

网管员世界

NETADMIN WORLD MAGAZINE

2011

超值精华本

《网管员世界》杂志社 编

N E T A D M I N W O R L D

Broadview[®]
www.broadview.com.cn

安全管理 : -----

以网络安全的实用性和应用性文章呈现给广大的读者,帮助读者朋友从容应对网络安全方面的问题。

故障诊断 : -----

既可以作为网管员在日常工作中排障查错的工具手册,又可作为网管员提高网络管理水平的技术参考。

系统运维 : -----

剖析在操作系统和应用软件使用过程中遇到的各类问题的解决方法,为网管员朋友在操作系统和应用软件的配置和管理方面提供了众多的方法和技巧。

设备运维 : -----

为广大网络管理人员管理和维护网络提供了实战经验和参考,能够帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。

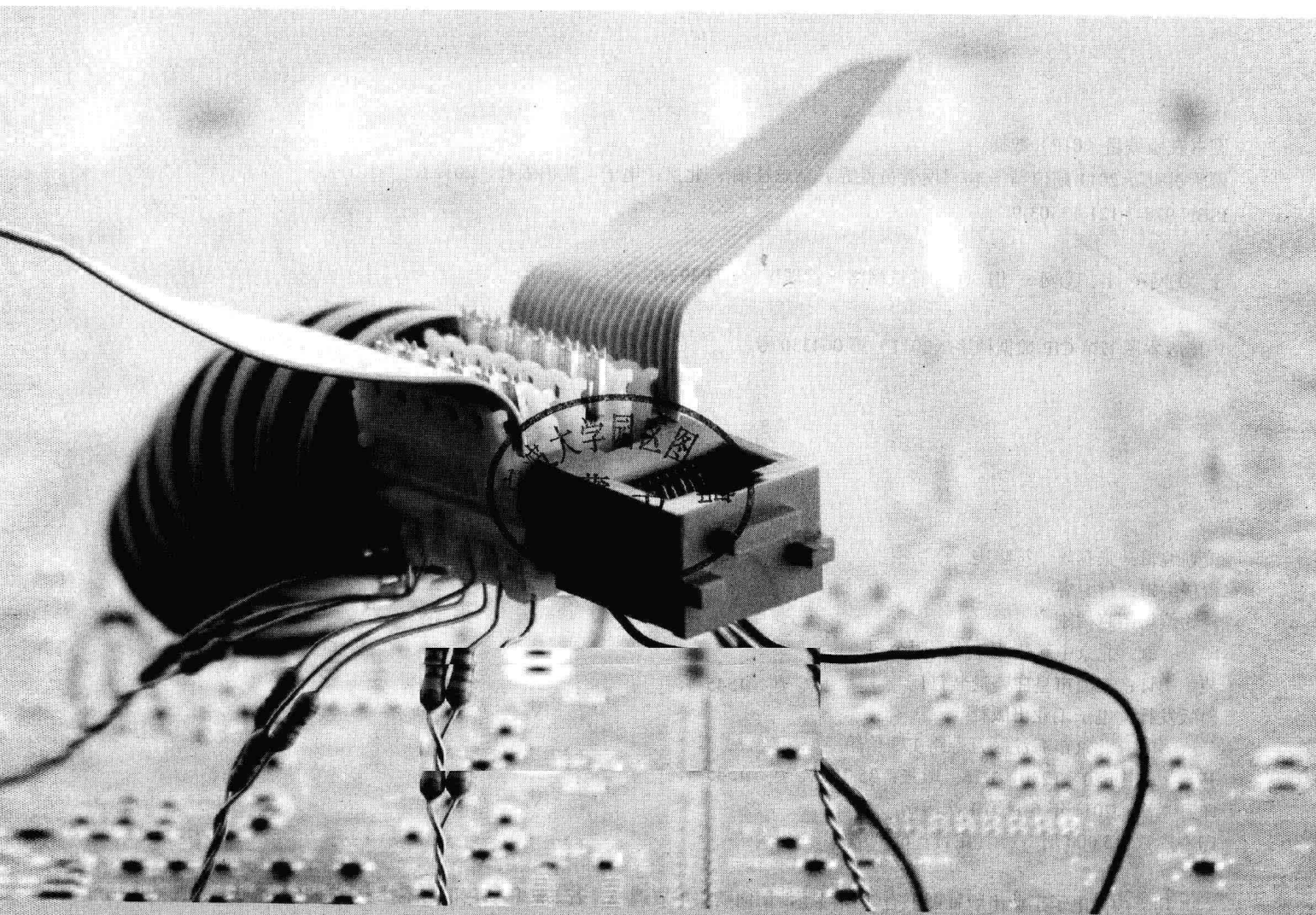
网管员世界

NETADMIN WORLD MAGAZINE

2011

超值精华本

《网管员世界》杂志社 编



电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内容简介

《网管员世界》月刊是面向网络技术管理人员的实用性期刊。本书是2010年《网管员世界》各期内容的汇集，按照栏目分类汇总，内容详尽实用，保存价值高。全书分为安全管理、故障诊断、系统运维、设备运维等部分，共精选数百篇实用、精彩的技术文章，是广大网管员不可多得的业务指导书。

