## Contents at a Glance

- **Introduction** xxiii

### Part I: Capacity Planning
- **CHAPTER 1** Measuring and Troubleshooting Resource Usage 3
- **CHAPTER 2** Predict Future Resource Needs 27

### Part II: Managing the Kernel
- **CHAPTER 3** Kernel Components and Compiling 41
- **CHAPTER 4** Kernel Runtime Management and Troubleshooting 63

### Part III: Managing System Startup
- **CHAPTER 5** Customizing SysV-init System Startup 91
- **CHAPTER 6** Administrating System Recovery 109
- **CHAPTER 7** Alternate Boot Loaders 135

### Part IV: Managing Filesystem and Devices
- **CHAPTER 8** Operating the Linux Filesystem 151
- **CHAPTER 9** Maintaining a Linux Filesystem 171
- **CHAPTER 10** Creating and Configuring Filesystem Options 195

### Part V: Administrating Advanced Storage Device
- **CHAPTER 11** Configuring RAID 211
- **CHAPTER 12** Adjusting Storage Device Access 231
- **CHAPTER 13** Logical Volume Manager 253

### Part VI: Configuring the Network
- **CHAPTER 14** Basic Network Configuration 281
- **CHAPTER 15** Advanced Network Configuration and Troubleshooting 299
- **CHAPTER 16** Troubleshooting Network Issues 319

### Part VII: Performing System Maintenance
- **CHAPTER 17** Make and Install Programs from Source 343
- **CHAPTER 18** Backup Operations 359
- **CHAPTER 19** Notify Users on System-Related Issues 379

### Part VIII: Administrating Domain Name Server
- **CHAPTER 20** Basic DNS Server Configuration 395
- **CHAPTER 21** Create and Maintain DNS Zones 417
- **CHAPTER 22** Securing a DNS Server 439
Contents

Introduction xxiii

Part I: Capacity Planning

Chapter 1 Measuring and Troubleshooting Resource Usage 3
   “Do I Know This Already?” Quiz 3
   Foundation Topics 6
   Monitoring Your System 6
   CPU Monitoring 7
      Basic CPU Load Information 7
      Detailed CPU Load Information 7
   Memory Monitoring 10
      Basic Memory Usage Information 10
      Detailed Memory Usage Information 11
   Disk I/O Monitoring 12
      Listing Open Files 14
   Network I/O Monitoring 17
   Additional Monitoring Tools 18
      Listing Processes 18
      Displaying User Activity 21
   Exam Preparation Tasks 22
   Review All Key Topics 22
   Define Key Terms 23
   Review Questions 23

Part II: Managing the Kernel

Chapter 2 Predict Future Resource Needs 27
   “Do I Know This Already?” Quiz 27
   Foundation Topics 29
   The collectd Daemon 29
      Configuring collectd 29
      Installing collectd 31
   Monitoring Solutions 33
      Nagios 33
      MRTG 33
      Cacti 33
      sar 34
      Further Considerations 34
   OK, Now What? 34
   Exam Preparation Tasks 36
   Review All Key Topics 36
   Define Key Terms 36
   Review Questions 36
Chapter 3  Kernel Components and Compiling  41
“Do I Know This Already?” Quiz  41
Foundation Topics  43
Kernel Components  43
   Kernel Documentation  43
   Tweaking the Kernel  44
   Kernel Images  45
Compiling the Kernel  46
   Cleaning the Kernel  47
   Create the Configuration File  48
   Compiling the Kernel  55
Additional Make Targets  57
Exam Preparation Tasks  58
Review All Key Topics  58
Define Key Terms  58
Review Questions  58

Chapter 4  Kernel Runtime Management and Troubleshooting  63
“Do I Know This Already?” Quiz  63
Foundation Topics  65
Kernel Modules  65
   Module Files  65
   Listing Modules That Are Loaded  67
   Loading Modules into Memory  68
   Unloading Modules from Memory  71
   Listing Modules Information  71
   The /proc/sys Filesystem  73
   Module Aliases  76
Displaying Hardware Information  77
   The lspci Command  77
   The lsdev Command  81
   The lsusb Command  82
   The udev System  85
Exam Preparation Tasks  87
Review All Key Topics  87
Define Key Terms  87
Review Questions  88

Part III: Managing System Startup

Chapter 5  Customizing SysV-init System Startup  91
“Do I Know This Already?” Quiz  91
Foundation Topics  93
Chapter 6  Administrating System Recovery  109

“Do I Know This Already?” Quiz  109

Foundation Topics  111

Understanding the Boot Process  111

The BIOS/UEFI Phase  111
The Boot loader Phase  111
The Kernel Phase  112
The Post-Kernel Phase  113

GRUB  113

Legacy GRUB Configuration  114
Changing Legacy GRUB During Boot  117
Booting to Single User Mode in Legacy GRUB  120
Securing Legacy GRUB  122
GRUB 2 Configuration  125
Saving GRUB 2 Changes  127
GRUB 2 Titles  127
Booting to Single User Mode in GRUB 2  128
Securing GRUB 2  128

Fixing Filesystems  130
Exam Preparation Tasks  131
Review All Key Topics  131
Define Key Terms  131
Review Questions  132

Chapter 7  Alternate Boot Loaders  135

“Do I Know This Already?” Quiz  135

Foundation Topics  137
LILO  137
Chapter 12  Adjusting Storage Device Access  231

“Do I Know This Already?” Quiz  231
Foundation Topics  233
DMA, hdparm, and sdparm  233
The hdparm Command  234
The sdparm Command  236
System Resources  237
Kernel Parameters  239
iSCSI  241
Target Configuration  242
Initiator Configuration  244
Exam Preparation Tasks  248
Review All Key Topics  248
Define Key Terms  248
Review Questions  249

Chapter 13  Logical Volume Manager  253

“Do I Know This Already?” Quiz  253
Foundation Topics  255
Logical Volume Manager Concepts  255
Advantages of LVM on a System with a Single Drive  257
LVM Essentials  258
Extents  259
Logical Volumes  262
Device Naming  263
Using Logical Volumes and Additional LVM Commands  264
Displaying LVM Information  265
Additional LVM Commands  268
Resizing Logical Volumes  271
LVM Snapshots  274
Exam Preparation Tasks  277
Review All Key Topics  277
Define Key Terms  278
Review Questions  278

Part VI: Configuring the Network

Chapter 14  Basic Network Configuration  281

“Do I Know This Already?” Quiz  281
Foundation Topics  283
Part VII: Performing System Maintenance

Chapter 17 Make and Install Programs from Source 343

“Do I Know This Already?” Quiz 343
Foundation Topics 345
Securing and Unpacking Source Code 345
  D.ownloading Source Code on RPM-Based Systems 345
  D.ownloading Source Code on Debian-Based Systems 347
  D.ownloading Source Code from Original Source 348
  Unpacking the Source Code 349
Building and Installing from Source Code 350
Applying Patches 353
Exam Preparation Tasks 354
Review All Key Topics 354
Define Key Terms 355
Review Questions 355

Chapter 18 Backup Operations 359

“Do I Know This Already?” Quiz 359
Foundation Topics 361
Backup Strategy 361
  What Needs to Be Backed Up? 361
  How Often? 364
  Full or Incremental? 364
  Where Will the Backup Be Stored? 367
  What Backup Tool Will Be Used? 367
Standard Backup Utilities 368
  The dd Command 368
  The tar Command 369
  The rsync Command 373
Third-Party Backup Utilities 374
  Amanda 374
  Bacula 374
  BackupPC 374
Exam Preparation Tasks 375
Review All Key Topics 375
Define Key Terms 375
Review Questions 375

Chapter 19 Notify Users on System-Related Issues 379

“Do I Know This Already?” Quiz 379
The Address Record Type 425
The Canonical Name Type 425
The Name Server Record Type 426
The Mail eXchange Record Type 426
The PoinTeR Record Type 427
Putting It All Together 427
Testing the DNS Server 431
The dig Command 432
The \texttt{nslookup} and \texttt{host} Commands 433
Exam Preparation Tasks 434
Review All Key Topics 434
Define Key Terms 434
Review Questions 434

Chapter 22  
Securing a DNS Server 439
“Do I Know This Already?” Quiz 439
Foundation Topics 441
Send BIND to Jail 441
Create the chroot Directory and Files 442
Configure Named to Started in the Jail 443
Split BIND Configuration 443
Transaction Signatures 446
The \texttt{dnssec-keygen} Command 447
The \texttt{dnssec-signzone} Command 448
Exam Preparation Tasks 449
Review All Key Topics 449
Define Key Terms 449
Review Questions 450

Part IX: Configuring Web Services
Chapter 23  
Implementing a Web Server 453
“Do I Know This Already?” Quiz 453
Foundation Topics 455
Basic Apache Web Server Configuration 456
Starting the Apache Web Server 457
Apache Web Server Log Files 458
Enable Scripting 459
Apache Web Server Security 463
Essential Settings 463
User Authentication 465
Virtual Hosts 466
Configuring IP-Based Virtual Hosts 466
<table>
<thead>
<tr>
<th>Chapter 24</th>
<th>Apache Configuration for HTTPS</th>
<th>473</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 25</td>
<td>Implementing a Proxy Server</td>
<td>489</td>
</tr>
<tr>
<td>Part X: Administrating File Sharing</td>
<td>Chapter 26</td>
<td>SAMBA Server Configuration</td>
</tr>
</tbody>
</table>
Mapping Local Accounts 517
Accessing SAMBA Servers 518
Mounting SAMBA Shares 520
Exam Preparation Tasks 521
Review All Key Topics 521
Define Key Terms 522
Review Questions 522

Chapter 27  **NFS Server Configuration**  525
“Do I Know This Already?” Quiz  525
Foundation Topics 527
Configuring an NFS Server 527
The /etc/exports File 527
User ID Mapping 529
NFS Server Processes 530
Understanding portmap 531
NFS Server Commands 533
Configuring an NFS Client 534
Review All Key Topics 536
Define Key Terms 537
Review Questions 537

Part XI: Managing Network Clients

Chapter 28  **DHCP Configuration**  541
“Do I Know This Already?” Quiz  541
Foundation Topics 543
DHCP Configuration Basics 543
The ddns-update-style and Ignore client-updates Directives 545
The Subnet Directive 545
Configuring Static Hosts 547
Configuring BOOTP Hosts 547
DHCP Log Files 548
Configuring a DHCP Relay Agent 549
Exam Preparation Tasks 550
Review All Key Topics 550
Define Key Terms 550
Review Questions 550

Chapter 29  **PAM Authentication**  555
“Do I Know This Already?” Quiz  555
Foundation Topics 557
PAM Configuration Basics 557
PAM Types 559
Control Values 562
PAM Modules 564
  The pam_unix Module 565
  The pam_cracklib Module 565
  The pam_limits Module 566
  The pam_listfile Module 568
Exam Preparation Tasks 569
Review All Key Topics 569
Define Key Terms 569
Review Questions 569

Chapter 30 Configuring an OpenLDAP Server 573
  “Do I Know This Already?” Quiz 573
Foundation Topics 576
Key LDAP Terms 576
The slapd.conf File 579
  Customize Your LDAP Domain 579
  Configuring Logging 581
  Configuring the Database Directory 582
Starting the LDAP Server 582
OpenLDAP Objects 584
  OpenLDAP Schemas 584
OpenLDAP Database Changes 586
Exam Preparation Tasks 589
Review All Key Topics 589
Define Key Terms 589
Review Questions 590

Chapter 31 LDAP Client Usage 593
  “Do I Know This Already?” Quiz 593
Foundation Topics 595
Using the ldapdelete Command 596
Using the ldapsearch Command 597
Using the ldappasswd Command 600
Exam Preparation Tasks 601
Review All Key Topics 601
Review Questions 601

Part XII: Administrating E-Mail Services

Chapter 32 Using E-mail Servers 605
  “Do I Know This Already?” Quiz 605
Foundation Topics 607
SMTP Basics 607
Configuring Postfix 609
  Postfix Configuration File 610
About the Author

William “Bo” Rothwell At the impressionable age of 14, Bo crossed paths with a TRS-80 Micro Computer System (affectionately known as a “Trash 80”). Soon after, the adults responsible for Bo made the mistake of leaving him alone with the TRS-80. He immediately dismantled it and held his first computer class, showing his friends what made this “computer thing” work.

Since that experience, Bo’s passion for understanding how computers work and sharing this knowledge with others has resulted in a rewarding career in IT training. His experience includes Linux, Unix, and programming languages such as Perl, Python, Tcl, and BASH. He is the founder and president of One Course Source, an IT training organization.

Dedication

To Sarah, my fiancée and best friend: You have the patience of a saint and without your support, I could never have written this book.

To Julia, my daughter: You didn’t deserve at least half the times I yelled at you. Thanks for putting up with your grumpy Dad.

Acknowledgments

I feel like one of those actors who has been awarded an Oscar and tries to rattle off a bunch of names, trying to say thank you to everyone. I’m not limited to five minutes, but I am worried about missing someone!

To Sarah and Julia, my fiancée and daughter, thank you again for all your support, encouragement, and patience.

To my Dad, Richard Rothwell: I hated having to write and rewrite my papers growing up. I dreaded bringing you “draft #5” knowing there would have to be a “draft #6.” But those experiences allowed me to become a good writer, and I can’t thank you enough for that. (However, please don’t send me a marked-up copy of this book!)

To my Mom, Ann Rothwell: For every endeavor I have tackled in my life, from those first steps as a toddler to writing this book, you and Dad have been the backbone of support in my life. A great many of my successes are the direct result of your support and encouragement. Thank you!

A special thanks to the production and editorial team at Pearson: Mary Beth Ray, Ellie Bru, Mandie Frank, and Geneil Breeze.

Finally, thank you very much Ross Brunson and Keith Wright for your hard work as technical reviewers for this book. Your feedback made this a much better publication than I could have managed alone.
About the Technical Reviewers

Ross Brunson  Ross has more than 20 years of experience as a Linux and Open Source trainer, training manager, and technologist and is author of the popular *LPIC-1 Exam Cram* (Que Publishing), as well as the Pearson IT Certification *LPIC-1 Certification Guide*. Ross is currently senior training/certification engineer at SUSE and recently spent almost five years as the director of member services for the Linux Professional Institute, where he contributed to placing several LPI courses into the Cisco Networking Academy, conducted dozens of Train-the-Trainer sessions, and provided sales enablement support for the worldwide Master Affiliate network spanning 100+ countries. Ross holds a number of key IT certifications; is author of several successful technical books and dozens of technical courses for major organizations (including the first LPI Certification Bootcamps); and is skilled at both contributing to and building community around IT products. He lives in Paradise Valley, Montana, with his family and enjoys traveling, winter sports, and photography.

Keith Wright  has been working as an instructor teaching computer courses since 1993. Currently, he teaches courses in Perl, Python, Project Management, Solaris, Web Development, Linux System Administration, Security, and Performance Optimization. In addition, he finds work as an author, technical editor, and photographer, and has published more than a dozen applications for Android devices.

We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we’re doing right, what we could do better, what areas you’d like to see us publish in, and any other words of wisdom you’re willing to pass our way.

We welcome your comments. You can e-mail or write to let us know what you did or didn’t like about this book—as well as what we can do to make our books better. Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book’s title and author as well as your name and e-mail address. We will carefully review your comments and share them with the author and editors who worked on the book.

E-mail: feedback@pearsonitcertification.com
Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *LPIC-2 Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780789757142 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.
Introduction

Odds are you are reading this book because you have successfully passed the Linux+ or LPIC-1 certification exams and you are ready for the next challenge. This book focuses on one major goal: to help you prepare to pass the LPIC-2 exams (Exam 201 and Exam 202).

These are challenging exams because they cover a wide range of advanced Linux topics. In fact, some of these topics are large enough to be covered in books of their own.

It is important to realize that this book's primary goal is to help you prepare to pass the LPIC-2 exam. As a result, the depth of the topics is specifically limited to what is exam-testable.

The rest of this introduction focuses on two topics: the LPIC-2 exam and a description of this book.

The LPIC-2 Exam

The Linux Network Professional Certification (LPIC-2) was first introduced in November 2001. To earn this certification, you need to pass two exams: 201 and 202. You also need to have an active LPIC-1 certification to be eligible to earn the LPIC-2 certification. Make sure you take the LPIC-2 exams within five years of earning your LPIC-1 certification.

The primary focus of the LPIC-2 exam is the skills that a Linux administrator should have to manage small- to medium-sized network environments. You will find a bit of redundancy with the topics on the LPIC-1 certification exams, but you should also expect the exam questions to deal with a deeper level of knowledge. For example, both exams list SysV-init system startup as an exam objective, but the questions are more challenging on the LPIC-2 exam than on the LPIC-1 exam.

