Thomas Schenk et, al.

Caldera® OpenLinux™ System Administration

Expert Insight

This book provides, in one place, the core information a system administrator needs to know to administer any system that has Caldera OpenLinux including:

- Networking in NT, NetWare, and UNIX Environments
- Filesystem and Disk Management
- Backups and Disaster Recovery
- Configuring the X-Window System
- Shells and Scripting
- System Monitoring and Tuning
- Internet Services

Authoritative Advice

Implement the advice from expert author Thomas Schenk to meet all of your OpenLinux system administration needs

SAMS

Unleashed

FROM KNOWLEDGE TO MASTERY

Contents

Introduction 1

So You Want to Be a System Administrator 1
Who Is This Book's Intended Audience? 1
What Do You Need to Know Prior to Reading This Book? 1
What Will You Learn from This Book? 2
What Software Will You Need? 2
How This Book Is Organized 2
Conventions Used in This Book 4

PART I Introduction to Linux System Administration 5

1 What Is a Systems Administrator? 7

The Linux System Administrator 8
A Simple Definition 8
The SAGE Definition 9
Required Background and Skills 11
The Linux Person 11
Customer Service Orientation 12
The Ability to Thrive on Challenge 12
System Administrator Duties and Responsibilities 13
User Management 13
Hardware and Software Maintenance 14
Network Administration 14
Summary 15

2 Essential Tools for System Administrators 17

Power Tools for Superusers 18
UNIX Commands for Power Users 18
The Caldera OpenLinux Administration System (COAS) and LISA 31
Web Resources for Administrators 33
The Linux Documentation Project 34
Linux Kernel Archives and Kernelnotes 35
Linuxcare 36
Linux Today 37
Other Web Sites of Interest 38
Other Sources of Information 38
Mailing Lists 39
FTP Archives 40
Newsgroups 41
Summary 42

PART II Linux Essentials 43

3 Installation Strategies 45

Default Installation Versus Customized Approaches 46
Individual Installations 46
Scalability Issues 48
Cloning Installations 48
A Homegrown Approach 48
A Template-Based Approach 59
Establishing an Installation Template 60
Class-Based Customization 62
An Implementation Example 64
Summary 66

4 Where Do I Find...? 67

Hand Me That Map, Please 68
The Filesystem Hierarchy Standard 68
The Caldera Filesystem Layout 75
Examining Processes 77
The proc File System 77
Process Status Tools 83
Checking Devices 87
Device-Naming Scheme 93
Assigned Major and Minor Numbers 93
An Alternative Device Management Scheme 94
Summary 95

5 Starting Up and Shutting Down 97

Linux Boot Loaders 98
Boot Loader Overview 98
LILO, The Linux Loader 99
LILO Tips and Tricks 107
Alternatives to LILO 113
The Linux Boot Process and System Initialization Scripts 114
Kernel Startup and Device Initialization 114
/etc/inittab and rc Scripts 115
More About Runlevels 120
Shutting Down 123
Changing Runlevels 123
The `shutdown` Commands 124
Summary 125

6 System Failure Diagnosis and Recovery 127

Kernel Oops 128
Kernel Panic 129

Hardware Errors 129
BIOS Problems 130
Plug-and-Play (PnP) Devices 131
PCI Devices 131
Diagnostic Tools 133
Using /proc for Diagnosis 133
The `isapnp` Program 134
Network Interface Card (NIC) Diagnostics 134
DOS Diagnostics 137
Building and Using Rescue Disks 137
Building (or Borrowing) a Rescue Disk 138
Starting a Rescue Session 139
Rescue Disk Toolkit 139
Rebuilding LILO 139
Rewriting Configuration Files 140
Repairing a Partition 140
Emergency File Copying 141
Recovering Deleted Files 142
Analysis of System Logs 143
Interpreting Log Messages 143
Locating the Source of Kernel Errors 145
Decoding Kernel Errors 147
Using the System.map File 149
Seeking Assistance 150
Summary 151

PART III Filesystem and Disk Management 153

7 Filesystems 155

The Physical Realm 156
Single Versus Multiple Disks 156
Partitioning Strategies 157
Partitioning Using `fdisk` 159
Partitioning Using `cfdisk` 162
Partitioning Using `sfdisk` 164
Partitioning Using Lizard 167
Filesystem Creation and Management 168
Filesystem Tools 168
Developing Space Allocation Strategies and Estimating Growth 177
Filesystem Types 178
The Minix Filesystem 178
The Extended 2 Filesystem 179
Other Filesystem Types 179