本书读者对象以网络管理技术人员（网管员）为主，涵盖网络管理主管、网络爱好者、准网管和所有关注网络应用与网络事业发展的人士。

未经许可，不得以任何方式复制或抄袭本书的部分或全部内容。

版权所有，侵权必究。

图书在版编目（CIP）数据

网管员世界 2011 超值精华本/《网管员世界》杂志社编.—北京：电子工业出版社，2011.6

ISBN 978-7-121-13303-9

I. ①网… II. ①网… III. ①计算机网络—管理IV. ①TP393.07

中国版本图书馆 CIP 数据核字（2011）第 064330 号

策划编辑：张春雨 符隆美

责任编辑：付睿

特约编辑：赵树刚

印刷：北京中新伟业印刷有限公司

装订：三河市皇庄路通装订厂

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开本：880×1230 1/16 印张：35.75 字数：1545 千字

印次：2011 年 6 月第 1 次印刷

印数：5 000 册 定价：65.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010) 88258888。

FOREWORD 前言

《网管员世界》作为一本面向网络管理技术人员的专业杂志，已经走过了五年的风雨历程。长期以来，《网管员世界》杂志一直以提高企业 IT 基础设施运营水平、提高企业网管人员的管理水平为目标和宗旨，为企业的网络技术人员提供了一个交流技术和经验的平台，成为网络管理技术人员中颇具影响力的 IT 专业媒体。为了更好地帮助广大网络技术人员提高网络管理技术水平，《网管员世界》杂志特别推出《网管员世界》2011 超值精华本，内容包括 2010 年全年《网管员世界》杂志中安全管理、故障诊断、系统运维、设备运维等栏目的所有精彩文章汇总。本书主要包括的内容如下。

- **安全管理：**网络安全是网管员在日常工作中关注的重点，安全管理将几十篇关于网络安全的实用性和应用性的文章呈现给广大读者，帮助读者朋友从容应对网络安全方面的问题。
- **故障诊断：**收集了《网管员世界》杂志社 2010 年故障诊断栏目中的精华文章和优秀专题，既可以作为网管员在日常工作中排障查错的工具手册，又可作为网管员提高网络管理水平的技术参考。
- **系统运维：**操作系统和各种应用程序的配置和管理也是网管员的工作范畴，系统运维以数十篇精彩的实例文章，剖析在操作系统和应用软件使用过程中遇到的各类问题的解决方法，为网管员朋友在操作系统和应用软件的配置和管理方面提供了众多的方法和技巧。
- **设备运维：**对于广大网络管理人员来说，网络设备的管理和维护是他们工作的主要组成部分，设备维护以大量精彩翔实文章为广大网络管理人员管理和维护网络提供了实战经验和参考，能够帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。

《网管员世界》杂志社

本书编委会

主 编: 孙浩峰

编 委: 张碧薇 孙红娜 袁绍军



《网管员世界》杂志社荣誉出品

网管员世界
NETADMIN WORLD MAGAZINE

CONTENTS 目录

第 1 章 安全管理

网站安全从小处着手	2	管好“人的行为”	19
系统安全	2	您的网络中有哪些“人”	19
网站配置安全	2	不同的“人”引发不同的风险	19
程序代码安全	2	管理人的行为的管理措施	21
数据库安全	3	管理人的行为的技术措施	21
用 DHCP 服务器保接入网络安全	3	Solaris 10 下的防火墙和 NAT 配置	23
安全接入思路	3	包过滤防火墙 IPFilter	23
创建合法性规则	4	编写 IPFilter 规则	23
配置合法上网参数	4	动手编写第一个规则	24
设置合法性标记	5	关闭 Solaris IP 过滤防火墙	25
控制网络接入安全	5	Solaris IP 过滤防火墙的监控和管理	25
Windows 7 加强自身安全两招	5	IPFilter 的不足	26
不让远程连接“拖累”系统	5	Solaris 10 NAT 配置实战	26
不让木马“进驻”临时文件	5	测试环境	27
在 IE 中限制访问某些网站	6	有毒环境下的安装测试	27
在 IE 中受管制的站点	6	小结	28
使用组策略阻止网站	6	有毒环境安全模式下安装测试	28
阻止部分用户访问网站	7	小结	28
给文件服务器聘个审核员	7	系统恢复测试	28
File System Auditor 介绍	7	自我免疫能力测试	29
FSA 安装须知	7	直面黑客的恶劣行径	30
运行配置	7	网站后台进不去了	30
查看审核效果	8	处理过程	30
小解“映像劫持”	9	小结	30
“映像劫持”实验	9	网站数据库服务器的安全维护	31
防范“映像劫持”	9	当病毒让桌面无法进入时	31
验证防范措施有效性	9	手术工具	31
用 360 安全卫士给内网打补丁	10	术前准备	31
文件服务器设置	10	手术过程	32
网管 PC 设置	10	防火墙作桥梁联通内外网	32
用户 PC 设置	10	防范 DDoS 攻击	33
网络版应用秘籍	10	DDoS 的检测	33
解决网络版管理故障	10	防范 DDoS 攻击	33
日志分析让升级一目了然	12	基于角色的防范	35
复合更新帮助移动设备升级	13	手动清除顽固恶意启动项	36
解决策略更改难题	14	漏洞, 黑洞! 如何管好安全漏洞	36
防火墙 route 模式部署实例	15	漏洞产生的危害	36
第一步: 连接	16	漏洞管理的必要性	37
第二步: 基本配置	16	漏洞管理的基本原则	37
第三步: 路由配置	16	漏洞管理的基本流程	37
第四步: 策略配置	16	漏洞扫描	38
为网络通信开辟绝密通道	17	部署漏洞管理系统	40
软件运行原理	17	让应用服务器更安全	41
安装服务器端程序	18	操作系统的安全设置	41
安装客户端程序	18	信息服务器的安全设置	43
		数据库服务器的安全设置	43