VERY IMPORTANT: The LPIC-2 exam has a “shelf life” of five years. While topics and techniques change (sometimes rapidly) in Linux, the LPIC-2 exam does not immediately change. As a result, some of the topics that you will be tested on are no longer the standard that you find in most modern Linux distributions. I have made a point throughout the book to highlight which topics are slightly older because this should have an impact on your study methods.

For example, one of the exam objectives is 202.1 Customizing SysV-init system startup. Most modern distributions of Linux now use a different startup system (either Upstart or SystemD). For the purposes of the exam, you want to focus your studies on SysV-init. In these situations, I provide a suggestion as to which Linux distribution you should use to practice.

Contents of the 201 and 202 Exams

Every student who takes an exam wants to know what’s on the exam. As with all their exams, LPI publishes a set of exam topics. These exam topics give general guidance as to what’s on the exam.

You can find the exam topics at www.lpi.org. The most memorable way to navigate is to go to https://www.lpi.org/study-resources/ and look for the LPIC-2 201 Objectives and the LPIC-2 202 Objectives.
Table I-1 lists the topics on the 201 and 202 exams, with a reference to the chapter or chapters of this book that covers the topic.

<table>
<thead>
<tr>
<th>Exam Section/Objective</th>
<th>Chapter Where Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topic 200: Capacity Planning</strong></td>
<td></td>
</tr>
<tr>
<td>200.1 Measure and Troubleshoot Resource Usage</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>200.2 Predict Future Resource Needs</td>
<td>Chapter 2</td>
</tr>
<tr>
<td><strong>Topic 201: Linux Kernel</strong></td>
<td></td>
</tr>
<tr>
<td>201.1 Kernel Components</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>201.2 Compiling a Kernel</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>201.3 Kernel Runtime Management and Troubleshooting</td>
<td>Chapter 4</td>
</tr>
<tr>
<td><strong>Topic 202: System Startup</strong></td>
<td></td>
</tr>
<tr>
<td>202.1 Customizing SysV-init System Startup</td>
<td>Chapter 5</td>
</tr>
<tr>
<td>202.2 System Recovery</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>202.3 Alternate Boot loaders</td>
<td>Chapter 7</td>
</tr>
<tr>
<td><strong>Topic 203: Filesystem and Devices</strong></td>
<td></td>
</tr>
<tr>
<td>203.1 Operating the Linux Filesystem</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>203.2 Maintaining a Linux Filesystem</td>
<td>Chapter 9</td>
</tr>
<tr>
<td>203.3 Creating and Configuring Filesystem Options</td>
<td>Chapter 10</td>
</tr>
<tr>
<td><strong>Topic 204: Advanced Storage Device Administration</strong></td>
<td></td>
</tr>
<tr>
<td>204.1 Configuring RAID</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>204.2 Adjusting Storage Device Access</td>
<td>Chapter 12</td>
</tr>
<tr>
<td>204.3 Logical Volume Manager</td>
<td>Chapter 13</td>
</tr>
<tr>
<td><strong>Topic 205: Network Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>205.1 Basic Networking Configuration</td>
<td>Chapter 14</td>
</tr>
<tr>
<td>205.2 Advanced Network Configuration and Troubleshooting</td>
<td>Chapter 15</td>
</tr>
<tr>
<td>205.3 Troubleshooting Network Issues</td>
<td>Chapter 16</td>
</tr>
<tr>
<td><strong>Topic 206: System Maintenance</strong></td>
<td></td>
</tr>
<tr>
<td>206.1 Make and Install Programs from Source</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>206.2 Backup Operations</td>
<td>Chapter 18</td>
</tr>
<tr>
<td>206.3 Notify Users on System-Related Issues</td>
<td>Chapter 19</td>
</tr>
<tr>
<td>Exam Section/Objective</td>
<td>Chapter Where Covered</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>Topic 207: Domain Name Server</strong></td>
<td></td>
</tr>
<tr>
<td>207.1 Basic DNS Server Configuration</td>
<td>Chapter 20</td>
</tr>
<tr>
<td>207.2 Create and Maintain DNS Zones</td>
<td>Chapter 21</td>
</tr>
<tr>
<td>207.3 Securing a DNS Server</td>
<td>Chapter 22</td>
</tr>
<tr>
<td><strong>Topic 208: Web Services</strong></td>
<td></td>
</tr>
<tr>
<td>208.1 Implementing a Web Server</td>
<td>Chapter 23</td>
</tr>
<tr>
<td>208.2 Apache Configuration for HTTPS</td>
<td>Chapter 24</td>
</tr>
<tr>
<td>208.3 Implementing a Proxy Server</td>
<td>Chapter 25</td>
</tr>
<tr>
<td>208.4 Implementing Nginx as a Web Server and a Reverse Proxy</td>
<td>Chapter 25</td>
</tr>
<tr>
<td><strong>Topic 209: File Sharing</strong></td>
<td></td>
</tr>
<tr>
<td>209.1 SAMBA Server Configuration</td>
<td>Chapter 26</td>
</tr>
<tr>
<td>209.2 NFS Server Configuration</td>
<td>Chapter 27</td>
</tr>
<tr>
<td><strong>Topic 210: Network Client Management</strong></td>
<td></td>
</tr>
<tr>
<td>210.1 DHCP Configuration</td>
<td>Chapter 28</td>
</tr>
<tr>
<td>210.2 PAM Authentication</td>
<td>Chapter 29</td>
</tr>
<tr>
<td>210.3 LDAP Client Usage</td>
<td>Chapter 31</td>
</tr>
<tr>
<td>210.4 Configuring an OpenLDAP Server</td>
<td>Chapter 30</td>
</tr>
<tr>
<td><strong>Topic 211: E-mail Services</strong></td>
<td></td>
</tr>
<tr>
<td>211.1 Using E-mail Servers</td>
<td>Chapter 32</td>
</tr>
<tr>
<td>211.2 Managing Local E-mail Delivery</td>
<td>Chapter 33</td>
</tr>
<tr>
<td>211.3 Managing Remote E-mail Delivery</td>
<td>Chapter 34</td>
</tr>
<tr>
<td><strong>Topic 212: System Security</strong></td>
<td></td>
</tr>
<tr>
<td>212.1 Configuring a Router</td>
<td>Chapter 35</td>
</tr>
<tr>
<td>212.2 Securing FTP Servers</td>
<td>Chapter 36</td>
</tr>
<tr>
<td>212.3 Secure Shell (SSH)</td>
<td>Chapter 37</td>
</tr>
<tr>
<td>212.4 Security Tasks</td>
<td>Chapter 38</td>
</tr>
<tr>
<td>212.5 OpenVPN</td>
<td>Chapter 38</td>
</tr>
</tbody>
</table>
How to Take the LPIC-201 and LPIC-202 Exams

To take the LPIC-2 exams, start at lpi.org to get a member ID and a link to pearsonvue.com/lpi/ to schedule an exam.

Who Should Take This Exam and Read This Book?

This book is intended for anyone wanting to prepare for the LPIC-2 certification exams. The audience includes self-study readers—people who pass the test by studying 100% on their own.

This book is also an excellent primer for many topics that a Linux system administrator is responsible for handling. The information in this book can also be used as a reference for when the gray matter storage device between your ears fails to return the necessary information.

Book Organization

This book contains 39 chapters, plus a glossary and an appendix. The topics all focus in some way on LPIC-2 certification topics, making the topics somewhat focused, but with deep coverage on those topics.

The book organizes the topics into 14 major parts. The following list outlines the major part organization of this book:

- **Part I, “Capacity Planning”:** This part includes two chapters, which focus on tools designed to determine resource usage. Using this information, you can determine what additional resources may be needed in the future:
  - **Chapter 1, “Measuring and Troubleshooting Resource Usage”:** This chapter covers the tools and terms that you should know about when measuring the resources used by the system.
  - **Chapter 2, “Predict Future Resource Needs”:** This chapter covers the tools and techniques to predict what your system will need in the future, not only to help you avoid disasters, but also to provide you with the means to proactively maintain your system’s health.

- **Part II, “Managing the Kernel”:** The focus on this part is the kernel:
  - **Chapter 3, “Kernel Components and Compiling”:** In this chapter you learn about kernel parameters, discover kernel documentation that helps you understand these parameters, and learn how to create a custom kernel.
  - **Chapter 4, “Kernel Runtime Management and Troubleshooting”:** The focus of this chapter is to learn how to load LKMs, unload them from memory, and view information about the modules, not to memorize what the different modules do. You also learn how to fine-tune LKMs by adjusting module parameters.

- **Part III, “Managing System Startup”:** As an administrator you need to be able to administer how the system boots. This part focuses on how the boot process works and what changes you can make as an administrator:
  - **Chapter 5, “Customizing SysV-init System Startup”:** This chapter focuses on understanding the boot process of SysV-init systems as well as how to modify how these systems boot.
- Chapter 6, “Administering System Recovery”: In this chapter you learn the skills that enable you to recover a system that will not boot properly.

- Chapter 7, “Alternate Boot loaders”: In this chapter you learn how to configure LILO, the LInux LOader. You also learn about other boot loaders, including syslinux, extlinux, isolinux, and pxelinux.

- Part IV, “Managing Filesystem and Devices”: Local filesystems are stored on devices such as partitions. The ability to make partitions and place filesystems on these partitions is a critical component of the functions of a system administrator:
  - Chapter 8, “Operating the Linux Filesystem”: This chapter explains how the mounting process works.
  - Chapter 9, “Maintaining a Linux Filesystem”: In this chapter you learn about different Linux filesystems, including the family of ext-based filesystems and the xfs filesystem. You learn how to create these filesystems as well as how to maintain them. You also learn how to create swap devices and utilize SMART, a method of monitoring your hard disks.
  - Chapter 10, “Creating and Configuring Filesystem Options”: This chapter focuses on understanding the essentials about removable media filesystems, including ISO9660, HFS, and UDF. You also learn about encrypted filesystems and the autofs system.

- Part V, “Administering Advanced Storage Device”: In addition to regular partitions, you can use software RAID and LVM (Logical Volume Manager) devices to store files locally:
  - Chapter 11, “Configuring RAID”: This chapter focuses on how to set up and maintain software RAID devices on Linux distributions.
  - Chapter 12, “Adjusting Storage Device Access”: This chapter is somewhat of a hodgepodge chapter, covering a wide range of storage topics not covered in previous chapters. This includes covering iSCSI (a network-based implementation of SCSI), tools related to storage device system resources, as well as kernel parameters related to storage devices.
  - Chapter 13, “Logical Volume Manager”: This chapter covers Logical Volume Manager (LVM), a technology that can be used in place of traditional partitions.

- Part VI, “Configuring the Network”: This part focuses on configuring and troubleshooting network interfaces:
  - Chapter 14, “Basic Networking Configuration”: The focus of this chapter is basic networking commands, such as ifconfig, arp, and the route commands. The topic of wireless networking commands is also covered in this chapter.
  - Chapter 15, “Advanced Network Configuration and Troubleshooting”: The focus of this chapter is commands that gather network information, primarily to aid the process of troubleshooting problems. The topic includes commands that probe remote systems (the ping and nmap commands), display local network information (the nc, netstat, and lsif commands), and sniff local network packets (the tcpdump command).
Chapter 16, “Troubleshooting Network Issues”: This chapter focuses on files used to configure and troubleshoot network-related issues. You learn about the different configuration files that exist on Debian and Red Hat–based systems. Various troubleshooting tools are covered to provide you with the skills to fix network issues.

Part VII, “Performing System Maintenance”: This part contains a collection of topics, including installing software via source code, backing up filesystems, and sending messages to users:

Chapter 17, “Make and Install Programs from Source”: In this chapter you learn where you can access source code. After downloading it to your system, you learn how to “unpack” and configure the source code. Finally, you learn how to install and patch the source code.

Chapter 18, “Backup Operations”: This chapter introduces some of the basics that you should know about when creating your backup strategy. You learn how to answer the questions of what should be backed up and what tools should be used. You also learn about some of the standard backup tools that come with Linux as well as some of the third-party tools available.

Chapter 19, “Notify Users on System-Related Issues”: In this chapter you learn how to display both pre-login messages and post-login messages. You also learn how to send broadcast messages to all users who are currently logged in to the system.

Part VIII, “Administrating Domain Name Server”: This part focuses on configuring and securing a DNS server:

Chapter 20, “Basic DNS Server Configuration”: This chapter focuses on understanding the essential concepts and terms of DNS as well as how to administer the primary BIND configuration file. You also are introduced to some of the essential commands that help you administer a DNS server.

Chapter 21, “Create and Maintain DNS Zones”: In this chapter you learn how to configure a DNS zone by modifying the /etc/named.conf file and creating zone files.

Chapter 22, “Securing a DNS Server”: The focus of this chapter is to make DNS more secure.

Part IX, “Configuring Web Services”: This section focuses on configuring and securing web servers and proxy servers:

Chapter 23, “Implementing a Web Server”: This chapter introduces the Apache Web Server. You learn how to perform basic configuration changes to both its primary configuration files and “include” directory configuration files.

Chapter 24, “Apache Configuration for HTTPS”: This chapter focuses on HTTPS, the Hypertext Transfer Protocol with SSL (Secure Sockets Layer) for authentication and encryption. You learn about the concepts of SSL and how it can be used to allow a client system to authenticate an Apache Web Server.

Chapter 25, “Implementing a Proxy Server”: In this chapter you are introduced to the concept of proxy servers. You learn how to configure a proxy server, including how to limit access to the server.
Part X, “Administrating File Sharing”: Files are typically shared between systems via either SAMBA or NFS. This part focuses on configuring these services:

- Chapter 26, “SAMBA Server Configuration”: In this chapter you learn about the Samba server, including key configuration settings.
- Chapter 27, “NFS Server Configuration”: In this chapter you learn how to set up an NFS server and connect to it from an NFS client. You also learn how to secure portmap, the service that grants access to NFS servers.

Part XI, “Managing Network Clients”: This part covers a collection of services, including DHCP, PAM, and LDAP:

- Chapter 28, “DHCP Configuration”: This chapter covers DHCP server configuration.
- Chapter 29, “PAM Authentication”: This chapter covers PAM (pluggable authentication modules), a component of Linux designed to authorize and authenticate user accounts.
- Chapter 30, “Configuring an OpenLDAP Server”: This chapter introduces LDAP (Lightweight Directory Access Protocol), a distributed directory service.
- Chapter 31, “LDAP Client Usage”: This chapter focuses on the OpenLDAP database. You learn how to use the `ldapadd` and `ldapdelete` commands to make changes to the database.

Part XII: “Administrating E-mail Services”: This section focuses on administrating various e-mail services:

- Chapter 32, “Using E-mail Servers”: In this chapter you learn features such as configuration of e-mail addresses, implementing e-mail quotas, and managing virtual e-mail domains.
- Chapter 33, “Managing Local E-mail Delivery”: In this chapter you learn how to set up procmail rules, both systemwide as an administrator and by individual user accounts.
- Chapter 34, “Managing Remote E-mail Delivery”: You learn about the protocols used by the MDA: IMAP (Internet Message Access Protocol) and POP (Post Office Protocol) in this chapter. You also learn how to configure MDA services, including Dovecot and Courier.

Part XIII, “Administrating System Security”: In this section several security features are introduced, including router configuration, FTP servers, SSH servers, and VPN:

- Chapter 35, “Configuring a Router”: In this chapter you learn how to configure a Linux system as a router and protect the internal network using a firewall. You also learn how to allow an internal, private network to access the Internet via NAT.
- Chapter 36, “Securing FTP Servers”: This chapter primarily focuses on how to set up a specific FTP server called the vsftpd server. You also learn some of the key command line options of the Pure-FTPD server.
- Chapter 37, “Secure Shell (SSH)”: This chapter primarily focuses on setting up a Secure Shell server, including the concepts of how the protocol works and key con-
configuration options. The Secure Shell client utilities also are covered, including how to customize the behavior of the utilities by modifying the SSH client configuration file.

- **Chapter 38, “Security Tasks and OpenVPN”:** You first learn about some key security tools, such as nmap, nc, snort, and fail2ban. You also learn how to discover important security alerts from sources such as Bugtraq, CERT, CIAC, and others. This chapter also covers the LPIC-2 objective of OpenVPN (Open Virtual Private Network).

- **Part XIV, “Final Preparation”:** This part concludes the book with recommendations for exam preparation:
  - **Chapter 39, “Final Preparation”:** This nontechnical chapter identifies and explains how to use various exam preparation tools, followed by a step-by-step strategy for using this book to prepare for the LPIC-201 and LPIC-202 exams.