Space Management and Quotas 180
Monitoring Space Usage 180
Local Versus Shared Filesystems 185
Establishing Filesystem Quotas....185
Summary 190

8 Adding or Replacing Disks 191

IDE Device Naming 192
IDE Disk Device Interface 192
Managing the /etc/fstab File 194
/etc/fstab File Format....194
Dissecting a Filesystem Configuration File (/etc/fstab) 195
SCSI Concerns 196
Selecting a Controller 198
Cabling Requirements 201
Device Termination and SCSI IDs 201
SCSI Device Naming 203
Other Devices 204
Summary 205

9 Linux and RAID 207

RAID Overview 208
Objectives of RAID....208
RAID Levels 210
Linux Software RAID....215
RAID Tools 215
Supported RAID Levels 220
Implementing Software RAID 226
Booting from a RAID Device 244
Hardware RAID and Linux 245
RAID Controller Drivers....246
External RAID Devices....247
Other Sources of Information....247
Summary....248

10 Removable Media Devices 251

Removable Media Devices 252
Floppy Drives 252
CD-ROM Drives 253
CD-R and CD-RW Drives....254
Parallel Port Storage Devices 265
Adding Support to Your Kernel....266
Configuring Zip Drives 267
Configuring Other Parallel Port ATAPI/IDE Devices....268
Using COAS For Device Configuration 269

Granting Access to Users 270
The mtools Package 270
Giving Users the Power to Mount 271
Automatic Mounting of Removable Media 273
A Hybrid Approach 274
Summary 275

PART IV Backups and Data Recovery 277

11 What to Back Up and How 279

Files to Back Up 280
System Configuration Files 280
User Files 281
Task-Oriented Files 281
Finding New Files 282
Determining Which Device to Use 283
Backup Strategies 283
Backup Commands 285
Choosing What to Back Up 287
Selecting a Strategy 288
Full Backups and Incrementals 291
Developing a Rotation Schedule 292
Rotation Example 1 293
Rotation Example 2 295
Reusing Backup Media 297
Developing Backup Scripts 300
Using the tar Command 301
Using dump and restore 302
Using cpio 303
Testing the Script 304
Third-Party Backup Software 304
Evaluating Backup Software 305
Summary 306

12 Media Selection and Storage 307

Sources of Information 308
Device Selection Criteria 308
The Autoloader Question 309
Media Selection Criteria 310
4mm DDS 311
8mm Exabyte 311
DLT 312
8mm/AIT 312

Tape Driver Interfaces 313
Floppy Tape Devices 313
ATAPI Tape Drives 313
SCSI Tape Devices 314
Storage Issues 315
Onsite Storage 315
Offsite Storage 315
Multiple Copies 316
Tape Escrow Services 316
Summary 317

13 Recovery from Data Loss 319

Some Data Loss Scenarios 320
User Errors 320
Viruses and Other Destructive Software 327
System Crackers and Malcontents 330
Hardware Failure 331
Other Disaster Scenarios 334
The Cost of Data Recovery 334
Direct Costs 334
Indirect Costs 335
Disaster Recovery Planning 336
Plan Development 337
Plan Maintenance 338
Summary 339

PART V Networking 341

14 TCP/IP and Ethernet 343

Network Layers 344
Network Access Layer 345
Internet Layer 345
Transport Layer 346
Application Layer 347
IP Addresses 347
Address Classes 347
Classless IP Addresses 348
Subnetting 349
Running TCP/IP over Ethernet 349
Ethernet Cards and Cables 350
Ethernet Hubs 351
Switches 351
Choosing Ethernet Media 352

Adding an Ethernet Interface 353
Routing 356
The Routing Table 357
Dynamic Routing 361
Name Services 367
DNS 368
Name Services on UNIX-Like Systems 369
Network Information Service 376
Summary 380

15 Sharing Resources 381

Sharing with Linux/UNIX Hosts 382
Sharing with Other Operating Systems 382
Setting Up Print Queues 383
Setting Up a Local Printer 383
Granting Access to Others 387
Setting Up a Remote Printer 391
Network File Services 392
NFS Server Configuration 393
The /etc/exports File 395
Using `exportfs` 397
NFS Client Configuration 398
AFS and Coda 400
The Automount Daemon and `autofs` 401
The BSD Automount Daemon 401
Linux `autofs` 404
Summary 406

16 Network Monitoring 407

Why Monitor? 408
Monitoring Systems 408
The Network Access Point 409
Packet Capture System 409
The Analysis Engine 413
Logging Subsystem 413
User Interface 413
Network Monitoring System Requirements 414
Deployment Methods 414
Sniffers 415
`tcpdump` 416
Uses for Sniffers 419
Dangers of Sniffers 421
Protecting Against Sniffers 422