特殊应用服务器的安全.....	43	正确设置瑞星 2009 高级企业版.....	74
Linux 服务器的安全设置.....	43	正确设置趋势科技 Office Scan.....	76
解决校园网站被挂马问题.....	44	正确设置赛门铁克 SEP.....	77
发现网站被挂马.....	44	切断病毒入侵的通道.....	78
查找木马根源.....	44	切断远程入侵通道.....	78
清除木马和后门文件.....	45	切断远程连接通道.....	79
站点恢复测试.....	46	切断自动传播通道.....	79
防止网站被挂马的基本原则.....	46	切断共享入侵通道.....	79
利用组策略进行安全整改.....	47	揭开杀毒网站不能访问之谜.....	80
主机脆弱性分析.....	47	服务器 A 不能升级了.....	80
安全整改方法.....	47	临时解决问题.....	80
会补才强壮——如何打好系统补丁.....	53	找到真正的问题源.....	80
打补丁的重要性.....	53	事后感悟.....	81
打补丁易陷入误区.....	53	一起网络病毒的困扰.....	81
容易出现的问题.....	54	病毒症状.....	81
补丁管理的基本流程.....	55	查找病毒主机.....	81
补丁的测试.....	56	找到问题的根源.....	82
补丁的部署安装.....	57	总结.....	82
为 Windows Server 2008 设卡.....	60	用 OmniPeek 避免信息泄露.....	82
针对 Oracle 监听器的 DoS 防范.....	62	监控环境搭建.....	83
监听器的工作原理.....	62	分析数据包.....	83
实验环境.....	63	报文还原, 锁定 IP.....	84
正常运行情况.....	63	多种措施为机关网络护航.....	85
服务器 A 攻击步骤.....	63	加强入侵防御检测措施.....	85
攻击效果.....	65	加强防火墙的配置与应用.....	85
攻击防范.....	65	加强木马检测, 严格控制移动存储设备的使用.....	85
网络病毒请勿扰.....	67	构筑安全的服务器.....	85
网络环境.....	67	加强电脑准入措施.....	85
病毒分析.....	67	方便 = 高危! ——移动设备带来的威胁与防范策略.....	86
防护措施.....	67	移动设备 = 移动炸弹.....	86
写在最后.....	67	用管理措施避免移动炸弹.....	88
存储介质维修和报废时不能马虎.....	67	用技术手段避免移动炸弹.....	89
数据清除时存在误区.....	68	PPPoE 配置防 ARP 欺骗.....	91
维修过程中存在隐患.....	68	局域网 PPPoE 网络拓扑.....	91
报废过程中存在隐患.....	68	PPPoE 配置及注意问题.....	91
规范存储介质处理工作.....	68	PPPoE 客户端设置.....	92
定期检查涉密系统.....	68	小结.....	92
堵塞管理制度漏洞.....	68	感受 Avira 安全组合套装.....	93
使用 PGP 确保数据隐密和完整.....	68	改造政务应用系统安全架构.....	94
GnuPG 简介.....	68	升级改造迫在眉睫.....	94
详细使用方法.....	69	改造的基本思路.....	94
GnuPG 使用实例.....	71	改造的具体方向.....	94
GnuPG 使用技巧.....	72	八步实现数据库安全.....	95
合理设置杀毒软件.....	73	发现.....	95
选择反病毒产品的误区.....	73	漏洞和管理配置的管理.....	95
选择反病毒产品的依据.....	73	加固.....	95

CONTENTS

SQL Server 的安全配置	96	第二步, 对列表中的文件进行权限设置	117
SQL Server 安全的基本概念	96	第三步, 整合批处理	117
对变更的审核	96	后记	118
数据库活动的监视	96	阻击流氓软件	118
审核	96	第一步, 常规查杀	118
认证、访问控制、权利管理	96	第二步, PE 上阵	118
加密	96	第三步, 查到真凶	118
服务器安全	97	第四步, 清除流氓	118
数据库安全	98	域用户认证上网实施策略	119
模式安全	99	安装服务器	119
对象安全	99	Forefront TMG 认证配置	120
结论	100	天融信防火墙认证配置	120
基于 VLAN 的防火墙组网实例	100	寻找蠕虫攻击源	121
防火墙的接口特性	100	蠕虫病毒攻击行为分类	121
基于 VLAN 的防火墙应用实例	100	蠕虫病毒攻击源的定位	121
实例中防火墙与交换机的具体配置	101	总结	123
写在最后	102	别让下载乱了安全阵脚	124
构建透明防火墙	103	浏览器设置	124
环境搭建	103	设置组策略隐藏 Internet 选项	124
编译安装 Iptables-1.4.0	104	禁止非管理员用户使用组策略	124
编译安装 bridge-utils	104	如何保证数据安全	125
配置防火墙策略	105	数据面临的威胁	125
赤手空拳寻找 ARP 毒源	108	数据安全要点	126
掉网现象时有发生	108	保证数据安全的技术	126
ARP 病毒捣乱?	108	避免 Web 服务器被入侵	130
巧妙定位 ARP 毒源	108	控制目录安全性	130
隔离清除 ARP 病毒	109	控制文件安全性	131
双防火墙下构建专用商务网站	109	控制账号安全性	131
架设防火墙的目的	110	Linux 系统安全要点	132
总部网络拓扑概述	110	保障移动硬盘安全	132
规划物流系统网络并进行拓扑连接	110	控制移动硬盘连接安全	132
配置物流系统防火墙	110	控制移动硬盘使用安全	133
配置路由	111	控制移动硬盘泄露信息	133
配置路由	111	控制移动硬盘数据安全	134
冷启动内存映像攻击对策	112	修改注册表防止病毒感染优盘	134
冷启动内存映像攻击方法	112	修复另类的 IE 默认主页篡改	135
冷启动内存映像攻击工具的下载和创建	113	手工清除木马技巧	135
基于 USB 磁盘启动的冷启动内存映像攻击	113	发现木马	136
基于 PXE 方式的冷启动内存映像攻击	114	查找木马	136
分析内存映像文件	114	手工清除	137
应对之策	114	当心 Windows 7 欺诈性接入点	138
黑客入侵事件引发的思考	114	打造安全 ASP.NET 服务器	138
入侵案例	115	架设 ASP.NET 基本平台	138
事后体会	115	设置和管理账户	139
批量修改网站同类文件访问权限	116	权限设置	139
应用背景	116	网络服务安全管理	139
第一步, 生成需要设置权限的文件列表	116		