In addition to the core chapters, this book also has:

- **Glossary:** The glossary contains definitions for all the terms listed in the “Define Key Terms” sections at the conclusions of Chapters 1 through 38.
- **Appendix A, “Answers to ‘Do I Know This Already?’ Quizzes and Review Questions:** Includes the answers to all the questions from Chapters 1 through 38.

### Book Features and Exam Preparation Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it, but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don’t know, and be well prepared for the exam. These tools include:

- **“Do I Know This Already?” Quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter.
- **Foundation Topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam Preparation Tasks:** These sections list a series of study activities that should be done after reading the Foundation Topics section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include:
  - **Key Topics Review:** The Key Topic icon appears next to the most important items in the Foundation Topics section of the chapter. The Key Topics Review activity lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic. Review these topics carefully.
■ **Definition of Key Terms:** Although certification exams might be unlikely to ask a question such as “Define this term,” the LPIC-201 and LPIC-202 exams require you to learn and know a lot of terminology. This section lists some of the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary.

■ **End of Chapter Review Questions:** Confirm that you understand the content that you just covered.

**Companion Website**

Register this book to get access to the Pearson IT Certification test engine and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to [www.pearsonITcertification.com/register](http://www.pearsonITcertification.com/register) and log in or create a new account.
2. Enter the ISBN: 9780789757142
3. Answer the challenge question as proof of purchase.
4. Click on the Access Bonus Content link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following these steps, visit [www.pearsonITcertification.com/contact](http://www.pearsonITcertification.com/contact) and select the Site Problems/Comments option. Our customer service representatives will assist you.

**Pearson IT Certification Practice Test Engine and Questions**

The companion website includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode or take a simulated exam that mimics real exam conditions. You can also serve up questions in a Flash Card Mode, which displays just the question and no answer, challenging you to state the answer in your own words before checking the actual answer to verify your work.

The installation process requires two major steps: installing the software and then activating the exam. The website has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam (the database of exam questions) is not on this site.

**Note:** The cardboard DVD sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activa-
tion code. Also included on the paper is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows XP (SP3), Windows Vista (SP2), Windows 7, or Windows 8
- Microsoft .NET Framework 4.0 Client
- Pentium-class 1 GHz processor (or equivalent)
- 512 MB RAM
- 650 MB disk space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

The software installation process is routine as compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the cardboard sleeve.

The following steps outline the installation process:

1. Download the exam practice test engine from the companion site.
2. Respond to Windows prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the cardboard sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

Once the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the Activate Exam button.
3. At the next screen, enter the activation key from the paper inside the cardboard sleeve in the back of the book. Once entered, click the Activate button.
4. The activation process downloads the practice exam. Click Next, and then click Finish.
Introduction

When the activation process completes, the My Products tab should list your new exam. If you do not see the exam, make sure that you have selected the My Products tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the Open Exam button.

To update a particular exam you have already activated and downloaded, display the Tools tab and click the Update Products button. Updating your exams ensures that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Certification Practice Test exam engine software, display the Tools tab and click the Update Application button. You can then ensure that you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process and the registration process, only have to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another Pearson IT Certification Cert Guide, extract the activation code from the cardboard sleeve in the back of that book; you do not even need the exam engine at this point. From there, all you have to do is start the exam engine (if not still up and running) and perform steps 2 through 4 from the previous list.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the “Do I Know This Already?” quizzes at the beginning of each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. See the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

LPIC-2 Exam Updates

Over time, reader feedback allows Pearson to gauge which topics give our readers the most problems when taking the exams. Additionally, LPIC does occasionally make minor updates to the LPIC-2 exam. We address that all in Appendix B “LPIC-2 Exam Updates.”

To assist readers with keeping up to date, the author might create new materials clarifying and expanding on those troublesome exam topics as well as changes to the LPIC-2 exams. This material can be found at http://www.pearsonitcertification.com/title/9780789757142. Alternatively this material can also be found at http://www.OneCourseSource.com/LPIC-2-book.
This chapter covers the following topics:

- How to access source code
- How to unpack and build source code
- How to patch source code

This chapter covers the following objective:

- 206.1 Make and Install Programs from Source
This chapter covers the following topics:

- How to develop a backup strategy
- How to use standard backup tools
- Third-party backup tools

This chapter covers the following objective:

- 206.2 Backup Operations
Almost every seasoned system administrator, as well as many end users, has horror stories that revolve around lost data. Millions of dollars have been lost and heads have rolled because either no backup strategy was put in place or the backup strategy wasn’t followed.

Data is a serious business, and you don’t want to be the one, hat in hand, explaining why critical company data has been lost forever. You must create a solid backup strategy and make sure it is implemented correctly.

This chapter introduces some of the basics that you should know when creating your backup strategy. You learn to answer the questions of what should be backed up and what tools should be used. You also learn about some of the standard backup tools that come with Linux as well as some of the third-party tools that are available.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read this entire chapter or simply jump to the “Exam Preparation Tasks” section for review. If you are in doubt, read the entire chapter. Table 18-1 outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions Covered in This Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Strategy</td>
<td>1</td>
</tr>
<tr>
<td>Standard Backup Utilities</td>
<td>2, 3</td>
</tr>
<tr>
<td>Third-Party Backup Utilities</td>
<td>4</td>
</tr>
</tbody>
</table>
1. Which directory cannot be placed in a separate filesystem from the root filesystem?
   a. /boot
   b. /etc
   c. /var
   d. None of the above

2. The _____ command is designed to back up the contents of entire disk drives, regardless of the data on the disk drive.
   a. zip
   b. tar
   c. dd
   d. rsync

3. To specify the block size, use the _____ option to the dd command.

4. Which of the following is considered a third-party backup utility available for the Linux operating system.
   a. BackLinuxUp
   b. CompleteBackup
   c. Amanda
   d. Rebecca
Foundation Topics

Backup Strategy

As an administrator, it is your responsibility to develop a solid backup strategy. To create this strategy, you need to answer the following questions:

- **What needs to be backed up?**—This is a critical question because it has an impact on the answers to the rest of the questions. While answering this question, you should consider breaking down your filesystem into smaller components to create a more efficient backup strategy.

- **How often?**—Several factors come into play when answering this question. If you have broken down your filesystem into smaller components, you are really going to answer this question for each component, as the answer varies depending on what is being backed up.

- **Full or incremental?**—A full backup is when everything is backed up, regardless of whether any changes have been made since the last backup. An incremental backup is when a backup is performed only on the files that have changed since a previous backup. Some backup utilities allow for complex backup strategies based on several different levels of incremental backups.

- **Where will the backup be stored?**—Will you use tape devices, optical devices (CD-ROMS/DVDs), external storage devices (USB drives), or network-accessible storage locations? Each storage location has inherent advantages and disadvantages.

- **What backup tool will be used?**—The decision that you make regarding the backup tool has a significant impact on the process of backing up and restoring data. Most Linux distributions come with several tools installed by default, such as the `dd` and `tar` commands. In many cases, additional tools are freely available; you just need to install them from the distribution repository. In addition to the tools that come with the distribution, you may want to consider exploring third-party tools, which typically offer more robust solutions.

What Needs to Be Backed Up?

One of the reasons why administrators tend to use multiple partitions (or logical volumes) when installing the operating system is that this lends to developing good backup strategies. Certain directories change more often than others. By making these separate filesystems, you can make use of filesystem features to perform the backup.
For example, it is normally a good idea to back up data not actively being modified. This can pose challenges when backing up users’ home directories. By making `/home` a separate partition, the partition can then be unmouted and a backup can be performed directly from the partitions. Even better: Make the `/home` filesystem on a logical volume and use LVM snapshots to create a “frozen” view of the filesystem in the `/home` directory. This allows users to continue to work on the filesystem while you back up the data.

This doesn’t mean that you will always make separate filesystems for each directory structure that you want to back up. In fact, in some cases, like the `/etc` directory, this isn’t even possible ( `/etc` must be in the same filesystem as the `/` filesystem). However, whenever possible, it is generally a good idea to create separate filesystems for directory structures that you are incorporating in your backup strategy.

**Note:** You will see that I tend to use the terms “directory” and “filesystem” interchangeably in this chapter. As you know, not all directories represent entire filesystems, just the ones that are mount points. However, because I am strongly suggesting that the directories in Table 18-2 be mount points for filesystems, I decided to use the terms “directory,” “directory structure,” and “filesystem” interchangeably when I am discussing these sorts of directories.

So, what directories/filesystems should you consider including in your backup strategy? Table 18-2 highlights the ones that are commonly part of a backup strategy.

<table>
<thead>
<tr>
<th>Directory/Filesystem</th>
<th>Why You Should Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/home</code></td>
<td>If your system has any regular users, this directory structure is certain to be a part of your backup strategy. On servers with no regular users, however, this directory is normally ignored when developing the backup strategy.</td>
</tr>
<tr>
<td><code>/usr</code></td>
<td>The <code>/usr</code> directory rarely changes as this is the location of most of the system’s commands, documentation, and programs. This directory structure normally only changes when new software is added to the system or when existing software is updated. Some administrators argue not to ever back up <code>/usr</code> because if something goes wrong, you can always just reinstall the software. The flaw in this reasoning is that few administrators keep a list of all the software installed on all the systems they administer. So, you should include this directory in your backup strategy.</td>
</tr>
</tbody>
</table>
### Directory/Filesystem | Why You Should Consider
---|---
/bin | If you back up the /usr directory, consider including the /bin directory as some of the operating system software is installed in this directory structure.
/sbin | If you back up the /usr directory, consider including the /sbin directory as some of the operating system software is installed in this directory structure.
/opt | If you have a lot of third-party software installed on your system, you may consider backing up this directory. This isn’t typically the case in most Linux distributions.
/var | The primary data stored in the /var directory structure includes log files, the incoming email queue, and the print queue. The print queue should not need backing up, but log files and the email queue may be important, depending on the function of the system. Typically this filesystem is backed up on servers, but often ignored on desktop systems.
/boot | The kernel is located in this directory structure. If you install a new kernel, consider backing up this directory structure. Typically it is not backed up on a regular basis.
/lib and /lib64 | If you back up the /usr directory, consider including the /lib and /lib64 directories as the operating system libraries are installed in these directory structures. As software is added to the system, new libraries are sometimes added as well.
/etc | This directory structure is often overlooked in the backup strategy, but it is also often the directory that changes most frequently. Regular system administration tasks, such as administering software configuration files and managing user/group accounts, result in changes in the /etc directory structure. On an active system, this directory should be backed up on a regular basis. Important note: The /etc directory must be a part of the / filesystem; it cannot be a separate filesystem.

### Which directories/filesystems should you never back up? The following directories either are not stored on the hard drive or contain temporary information that never needs to be backed up:
- /dev
- /media
- /mnt
- /net
How Often?

There is no exact rule that tells you how often to perform backups. To determine how often to perform backups, determine which directories/filesystems you are going to back up and then get an idea of how often data changes on each of them.

Based on your observations, you should be able to determine how often to perform backups. It will likely be a different schedule for different directories, and you also need to consider how often to perform full versus incremental backups.

Full or Incremental?

Not all software tools provide the flexibility to perform incremental backups. But if you are using one that does provide this feature, consider including it in your backup strategy.

If the backup tool does provide incremental backups, there are probably several different levels available. For example:

- A level 0 backup would be a full backup.
- A level 1 backup would back up all files that have changed since the last lower backup (level 0).
- A level 2 backup would back up all files that have changed since the last lower backup (level 0 or 1).

Typically these incremental backups would include the values 1–9. So level 9 backup would back up all files that have changed since the last lower backup (which could be level 0, level 1, level 2, etc.).

To better understand incremental backups, first look at Figure 18-1.
The strategy in Figure 18-1 demonstrates a four-week backup period. Every four weeks this cycle repeats. On the first day of the period, a full (level 0) backup is performed. The next day, Monday, a level 2 backup is performed. This backs up everything that changed since the last lower number backup (level 0), essentially one day’s worth of changes.

On Tuesday, a level 3 backup is performed. This backs up everything that has changed since the last lower backup, the level 2 performed on Monday. Each day during the week, a backup is performed that backs up the last 24 hours of changes to the directory/filesystem.

The following Sunday, a level 1 backup is performed. This backs up all changes since the last lower backup, the level 0 performed at the beginning of the cycle. Essentially, this backs up a week’s worth of changes.

The advantage of this backup plan is that the backups each night take comparatively little time. Sunday’s backups take longer each week, but the rest of the week is a relatively small backup.

The disadvantage of this backup plan is in the recovery. If the filesystem must be restored because the data was lost on Friday of the third week, then the following restores must be performed in order:

- The level 0 backup
- The level 1 backup performed on Sunday of week 3
- The level 2 backup performed on Monday of week 3
- The level 3 backup performed on Tuesday of week 3
The level 4 backup performed on Wednesday of week 3
The level 5 backup performed on Thursday of week 3

Now compare the previous backup strategy from Figure 18-1 with the backup strategy in Figure 18-2.

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thur</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 2</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thur</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 3</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thur</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 4</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thur</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

**Figure 18-2**  Backup strategy #2

With the backup strategy in Figure 18-2, you also perform a full backup on the first day of the cycle. The backups performed Monday through Saturday back up all files that have changed since Sunday. The backup performed on the following Sunday includes all files that have changed since the first backup of the cycle.

The disadvantage of this method is each backup takes more time as the week progresses. The advantage is the recovery process is easier and quicker. If the filesystem must be restored because the data was lost on Friday of the third week, then the following restores must be performed in order:

- The level 0 backup
- The level 1 backup performed on Sunday of week 3
- The level 5 backup performed on Thursday of week 3

There are many other backup strategies, including the famous Tower of Hanoi, which is based on a mathematical puzzle game. The important thing to remember is that you should research the different methods and find the one that is right for your situation.
Where Will the Backup Be Stored?

**Note:** Consider following the 3-2-1 rule: Store three copies of all important backup data. Use at least two types of media for the backups. Make sure at least one backup is offsite.

There are four primary locations where you can store backup data. Table 18-3 describes each and provides some of the advantages and disadvantages that you should consider.

**Table 18-3  Backup Storage Locations**

<table>
<thead>
<tr>
<th>Location</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tape</td>
<td>Low cost</td>
<td>Slow</td>
</tr>
<tr>
<td></td>
<td>Medium shelf life</td>
<td>Requires special hardware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires a lot of maintenance</td>
</tr>
<tr>
<td>Disk</td>
<td>Fast</td>
<td>Not portable</td>
</tr>
<tr>
<td></td>
<td>Easily available</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td>Normally easily available</td>
<td>Depends on network access</td>
</tr>
<tr>
<td></td>
<td>Easy to have data secured offsite</td>
<td>Could be expensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Could be slow</td>
</tr>
<tr>
<td>Optical media</td>
<td>Decent speed</td>
<td>Low storage capacity</td>
</tr>
<tr>
<td></td>
<td>Low cost</td>
<td>Most often “once write,” can’t be</td>
</tr>
<tr>
<td></td>
<td>Hardware easy to obtain and</td>
<td>reused</td>
</tr>
<tr>
<td></td>
<td>affordable</td>
<td></td>
</tr>
</tbody>
</table>

What Backup Tool Will Be Used?

The rest of this chapter explores different backup tools. The following tools are explored as they are all LPIC-2 exam objectives:

- `dd`
- `tar`
- `rsync`
- Amanda
- Bacula
- BackupPC
In addition to these backup tools, you should be aware of a few other tools used for creating and restoring files:

- **dump/restore**—Not used as often as in the past, these tools were designed to back up and restore entire filesystems. They do support both full and incremental backups, which makes them one of the few standard backup tools that have this feature.

- **cpio**—Similar to the **tar** command, the **cpio** command can be used to merge files from multiple locations into a single archive.

- **gzip/gunzip**—While the **gzip** command doesn’t provide an essential feature that you want a backup tool to provide (namely, it doesn’t merge files together), it does compress files. As a result, it could be used to compress a backup file.

- **bzip2/bunzip2**—While the **bgzip2** command doesn’t provide an essential feature that you want a backup tool to provide (namely, it doesn’t merge files together), it does compress files. As a result, it could be used to compress a backup file.

- **zip/unzip**—An advantage of this tool is not only does it merge files together and compress them, but it uses a standard compression technique used on multiple operating systems, including many non-Linux operating systems.

**Note:** These utilities are not part of the LPIC-2 exam objectives, but they are important ones to consider when you are deciding which backup utility to use.

