

Table of Contents

Appendix A. The Five–Minute RCS Tutorial.....	1
A.1. References for More Information.....	2
Appendix B. The Ten–Minute LDAP Tutorial.....	4
B.1. LDAP Data Organization.....	5
Appendix C. The Eight–Minute XML Tutorial.....	9
C.1. XML Is a Markup Language.....	9
C.2. XML Is Picky.....	10
C.3. Two Key XML Terms.....	12
C.4. Leftovers.....	13
Appendix D. The Fifteen–Minute SQL Tutorial.....	14
D.1. Creating /Deleting Databases and Tables.....	15
D.2. Inserting Data into a Table.....	16
D.3. Querying Information.....	17
D.3.1. Retrieving All of the Rows in a Table.....	18
D.3.2. Retrieving a Subset of the Rows in a Table.....	18
D.3.3. Simple Manipulation of Data Returned by Queries.....	19
D.3.4. Adding the Query Results to Another Table.....	20
D.4. Changing Table Information.....	21
D.5. Relating Tables to Each Other.....	22
D.6. SQL Stragglers.....	23
D.6.1. Views.....	23
D.6.2. Cursors.....	24
D.6.3. Stored Procedures.....	24
Appendix E. The Twenty–Minute SNMP Tutorial.....	26
E.1. SNMP in Practice.....	31
Preface.....	37
0.1. How This Book Is Structured.....	37
0.2. Typographical Conventions.....	38
0.3. How to Contact Us.....	39
0.4. Acknowledgments.....	40
1.1. System Administration Is a Craft.....	43
1.2. How Perl Can Help.....	43
1.3. This Book Will Show You How.....	43
1.4. What You Need.....	45
1.5. Locating and Installing Modules.....	46
1.5.1. Installing Modules on Unix.....	48
1.5.2. Installing Modules on Win32.....	48
1.5.3. Installing Modules on MacOS.....	49
1.6. It's Not Easy Being Omnipotent.....	49
1.6.1. Don't Do It.....	50
1.6.2. Drop Your Privileges as Soon as Possible.....	50
1.6.3. Be Careful When Reading Data.....	50
1.6.4. Be Careful When Writing Data.....	51
1.6.5. Avoid Race Conditions.....	52
1.6.6. Enjoy.....	53
1.7. References for More Information.....	53
2.1. Perl to the Rescue.....	54

Table of Contents

Preface

2.2. Filesystem Differences.....	55
2.2.1. Unix.....	55
2.2.2. Microsoft Windows NT/2000.....	56
2.2.3. MacOS.....	56
2.2.4. Filesystem Differences Summary.....	56
2.2.5. Dealing with Filesystem Differences from Perl.....	58
2.3. Walking or Traversing the Filesystem.....	58
2.4. Walking the Filesystem Using the File::Find Module.....	59
2.5. Manipulating Disk Quotas.....	59
2.5.1. Editing Quotas with edquota Trickery.....	64
2.5.2. Editing Quotas Using the Quota Module.....	72
2.6. Querying Filesystem Usage.....	73
2.7. Module Information for This Chapter.....	77
2.8. References for More Information.....	78
3.1. Unix User Identity.....	80
3.1.1. The Classic Unix Password File.....	80
3.1.2. Extra Fields in BSD 4.4 passwd Files.....	82
3.1.3. Binary Database Format in BSD 4.4.....	82
3.1.4. Shadow Passwords.....	83
3.2. Windows NT/2000 User Identity.....	87
3.2.1. NT/2000 User Identity Storage and Access.....	87
3.2.2. NT/2000 User ID Numbers.....	88
3.2.3. NT/2000 Passwords.....	89
3.2.4. NT Groups.....	89
3.2.5. NT/2000 User Rights.....	90
3.3.1. The Backend Database.....	91
3.3.1.1. Writing XML from Perl.....	92
3.3.1.2. Reading XML using XML::Parser.....	94
3.3.1.3. Reading XML using XML::Simple.....	97
3.3.1.4. Writing XML using XML::Simple.....	98
3.3.2. The Low–Level Component Library.....	100
3.3.2.1. Unix account creation and deletion routines.....	102
3.3.2.2. Windows NT/2000 account creation and deletion routines.....	105
3.3.3. The Process Scripts.....	107
3.3.4. Account System Wrap–Up.....	110
3.3. Building an Account System to Manage Users.....	110
3.4. Module Information for This Chapter.....	113
3.5. References for More Information.....	116
3.5.1. Unix Password Files.....	120
3.5.2. NT User Administration.....	122
3.5.3. XML.....	122
3.5.4. Other.....	122
4.1. MacOS Process Control.....	123
4.2. NT/2000 Process Control.....	123
4.2.1. Using the Microsoft Resource Kit Binaries.....	124
4.2.2. Using the Win32::IProc Module.....	125
4.2.3. Using the Win32::Setupsup Module.....	125
4.2.4. Using Window Management Instrumentation (WMI).....	127
4.3. Unix Process Control.....	127
4.3.1. Calling an External Program.....	128
4.3.2. Examining the Kernel Process Structures.....	131