Traffic Analyzers 422
ntop 423
Determining Network Bottlenecks 429
Analyzing Types of Traffic 430
Summary 432

17 Integrating with Windows NT Networks 433

Networking the Windows Way 434
Speaking the Lingo 434
A Simple NT Network 435
Linux and Samba in an NT Environment 436
Samba Overview 436
Analyzing the Samba Configuration File 449
Linux and Samba as a Client OS 456
Linux and Samba as a Server OS 459
Sources of Samba Help 463
Summary 464

18 Integrating with Other Network Operating Systems 465

Using the Right Tool for the Job 466
Linux in a NetWare Environment 467
NetWare Interoperability Options 467
The IPX Protocol 468
Linux as NetWare Client 469
Linux as NetWare Server 470
Starting the marsnwe Server 483
Linux in an AppleTalk Environment 484
Configuring Kernel AppleTalk Support 484
Configuring AppleTalk Services on Linux 485
Starting the Netatalk Server 495
Summary 496

Part VI Internet Services 497

19 Setting Up Internet Services 499

Choosing Services to Offer 500
Low-Level Services 500
Internet Services 500
Other Internet Services 501
The Internet Server inetd 501
The /etc/inetd.conf File 502
Using TCP-Wrappers 504
Logging 505
Access Control 505
Testing tcpd Configuration 507

xinetd as an Alternative to inetd 508
Standard Services: Remote Login, Execution, and File-Copy 511
telnet 511
The R-Commands 512
Secure Shell 517
Summary 521

20 Electronic Mail 523

MTAs, MUAs, and MDAs 524
SMTP Services 525
POP and IMAP Services 525
Dealing with Spam 527
Choosing an MTA 528
sendmail 528
smail 535
qmail 543
exim 544
fetchmail 547
Supporting Multiple Email Clients 549
Spool Access 549
Locking Issues 549
Using Popular Linux Email Clients 550
mail and mailx 550
elm and pine 551
xfmail 551
Managing Aliases 552
Structuring Aliases 552
Mandatory Aliases 553
Aliases Versus Mailing Lists 554
Distributed Management of Aliases 554
Mailing Lists with majordomo 554
Moderated Versus Unmoderated Lists 555
Open Versus Closed Lists 556
Privacy and Security 556
To Archive or Not to Archive 556
Archiving and FTP 557
Configuring a Digest-Only List 557
Summary 569

21 FTP and Anonymous FTP 571

FTP Objectives 572
FTP Connection Types 573

Allowing FTP Access to Your Servers 573
wuarchive-ftpd 574
wu-ftpd Information Sources 579
Alternative FTP Servers 581
Security and Legal Issues 582
Protecting Your FTP Servers 583
Modifying File Permissions and Removing Unneeded Files 594
Dealing with Warez D00dz 594
Summary 599

22 Web Serving 601

Apache 602
About the Apache Project 603
Installing Apache 604
Starting and Stopping Apache 605
Configuring Apache 606
Various Configuration Techniques 612
Security Tips 616
Apache Modules 617
Virtual Hosts 620
Apache Add-ons 624
Squid 625
Features of Squid 626
Starting Squid 626
Configuring Squid 627
Other Web Servers 628
Roxen Challenger 628
Stronghold 628
IBM HTTP Server Powered by Apache 629
Boa 629
dhttpd 629
fhttpd 629
ghttpd 630
thttpd 630
WN 630
Summary 631

23 News Services 633

So You Want to Run a News Server? 634
Capacity Planning 634
Running a News Server 636
Outsourcing News Services 637

INN and Friends 637
Installing INN 638
Choosing an Article Storage Format 642
Configuring INN 643
Spam Filtering Options with INN 661
Diablo 661
Using nntpcache 662
News Clients 664
Text Clients 664
Graphical Clients 666
Alternatives for Reading News 670
Places to Ask Questions and Find Answers 670
Summary 671

24 Internet Telephony and Conferencing 673

The Problems 675
Latency 675
Quality of Service 675
Packet Dropping 675
Software Requirements 676
Monopoly Power 676
Hardware Requirements 676
The Multicast Backbone 677
Internet Relay Chat (IRC) 680
ircII 681
Zircon, an X11 Client for IRC 683
kSirc 685
BitchX 686
ICQ and Clones 687
ICQ, IP-Masquerading, and Firewalls 687
JavaICQ from Mirabilis 687
licq 689
micq 690
Multimedia Conferencing Tools 691
Speak Freely 693
Q-SeeMe 694
CU-SeeMe 695
Summary 695