### Standard Backup Utilities

These utilities are considered standard as you can expect them to be on just about every distribution of Linux. The advantage of this is that not only can you use the tools to perform a backup on just about every system, but even more importantly, you can view and restore the backups on just about every system. It is frustrating and time-consuming to deal with an esoteric backup file that you lack the software for to even determine what is in the backup.

### The dd Command

The **dd** command is useful to back up entire devices, either entire hard disks, individual partitions, or logical volumes. For example, to back up an entire hard disk to a second hard disk, execute a command like the following:

```
[root@localhost ~]# dd if=/dev/sda of=/dev/sdb
```
The `if` option is used to specify the input device. The `of` option is used to specify the output device. Make sure when you execute this command that the `/dev/sdb` hard disk is at least as large as the `/dev/sda` hard disk.

What if you don’t have a spare hard disk, but you have enough room on a device (such as an external USB hard disk)? In this case, place the output into an image file:

```
[root@localhost ~]# dd if=/dev/sda of=/mnt/hda.img
```

You can also use the `dd` command to back up the contents of a CD-ROM or DVD into an ISO image:

```
[root@localhost ~]# dd if=/dev/cdrom of=cdrom.iso
```

The ISO image file can be used to create more CD-ROMs. Or it can be shared via the network to make the contents of the CD-ROM easily available (rather than passing the CD-ROM disc around the office).

It is also helpful to know that both image and ISO files can be treated as regular file-systems in the sense they can be mounted and explored:

```
[root@localhost ~]# mkdir /test
[root@localhost ~]# mount -o loop /mnt/had.img /test
```

One of the advantages of the `dd` command is that it can back up anything on the hard disk, not just files and directories. For example at the beginning of each disk is an area called the MBR (master boot record). For the boot disk the MBR contains the boot loader (GRUB) and a copy of the partition table. It can be useful to have a backup of this data:

```
[root@localhost ~]# dd if=/dev/sda of=/root/mbr.img bs=512 count=1
```

The `bs` option indicates the block size, and the `count` indicates how many blocks to back up. The values of 512 and 1 make sense because the MBR size is 512 bytes.

I would suggest storing the MBR image on an external device. If the system fails to boot because of a corrupted MBR, you can boot off a recovery CD and restore the MBR with a single command:

```
[root@localhost ~]# dd if=mbr.img of=/dev/sda
```

### The `tar` Command

The `tape` archive command was originally designed to back up filesystems to tape devices. While many people now use the `tar` command to back up to nontape devices, you should be aware of how to use tape devices as well.

Tape device names in Linux follow the `/dev/st*` and `/dev/nst*` convention. The first tape device name is assigned the device name of `/dev/st0`, and the second tape device is accessible via the `/dev/st1` device name.
The name /dev/nst0 also refers to the first tape device, but it sends a no rewind signal to the tape device. This is important for when you need to write multiple volumes to the tape. The default behavior of the tape drive is to automatically rewind when the backup is complete. If you wrote another backup to the same tape, you would end up overwriting the first backup unless you used the /dev/nst0 device name when performing the first backup.

If you are working with tape devices, you should be aware of the `mt` command. This command is designed to allow you to directly manipulate the tape devices, including moving from one volume to another and deleting the contents of a tape. Some common examples:

```
[root@localhost ~]# mt -f /dev/nst0 fsf 1          #skip forward one file
[root@localhost ~]# mt -f /dev/st0 rewind          #rewinds the tape
[root@localhost ~]# mt -f /dev/st0 status          #prints information about
    tape device
[root@localhost ~]# mt -f /dev/st0 erase           #erases tape in tape
```

**Note:** For the following examples I am going to assume that you don’t have a tape drive in your system. The examples provided for the `tar` command place the tar ball in a regular file; however, if you have a tape drive, you can just replace the filename with your tape device file.

To create a backup (AKA, a tar ball) with the `tar` utility, use the `-c` (create) option in conjunction with the `-f` (filename) option:

```
[root@localhost ~]# tar -cf /tmp/xinet.tar /etc/xinetd.d
tar: Removing leading '/\' from member names
```

The leading / characters are removed from the filenames, so instead of backing up absolute pathnames, the pathnames are relative. This makes it easier to specify where the files are restored. Having the leading / would result in files always being stored in the exact same location.

To see the contents of a tar ball, use the `-t` (table of contents) option in conjunction with the `-f` option, as shown in Example 18-1.

**Example 18-1  Contents of a tar Ball Using tar -tf**

```
[root@localhost ~]# tar -tf /tmp/xinet.tar
etc/xinetd.d/
    etc/xinetd.d/rsync
```
You often want to see detailed information when listing the contents of the tar ball. Include the -v (verbose) option to see additional information, as shown in Example 18-2.

Example 18-2  The -v Option to See Details of the tar Ball

```
[root@localhost ~]# tar -tvf /tmp/xinet.tar
drwxr-xr-x root/root         0 2015-11-02 11:52 etc/xinetd.d/
-rw-r--r-- root/root       332 2014-03-28 03:54 etc/xinetd.d/rsync
-rw------- root/root      1159 2013-10-07 10:35 etc/xinetd.d/discard-stream
-rw------- root/root      1157 2013-10-07 10:35 etc/xinetd.d/discard-dgram
-rw------- root/root      1149 2013-10-07 10:35 etc/xinetd.d/time-dgram
-rw------- root/root      1148 2013-10-07 10:35 etc/xinetd.d/echo-dgram
-rw------- root/root      1148 2013-10-07 10:35 etc/xinetd.d/daytime-stream
-rw------- root/root      1148 2013-10-07 10:35 etc/xinetd.d/chargen-stream
-rw------- root/root      1149 2013-10-07 10:35 etc/xinetd.d/daytime-dgram
-rw------- root/root      1150 2013-10-07 10:35 etc/xinetd.d/time-stream
-rw------- root/root      1212 2013-10-07 10:35 etc/xinetd.d/tcpmux-server
```

To extract all the contents of the tar ball into the current directory, use the -x (extract) option in conjunction with the -f option, as shown in Example 18-3.

Example 18-3  Using tar -xf for Extracting Contents from the tar Ball

```
[root@localhost ~]# cd /tmp
[root@localhost tmp]# tar -xf xinet.tar
[root@localhost tmp]# ls
```
Suppose your tar ball contains thousands of files and you only need a few files. You can list the filenames at the end of the `tar` command to perform this partial restore:

```
[root@localhost tmp]# tar -xf xinet.tar etc/xinetd.d/rsync
[root@localhost tmp]# ls etc/xinetd.d/rsync
```

There are many options to the `tar` command; consult Table 18-4 to learn about some of the more useful options (including those already covered, which are listed in **bold**).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-A</td>
<td>Append to an existing tar ball.</td>
</tr>
<tr>
<td>-c</td>
<td>Create a tar ball.</td>
</tr>
<tr>
<td>-C</td>
<td>Set the current directory.</td>
</tr>
<tr>
<td>-d</td>
<td>Display the difference between an existing tar ball and what is currently on the filesystem.</td>
</tr>
<tr>
<td>--delete</td>
<td>Delete files from tar ball; not possible on tapes.</td>
</tr>
<tr>
<td>-j</td>
<td>Compress tar ball with the bzip2 command.</td>
</tr>
<tr>
<td>-t</td>
<td>List the table of contents of the tar ball.</td>
</tr>
<tr>
<td>-x</td>
<td>Extract the contents of the tar ball.</td>
</tr>
<tr>
<td>-z</td>
<td>Compress tar ball with the gzip command.</td>
</tr>
<tr>
<td>-W</td>
<td>Attempt to verify after writing. Note: One of the objectives on the exam is to verify the integrity of backup files, so you may be asked a question regarding this option.</td>
</tr>
</tbody>
</table>
The rsync Command

The `rsync` command provides a different set of backup features than those provided by the `tar` and `dd` commands. It is designed to back up files to a remote system. It can communicate via SSH, making the backup process secure. Additionally, it only backs up files that have changed since the last backup.

For example, the command shown in Example 18-4 performs a recursive backup of the `/etc/xinetd.d` directory to the `/backup` directory of the `server1` machine.

Example 18-4  The `rsync` Command

```
[root@localhost ~]# rsync -av -e ssh /etc/xinetd.d server1:/backup
root@server1's password:
sending incremental file list
xinetd.d/
xinetd.d/chargen-dgram
xinetd.d/chargen-stream
xinetd.d/daytime-dgram
xinetd.d/daytime-stream
xinetd.d/discard-dgram
xinetd.d/discard-stream
xinetd.d/echo-dgram
xinetd.d/echo-stream
xinetd.d/rsync
xinetd.d/tcpmux-server
xinetd.d/telnet
xinetd.d/time-dgram
xinetd.d/time-stream
sent 14235 bytes  received 263 bytes  1159.84 bytes/sec
total size is 13391  speedup is 0.92
```

The options used from the previous command: `-v` = verbose, `-a` = archive, `-e ssh` = execute via ssh. The first argument is what to copy, and the second argument is where to copy it.

Suppose a change takes place to one of the files in the `/etc/xinetd.d` directory:

```
[root@localhost ~]# chkconfig telnet off  #changes /etc/xinetd.d/telnet
```

Note that when the `rsync` command is executed again, only the modified file is transferred:

```
[root@localhost ~]# rsync -av -e ssh /etc/xinetd.d server1:/backup
root@server1's password:
```
Third-Party Backup Utilities

Many third-party backup utilities are available for Linux. If you are studying for the LPIC-2 certification exam, you should realize that the exam objective states “Awareness of network backup solutions such as Amanda, Bacula, and BackupPC.” This means you should understand what these solutions provide, but don’t need to know any details.

Amanda

The Advanced Maryland Automatic Network Disk Archiver (AMANDA) is an open source software tool popular on both UNIX and Linux distributions. While there is a freely available community version, there is also an enterprise version that provides support (for a fee, of course).

Amanda provides a scheduler, making it easier for a system administrator to automate the backup process. It also supports writing to either tape device or hard disk.

Bacula

Bacula is an open source product that supports clients from different platforms, including Linux, Microsoft Windows, OS X, and UNIX. One of the compelling features of Bacula is the capability to automate backup, freeing the system administrator from this routine task.

Configuration of Bacula on the server side can be accomplished via a web interface, GUI-based tools, or command line tools.

One disadvantage of Bacula is that the format of the backup data is not compatible with other backup formats, such as the tar command’s format. This makes it difficult to deal with the backup data unless you have the Bacula tools installed on the system.

BackupPC

The BackupPC software provides a disk-to-disk solution that includes a web-based front end. Because it runs through a web interface, no client software needs to be installed. The server software provides the web interface to perform the backup.
Another advantage of BackupPC is that the server runs on many different Linux distributions as well as on several UNIX systems. The software also supports several standard protocols to transfer the data, including NFS, SSH, rsync, and SMB (Server Message Blocks, a Microsoft Windows protocol). This provides you with flexibility in backing up data from different client systems.

**Exam Preparation Tasks**

**Review All Key Topics**

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 18-5 lists a reference of these key topics and the page numbers on which each is found.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paragraph</td>
<td>What should be backed up</td>
<td>361</td>
</tr>
<tr>
<td>Figure 18-1</td>
<td>Incremental backups</td>
<td>365</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Storage solutions</td>
<td>367</td>
</tr>
<tr>
<td>Paragraph</td>
<td>The dd command</td>
<td>368</td>
</tr>
<tr>
<td>Paragraph</td>
<td>The tar command</td>
<td>369</td>
</tr>
<tr>
<td>Paragraph</td>
<td>The rsync command</td>
<td>373</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Third-party backup utilities</td>
<td>374</td>
</tr>
</tbody>
</table>

**Define Key Terms**

Define the following key terms from this chapter and check your answers in the glossary:

- Tower of Hanoi
- Tape device
- Tar ball
- Amanda
- Bacula
- BackupPC

**Review Questions**

The answers to these review questions are in Appendix A.
1. For tools that use numbers to specify full and incremental backups, what number specifies a full backup?

2. Which of the following directories do not need to be backed up? (Choose two.)
   a. /etc
   b. /var
   c. /dev
   d. /sys

3. Which of the following directories do not need to be backed up? (Choose two.)
   a. /usr
   b. /tmp
   c. /proc
   d. /boot

4. The ____ command is used to remotely back up data; by default it only backs up data that has changed since the last time the command was used.

5. Which of the following backup storage locations is likely to be the fastest?
   a. CD-ROM
   b. Tape
   c. Hard disk
   d. Remote network location

6. Which option to the dd command specifies the device that you are backing up?
   a. count=
   b. bs=
   c. of=
   d. if=

7. Fill in the following to mount the test.iso file under the /mnt directory:
   mount -o ____ test.iso /mnt.

8. The “no rewind” device name for the first tape device on the system is /dev/____.
9. Which option to the `tar` command is used to extract data from a tar ball?
   a. `-a`
   b. `-x`
   c. `-e`
   d. `-X`

10. The ___ option to the `rsync` command is used to enable data transfer via SSH.
Symbols

~ (approximate match filter expression), 599
* (asterisks)
  pattern matching character, 626
  wildcard filter expression, 599
, (commas) SAMBA configuration file
  comments, 510
# (comments), 510
/* */ (C style comments), 405
// (C++ style comments), 405
@ (current origin) character, 422
/ directory, 153
>= (equal to or greater than filter expres-
  sion), 599
<= (equal to or less than filter expres-
  sion), 599
= (exact match filter expression), 599
! (exclamation point)
  logical not operator, 599
  negation character, 407
& (logical and) operator, 599
\n pattern matching character, 626
^ pattern matching character, 626
. pattern matching character, 626
+ pattern matching character, 626
| (pipe)
  logical or operator, 599
  pattern matching character, 626
$ pattern matching character, 626
# (Unix style comments), 405
-6 option (nc command), 312

A
-a option
  exportfs command, 534
  mount command, 164
  rsync command, 373
  smbpasswd command, 517
  sysct1 command, 73-74
-A option
  iptables command, 654
tar command, 372
ACCEPT target, 653
access
  anonymous FTP
    not permitted, 666-667
    Pure-FTPD, 670
    testing, 666
Apache Web Server client restrictions,
  463-464
control, 587-588
FTP servers, 667-669
NFS servers, 532-533
SAMBA server shares, 518
services, 333
SSH user logins, 682-683
system files, 441
access_log file, 458
accounts
  anonymous, 666
  PAM, 559-560
  root, 580
SAMBA
  creating, 516-517
  data, storing, 512
  local accounts, mapping, 517-518
user
  adding to etc/vsftpd.ftpusers, 668
  FTP server access, limiting, 667-669
  superuser, creating, 129
Windows, mapping, 517
acl statement, 494
Address Resolution Protocol (ARP), 286
addresses
  destination, 612
IP
  active, displaying, 306
  banning, 696
  boistnames conversion to, 325
  boistname translations, 286
  load balancing, 399
  MAC address translation, 286
addresses

static, assigning, 327  
white listing, 697  
IPv4 loopback, 323  
IPv6 DHCP, 327  
MAC, 286  
predefined, 407  
Advanced Technology (AT), 233  
alerts (security)  
monitoring, 695  
services, 698  
aliases (Postfix), 612-614  
allow-query setting (etc/named.conf file), 406  
AllowGroups keyword (etc/ssh/sshd_config file), 683  
AllowUsers keyword (etc/ssh/sshd_config file), 682  
alternation pattern matching character (|), 626  
Amanda (Advanced Maryland Automatic Network Disk Archiver) utility, 374  
anon_max_rate directive (svftpd servers), 669  
anon_mkdir_write_enable setting (anonymous FTP), 666  
anon_upload_enable setting (anonymous FTP), 666  
anonymous_enable setting (anonymous FTP), 666  
anonymous FTP  
  Pure-FTPd access, 670  
vsftpd servers, 665-667  
another program action, 627  
Apache Web Servers, 455  
  configuration file  
  directives, 456-457  
  example, 456  
  location, 455  
killing off extra servers, 464  
log files, 458  
maximum number of clients, 464  
modules, loading, 460  
scripting, enabling  
  Perl, 461-462  
  PHP, 459-460  
security, 463-464  
SSL  
  CA chain, 484  
  certificate file location, 484  
  certificates directory, 484  
  ciphers, 485  
  client authentication, 484  
  directives, 484-485  
  header response information, 485  
  implementing, 477-478  
  private key file location, 484  
  protocol, specifying, 485  
  traces, 485  
  turning on/off, 484  
starting, 457-458  
user authentication, 465-466  
verifying, 457  
versions, 457  
virtual hosts, 466-467  
apache2ctl utility, 457  
approximate match filter expression (~), 599  
ap-get command, 347, 637  
architecture (system), 382  
arguments  
  iostat command, 9  
  openssl command, 479-480  
SSLProtocol directive, 485  
ARP (Address Resolution Protocol), 286-287  
ar command, 286  
  advantages, 288  
  -d option, 287  
  replacing with ip command, 289  
arerisks (*)  
  pattern matching character, 626  
  wildcard filter expression, 599  
asymmetric cryptography, 475  
async option (etc/fstab file), 164  
  -at option (netstat command), 309  
AT (Advanced Technology), 233  
ATA (AT Attachment), 233  
ATAPI (ATA Packet Interface), 233  
attacks  
  hijack, 441  
  man-in-the-middle, 477  
  attempts option (etc/resolv.conf file), 322
attributes
  defined, 576
  PVs, 270
-au option (netstat command), 309
auth PAM configuration type, 559
auth_param statement, 494
authdaemonrc daemon, 638
authentication
  Apache Web Server, 465-466
  clients, 494
  PAM, 555
    configuration file, 557
    configuration types, 559-562
    control values, 562-564
    etc/pam.d directory contents, 558
    features, 557
  SSH, 683
  SSL clients, 484
authoritative name servers, 398, 420
autofs, 204-207
+auto.master setting (etc/auto.master file), 205
auto option (etc/fstab file), 164
automatic filesystems, mounting, 160-162, 204-207
awareness topics, 716