Table of Contents

Preface

4.3.3. Using the /proc Filesystem.....	135
4.3.4. Using the Proc::ProcessTable Module.....	140
4.4. Tracking File and Network Operations.....	141
4.4.1. Tracking Operations on Windows NT/2000.....	141
4.4.2. Tracking Operations in Unix.....	142
4.5. Module Information for This Chapter.....	142
4.5.1. Installing Win32::IProc.....	146
4.5.2. Installing Win32::Setupsup.....	146
4.6. References for More Information.....	149
5.1. Host Files.....	153
5.1.1. Generating Host Files.....	154
5.1.2. Error Checking the Host File Generation Process.....	154
5.1.3. Improving the Host File Output.....	155
5.1.4. Incorporating a Source Code Control System.....	157
5.2.1. NIS+.....	157
5.2.2. Windows Internet Name Server (WINS).....	159
5.2. NIS, NIS+, and WINS.....	161
5.3. Domain Name Service (DNS).....	162
5.3.1. Generating DNS Configuration Files.....	165
5.3.1.1. Creating the administrative header.....	168
5.3.1.2. Generating multiple configuration files.....	170
5.3.2. DNS Checking: An Iterative Approach.....	171
5.3.2.1. Using nslookup.....	171
5.3.2.2. Working with raw network sockets.....	172
5.3.2.3. Using Net::DNS.....	173
5.4. Module Information for This Chapter.....	175
5.5. References for More Information.....	180
6.1. What's a Directory?.....	181
6.2. Finger: A Simple Directory Service.....	182
6.3. The WHOIS Directory Service.....	186
6.4. LDAP: A Sophisticated Directory Service.....	188
6.4.1. LDAP Programming with Perl.....	188
6.4.2. The Initial LDAP Connection.....	190
6.4.3. Performing LDAP Searches.....	190
6.4.4. Entry Representation in Perl.....	191
6.4.5. Adding Entries with LDIF.....	194
6.4.6. Adding Entries with Standard LDAP Operations.....	196
6.4.7. Deleting Entries.....	197
6.4.8. Modifying Entry Names.....	198
6.4.9. Modifying Entry Attributes.....	199
6.4.10. Putting It All Together.....	203
6.5. ADSI (Active Directory Service Interfaces).....	205
6.5.1. ADSI Basics.....	208
6.5.2. Using ADSI from Perl.....	209
6.5.3. Dealing with Container/Collection Objects.....	210
6.5.4. Identifying a Container Object.....	210
6.5.5. So How Do You Know Anything About an Object?.....	213
6.5.6. Searching.....	218
6.5.7. Performing Common Tasks Using the WinNT and LDAP Namespaces.....	218
6.5.8. Working with Users via ADSI.....	220
6.5.9. Working with Groups via ADSI.....	222