配置 IIS 服务	139	建立 MAC 数据库	165
建立一个 ASP.NET 站点	139	ARP 专用防火墙	165
C#.NET 实现防盗链	140	控制 BT 应用, 保护内网安全	166
工作原理	141	屏蔽 BT 下载端口	166
实施步骤	141	禁用 BT 下载程序	166
跨站脚本攻击及对策	142	限制连接服务器	167
跨站脚本攻击的概念	142	控制上传、下载速度	167
跨站脚本攻击的危害	142	禁止下载 BT 种子	167
跨站脚本攻击的方式与对策	142	各显神通加固 IE	168
防止跨站脚本攻击	143	关闭新的窗口, 防恶意广告	168
调教远程工具, 护驾远程控制	143	关闭脚本粘贴, 防隐私泄密	168
调教 Telnet	143	关闭保存功能, 防鱼龙混杂	168
调教 VPN 工具	144	关闭安全页面, 防安全破坏	169
调教远程桌面工具	145	关闭运行权限, 防病毒发作	169
从严管理账号, 控制访问安全	145	关闭颜色变化, 防目标暴露	169
取消组用户网络访问权	145	ARP 欺骗的检测与应对	169
为新用户设置合适权限	146	检测 ARP 欺骗	169
让特定用户拥有控制权	146	应对 ARP 欺骗	170
强制对用户进行网络验证	147	清除弹出广告	170
监控用户账号登录状态	147	杀毒需要掌握基本功	171
防范数据破坏的最佳实践	148	杀毒基本功	171
危机贯穿于数据生命周期中	148	杀毒前的准备	171
不同时期保护数据的技术手段	150	综合信息网络安全建设思路	172
恢复误删除的数据	152	企业综合信息网状况	172
拒绝 Word 杀手对数据的破坏	154	建立内网边界的准入体系	172
避免数据文件变成快捷方式	154	常见的杀毒方式	172
恢复被 Sola 病毒破坏的数据	155	建立身份认证实名系统	173
查杀破坏硬盘 MBR 的鬼影病毒	156	建立内网规则管理体系	173
数据备份, 预留一根救命稻草	156	您真的用好杀毒软件了吗	174
角色管理让 UNIX 更安全	158	您“安全退出”了吗	175
角色的概述	158	不得不提的浏览器运行机制	175
角色管理命令的使用	159	案例分析: 以登录淘宝网为例	175
使用 SMC 工具实现角色管理	160	深度探究	176
让网站服务器更安全	160	单机版也能自动离线升级	176
入侵案例	160	PHP 登录后台的防注入攻击	177
分析与防范	161	万能密码欺骗的一般原理	177
写在最后	162	PHP 下的万能密码欺骗	177
利用 FSA 监控审核需注意	162	应对办法	177
禁止优盘任意使用	163	解决 ARP 攻击六大妙招	178
按需为用户分类	163	妙招一, 使用 ARP 命令	178
创建优盘权限脚本	163	妙招二, 利用 BAT 批处理文件	178
营造安全使用环境	164	妙招三, 使用二分法查找	178
自动为用户分配权限	165	妙招四, 将 IP 地址与其对应的 MAC 地址进行静态绑定	178
ARP 欺骗防范措施	165	妙招五, 采用动态 ARP 检查	179
DHCP 结合静态 IP 捆绑法	165	妙招六, 网管型交换机的时间优势	179
网关上 IP 与 MAC 绑定	165		