B
b command, 120
B flag (procmail utility), 625
-b option
  free command, 10
  ldapsearch command, 598
background NFS mounts, 535
BackupPC utility, 374-375
backups
  compressing/uncompressing, 368
data, selecting for, 361-363
directories, selecting for, 362-363
filesystems
  LVM snapshots, 274-277
  selecting for, 362-363
frequency, 364
full, 366
incremental, 364-366
MBR, 369
merging files into single archives, 368
remote systems, 373-374
storing, 367
strategies, creating, 361
tape devices, 369-370
tar balls, 370
  appending to existing, 372
  compressing, 372
  contents, displaying, 370-371
  creating, 372
  current directory, setting, 372
  deleting files from, 372
  differences, displaying, 372
  extracting contents, 371-372
  partial restore, 372
  table of contents, displaying, 372
  verifying, 372
  third-party utilities, 374-375
Tower of Hanoi, 366
user home directories, 362
utilities
  dd command, 368-369
  selecting, 367
  tar command, 369-372
xfs filesystems
  xfsdump command, 184-186
  xfstest command, 186-187
Bacula utility, 374
banner_file directive (svftpd servers), 669
banner setting (SSH login setting), 683
banners (svftpd servers), 669
banning hosts, 697
bantime setting (fail2ban configuration), 697
base_dir setting (Dovecot server), 641
baselines (monitoring), 35
Basic Input/Output System (BIOS), 111
baudrate, 382
beginning of line pattern matching character (^), 626
benchmarking tests, 235-236
bin directory, 363
BIND (Berkeley Internet Name Domain), 399
configuring, 403-406
  configuration file, 403-406
  DNSSEC, 406
dump file location, 405
ports/interfaces for listening to, 405
Process IDs, 406
recursion, 406
statistical information from memory, copying, 405
systems for responding, 406
TSIG session key storage, 406
workdir directory, 404
defined, 399
rndc command, 408-411
split configuration, 443-445
forwarders, 445
internal/external network example, 444-445
techniques, 444
bindkeys-file setting (etc/named.conf file), 406
BIOS (Basic Input/Output System), 111
BIOS/UEFI (Basic Input/Output System)
(Unified Extensible Firmware Interface)
boot process phase, 111
blkid command, 163
block devices, 52
block group descriptors, 181
blocks, 181
blocks in/out, 12
Boolean operators, 599
boot directory, backing up, 363
boot loaders
boot process, 111-112
EXTLINUX, 144
GRUB 2. See GRUB 2
installing, 112
ISOLINUX, 144-145
Legacy GRUB. See Legacy GRUB
LILO
boot: prompt, 141
boot screen, 140
configuring, 137-139
GRUB, compared, 137
overview, 137
security, 142
single user mode, booting, 141
networking, 94
no GUI, 94
phases, 111
BIOS/UEFI, 111
bootloader, 111-112
kernel, 112-113
post-kernel, 113
PXELINUX boot loader, 145-146
rebooting the system, 94
runlevels, 93
default, 96
features, 94
modifying, 101-104
sets, 93-94
switching, 104
single user mode, 94
GRUB 2, 128
Legacy GRUB, 120-122
LILO, 141
SYSLINUX boot loader, 143-144
boots scripts, 98-102
-boot option (etc/lilo.conf file), 139
boot: prompt, 141
boot/grub2/grub.cfg, 125
boot grub/grub.cfg, 125
boot grub/grub.conf file, 114-117
common settings, 115
encrypted password, adding, 123
title section, 116
BOOTP hosts (DHCP), 547-548
boss screens, 332
broadcasting user messages
shutdowns, 389-390
wall, 387-389
-bs option (dd command), 369
B-tree filesystem. See HFS filesystems
Btrfs filesystems, 154, 175
BugTraq, 698
build-key-server script, 701-703
built-in targets, 653
bunzip command, 350
bunzip2 command, 368
bytes option (free command), 10
bzImage files, 46
bzip2 command, 368
C

C command, 120
c flag (procmail utility), 625
-c option
fdisk command, 176
iostat command, 7-8
netstat command, 18
ping command, 301
Pure-FTPd command line, 670
tar command, 372
-C option
Pure-FTPd command line, 670
tar command, 372
C style comments (/ * */, 405
cache_dir statement, 493

caches
name servers, 398
named, 410
poisoning (DNS), 447
static data, 493
Cacti, 33-34
CA.pl script, 482
CAs (Certificate Authorities), 476
chains, 484
configuring, 700
CSRs, 481-482
digital signatures, 476
self-signed certificates, 477
self-signed keys, creating, 480
cat command, 224-225
cd command, 700
CDs
backing up, 369
ejecting, 240
CERT (Computer Emergency Response Teams), 698
CERT-CC (CERT Coordination Center), 698
Certificate Signing Requests. See CSRs certificates
client, 703-705
digitally signed
CAs, 476
creating, 478-483
CSR, 479
RSA key file, 478
directory location, 484
file location, 484
self-signed, 477, 480
server, 701-703
signing requests, 479
creating, 481
signing, 482
SSL
creating, 478-483
CSRs, 479-481
RSA key file, creating, 478
self-signing, 480
signing requests, 482
storing, 483
storing, 483
-cf option (tar command), 370
chkconfig command, 102-104
choose all that apply exam questions, 721-722
choose multiple exam questions, 721
chown command, 443
chroot jail
  configuring named process to start in chrooted jail, 443
defined, 441
directories, 442-443
vsftpd servers, 669
chroot_local_users directive (vsftpd servers), 669
chroot/named/dev directory, 442
chroot/named/etc directory, 442
chroot/named/var/named directory, 442
chroot/named/var/run directory, 442
CIFS (Common Internet File System), 509
ciphers, 485
classes, 576
clean target (make command), 48
cleaning kernel, 47-48
client-side DNS settings, defining, 321
clients
  authentication, 494
certificates, creating, 703-705
FTP, 669
iSCSI, 241
NFS
  mount information, displaying, 534
  mounting NFS shares, 534
  persistent mounts across reboots, 535
  unmounting NFS shares, 535
  verifying NFS shares mounts, 534
OpenVPN, 706-708
proxy server configuration, 500-503
SSH commands, 684-687
SSL authentication, 484
utilities, 509
CNs (common names), 577, 598
collected daemon
  collected data, displaying/analyzing, 29
  configuring, 29-31
  features, 29
  installing, 31-32
  statistics for monitoring, 30
comma (,) SAMBA configuration file
  comments, 510
command field (etc/inittab file), 95
command line, 670
command line interface (NetworkManager), 338
commands
  apt-get, 347, 637
  arp, 286
    advantages, 288
    -d option, 287
    replacing with ip command, 289
  b, 120
  BIND, 408-411
  blkid, 163
  bunzip, 350
  bunzip2, 368
  bzip2, 368
c, 120
cat, 224-225
cd, 700
  chkconfig, 102-104
  chown, 443
cpio, 368
cryptsetup, 202-203
d, 368-369
ddebugfs, 182-184
depmod, 66
diff, 353
dig, 412, 432-433
dmesg, 86, 330
dnssec-keygen, 447-448
dnssec-signzone, 448-449
dovecot -n, 639
dracut, 113
dump, 274, 368
dumpdb, 410
dumpe2fs
  ext-based filesystems, 179-180
    filesystem features, 181
e2label, 162-163
egrep, 626
etc/rc5.d directory, executing, 98-99
exportfs, 533
fdisk, 176, 220
flush, 410
mkfs, 177-178
mkinitrd, 113
mkisofs
  HFS filesystems, 200
  -J option, 199
  removable media filesystems, creating, 198
  -R option, 199
  UDF filesystems, 200
modinfo, 72-73
modprobe
  kernel module parameters, setting, 72
  loading into memory, 70
  –r option, 71
mount, 165
  -a option, 164
  loading into memory, 69
  mounted filesystems, displaying, 155-157
  NFS shares, 534
  –o option, 158
  -ro option, 158
  -t option, 159
mpstat, 10
mt, 370
mtr, 332
named-checkconfig, 431
named-checkzone, 431-432
netstat
  -at option, 309
  -au option, 309
  -c option, 18
  -e option, 309
  -i option, 309
  -l option, 309
  -lt option, 18
  -lu option, 18
  network I/O monitoring, 17-18
  -n option, 18, 309
  -p option, 18, 309
  -r option, 18
  -rloption, 18
  -r option, 17
  -s option, 17, 307
network troubleshooting, 336
nfsstat, 534
nmap
  -flist option, 306
  network ports reachability, 302-303
  -O option, 305
  port scanning, 303
  probing machines, 305
  -S option, 306
  -Su option, 303
  -sV option, 304
nmlookup, 518
nmcli, 338
nm-tool, 337
nslookup, 433
openssl
  CSRs, creating, 479
  RSA key file, creating, 478
passwd, 121
ping
  -c option, 301
  -f option, 302
  remote systems, 301-302
proconf, 610-611
procmail -h, 625
ps, 18-19
pstree, 19
pvchange, 270
pvcreate, 258
pvdisplay, 262, 267
pvmove, 270
pvremove, 270
reconfig, 411
resize2fs, 272-273
restore, 368
rmmod, 71
rnet, 410
rndc-confgen, 408
route
  advantages, 288
  displaying routing tables, 287
  replacing with ip command, 289
routing tables, 308
rpcinfo, 531
rpm2cpio, 346
rsync, 373-374
sar
  CPU monitoring, 9
  disk I/O monitoring, 14
  as monitoring tool, 34
scp, 687  
scsi_id, 246  
sftp, 687  
sdparm, 236  
showmount, 534  
shutdown, 96, 389-390  
slapadd, 577  
slapcat, 587, 595  
slapindex, 587  
slappasswd, 580  
smartctl, 190-191  
smbclient, 518  
smbpasswd, 517  
smbstatus, 520  
source, 701  
ssh, 685-686  
SSH client, 684-687  
ssh-keygen, 683  
stat, 183  
status, 411  
stop, 411  
swapon, 166-167, 189  
sync, 166  
sysctl, 73-74  
tar  
  -A option, 372  
  backups, 369-372  
  -cf option, 370  
  -c option, 372  
  -C option, 372  
  -delete option, 372  
  -d option, 372  
  filenames, listing at end, 372  
  -j option, 350, 372  
  source code, unpacking, 349  
  -tf option, 370  
  -t option, 372  
  -v option, 371  
  -W option, 372  
  -xf option, 371  
  -x option, 372  
  -xzf option, 349  
  -z option, 372  
tcpdump, 313-314  
telinit, 104  
testparm, 515-516  
tgt-admin --show, 243  
top, 20  
traceart, 330-331  
tune2fs, 182  
tunedadm monitor, 86  
uname  
  current kernel, displaying, 65  
  platforms, determining, 352  
unmount, 155  
unzip, 368  
update-re, 102-103  
uptime, 7  
vchange, 270  
vgdisplay, 260-261  
  after LV creation, 265-267  
  -v option, 261  
vgextend, 270  
vmsstat, 11-12  
w, 21  
wall, 387-389  
watch, 21  
xfs_check, 189  
xfsdump, 184-186  
xfs_info, 187  
xfs_repair, 188-189  
xfsrestore, 186-187  
yumdownloader, 346  
zip, 368  

comments  
etc/SAMBA/smb.conf file, 510  
  files, adding, 405  
  zone files, 421  

Common Internet File System (CIFS), 509  
common names (CNs), 577, 598  

compiling kernel  
  cleaning the kernel, 47-48  
  configuration file, creating, 48-50  
  source code, downloading, 47  
  unpacking, 47  

compressing  
  files, 368  
  tar balls, 372  

Computer Emergency Response Teams (CERT), 698
configuration files

Apache Web Server configuration, 456-457
boot/grub2/grub.cfg, 125
boot/grub/grub.cfg, 125
boot/grub/grub.conf, 114-117
common settings, 115
encrypted password, adding, 123
title section, 116
Courier, 637-639
etc/courier/authdaemonrc, 637
etc/courier/imapd, 637
etc/default/grub
changes, saving, 127
common settings, 126
glob section, 125
etc/dhcpd.conf, 543
ddn-update-style directive, 545
example, 543-544
ignore client-updates directive, 545
subdirectives, 546
subnet directive, 545-546
etc/dovecot/dovecot.conf, 639
/etc/fail2ban/jail.conf, 696
/etc/iscsi/iscsid.conf, 244
etc/lilo.conf, 137
glob section, 138
images, 139
kernel file location, 139
security options, 142
/etc/named.conf
allow-query setting, 406
comments, adding, 405
glob section, 407
logging settings, 407
settings, 405-406
zone file entries, 420-421
zone settings, 407
/etc/postfix/main.cf, 610-611
/etc/resolv.conf, 400
/etc/ssh/sshd_config, 681
AllowGroups keyword, 683
AllowUsers keyword, 682
DenyGroups keyword, 683
DenyUsers keyword, 682
ListenAddress keyword, 681
LogLevel keyword, 681
Port keyword, 681
Protocol keyword, 681
t/etc/sysctl.conf, 74, 649
t/etc/tgt/targets.conf, 242
t/etc/vsftpd/vsftpd.conf, 665, 669
t/etc/yum.conf, 345
$HOME/.procmailrc, 623
kernel, creating, 48-50
block devices, selecting, 52
device drivers, selecting, 51
make config command, 48
make menuconfig command, 48
named servers, reloading, 408
network, 321
t/etc/hosts, 323-324
t/etc/network/interfaces, 326
t/etc/network-scripts directory, 327
t/etc/resolv.conf, 321-323
pam.conf, 557
slapd.conf, 576-581
Squid, 493
syslinux.cfg, 144
configuring
BIND, 403-406
configuration file, 403-406
DNSSEC, 406
dump file location, 405
ports/interfaces for listening to, 405
Process IDs, 406
connections