PART VII Security and Firewalls 697

25 Security Principles 699

Determining Your Security Needs 700
Types of Attacks 701

Securing Your Caldera Server 702
Passwords 702
System Files 708
Physical Security: Minimizing the Physical Risks 723
Securing Services 724
Check Your Log Files 726
Check Your Network Interfaces 727
Check for New setuid/setgid Files 727
Check /var/spool/cron 727
Check /var/spool/atjobs 728
Check for Altered System Files 728
Be Aware of the Latest Threats 728
Keep Your Software Up-To-Date! 728
Developing Security Policies 729
Setup Policies 729
Maintenance Policies 730
Reaction Policies 730
Making the Rules 730
Enforcing Strict Compliance 731
Dealing with Infractions 731
Summary 734

26 Firewalls 735

Types of Firewalls 736
Bastion Hosts 737
Firewall Policy 739
Linux Proxy Services 740
Linux Kernel Configuration 741
Transproxy 0.3 743
SOCKS Proxy Server 744
Squid 2.2 747
TIS Firewall Toolkit 749
Setting Up a Firewall 753
Packet Filtering 753
Packet Filtering with Linux 753
Debugging Firewalls 764
Summary 765

27 The Security Administrator's Toolbox 767

Building Your Security Administrator's Toolbox 768
Granting Privileges with sudo 768
Other Useful Tools 776
Sources of Security Tools 779

Security Resources on the Web 780
The USENIX Web Site 781
Caldera Security Information 781
Linux Portal Sites 781
Other Sources of Information 782
`comp.security.announce` and Other Usenet Newsgroups 782
Security Mailing Lists 784
Summary 786

28 I've Been Hacked...What Now? 787

Intruder Alert! Rules of Engagement 788
Gathering Evidence of Intrusion 789
Determining the Extent of Intrusion 790
Analyzing System Logs 790
Intrusion Detection Tools 792
Trinux as a Security Tool 793
Cleaning Up 798
Starting from Scratch 799
Deciding When to Throw in the Towel 799
Trusting Your Backups 800
Reinstalling from Media 801
Summary 801

PART VIII User Management and Interaction 803

29 Users and Groups 805

Working with Users and Groups 806
Establishing Groups 806
The Evils of Shared Accounts 807
Adding and Deleting User Accounts 808
Dealing with Disgruntled Users 808
Adding a User Manually 808
Some Notes on Editing /etc/passwd and /etc/group Manually 811
Adding a User Using the Command-Line Tools 811
Adding a User Using the GUI Tools 812
Editing Users with COAS 815
Manipulating User Accounts in Batch Mode 820
Disabling User Accounts 820
Deleting a User Account 820
`userdel` 821
Searching for User Files 821
Working with System Files 822
The /etc/passwd file 822
The /etc/group File 823

The /etc/shadow File 824
The /etc/gshadow File 825
The /etc/login.defs File 826
The /etc/skel and /etc/skel.d Directories 826
Using Groups Effectively 826
groupadd 827
groupdel 827
groupmod 827
grpck 828
Adding a Group Using the GUI Tools 828
Creating Groups with Clear Boundaries 829
Using Groups to Grant Permissions 829
Using the newgrp and sg Commands 830
newgrp 830
sg 830
Employing Other System Commands Related to Users and Groups 831
chage 831
chfn 831
chgrp 832
chown 832
chsh 833
gpasswd 833
groups 834
passwd 834
su 834
usermod 835
Summary 836

30 Helping Users 837

Users Are Not Losers 838
Establishing the Ground Rules 838
Dealing with Interruptions 841
Developing a Help Desk 844
Qualities of a Good Help Desk 845
Help Desk Manning Strategies 846
An Open Source Solution 847
Alternatives to WREQ 858
Learning How to Say No 859
The Customer Isn't Always Right 859
Dealing with Troublesome Users 860
Granting No Exceptions 862
Summary 863

PART IX Shells, Scripting, and Automation 865

31 Shells 867

Getting Started with Shells 868
Shell Differences and Similarities 868
Selecting a Shell for Interactive Use 870
Interactive and Noninteractive Modes 870
bash: The Bourne Again Shell 870
Features of bash 871
Wildcards 871
Aliases 873
Command-Line Completion 874
Pipes 875
Input and Output Redirection 875
History 876
Command-Line Editing 878
Job Control 879
Built-In Commands 881
Startup for Interactive Sessions 882
Startup for Noninteractive Sessions 883
Quoting 883
bash Variables 884
Modifying the Command Prompt 886
Advantages and Disadvantages of bash 887
tcsh: The Enhanced C Shell 887
Features of tcsh 887
Wildcards 888
Aliases 888
Command-Line Completion 889
Spelling Correction 889
Pipes 889
Input and Output Redirection 889
History 890
Job Control 891
Built-In Commands 892
Key Bindings 893
Startup and Shutdown for Interactive Sessions 896
Automatic, Periodic, and Timed Events 897
Variables 897
Editing the Command Prompt 899
Advantages and Disadvantages of tcsh 900