CONTENTS

EFS 让文件访问安全进行	179	防范措施	197
认识 EFS 功能	179	MySQL 数据库安全配置	198
加密重要文件	180	MySQL 数据库基本安全配置	198
备份还原密钥	180	安全体系建设的深层思考	198
进行安全访问	181	MySQL 数据库安全加固	200
稳扎稳打应对数据库损害	182	用组策略提升 IE 安全	202
发生了什么	182		
遏制损害	182	第 2 章 故障诊断	
数据库日志可能成为关键	182	系统盘符更换之后的应对方法	205
检查其他日志	183	更换硬盘	205
调查内部人员	184	启动分区与系统分区的盘符发生对调	205
证据链的保全	184	经验总结	206
治理整顿	184	关于《路由器 IOS 升级失败之后》的个人观点	206
“零日”漏洞的挑战	185	Oracle 10g 登录错误两例	206
用 Web 过滤阻止非法通信	185	问题一	207
阻止或不阻止	185	问题二	207
Web 过滤实施策略	185	配置文件丢失导致 IIS 无法启动	208
选择适当的设备	186	故障分析	208
上网安全与行为管理实验	186	经验总结	208
作业行为的管理	187	反思	208
学生上网行为的管理	188	交换机端口间隔插	209
系统安全与软件使用行为管理	189	小知识	209
Telnet 认证方式安全性分析	190	部署 Exchange 邮件系统遇麻烦	209
Password 认证方式	191	Exchange 前后端体系	209
Ntlm 认证方式	191	误解前端服务器概念所致	209
选择正确的认证方式	191	解决方案	210
拿什么消除过期 Plugins	192	经验总结	211
“扼杀” ARP	192	瑞星 2010 防火墙导致 FTP 上传故障	211
ARP 欺骗的现象	192	故障排查	211
ARP 病毒的检测方法	193	ISA Server 2006 疑难问题解决	212
处理方案	193	ISA 502 错误	212
预防和注意事项	194	不能访问某些网站	212
警惕内部人员威胁	194	经验总结	212
离职员工的“小动作”	194	使用 Bandwidth Splitter 流量控制软件问题	213
掌握敏感数据员工的违规操作	195	关于 Crontab 的一场虚惊	213
“热心”的 IT 部门员工	195	发现问题	213
保护数据需要注意的问题	195	解决问题	213
渗透测试注意事项	196	关于 cron	213
测试范围	196	解决 ISA 发布 OWA 的域名问题	214
约束条件	196	问题原理分析	214
黑盒测试与白盒测试	196	“500”错误的解决	215
谁来进行渗透测试	196	“403”错误的解决	215
渗透测试的风险	196	经验总结	216
气象信息网络安全问题浅探	197	奇怪的浏览器显示故障	216
网络安全现状	197	故障现象	216
影响网络安全的主要因素	197		

故障分析及排除	216	TCP/IP 体系结构	232
经验总结	216	分层网络故障排查	232
揭开服务器失效的真相	217	又是灰尘惹的祸	233
光纤单通故障处理案例	218	故障分析	233
混乱的故障	218	故障解决	233
现场环境	218	故障原因分析	234
故障处理	218	经验总结	234
常见光纤衰减大的几种原因	218	探究以太网自动协商失败故障	234
经验总结	219	故障一	234
都是垃圾邮件惹的祸	219	故障二	234
问题排查	219	探究故障原因	234
关于 NDR 垃圾邮件	220	打印系统服务故障新花样	235
Exchange 中继	220	故障排查	235
解决方案	221	故障处理	236
经验总结	222	经验总结	236
软件 Bug 导致广播风暴	222	排除服务器 RAID 故障的启示	236
环境描述	222	故障分析与排除	236
故障现象描述	222	启示之一：按服务器服务类别选择 RAID 类型	237
故障排查过程	222	启示之二：依据故障现象，分析故障原因，准确定位故障点	237
DHCP Snooping+DAI 工作原理	222	启示之三：及时巡查核心设备，精心应对每一例故障	237
故障排除方法	223	启示之四：数据备份是网管人员不可或缺的工作	238
故障分析	223	文件收发出错为哪般	238
内存问题造成系统启动故障	223	桌面管理软件引发网络风暴	239
雷击背后的故障	224	故障描述	239
网线出现环路	224	排错步骤	239
交换机发生短路	225	经验总结	239
经验总结	225	邮件服务器为何被退信	240
更换设备网不通	225	硬盘版 Windows 7 为何无法启动	240
设置不变网却不通	225	故障现象	240
一波刚平一波又起	225	原因分析	240
了解网络结构	226	小工具解决大问题	241
故障解决	226	无线网卡无法识别故障	241
经验总结	227	故障现象	242
数据库过大导致 IIS6 出错	227	故障排查	242
问题解决过程	227	故障处理	242
问题回顾	228	再次实验	242
经验总结	228	小冲突与大危害	242
网卡的奇怪故障	228	地址冲突导致本地连接故障	243
用 Ping 命令切勿忽视源地址	228	故障现象：本地连接图标消失	243
Ping 命令的基本工作原理及数据包格式	229	深入追踪故障原因	243
网络拓扑情况及规划	229	重现本地连接图标	244
网络调试步骤及出现的问题	230	解除浏览器运行故障	245
经验总结	230	在 Windows XP 操作系统中卸载 IE8	245
限制 IP 连接数解决流量异常故障	230	在 Windows Vista 或 Windows Server 2008 下删除	
原来是“回路”惹的祸	231		
局域网故障管理	232		