recursion, 406
statistical information from memory, copying, 405
systems for responding, 406
TSIG session key storage, 406
working directory, 405
CAs, 700
collectd daemon, 29-31
Courier servers
  authdaemonrc daemon, 638
  configuration files, 637
  imap daemon, 638
  POP daemon, 639
DHCP servers
  configuration file, 543-544
  DDNS updates, 545
  IP information for, 545-546
DNS slave servers, 420
Dovecot servers
  clean configuration, 639-640
  settings, 641
t/c/fail2ban/jail.conf, 697
firewalls, 695
  chains, 652
  examples, 653-654
  features, 650
  filtering, 650, 654
  options, 654
  targets, 653
GRUB 2, 125-130
iSCSI initiators, 244
LDAP, 579-580
Legacy GRUB
  configuration file, 114-117
  default settings, 115
  initrd parameter, 116
  kernel parameter, 116
  menu, hiding, 115
  root parameter, 116
  splashimages, 115
  timeouts, 115
  title parameter, 116
LILO
  configuration file, 137
  global options, 138
images, 139
kernel file location, 139
Linux system as routers, 649
named process to start in chrooted jail, 443
NFS servers
  etc/exports file, 527-528
  NFS client mount information, displaying, 534
  NFS servers access, 532-533
  NFS software, installing, 527
  processes, 530-531
  RPC service, 527, 531
  shared resources, displaying, 533
  sharing options, 528
  UID mapping, 529-530
PAM
  environment, 560
  etc/pam.d directory, 558
  pam.conf file, 557
Pure-FTPD, 670
SAMBA
  configuration file, 510
  directory shares, 514
  global settings, 511-512
  home directories, 512-513
  printers, 513-514
  share security, 514
  verifying, 515-516
split BIND, 443-444
  forwarders, 445
  internal/external network example, 444-445
  techniques, 444
SSH servers
  authentication, 683
  log messages, 681
  network card connections, 681
  ports, 681
  protocol connections, 681
  user logins, 682-683
  targets, 243
VPNs, 705
Connection Editor, 338
connections
  FTP clients, 669
  POP versus IMAP, 636
  SSH, 681
control values (PAM), 562-564
count argument (iostat command), 9
courier-imap package, 636
courier-pop package, 636
Courier servers, 636-637
  configuration files, 637
  configuring, 638-639
  installing, 637
  Maildir format, 638
  as SMTP server, 636
cpio command, 368
CPU, monitoring, 6-7
  iostat command, 7-9
  load average, 7
  mpstat command, 10
  sar command, 9
creating
  backup strategies, 361
    backup data, storing, 367
    frequency, 364
    full backups, 366
    incremental backups, 364-366
    utilities, selecting, 367
    what needs to be backed up, determining, 361-363
  client certificates, 703-705
  custom shares, 514
  DNS servers, 427-431
  encrypted filesystems, 202-203
  etc/rndc.conf file, 408-409
  files, 368
  filesystems, 177-178
  GRUB encrypted password, 122
  initramfs files, 113
  initrd files, 113
  kernel configuration file, 48-50
    block devices, selecting, 52
    device drivers, selecting, 51
    make config command, 48
    make menuconfig command, 48
  labels, 162
  LVs, 262-263
  partitions, 176-177
removable media filesystems, 200
  HFS, 200
  ISO9660, 198-199
  UDF, 200
repository files, 345
reverse lookup zones, 421
SAMBA user accounts, 516-518
server certificates, 701-703
source code
  configure script, executing, 350-351
  directory storage, 352
  Makefile, 352-353
  platforms, determining, 352
SSL certificates, 478-483
  CSRs, 479-481
  RSA key file, 478
  self-signing, 480
  signing requests, 482
  storing, 483
tar balls, 370-372
  appending to existing, 372
  compressing, 372
  contents, displaying, 370-371
  current directory, setting, 372
  deleting files from, 372
  differences, displaying, 372
  extracting contents, 371-372
  partial restore, 372
  table of contents, displaying, 372
  verifying, 372
targets, 242
  zone files, 421
cryptsetup command, 202-203
CSRs (Certificate Signing Requests), 479
  creating, 481
  generating, 479
  signing, 482
C++ style comments (//), 405
crtlaltdel keyword, 96
cups options setting (SAMBA), 512
CUPS printers, sharing, 512-514
current origin (@), 422
custom shares (SAMBA), 514
customizing
  LDAP domains, 579-580
  login prompt messages, 381-382
D

D flag (procmail utility), 625
-d option
  arp command, 287
  hdparm command, 235
  iostat command, 12
  lsusb command, 82-84
  sar command, 14
  tar command, 372
-D option
  ldapdelete command, 596
  ldappasswd command, 600
daemons
  authdaemonrc, 638
  collectd
    collected data, displaying/analyzing, 29
    configuring, 29-31
    features, 29
    installing, 31-32
    statistics for monitoring, 30
  iscsid, 244
  NetworkManager, 337-339
    command line interface, displaying, 338
    components status, 338
    current network device status, 337
    disabling, 337
    etc/resolv.conf file, populating, 323
    existence, checking for, 337
    GUI-based tool, 338
    overview, 337
    WiFi, disabling, 338
  POP, 639
  smartd, 190
  tgtd, 242
  udevd, 85-86, 246
data
  backups
    selecting for, 361-363
    storing, 367
  collected by collectd daemon, displaying/analyzing, 29
  Dovecot server, storing, 641
  moving between PVs, 270
  parity, 215
  SAMBA account, storing, 512
  SOA records, 423
  static, 493
databases (OpenLDAP)
  access control, 587-588
  changes, 586-588
  deleting objects, 596
  directory, 582
  passwords, 600-601
  populating, 595
  searching for objects by
    Boolean operators, 599
    common names, 598
    filter expressions, 599-600
    types, 597-598
dates, displaying at login prompt, 382
dd command, 368-369
ddns-update-style directive, 545
Debian-based systems
  boot scripts, 102
  DRUB 2 configuration file, 125
  etc/HOSTNAME file, 325
  etc/network/interfaces file, 326
  repositories, 347
  runlevel set, 93
  source code, downloading, 347-348
  update-grub command, 127
  update-rc.d command, 102-103
  var/log/boot.log file, 330
  var/log/syslog file, 328
debugfs command, 182-184
DEBUG log levels (SSH), 682
DEBUG_LOGIN setting (authdaemonrc daemon), 638
debugging, 182-184
default-lease-time subdirective, 546
-default option
  etc/fstab file), 163
  etc/lilo.conf file, 139
-delete option (tar command), 372
deleted files, displaying, 184
deleting
  ARP table entries, 287
  gateways, 288
  OpenLDAP database objects, 596
  PVs from VGs, 270
RAID devices, 225
swap devices, 167
tar ball files, 372
deny client-update directive, 545
DenyGroups keyword (etc/ssh/sshd_config file), 683
DenyUsers keyword (etc/ssh/sshd_config file), 682
dependencies (kernel modules), displaying, 66
depmod command, 66
des3 option, 479
descriptors (device)
  block group, 181
  labels, 162-163
  UUIDs, 163
destination addresses, 612
Destination NAT (DNAT), 647
device field (mount command), 156
device_to_mount field (etc/fstab file), 161
devices
  active network, displaying, 283
  block, 52
  converting to PVs, 258
descriptors, 162-163
drivers, 51
files, 442
hardware, 237
information, displaying
  lsdev command, 81-82
  lspci command, 77
  lspci -k command, 80
  lspci -v command, 78-79
  lspci -vv command, 79
  udevd daemon, 85-86
  var/log/messages file, 84
I/O statistics, displaying, 12-13
iSCSI target names, 244-245
kernel module associations, displaying, 80
mapper names, 13
naming, 263-264
network, 337
partitions, 176-177
PCI, 77-79
RAID
  creating, 221-223
  managing, 224-226
  partitions versus entire hard disks, 219-220
SCSI, 236
storage
  information, displaying, 237-239
  kernel parameter affects, 239-241
swap, 166-167, 189-190
tape, 369-370
TTY, 382
USB, 82-84
UUIDs, 163
dev option (etc/fstab file), 164
dev/mapper/VG-LV naming convention, 264
dev/VG/LV naming convention, 264
df plugin, 30-31
DFS (Distributed File System), 509
dhclient utility, 323
DHCP (Dynamic Host Configuration Protocol), 541
dhcp package, 543
DHCP servers
  configuration file, 543-544
  DDNS updates, 545
  IP information for, 545-546
  IPv6 DHCP addresses, 327
  log files, 548-549
  packages, 543
  relay agents, 549
  rogue, 543
  static hosts, 547-548
  virtual machines, 543
dhcp3-server, 543
dhcp4-server, 543
dhcp-server package, 543
diff command, 353
Diffie-Hellman parameters, 703
dig (domain information grooper), 336
dig command, 412, 432-433
Digital Signature Algorithm (DSA), 479
digital signatures, 476
dir, 205
direct autofs maps, 207
**directives**
Apache Web Server, 456–457
DHCP server, 545–546
etc/vsftpd/vsftpd.conf file, 669
modules, loading, 460
SSL-based Apache, 484–485
subnet, 544
userlist_denial, 668
userlist_enable, 668
userlist_file, 668

**Direct Memory Access (DMA), 233–235**

**directories**
/
Apache Web Server configuration file location, 455
backing up, selecting for, 362–363
bin, 363
BIND working, configuring, 405
boot, 363
chroot, 442–443
etc, 363
etc/courier, 637
etc/dovecot/conf.d, 639
etc/init.d, 101–102
etc/modprobe.d, 76–77
etc/openvpn, 703
etc/openvpn/easy-rsa/keys, 703
etc/pam.d, 558
etc/pki, 483
etc/rc5.d, 98–99
etc/squid, 493
etc/ssl, 483
etc/sysconfig/network-scripts, 327
etc/udev/rules.d, 85–86
/etc/yum.repo.d, 345
files, 182
home
backing up, 362
procmail, adding, 624
include (Dovecot server), 641
LDAP, 577, 582
lib, 363
lib64, 363
lib/modules, 65–66
lib/modules/kernel_version, 65–66
mail spool, 624
opt, 363
proc/sys, 44–45, 73
sbin, 363
shares, 514
sharing from NFS servers to NFS clients, 527–528
tar balls
    contents, extracting into, 371
    current, setting, 372
user home
backing up, 362
sharing, 512–513
usr, 362
usr/share/doc/kernel-doc/Documentation, 43
usr/share/easy-rsa, 700
usr/src, 47, 349
usr/src/linux/Documentation, 43
var, 363
var/log/SAMBA, 516
var/named, 419
var/spool/postfix, 610
var/www/html, 458

**directory servers, 573**

**directory setting (etc/named.conf file), 405**

**dirmessage_enable setting (anonymous FTP), 666**

**disable_vrfy_command setting (Postfix), 612**

**disabling**
DMA support, 235
file uploads on vsftpd servers, 669
NetworkManager daemon, 337
promiscuous mode, 285
suid permission set, 164
WiFi, 338

**disk plugin, 30**

**disks**
backups, 367
drives, mirroring, 214
hard

benchmarking tests, 235–236
converting to PVs, 258
DMA support, enabling/disabling, 235
disks

IDE, 116
information, displaying, 234
SATA, 116
single hard disk systems, 257-258
SMART, 190-191
striping, 214
versus partitions for RAID devices, 219-220
I/O, monitoring, 6
iostat command, 12-13
lsblk command, 12
lsof command, 14-17
sar command, 14
displaying
active IP addresses, 306
ARP table, 286
boss screens, 332
collected data from collectd daemon, 29
CPU statistics
iostat command, 7-9
mpstat command, 10
sar command, 9
deleted files, 184
device I/O statistics, 12-13
directory files, 182
disk I/O statistics
iostat command, 12-13
lsof command, 14-17
sar command, 14
etc/initab file, 94
hardware information
ldev command, 81-82
lpci command, 77
lpci -k command, 80
lpci -v command, 78-79
lpci -vv command, 79
lpci -vvv command, 79
udevd daemon, 85-86
var/log/messages file, 84
interrupts, 237
kernel module
dependencies, 66
device associations, 80
kernel ring buffer, 328
labels, 163
libwrap library services, 333
libwrapped services, 333
local hostnames, 325-326
local networks
packet information, 307
traffic, 313-314
LV information, 267
memory statistics, 10-12
mounted filesystems, 155
etc/mount file, 156
proc/mounts file, 157
named server status, 411
networks
information, 283-285
interfaces, 306-309
I/O statistics, 17-18
NetworkManager, 338
NFS, 533-534
nonresponsive internal gateways, 330-332
parameters (modules), 72-73
partitions, 176
Postfix configuration settings, 610-611
processes
relationships, 19
statistics, 18-20
using the filesystem, 159
PVs, 262, 267
PVs/LVs associated with VGs, 261
root servers, 400-401
routing tables, 287
local networks, 308
remote systems, 306
SAMBA server
shares, 518
status, 520
SCSI device information, 236
storage device information, 237-239
tar ball contents, 370-371
USB device information, 82-84
UUIDs (devices), 163
VG information, 260-261, 265-267
WiFi
interface parameters, 290-291
wireless routers available, 291-293
distclean target (make command), 29
distinguished names (DNs), 577
Distributed File System (DFS), 509

distributions for exam preparation, 718-719
djbdns servers, 399
DMA (Direct Memory Access), 233-235
DMCrypt kernel module, 201
dmesg command, 86, 330
DNAT (Destination NAT), 647
DNS (Domain Name Service), 397

BIND

commands, 408-411
configuring, 403-406

cache
poisoning, 447
name servers, 398

chroot jail

configuring named process to start in chrooted jail, 443
copying files to directories, 442-443
creating directories, 442
defined, 441

current status, displaying, 411
defined, 398
dump files, creating, 410
etc/resolv.conf file, 321
multiple, 400
SOA records, 423
stopping, 411
testing, 431-433
zone files, reloading, 408

slave servers, 420
split configuration, 443-445
subdomains, 398
top-level domains, 397
TTL, 398
views, 444
zone files

@ (current origin) character, 422
comments, 421
creating, 421
defined, 398
etc/named.conf file entries, 420-421
local host file, 419
record fields, 422
reverse lookup, 421
root servers, listing of, file, 419
storage location, 419
storing in chroot directory, 442
syntax, 421-422
transferring, 421, 446
TTL, 422
zone records, 423-425