Other Shells 900
The Z Shell 901
The Public Domain Korn Shell 901
The K Desktop Environment 902
Summary 902

32 Shell Scripting 903

Introduction to Shell Scripting 904
The Importance of Shell Scripting 904
Interpreted Versus Compiled 906
Selecting Your Scripting Shell 907
Standardization 908
Shell Scripting Using bash 908
bash Syntax 909
Creating and Using Variables 911
Expressions 915
Control Structures 919
Built-In Commands 925
Parsing Command-Line Parameters 934
Using Functions 936
Some Sample bash Scripts 938
Debugging Shell Scripts 940
Perl Scripting 941
Features of Perl 941
Getting Started with Perl 942
Control Structures 943
Learning More 944
Other Scripting Languages 945
Tcl/Tk 945
Python 946
Programming Tools 947
`make` 947
RCS 948
CVS 949
Summary 949

33 Automation 951

Managing Chaos 952
Automating Tasks 954
Automation Is Your Friend 955
Using `at` for One-Time Tasks 956
The `at` Utility 956
Examples of Using `at` 959

The batch Utility 961
The atq Utility 962
The atrm Utility 963
The atrun Utility 963
The at Daemon 964
Specifying Which Users Can Use at 965
Using cron 965
cron Startup 966
Using crontab Effectively 967
The Anatomy of a crontab Entry 969
Global cron Files 972
Examples of Using cron 972
Specifying Which Users Can Use cron 973
Debugging cron Jobs 974
Capturing Output 974
Using printf and echo as Debugging Tools 974
Examining the Log Files 976
Summary 977

PART X System Tuning and Kernel Building 979

34 Tuning Your Linux System 981

Tuning Considerations 982
General Tuning Areas 982
Unrequired Services 984
Weighing Costs and Benefits of Tuning 985
Hardware and Man Hours 985
Risk 986
Performance Measurement Techniques 987
Console Tools 988
Graphical Utilities 994
Real-Time Versus Gathered Performance Data 996
Process Management 997
Checking the Network Interface 998
Memory and Swap Space 999
Choosing the Right Amount of RAM 999
Swap Space Priorities 1002
Swap Partitions Versus Swap Files 1005
Kernel Tuning via /proc 1006
What Is /proc? 1007
Tunable Parameters in /proc 1009
Using echo to Alter System Behavior 1009
Summary 1010

35 Customizing the Linux Kernel 1011

Using the Source....1012
Why Recompile?....1012
Obtaining the Source....1013
Kernel Sources and Patches Provided by Caldera....1016
Kernel Source Code Layout....1018
Patching the Kernel Source....1019
Official Versus Unofficial Patches....1020
Where to Obtain Patches....1021
Kernel Loadable Modules....1022
Advantages of Modular Kernels....1023
Enabling Module Support....1024
The Module Utilities....1025
When Not to Use Modules....1026
Kernel Building....1027
Configuring the Linux Kernel....1027
Tweaking the Makefile....1052
Handling Multiple Versions of the Kernel....1053
Custom Installation Scripts....1057
Running `make`....1058
Summary....1059

36 Case Study 1061

A Brief Background....1062
Organizational Initiatives....1062
Director of Technology....1062
The Challenge....1063
Against the Odds....1063
Requirements....1064
Constraints....1065
Facilities and Connectivity....1065
Budget Constraints....1065
Technical Expertise and Knowledgeable Management....1066
The Carlos Effect....1067
Enter Linux and Caldera's OpenLinux 2.2....1067
OpenLinux Helps APISD Meet Requirements....1068
OpenLinux and the Internet....1069
Specifications....1069
Short-Term Objectives....1070
Long-Term Objectives....1070
Documenting the Project....1071
Web Server....1072

Network Authentication, Access, and User Administration 1073
Networking Macintosh Computers in the Linux Environment 1075
Administrative Control 1077
Internet Access.....1078
Distributing the TAAS Grading Application.....1079
Electronic Mail 1079
Centralized Management.....1080
Content Management Using TCP Wrappers.....1082
Using an FTP Server 1083
Reviewing the Aransas Pass Independent School District Case Study 1083

Index 1085