 302
15.5.3 与远程站点管理员联系 302
15.6 小结 305
15.7 复习题 305
第16章 计算策略和协定 306
16.1 可接受用法策略 306
16.1.1 定义服务的预期使用目的 307
16.1.2 列出被禁止的行为 307
16.1.3 阐述违反策略的后果 307
16.2 用户的权利与责任 308
16.2.1 权利类型 308

16.2.2 责任类型　308
16.3 安全策略　309
16.3.1 选择站点安全管理员　309
16.3.2 定义安全目标　309
16.3.3 事件响应过程　312
16.3.4 让其他人员参与安全策略的制定　312
16.3.5 强制实施安全策略　313
16.4 安全弃权　313
16.5 使用隐性协定　314
16.6 小结　315
16.7 复习题　315
第五部分 附录
附录A 参考书目　317
附录B 问题答案　326
Unix系统管理

《Unix系统管理》

精彩短评

1、适用于有经验的系统管理员

《Unix系统管理》

版权说明