DNs (distinguished names), 577
dnsmasq servers, 399
dns plugin, 30

DNSSEC (Domain Name System Security Extensions)
BIND configuration settings, 406
private/public keys, creating, 447-448
zone files, 448-449
dnssec-enable setting (etc/named.conf file), 406
dnssec-keygen command, 447-448
dnssec-lookaside setting (etc/named.conf file), 406
dnssec-signzone command, 448-449
dnssec-validation setting (etc/named.conf file), 406
documentation
kernel, 43-44
SAMBA 3, 510
DocumentRoot directive, 456
domain information groper (dig), 336
Domain Name Service. See DNS
domain-name-servers subnet-mask subdirectory, 546
domain-name subdirectory, 546
domains
LDAP, 577-580
names
defined, 397
fully qualified (FQDNs), 397
Postfix, 612-614
specifying for searching (etc/resolv.conf file), 322
subdomains, 398
top-level, 397
dovecot -n command, 639
Dovecot servers, 639
clean configuration, 639-640
data, storing, 641
include directory, 641
installing, 639
interfaces for listening, 641
mailboxes, finding, 641
protocols, 641
settings, 641-643
downloading source code
Debian-based systems, 347-348
from original sources, 348-349
kernel, 47
RPM-based systems, 345-347
dracut command, 113
drivers (devices), 51
drives
boot, 139
disk, mirroring, 214
single drive systems, 257-258
striping, 214
DROP target, 653
DSA (Digital Signature Algorithm), 479
dump command, 274, 368
dump files, 410
dumpdb command, 410
dumpe2fs command
ext-based filesystems, 179-180
filesystem features, 181
dump-file setting (etc/named.conf file), 405
dump_level field (etc/fstab file), 161
DVDs, backing up, 369
Dynamic Host Configuration Protocol (DHCP), 541
E
-e option
netstat command, 309
Pure-FTPd command line, 670
-E option, 670
-e ssh option (rsync command), 373
e2label command, 162-163
egde command, 626
El Torito extension (ISO9660 filesystem), 144, 198
e-mail
drivers (devices), 51
drives
boot, 139
disk, mirroring, 214
single drive systems, 257-258
striping, 214
DROP target, 653
DSA (Digital Signature Algorithm), 479
dump command, 274, 368
dump files, 410
dumpdb command, 410
dumpe2fs command
ext-based filesystems, 179-180
filesystem features, 181
dump-file setting (etc/named.conf file), 405
dump_level field (etc/fstab file), 161
DVDs, backing up, 369
Dynamic Host Configuration Protocol (DHCP), 541
E
-e option
netstat command, 309
Pure-FTPd command line, 670
-E option, 670
-e ssh option (rsync command), 373
e2label command, 162-163
egde command, 626
El Torito extension (ISO9660 filesystem), 144, 198
e-mail
addresses
action, 627
SOA records, 424
Courier server, 636-637
authdaemonrc daemon, 638
configuration files, 637
imap daemon, 638
installing, 637
Maildir format support, 638
POP daemon, 639
as SMTP server, 636
Dovecot server, 639
clean configuration, 639-640
data, storing, 641
include directory, 641
installing, 639
interfaces for listening, 641
mailboxes, finding, 641
protocols, 641
settings, 641-643
exim server, 605, 615
harvesting prevention, 612
IMAP, 635-636
mail spool directory, choosing, 624
messages
  handling with POP versus IMAP, 636
  retrieving with POP versus IMAP, 636
  storing, 610, 628-629
POP, 636
Postfix, 605
  aliases, 612-614
  all configuration settings, displaying, 610
  client outgoing hostnames, 612
  configuration file, 610-611
  destination addresses, 612
  domains, 612
  e-mail harvesting prevention, 612
  hostnames, 612
  interfaces for listening, 612
  monitoring, 616
  relay setting, 612
  settings, displaying, 611-612
  var/spool/postfix directory, 610
  virtual domains, 614
procmail
  advantage over MTAs, 623
  defined, 621
  installing, 623
  lockfile, 626
  MTA automatic usage, determining, 623
  rules, 625-628
  as SPAM filter, 624
RFCs, 607
sending, 608
sendmail server, 605, 615
servers, monitoring, 616
SMTP, 607-608
enabled setting (fail2ban configuration), 697
enabling
  ARP, 286
  DMA support, 235
  DNSSEC, 406
  executable files, 164
  IPv6 DHCP addresses, 327
  promiscuous mode, 285
scripting
  Perl, 461-462
  PHP, 459
SSL, 484-485
  suid permission set, 164
  swap devices, 167
  targets, 243
encrypting
  file level, 201
  filesystems, 201
    benefits, 201
    creating, 202-203
    Linux Unified Key Setup (LUKS), 201
  passwords, 122
  Triple DES, 479
end of line pattern matching character ($), 626
environment, 560
equal to or greater than filter expression (>=), 599
equal to or less than filter expression (<=), 599
error_log file, 458
errors
  bad superblocks, 181
  kernel, 330
  unmounting filesystems, 159
ESMTP (Extended SMTP), 607
e tc/apt/sources.list file, 347
e tc/auto.master file
  CentOS 7.X system example, 204
  default settings, 205
e tc/auto.misc file, 206
e tc/courier/authdaemonrc file, 637
e tc/courier/imapd file, 637-639
e tc/courier/pop3d file, 637
e tc/courier/pop3d file, 637
e tc/default/grub file
  changes, saving, 127
  common settings, 126
  example, 125
e tc/dhcp/dhcpd.conf file, 543
  ddns-update-style directive, 545
  example, 543-544
ignore-client-updates directive, 545
subdirectives, 546
subnet directive, 545, 546
etc directory, 363
etc/dovecot/conf.d directory, 639
etc/dovecot/dovecot.conf file, 639
etc/exports file
  hostnames, 528
  NFS sharing options, 528
  syntax, 527
etc/fail2ban/jail.conf file, 696-697
etc/fstab file
  default options, 163-165
  filesystems, mounting, 160-161
  NFS mount options, 535-536
  persistent NFS mounts across reboots, 535
  UUIDs, 163
etc/grub.d/40_custom file, 128
etc/HOSTNAME file, 325
etc/hosts.allow file, 334-335, 532
etc/hosts.deny file, 334-335, 532
etc/hosts file
  format, 323
  IPv4 loopback addresses, 323
  local network name resolution, 323-324
etc/init.d directory, 101-102
etc/init.tab file
  contents, displaying, 94
  fields, 95
  keywords, 96-97
  Red Hat-based system typical entries, 97
etc/iscsi/iscsid.conf file, 244
etc/issue file, 381-382
etc/lilo.conf file, 137
  example, 138
  global options, 138
  images, 139
  kernel file location, 139
  security options, 142
etc/modprobe.d directory, 76-77
etc/mntab file
  mounted filesystems, displaying, 156
  proc/mounts file, compared, 157
etc/named.conf file
  allow-query setting, 406
  comments, adding, 405
  example, 403-404
  include settings, 407
  logging settings, 407
  settings, 405-406
  zone file entries, 420-421
  zone settings, 407
etc/network/interfaces file, 326
etc/openvpn directory, 703
e tc/openvpn/easy-ras/keys directory, 703
e tc/pam.d directory, 558
e tc/pam.d/system-auth file, 565
e tc/pki directory, 483
e tc/postfix/main.cf file, 610-611
e tc/proocmailrc file, 624
e tc/rc5.d directory, 98-99
e tc/rc5.d/S55sshd script, 100
e tc/rc.d/rc script, 98
e tc/rc.d/rc.sysint script, 98
e tc/resolv.conf file, 321-323
  attempts, 322
  DNS, 321, 400
  domains, specifying for searching, 322
  populating, 323
  resolver settings, 322
  route, 322
  timeouts, 322
etc/rndc.conf file
  creating, 408-409
  permissions, 410
etc/SAMBA/smb.conf file, 510
  comments, 510
  example, 510
  global section, 511-512
  homes section, 512-513
  printers section, 513-514
  verifying, 515-516
etc/shadow file, 562
etc/squid directory, 493
e tc/ssh/sshd_config file, 681
  AllowGroups keyword, 683
  AllowUsers keyword, 682
  DenyGroups keyword, 683
  DenyUsers keyword, 682
  ListenAddress keyword, 681
LogLevel keyword, 681
Port keyword, 681
Protocol keyword, 681
/etc/ssl directory, 483
/etc/sysconfig/network file, 327
/etc/sysconfig/network-scripts directory, 327
/etc/sysconfig/network-scripts/ifcfg-eth0 file, 327
/etc/sysctl.conf file, 74, 649
/etc/tgt/targets.conf file, 242
/etc/udev/rules.d directory, 85-86
/etc/vsftpd.ftpsers file, 668
/etc/vsftpd/vsftpd.conf file, 665, 669
/etc/yum.conf file, 345
/etc/yum.repo.d directory, 345
ethtool, 336
exact match filter expression (=), 599
exam preparation
distributions, 718-719
exam facts, 714
exam objectives, 714-716
  awareness topics, 716
  Key Knowledge Areas, 716
LPI.org website, 714
  subtopic weight, 716
  topics/subtopics, 715
immediately before, 714
question types, 719-720
  choose all that apply, 721-722
  choose multiple, 721
  fill-in-the-blank, 723
  single answer multiple choice, 720
studying, 717
  machines, 717
  virtual machines, 718
  what not to do, 718
things to remember, 724
exclamation points (!)
logical not operator, 599
negation character, 407
exec option (etc/fstab file), 164
executable files, enabling, 164
exim e-mail server, 605
expiry value (SOA records), 424
exportfs command, 533
ext2 filesystems, 173
debbuging, 182-183
defined, 154
details, displaying, 179-181
fsck command, 130, 179
modifying, 182
ext3 filesystems, 173-174
debbuging, 182-183
defined, 154
details, displaying, 179-181
fsck command, 130, 179
journals, 173
modifying, 182
ext4 filesystems, 174
debbuging, 182-183
defined, 154
details, displaying, 179-181
fsck command, 130, 179
modifying, 182
mount options, 165
Extended Integrated Drive Electronics (EIDE), 233
Extended SMTP (ESMTP), 607
extensions
  ISO9660 filesystem, 198
  Joliet, 199
  Rock Ridge, 199
targets, 653
extents
  logical, 262
  physical, 259-260
EXTLINUX boot loader, 144

F
-f option (ping command), 302
fail2ban utility, 696-697
FAT filesystems, 69, 143
fdisk command, 176, 220
-fe option (ps command), 18
fields
  etc/fsatb file, 161
  etc/inittab file, 95
  mount command, 156
file-handles allocation, modifying, 45
file-max file, 44-45
Apache Web Server configuration directives, 456-457
example, 456
location, 455
boot/grub2/grub.cfg, 125
boot/grub/grub.cfg, 125
boot/grub/grub.conf, 114-117
common settings, 115
encrypted password, adding, 123
title section, 116
bzImage, 46
certificate, 484
compressing, 368
Courier, 638-639
creating/restoring utilities, 368
deleted, displaying, 184
device, storing in chroot directory, 442
directories, displaying, 182
dump, 410
encryption, 201
etc/apt/sources.list, 347
etc/auto.master
CentOS 7.X system example, 204
default settings, 205
etc/auto.misc, 206
etc/collectd/collectd.conf, 29-30
etc/courier/authdaemonrc, 637
etc/courier/impad, 637
etc/courier/pop3d, 637
etc/default/grub
changes, saving, 127
common settings, 126
example, 125
etc/dhcp/dhcpd.conf, 543-545
ddns-update-style directive, 545
example, 543-544
ignore client-updates directive, 545
etc/dovecot/dovecot.conf, 639
etc/exports
hostnames, 528
NFS sharing options, 528
syntax, 527
etc/fail2ban/jail.conf, 696-697
etc/fstab
default options, 163-165
NFS mount options, 535-536
persistent NFS mounts across reboots, 535
UUIDs, 163
etc/fstab/filesystems, mounting, 160-161
etc/grub.d/40_custom, 128
etc/HOSTNAME, 325
etc(hosts).allow, 334-335, 532
etc(hosts).deny, 334-335, 532
etc/init tab
contents, displaying, 94
fields, 95
keywords, 96-97
Red Hat-based system typical entries, 97
etc/is cs i/iscsid.conf, 244
etc/issue
login prompt, customizing, 381-382
special values, 382
etc/lilo.conf, 137
default settings, 138
global options, 138
images, 139
kernel file location, 139
security options, 142
etc/modprobe.d directory, 76-77
etc/mtab
mounted filesystems, displaying, 156
proc/mounts file, compared, 157
etc/named.conf
allow-query setting, 406
comments, adding, 405
default settings, 405
example, 403-404
include settings, 407
logging settings, 407
settings, 405-406
zone file entries, 420-421
zone settings, 407
etc/pam.d/system-auth, 565
etc/postfix/main.cf, 610-611
etc/pro cmailrc, 624
etc/resolv.conf, 400
etc/rdns.conf
creating, 408-409
permissions, 410
etc/SAMBA/smb.conf, 510
  comments, 510
elementary, 510
global section, 511-512
  bompes section, 512-513
  printers section, 513-514
  verifying, 515-516
etc/shadow, 562
  etc/samba.conf, 510
  annotations, 510
  global section, 511-512
  homes section, 512-513
  printers section, 513-514
  verifying, 515-516
etc/shadow, 562
  etc/shadow, 562
  etc/ssh/sshd_config, 681
  AllowGroups keyword, 683
  AllowUsers keyword, 682
  DenyGroups keyword, 683
  DenyUsers keyword, 682
  ListenAddress keyword, 681
  LogLevel keyword, 681
  Port keyword, 681
  Protocol keyword, 681
executive, enabling, 164
file-max, 44-45
global section, 511-512
  bompes section, 512-513
  printers section, 513-514
  verifying, 515-516
etc/sysconfig/network, 327
e tc/sysconfig/network, 327
e tc/sysconfig/network-scripts/ifcfg-eth0, 327
e tc/sysctl.conf, 74, 649
e tc/tgt/targets.conf, 242
e tc/udev/rules.d directory, 85-86
e tc/vsftpd/vsftpd.conf, 668
e tc/vsftpd/vsftpd.conf, 665, 669
e tc/yum.conf, 345
  executable, enabling, 164
  file-max, 44-45
  grub.cfg, 128
  $HOME/.procmailrc, 623
  initramfs, 113
  initrd, 113
  ISO image, 369
  kernel configuration, creating, 48-50
    block devices, selecting, 52
    device drivers, selecting, 51
    make config command, 48
    make menuconfig command, 48
  kernel image, 46
  LDIF, 584
  libphp5.so, 459
  local device, 246
  lockfiles, 626
  log
    Apache Web Server, 458
    DHCP, 548-549
  symbolic, installing, 190
  tar ball, 382
  undeleting, 183
  uncompressing, 368
  uninstalling, 368
  unzipping, 349-350
  sudo, 371
  server.conf.gz, 705
  slapd.conf, 576, 579-581
  source
    storing, 349
    unzipping, 349-350
Squid configuration, 493
  ssh_config, 684-685
  syslinux.cfg, 144
  tar ball, deleting, 372
  .tar.gz, 349
  uncompressing, 368
  undeleting, 183
  usr/share/doc/kernel-doc-2.6.32/
    Documentation/sysctl/fs.txt file, 44
  etc/named.conf file setting, 407
  LDAP, 581-582
  for network troubleshooting, 328-330
  SSH connections, configuring, 681
  var/log/SAMBA directory, 516
Makefile, 47, 352-353
  merging into single archives, 368
  mod_perl.so, 461
  modules.dep, 66
  network configuration, 321
    etc/hosts, 323-324
    etc/network/interfaces, 326
    etc/resolv.conf, 321-323
    etc/sysconfig/network-scripts directory, 327
  pam.conf, 557
  passwd.ldif, 595
  proc/devices, 238
  proc/devstats, 239
  proc/dma, 82
  proc/filesystems, 239
  proc/interrupts, 82, 237
  proc/ioports, 82
  proc/mounts
    displaying, 534
    etc/mtab file, compared, 157
    mounted filesystems, displaying, 157
  proc/partitions, 239
  proc/sys/dev/cdrom/lock, 240
  proc/sys directory, 73-74
  proc/sys/net/ipv4/ip_forward, 649
  repository, creating, 345
  RSA private key, creating, 478
  server.conf.gz, 705
  slapd.conf, 576, 579-581
  source
    storing, 349
    unzipping, 349-350
  Squid configuration, 493
  ssh_config, 684-685
  syslinux.cfg, 144
  tar ball, deleting, 372
  .tar.gz, 349
  uncompressing, 368
  undeleting, 183
  usr/share/doc/kernel-doc-2.6.32/
    Documentation/sysctl/fs.txt file, 44
var/log/messages, 84, 328
var/log/syslog, 84, 328
vmlinuz, 139
zImage, 46
zone
  @ (current origin) character, 422
  comments, 421
  creating, 421
  defined, 398
  DNSSEC, 448-449
  etc/named.conf file, 407, 420-421
  forward, 420
  local host file, 419
  record fields, 422
  reloading, 408
  reverse lookup, 421
  root servers, listing of, file, 419
  storage location, 419
  storing in chroot directory, 442
  syntax, 421-422
  transferring, 421, 446
  TTL, 422