Table of Contents

Preface

6.5.10. Working with File Shares via ADSI.....	222
6.5.11. Working with Print Queues and Print Jobs via ADSI.....	223
6.5.12. Working with NT/2000 Services via ADSI.....	225
6.6. Module Information for This Chapter.....	227
6.7. References for More Information.....	228
6.7.1. Finger.....	229
6.7.2. WHOIS.....	230
6.7.3. LDAP.....	230
6.7.4. ADSI.....	232
7.2.1. DBI Leftovers.....	233
7.1. Interacting with an SQL Server from Perl.....	234
7.2. Using the DBI Framework.....	234
7.3. Using the ODBC Framework.....	234
7.4. Server Documentation.....	234
7.4.1. MySQL Server via DBI.....	235
7.4.2. Sybase Server via DBI.....	237
7.4.3. MS–SQL Server via ODBC.....	238
7.5. Database Logins.....	240
7.6. Monitoring Server Health.....	244
7.6.1. Space Monitoring.....	245
7.6.2. Monitoring the CPU Health of a SQL Server.....	248
7.7. Module Information for This Chapter.....	249
7.8. References for More Information.....	250
7.8.1. SQL.....	251
7.8.2. DBI.....	253
7.8.3. ODBC.....	255
7.8.4. Other Topics.....	255
8.1.1. Getting sendmail (or Similar Mail Transport Agent).....	258
8.1.2. Using the OS–Specific IPC Framework.....	261
8.1.3. Speaking to the Mail Protocols Directly.....	261
8.1. Sending Mail.....	261
8.2. Common Mistakes in Sending Email.....	261
8.2.1. Overzealous Message Sending.....	262
8.2.1.1. Controlling the frequency of mail.....	262
8.2.1.2. Controlling the amount of mail.....	263
8.2.2. Subject Line Waste.....	263
8.2.3. Insufficient Information in the Message Body.....	264
8.3. Receiving Mail.....	264
8.3.1. Dissecting a Single Message.....	266
8.3.2. Dissecting a Whole Mailbox.....	268
8.3.3. Tracking Down Spam.....	269
8.3.3.1. Checking against a local blacklist.....	269
8.3.3.2. Checking against Internet–wide blacklists.....	271
8.3.4. Support Mail Augmentation.....	277
8.4. Module Information for This Chapter.....	277
8.5. References for More Information.....	279
9.1. Text Logs.....	279
9.2. Binary Log Files.....	280
9.2.1. Using unpack().....	281
9.2.2. Calling an OS (or Someone Else's) Binary.....	284
9.2.3. Using the OS's Logging API.....	287

Table of Contents

Preface

9.3. Stateful and Stateless Data.....	291
9.4. Disk Space Problems.....	296
9.4.1. Log Rotation.....	297
9.4.2. Circular Buffering.....	299
9.4.2.1. Input blocking in log processing programs.....	299
9.4.2.2. Security in log processing programs.....	300
9.5. Log Analysis.....	300
9.5.1. Stream Read–Count.....	302
9.5.1.1. A simple stream read–count variation.....	303
9.5.2. Read–Remember–Process.....	305
9.5.3. Black Boxes.....	307
9.5.4. Using Databases.....	307
9.5.4.1. Using Perl–only databases.....	309
9.5.4.2. Using Perl–cliented SQL databases.....	312
9.6. Module Information for This Chapter.....	312
9.7. References for More Information.....	313
10.1. Noticing Unexpected or Unauthorized Changes.....	313
10.1.1. Local Filesystem Changes.....	317
10.1.2. Network Service Changes.....	318
10.2. Noticing Suspicious Activities.....	326
10.2.1. Local Signs of Peril.....	328
10.2.2. Finding Problematic Patterns.....	328
10.3. SNMP.....	333
10.3.1. Using SNMP from Perl.....	335
10.4. Danger on the Wire.....	336
10.4.1. Perl Saves the Day.....	337
10.5. Preventing Suspicious Activities.....	338
10.6. Module Information for This Chapter.....	338
10.7. References for More Information.....	342
10.7.1. Change Detection Tools.....	344
10.7.2. SNMP.....	344
10.7.3. Other Resources.....	345
Colophon.....	350
Copyright © 2001 O'Reilly & Associates, Inc. All rights reserved.....	351
Logos and Trademarks.....	358
Disclaimer.....	358
Table of Contents.....	366

Chapter 1. Introduction.....	370
------------------------------	-----

Chapter 2. Filesystems.....	370
-----------------------------	-----

Chapter 3. User Accounts.....	371
-------------------------------	-----

Chapter 4. User Activity.....	371
-------------------------------	-----

Chapter 5. TCP/IP Name Services.....	372
--------------------------------------	-----

Chapter 6. Directory Services.....	373
------------------------------------	-----

Table of Contents

Chapter 7. SQL Database Administration.....	374
Chapter 8. Electronic Mail.....	374
Chapter 9. Log Files.....	374
Chapter 10. Security and Network Monitoring.....	375