CONTENTS

IE8	246	找到目标共享资源	255
路由器 DNS 设置故障一例	246	访问指定共享内容	255
故障现象	246	恢复共享列表显示速度	256
故障分析	246	解决路由包含问题	256
故障解决	246	发现问题	256
经验总结	247	解决过程	257
路由器升级引故障	247	经验总结	257
查病毒	247	两地携手 共排故障	257
查线路	247	参与人员及分工	257
路由器软件版本有问题	247	拓扑结构	257
经验总结	247	故障现象	257
网页遭遇篡改	247	网络分析篇	257
初步检查	248	程序代码排错篇	258
追根究底	248	经验总结	259
补救措施	248	浏览器冲突引发故障	259
经验总结	248	删除“我的电脑”下的 IE 图标	259
小毛病引起开机故障	249	故障现象	260
故障一	249	故障排查	260
故障二	249	经验总结	260
排查路由器频繁启动故障	249	详解交换机故障及排除	260
启动遇故障	249	物理层故障	260
去除灰尘	250	端口协商及自环故障	261
故障总结	250	VLAN 故障排除	261
解决 MySQL 的乱码	250	设备兼容性故障	261
查找故障原因	250	其他故障排除	261
解决故障思路	250	顺畅使用“共享”资源	262
故障排除过程	251	更改网段出口故障	262
经验总结	251	查看 IP 地址	262
交换机配置 PBR 报错	252	网络结构	262
报错一：%PLATFORM_PBR-3-UNSUPPORTED _RMAP: Route-map not supported for Policy- Based Routing	252	查看路由表	263
报错二：%PLATFORM_PBR-4-SDM_MISMATCH: PBR requires sdm template routing	252	STP 边缘端口及 BPDU 防护带来的故障	263
报错三：%PLATFORM_PBR-3-UNSUPPORTED _ RMAP: Route-map m-pbr not supported for Policy- Based Routing	252	故障描述	263
是谁阻塞了网络	252	故障判断	263
查交换机	253	问题实例	264
查病毒	253	MSTP 配置的相关问题	264
查网络环路	253	经验总结	265
寻根问底查原因	253	用 PDR 恢复数据	265
Windows 7 网络下的共享故障	254	探究蓝屏原因	266
权限使“任务计划”停步不前	254	解决系统安装蓝屏问题	266
解决 Windows 7 共享故障	254	系统安装方法	266
让“网络”图标重现桌面	255	网络频繁断线排查过程	267
		故障现象	267
		解决过程	267
		解决措施	267
		经验总结	268
		局域网故障排除一例	268

CONTENTS

故障现象	268	经验总结	283
故障排查	268	一起由 Hub 引起的故障	283
经验总结	269	故障描述	283
软件安装验证出错误	269	排错步骤	284
Serv-U FTP 服务器配置误区	270	经验总结	284
误区一：配置 Serv-U 中，域名等于客户端要 访问的域名。	270	ERP 系统为何无法连接	284
误区二：设置了虚拟目录等于目录允许访问	270	故障现象	284
双线路为何不能自动切换	271	解决过程	285
再遇“共享”难题	272	解决方法	285
服务被改引发网络故障	272	经验总结	285
故障原因	273	解决硬盘操作故障	286
解决方法	273	硬盘空间为何变小	286
故障原因	273	无法双击进入硬盘	286
解决方法	273	无法删除硬盘文件	287
故障原因	274	硬盘检测无法通过	287
解决方法	274	待机时硬盘无法休息	287
故障原因	274	光纤收发器电源故障解析	287
解决方法	274	主从域服务器不同步故障分析	288
设错网关让网络不堪重负	274	强制同步失败	288
网速突然变慢	275	故障排查	288
故障处理	275	经验总结	289
经验总结	276	校园网络故障解决四例	289
小心默认协议不匹配	276	增加的无线路由器无法上网	289
故障实例	276	正常工作的无线路由器突然无法上网	290
故障排除	277	本地网络连接速度显示为 10M	290
故障原因分析	277	一个虚拟子网网速变慢	290
串口负担让 VGA 信号失真	278	解决服务造成的打印故障	291
故障现象	278	网络掉包，物理线缆是“祸首”	291
故障分析	278	排查故障	291
排除故障	279	排除故障	292
排查环路故障	279	经验总结	292
IP 地址冲突的背后	279	U 盘故障引发软件安装错误	292
故障排查过程	279	IE 损坏殃及系统的搜索功能	293
解决方法	280	2M 专线为何不起作用	294
进一步的思考	280	故障分析	294
无法解析的 DNS 服务器	280	解决办法	294
服务器现状	280	路由器被冤枉了	295
网络接入设备	281	网线与传输速率不匹配故障	296
网络故障表现	281	故障排查	296
措施一	281	原因分析	297
措施二	281	故障排除	297
措施三	281	排除系统升级故障	298
故障分析	282	32 位与 64 位兼容问题	298
排除故障	282	域功能级别	298
集成网卡惹的祸	283	单网卡多 IP 引发故障	299

CONTENTS

故障现象	299	不启用 SNMP 服务进行安装网络打印机	312
排除过程	299	小结	313
查找故障原因	299	路由器的故障分析及排除	313
停电造成的奇怪故障	300	域账户频繁锁死为哪般	314
系统时间影响软件运行	300	拯救邮件服务器	315
网络故障常规处理方法	301	如何确定邮件服务器被列入禁用名单	315
故障排除方法分类	301	如何将邮件服务器从禁用名单中移除	316
典型案例	301	情况再次发生	316
总结并形成故障排除文档	301	防火墙引发终端连接失败	317
排查无线路由故障	301	工作环境	317
无线配置功能失效	302	连接失败	317
无法访问无线网络	302	深入排查	317
网络连接提示错误	302	解决问题	318
无法远程登录路由	302	故障原因分析	318
网络连接频繁掉线	302	故障反思	318
DNAT 映射出故障	303	系统试运行问题多	318
故障分析	303	问题一：无法正常安装 SQL Sever 2005 Express	319
故障解决	303	问题二：无法拷贝 SQL Sever 2005 数据库文件	319
FTP 服务模式很重要	303	问题三：无法附加数据库文件	319
登录 FTP 出问题	303	问题四：SQL Sever 2005 Express 与 Visual Studio 2005 无法建立关联	320
查看交换机策略设置	304	问题五：SQL Sever 用户 sa 无法登录	320
解决方案	304	问题六：客户端无法访问服务器端系统	320
知识链接：主动 FTP 与被动 FTP	304	问题七：SQL Server 服务程序无法访问网络	321
老电源遇到的新问题	305	网卡损坏众生相	321
“迷路”的系统变量	305	升级域控网速变慢	322
网络升级带来接入故障	306	故障现象	322
新购置模块损坏造成楼宇交换机不通	306	故障排查	322
情况不清造成百兆和千兆光模块混接	306	故障排除	322
消失的无线信号	307	经验总结	323
SNMP ENGINE “诱发”交换机 CPU 高负载	307	IIS 设置错误引发 WSUS 故障	323
初步排除故障	307	防火墙阻断 TCP 连接	324
测试查找故障原因	308	网络结构	324
分析故障原因	309	故障现象	324
故障解决	309	故障排除	324
经验总结	309	故障分析	325
别让管理距离迷了双眼	310	解决方法	325
无法登录网站	310	总结	325
故障分析及处理过程	310	一起源于主板的故障	326
经验总结	311	客户端为何无法加入域	326
软件版本并非越高越好	311	名称解析问题	326
网络打印机的非典型安装	311	权限问题	327
故障现象	311	数据通信（端口及防火墙）问题	327
默认配置引起的故障	312	查找 DHCP 服务进程占用内存故障	328
交换机的故障分析及排除	312	声音故障解决始末	329
故障分析	312	ISA 故障修复过程	330

故障现象	330	网站访问量时段图	348
排除过程	330	经验总结	349
经验小结	331	NFS 和 Samba 构建共享服务	349
VPN 中打开非 80 端口网速慢	331	安装 NFS 和 Samba	349
恢复故障 U 盘中的数据	332	配置 Samba 服务器	350
U 盘常见故障现象及可能引起的原因	332	配置 NFS 服务器	350
U 盘常见故障的数据恢复	332	Windows 共享、Samba 共享和 NFS 共享的综合使用	350
经验总结	333	访问共享资源	351
更改组网方式解决网络故障	333	一个 U 盘可以直接拔下的策略	351
原组网方式	333	Linux 下的编辑器与开发工具	352
新的组网方式	334	Linux 下常用的应用开发工具	352
出现的问题	334	Linux 下的文本编辑器	353
“破译”红外传输故障之谜	334	为 Linux 服务器更新静态路由	354
故障现象	335	Linux 下用网银	355
排查过程	335	Windows Server 2008 R2 中的远程协助	356
硬件排查	335	发布远程协助邀请	356
几点体会	336	远程协助	357
“望闻问切”排除网络故障	336	Windows Server 2008 R2 中的终端服务	357
网卡驱动丢失故障	337	Windows Server 2008 R2 中的终端服务	357
故障现象	337	安装终端服务	358
故障排查	337	创建签名证书	358
分析总结	338	安装签名证书	359
修复电子邮箱 Apache 故障	338	创建终端服务授权策略	359
故障表现	338	使用远程终端访问	360
故障恢复	338	Windows Server 2008 R2 终端服务远程程序	360
MAC 地址过滤，当心 VRRP	339	安装终端服务远程程序	361
网银超时故障排查	341	远程程序部署服务	361
浏览器问题	341	创建远程应用程序	361
验证码问题	341	设置终端服务远程程序用户	362
病毒问题	341	使用终端远程程序	362
局域网 NAT 问题	341	远程安装服务中集成驱动程序	362
单臂路由解决网络故障	342	收集驱动程序	363
“揪”出无法登录内网的祸首	342	集成驱动程序	363
事件起因	343	集成网卡驱动程序	364
问题追踪	343	配置 Linux 下的 TCP/IP 网络	364
经验总结	344	Linux 下的网络配置文件	364
视频线引起显示器故障	344	使用命令配置网络	364
		Linux 下的网络图形配置方式	365
		使用 Xinetd 启动 Linux 网络服务	366
		Windows 虚拟机中安装 Linux	367
		安装系统	367
		网络设置	368
		共享打印机设置	368
		创建基于 MNS 的服务器群集	369
		MNS 仲裁	369

第 3 章 系统运维

突破内网限制远程控制电脑	346
用 VNN 构建虚拟本地网	346
用 DameWare 远程控制电脑	346
经验总结	347
使用 Excel 进行 IIS 日志分析	347
分析前的准备工作	347
网站流量分析	348

CONTENTS

在 Node1 节点上创建第一个节点	370	测试远程连接	386
将 Node2 节点添加到群集中	370	有密码也自动登录	386
安装后的配置与观察	370	用网络分析技术管理网络	386
验证群集是否正常	370	是谁占用了我们的带宽	387
MNS 群集测试故障转移	370	在线音、视频类	387
“装入文件夹”功能扩大 C 盘空间	371	办公系统管理与维护	388
服务器现状	371	邮件系统的运行管理与维护	388
初步尝试	371	下载类软件	388
借助 NTFS 文件系统功能	371	其他类软件	388
合理部署网络分析软件	372	数据库的管理与维护	389
共享式网络	372	服务器安全的运行管理与维护	390
交换式网络 (带镜像功能)	372	Domino 服务器的备份和恢复	390
交换式网络 (不带镜像功能)	372	客户端的管理与维护	390
代理服务器共享上网	373	架设 PXE 服务器	391
带端口监控 (镜像) 的路由器	373	PXE 启动服务器的架设	391
Linux 系统中挂载 U 盘	373	PXE 启动 PE 的原理	392
开放环境应用瘦客户机	374	使用 Windows 2008 QoS 分配带宽	392
瘦客户机终端查询系统	375	QoS 设置	393
服务器端配置	375	设定客户机带宽	393
客户端配置	375	总结	394
中小企业应用开源的 P2P VPN N2N	376	文件保护功能确保系统稳定	394
中小企业 VPN 的选择	376	文件保护功能运行原理	394
选择 N2N	376	设置 Windows 文件保护扫描	394
N2N 构建 VPN	377	隐藏文件扫描进度窗口	395
经验总结	377	限制 Windows 文件保护缓存大小	395
让 Windows Server 2008 安全兼顾高效	378	指定 Windows 文件保护缓存位置	395
备份账户, 提升还原效率	378	跨 VLAN 扫描 IP 与 MAC 对应表	395
调用账号, 提升登录效率	378	巧解虚拟服务器 USB 问题	396
限制账号, 提升连接效率	378	共享 USB 设备	396
监视账号, 提升报警效率	379	操作步骤	396
空白账号, 提升控制效率	379	“USB Over Network”相关信息	397
将 Windows Server 2008 部署为 NAT 路由器	380	限制病毒修改系统时间	397
服务器网卡设置	380	方法一: 借助外部工具——360 安全卫士系统时间	
安装与配置路由和远程访问	380	防改工具	397
验证安装结果	381	方法二: 用 Windows XP 的组策略功能	397
小结	381	单台服务器托管解决方案	398
Linux 中应用远程桌面	381	以前方案存在的问题	398
理解 X Server	382	Windows Server 2008+ TMG2010+ Hyper-V Server	
Linux 下配置 XDM	382	不能共存	398
Windows 下 X-Win32 连接设置	383	解决思路	398
让火狐急速狂飙	384	单公网 IP 地址、单 Windows Server 2008 托管	
修改火狐自身设置, 提高 Firefox 响应速度	384	服务器、多虚拟机解决方案	399
设置本地 DNS 缓存, 加快 Firefox 访问速度	384	Solaris Zone 搭建测试环境	401
在 Windows Server 2008 中部署 SSH	385	Solaris 10 中的 Zone	402
安装 FreeSSHd	385	创建 Zone	402
设置 FreeSSHd	385	克隆 Zone	403

备份 Zone.....	403	网络共享文件夹管理.....	418
删除 Zone.....	403	共享文件夹权限与 NTFS 权限.....	419
用硬件卡克隆 Linux 集群.....	404	设置资源共享和 Web 共享.....	419
网络传输卡策略.....	404	SQL 2000 数据库迁移到 SQL 2005.....	420
恢复 Zone.....	404	场景介绍.....	420
软件传输策略.....	405	迁移规划.....	420
经验总结.....	406	SQL 2000 数据库迁移到 SQL 2005 的方案选择.....	420
穿透内网远程管理 Windows.....	406	方案测试.....	421
基于远程桌面配合边界策略的穿透.....	406	迁移后的测试.....	422
基于第三方软件的穿透.....	407	经验总结.....	422
探讨.....	408	远程更新 Web 网站.....	423
小结.....	408	Lotus 系统维护五例.....	424
正确设置 Windows Server 2008 服务器系统的上网参数.....	408	批量注册用户.....	424
搞定 Windows Server 2008 共享.....	408	设置用户邮箱限额.....	424
启用控制面板中网络和共享中心的共享和发现的各项功能.....	409	设置自动压缩.....	424
启用 Guest 账号, 修改组策略参数.....	409	修改邮件模板, 限制单个邮件大小.....	425
设置共享资源的访问权限.....	409	移动办公.....	425
SCCM 2007 电脑分组管理技巧.....	410	数据备份的方式.....	425
自动备份配置文件.....	411	OA 系统数据备份及运维.....	425
网站群内容管理系统.....	412	数据备份篇.....	426
基于 J2EE 的网站群内容管理系统.....	412	数据迁移篇.....	426
网站群内容管理系统的软硬件.....	412	数据恢复篇.....	427
J2EE、Tapestry、Spring、Hibernate 简介.....	413	经验总结篇.....	427
网站群内容管理系统主要模块功能.....	413	Windows 下守护进程脚本的实现.....	427
网站群内容管理系统的优势.....	414	使用 Tripwire 管理 Linux 文件.....	428
实施效果.....	414	软件安装.....	428
网络日常管理心得.....	414	创建密钥和签名.....	429
计算机命名规范化.....	414	编辑配置文件.....	429
网络内部 IP 和 MAC 地址登记.....	414	编辑策略文件.....	429
机房网络室登记.....	414	生成基准数据库.....	429
做好重要数据的日常备份工作.....	414	运行完整性检查.....	429
操作系统备份.....	414	查阅报告.....	430
对终端用户进行培训.....	414	升级基准数据库文件.....	430
Windows 下彻底卸载 Oracle.....	415	升级策略文件.....	430
第一步, 删除注册表中的相关项.....	415	改变 site key 和 local key.....	430
第二步, 修改系统的环境变量.....	415	利用 Samba 实现异构系统存储.....	430
第三步, 删除菜单和相关目录.....	416	网络环境.....	431
Linux 中使用软键盘.....	416	Smbclient 命令使用说明.....	431
安装软件包.....	416	实战演习.....	431
启动虚拟键盘.....	417	构建企业虚拟网络.....	432
实现不同 VLAN 间的网络唤醒.....	417	VMware NAT 服务.....	432
网络唤醒开机的基本原理.....	417	Team 中的虚拟网络.....	434
网络唤醒所需硬件支持及软件需求.....	418	让 VPN 连接访问内外网.....	435
实现不同 VLAN 网段之间的网络唤醒.....	418	不能访问的原因.....	435
		解决问题的思路.....	436
		实现步骤.....	436