filesystems
autofs, 204-207
backing up
  LVM snapshots, 274-277
  selecting for, 362-363
block group descriptors, 181
block size, 181
Btrfs
  defined, 154
  overview, 175
corrupt, fixing, 130
creating, 177-178
debugging, 184
deleted files, displaying, 184
encrypted, 201
  benefits, 201
  creating, 202-203
  Linux Unified Key Setup (LUKS), 201
ext2, 154, 173
ext3, 154, 173-174
ext4, 154, 165, 174
ext-based
details, displaying, 179-181
 ick command, 130, 179
  modifying, 182
features, 181
HFS, 155
inodes, counting, 181
ISO9660, 155
mounting
  access timestamp, 165
  automatically, 160-162, 204-207
  default options, 163-165, 181
  device files, allowing, 164
  executable files, enabling, 164
  labels, 162-163
  manually, 158-159
  mounted filesystems, displaying, 155-157
  as read-only, 164
  suid permission, set, 164
  syncing, 164
  users, restricting, 164
  UUIDs, 163
mount points, 153
physical, 153
proc
  devices file, 238
  diskstats file, 239
  filesystems file, 239
  interrupts file, 237
  partitions file, 239
  storage device information, 237-239
processes using, displaying, 159
removable media, 197
  creating, 198-200
  HFS, 197
  ISO9660, 197-198
  UDF, 198
resizing, 272-273
superuser reserved blocks counting, 181
swap, 166-167
types, listing of, 154-155
UDF, 155
unmounting, 155, 159-160
vfat, 69
virtual, 153-154
xfs-based, 175, 184
backing up and restoring, 184-187  
defined, 154  
information, displaying, 187  
problems, checking for, 189  
amounted, fixing, 188-189  
fill-in-the-blank exam questions, 723  
filter expressions (OpenLDAP databases), 599-600  
filtering  
iptables, 650-654  
packet, 650  
procmail rules, 625  
SPAM, 624  
finding  
kernel errors, 330  
OpenLDAP database objects by  
Boolean operators, 599  
common names, 598  
filter expressions, 599-600  
types, 597-598  
source code, 345  
findtime setting (fail2ban configuration), 697  
firewalls  
chains, 652  
configuring  
chains, 652  
examples, 653-654  
features, 650  
filtering, 650, 654  
options, 654  
targets, 653  
examples, 653  
filtering points, 650  
targets, 653  
troubleshooting, 333  
firmware, 111  
flush command, 410  
flushname command, 411  
foreground NFS mounts, 535  
formatting partitions as swap devices, 189  
FORWARD filtering point, 651  
forward lookups, 399  
forward proxy servers, 491  
forward zone files, 420  
forwarders (DNS)  
defined, 399  
split BIND configuration, 445  
FQDNs (Fully Qualified Domain Names), 397  
frameworks, 649  
free command, 10  
fsck command, 130, 179  
fsck_value field (etc/fstab file), 162  
fs_type field  
etc/fstab file, 161  
mount command, 156  
FTP (File Transfer Protocol)  
anonymous, 665  
access not permitted, 667  
Pure-FTPd access, 670  
settings, 666  
testing, 666  
uploading content, 666  
client connections, 669  
ProFTPD, 665, 670-671  
Pure-FTPd, 665, 670  
vsftpd, 665  
active versus passive mode, 671-674  
anonymous FTP, 665-667  
anonymous users uploading content, 666  
banners, 669  
chroot jailing local user accounts, 669  
configuration file, 663  
directives, 669  
file uploading, disabling, 669  
FTP client connections, 669  
installing, 665  
pri-login messages, 669  
transfer rates, 669  
user accounts, limiting, 667-669  
ftpd_banner directive, 669  
full backups, 366  
Fully Qualified Domain Names (FQDNs), 397  
fuser command, 159  
G  
-g option (free command), 10  
gateways  
adding/deleting, 288  
default, 288  
nonresponsive internal, 330-332  
routing table information, displaying, 287
host command, 411, 433
hostname command, 325-326
hostnames
  client outgoing, 612
  converting to IP addresses, 325
  displaying at login prompt, 382
etc/exports file, 528
local, 325-326
modifying, 325
Postfix, 612
translating into IP addresses, 286
hosts
  banning, 697
  defined, 397
  DHCP static, 547-548
  local, 419
  virtual, 466-467, 477
HSF (High Sierra Format), 197
HTML (HyperText Markup Language), 455
htop command, 22
HTTP (Hypertext Transfer Protocol), 455, 494
http_access statement, 494
httpd process, 457
http_port statement, 494
HTTPS (Hypertext Transfer Protocol with SSL), 473-475
  -human option (free command), 10
I
  -i option
    lvcreate command, 263
    lsof command, 310-311
    netstat command, 309
    smartctl command, 191
  -I option (hdparm command), 234
I/O (input/output), 6
  blocks in/out, 12
  disk, monitoring, 6, 12-17
  network, monitoring, 6, 17-18
ICMP (Internet Control Message Protocol), 302
IDE (Integrated Drive Electronics), 116, 233
id field (etc/inittab file), 95
idle value (iostat command), 8
IDs
  partitions, 220
  process, 406
IDS (Intrusion Detection System), 698
ifconfig command
  advantages, 288
  network information, 283
    primary network cards, 284-285
    temporarily modifying settings, 285
  replacing with ip command, 289
  -ifsit option (nmap command), 306
IfModule prefork.c directive, 460
  -if option (dd command), 369
ifup eth0 command, 328
ignoreip setting (fail2ban configuration), 697
images
  boot process, defining, 139
  ISO, 369
  kernel, 45-46
  splashimages, 115
IMAP (Internet Message Access Protocol), 608
  connections, 636
  Courier server, 636-637
    authdaemonrc daemon, 638
    configuration files, 637
    imap daemon, 638
    installing, 637
    POP daemon, 639
  Dovecot server, 639
    clean configuration, 639-640
    data, storing, 641
    include directory, 641
    installing, 639
    interfaces for listening, 641
    mailboxes, finding, 641
    protocols, 641
    settings, 641-643
  folders, 636
  implementing, 636
  message handling, 636
  POP, compared, 635-636
importing LDAP schemas, 579
!include setting (Dovecot server), 641
include directory (Dovecot server), 641
include PAM control value, 563
incremental backups, 364-366
indirect autofs maps, 205
INFO log level (SSH), 682
init command, 104
initdefault keyword, 96
initiators
configuring, 244
defined, 241
initramfs file, 113
initrd file, 113
initrd parameter, 116
inodes, counting, 181
INPUT filtering point, 651
input/output. See I/O
insmod command, 69
install option (etc/lilo.conf file), 139
installing
bootloaders, 112
collectd daemon, 31-32
Courier server software, 637
Dovecot server, 639
fail2ban, 696
NFS software, 527
OpenLDAP, 576
OpenVPN, 699
procmail, 623
Squid, 493
SSH software, 681
vsftpd servers, 665
Integrated Drive Electronics (IDE), 116, 233
interfaces
BIND listening, configuring, 405
Dovecot server listening, 641
network
displaying, 306
etc/network/interfaces configuration file, 326
etc/sysconfig/network-scripts directory, 327
flags, 285
local, 309
NetworkManager command line, 338
Postfix listening, 612
Internet Control Message Protocol (ICMP), 302
Internet Message Access Protocol. See IMAP
Internet Protocol (IP), 286
Internet Small Computer System Interface.
See iSCSI
interrupts, displaying, 237
interval argument (iostat command), 9
Interval value (etc/collectd/collectd.conf file), 29
Intrusion Detection System (IDS), 698
iostat command
CPU monitoring
arguments, 9
-c option, 7-8
iowait value, 8
values, 8
device I/O statistics, 12-13
disk I/O monitoring, 12-13
-d option, 12
iowait value (iostat command), 8
IP (Internet Protocol), 286
IP addresses
active, displaying, 306
banning, 696
hostnames conversion to, 325
hostname translations, 286
load balancing, 399
MAC address translation, 286
static, assigning, 327
white listing, 697
IP-based virtual hosts, 466-467
ip command, 289-290
ip6tables command, 650
iptables-ipv6 package, 650
iptables utility, 695
chains, 652
examples, 653-656
features, 650
filtering, 650, 654
options, 654
packet redirection, 657-658
rules, saving, 656-657
targets, 653
IPv4 loopback addresses, 323
IPv6 DHCP addresses, 327
isc-dhcp-server package, 543
iscsi daemon, 244
iSCSI (Internet Small Computer System Interface), 241
clients, 241
defined, 241
initiators, 244
LUNs, 242
targets
  creating, 242
defined, 241
  local devices, 244-247
  verifying configuration, 243
WWID, 241
iscsi script, 244
iscsiadm command, 244
iscsi-imitator-utils package, 244
ISO images, 369
ISO network model, 286
ISO9660 filesystems
  creating, 198-200
defined, 155
  extensions, 198
  overview, 197
ISOLINUX boot loader, 144-145
iwconfig command, 290-291
iwevent command, 294
iwlist command, 291-293
iwpriv command, 294
iwspy command, 294

J
-j option
  iptables command, 654
tar command, 350, 372
-J option (mkisofs command), 199
jail
  configuring named process to start in chrooted jail, 443
defined, 441
directories, 442-443
vftpdl servers, 669
Joliet extension (ISO9660 filesystem), 198-199
journals, 173

K
-k option
  lspci command, 80
  ns command, 312
  shutdown command, 390
kernel
  cleaning, 47-48
  compiling, 55
    cleaning the kernel, 47-48
    configuration file, creating, 48-50
    source code, downloading, 47
    unpacking, 47
  configuration file, creating, 48-50
    block devices, selecting, 52
    device drivers, selecting, 51
    make config command, 48
    make menuconfig command, 48
  documentation location, 43-44
  errors, finding, 330
  file-handles allocated, modifying, 45
  images, 45-46
  modifying, 44-45
  modules
    aliases, 76-77
defined, 43
dependencies, displaying, 66
device associations, displaying, 80
DMCrypt, 201
lib/modules/kernel_version directory, 65-66
Loadable Kernel Modules (LKM), 45
loaded, listing, 67-68
loading during boot process, 112-113
loading into memory, 68-71
modifying, 73-74
parameters, 65, 72-73
storage location, 65-66
 storing during boot process, 113
unloading from memory, 71
vfat, loading, 69-70
parameters
effects on storage devices, 239-241
  Legacy GRUB configuration, 114
  ring buffer, displaying, 328
source code, downloading, 47
unpacking, 47
website, 43

Key Knowledge Areas, 716
-key option (openssl command), 480

keys
asymmetric cryptography, 475
ciphers, 485
DNSSEC, creating, 447-448
private, 484
public, 683
RSA, 478
self-signing, 480
TSIG session, storing, 406
VPNs
  client certificates, 704
  server certificates, 703

keyword field (etc/inittab file), 95

keywords
AllowGroups, 683
AllowUsers, 682
DenyGroups, 683
DenyUsers, 682
etc/inittab file, 96-97
ListenAddress, 681
LogLevel, 681
PermitRootLogin, 682
Port, 681
Protocol, 681

kill command, 408

KVM, 718

L
-l option
  fdisk command, 176
  kill command, 408
  netstat command, 18, 309
  Pure-FTPd command line, 670

-L option
  iptables command, 654
  ldapsearch command, 599
  smbclient command, 518

labels (partitions)
  creating, 162
  displaying, 163

LANANA (Linux Assigned Names and Numbers Authority), 234
large-memory option (etc/lilo.conf file), 139
lba32 option (etc/lilo.conf file), 139
LDAP (Lightweight Directory Access Protocol), 573
  access control, 587-588
  attributes, 576
  classes, 576
  common names (CNs), 577
  configuration settings, 579-580
  database directory, 582
  directory structure, 577
  distinguished names (DNs), 577
domains, customizing, 579-580
  logging, 581-582
  objects, 576
  OpenLDAP. See OpenLDAP schemas
    defined, 576
    importing, 579
  servers, 580-584

ldapadd command, 586, 595
ldapdelete command, 587, 596
ldapmodify command, 587
ldappasswd command, 600-601
ldapsearch command, searching for objects by, 597-600
  Boolean operators, 599
  common names, 598
  filter expressions, 599-600
  output, 598-599
types, 597-598

ldd command, 333

LDIF (LDAP Data Interchange Format), 577, 584

Legacy GRUB, 113
  commands, executing, 120
  configuring
    configuration file, 114-117
    default settings, 115
    initrd parameter, 116
    kernel parameter, 116
    menu, bidding, 115
    root parameter, 116
    splashimages, 115
locations 805

timeouts, 115
title parameter, 116
GRUB 2, compared, 114
modifying during boot, 117-120
security, 122-124
single user mode, booting, 120-122
levels (RAID), 213
0, 214, 218
0+1, 217-219
1, 214, 218
4, 215, 218
5, 215, 219
10, 216, 219
50, 216, 219
lib directory, 363
lib64 directory, 363
lib/modules directory, 65-66
lib/modules/kernel_version directory
contents, 65
subdirectories, 66
libphp5.so file, 459
libwrap library
/etc/hosts.allow file, 334
services
accessing, 333
blocking access, 334
displaying, 333
Lightweight Directory Access Protocol. See LDAP
LILO (Linux LOader), 113
booting
boot: prompt, 141
boot screen, 140
single user mode, 141
configuring
configuration file, 137
global options, 138
images, 139
kernel file location, 139
GRUB, compared, 137
overview, 137
security, 142
lilo command, 140
linear RAID, 217
Linux Assigned Names and Numbers Authority (LANANA), 234
LLinux LOader. See LILO
Linux systems
configuring as routers, 649
Standard Base runlevel set, 93
Linux Unified Key Setup (LUKS), 201
ListenAddress keyword (etc/sshd/sshd_config file), 681
Listen directive, 456
listen-on setting (etc/named.conf file), 405
listen-on-v6 setting (etc/named.conf file), 405
listen setting (Dovecot server), 641
-list option (chkconfig command), 103-104
LKMs (Loadable Kernel Modules), 45
-LL option (ldapsearch command), 599
-LLL option (ldapsearch command), 599
load (CPU)
average, 7
balancing, 399
utilization statistics
iostat command, 7-9
mpstat command, 10
sar command, 9
load printers setting (SAMBA), 512
loading
Apache Web Server modules, 460
kernel modules
during boot process, 112-113
into memory, 68-71
LoadPlugin value (etc/collectd/collectd.conf file), 30
local_enable setting (anonymous FTP), 666
local hosts, 419
local_max_rate directive, 669
local networking
hostnames, 325-326
interface statistics, 309
login messages, 381-382
name resolution, 323-324
packet information, 307
routing tables, 308
traffic, displaying, 313-314
locations
backup storage, 367
kernel
documentation, 43-44
modules, 65-66
lockfiles, 626
log files
Apache Web Server, 458
DHCP, 548-549
etc/named.conf file setting, 407
LDAP, 581-582
for network troubleshooting, 328-330
SSH connections, configuring, 681
var/log/SAMBA directory, 516
logged in users, monitoring, 21
logical and operator (&), 599
logical extents, 262
logical not operator (!), 599
logical or operator (|), 599
Logical Unit Numbers (LUNs), 242
Logical Volume Management. See LVM
logical volumes. See LVs
logins
messages, 669
prompt, customizing, 381-382
SSH users, 682-683
LogLevel directive, 457
LogLevel keyword (etc/ssh/sshd_config file), 681
LOG target, 653
lookups, 399
loopback addresses, 323
lotop command, 22
low memory, 46
LPI Marketplace, 717
LPI.org website, 714
lsblk command, 12
ls command, 182
lsdev command, 81-82
lsmod command, 67-68
lsof command, 14-17, 310-311
lspci command, 77
-k option, 80
-v option, 78-79
-rv option, 79
-vvv option, 79
lsusb command, 82-84
-lt option (netstat command), 18
LUKS (Linux Unified Key Setup), 201
LUNs (Logical Unit Numbers), 242
-lu option (netstat command), 18
lvchange command, 270
lvcreate command, 262-263, 274
lvdisplay command, 267
lvextend command, 272
LVM (Logical Volume Management), 214
advantages, 256
commands, 268-270
device naming, 263-264
disadvantages, 256
implementations, 255
LVs
creating, 262-263
information, displaying, 267
logical extents, 262
making available to operating system, 264-265
resizing, 271-274
VG associations, displaying, 261
mental barriers, 255
overview, 253
PVs
adding to VGs, 259
attributes, modifying, 270
creating, 258
information, displaying, 262, 267
moving data between, 270
single drive systems, 257-258
snapshots, 256, 274-277
VGs
activating, 270
information, displaying, 260-261, 265-267
physical extents, 259-260
PVs/LVs associations, displaying, 261
size, extending, 270
visual representation, 259
lvm command, 268-270
lvreduce command, 271
LVs (logical volumes), 259
creating, 262-263
information, displaying, 267
logical extents, 262
making available to operating system, 264-265
resizing, 271-274
VG associations, displaying, 261
modifying  807

md5 pam_unix module option, 565
mdadm command, 221-223
MDAs (Mail Delivery Agents), 608, 635
Media Access Control (MAC), 286
-mega option (free command), 10
memory
   DMA (Direct Memory Access), 233
   high, 46
   low, 46
   modules, 68-71
   monitoring, 6, 10-12
      free command, 10
      vmstat command, 11-12
   virtual, 10
memstatistics-file setting (etc/named.conf file), 405
merging files into single archives, 368
messages
   digests, 476
   e-mail
      handling, 636
      retrieving, 636
      sending, 608
      storing, 610, 628-629
   log, 681
   login, 669
   pre-login, 381-382
   shutdown, 389-390
   wall, 387-389
mingetty command, 97
minimum value (SOA records), 425
MinSpareServers setting (Apache Web Server), 464
mirroring, 214
mkfs command, 177-178
mknitrd command, 113
mkisofs command
   HFS filesystems, 200
   -J option, 199
   removable media filesystems, creating, 198
   -R option, 199
   UDF filesystems, 200
modifying
   ext-based filesystems, 182
   hostnames, 325
modifying

kernel modules
  etc/sysctl.conf file, 74
  proc/sys directory, 44-45, 73
  sysctl command, 73-74
Legacy GRUB during boot, 117-120
network settings temporarily, 285
OpenLDAP database passwords, 600-601
PAM passwords, 560, 565
PV attributes, 270
runlevels, 101-104
tape devices, 370
modinfo command, 72-73
mod_perl.so file, 461
modprobe command
  kernel module parameters, setting, 72
  loading modules into memory, 70
  -r option, 71
mod_ssl module, 477-478
modules
  Apache Web Server, loading, 460
  kernel
    aliases, 76-77
    defined, 43
    dependencies, 66
    device associations, displaying, 80
    DMCrypt, 201
    lib/modules/kernel_version directory, 65-66
    Loadable Kernel Modules (LKM)s, 45
    loaded, listing, 67-68
    loading during boot process phase, 112-113
    loading into memory, 68-71
    modifying, 73-74
    parameters, 65, 72-73
    storage location, 65-66
    storing during boot process, 113
    unloading from memory, 71
    vfat, loading, 69-70
mod_ssl, 477-478
PAM, 564-569
modules.dep file, 66
monitoring
  CPU, 6-7
    iostat command, 7-9
    load average, 7
    mpstat command, 10
    sar command, 9
disk I/O, 6
  iostat command, 12-13
  lsblk command, 12
  lsdev command, 14-17
  sar command, 14
e-mail servers, 616
logged in users, 21
memory, 6, 10
  free command, 10
  vmstat command, 11-12
network I/O, 6, 17-18
processes
  detailed information, displaying, 18
  btop command, 22
  lotop command, 22
  ps command, 19
  pstree command, 19
  relationships, displaying, 19
  top command, 20
  w command, 21
  watch command, 22
security, 695
SMART devices, 190-191
systems, 6
tools
  baselines, 35
  Cacti, 33-34
  data, analyzing, 35
  measurement requirements, 34
  MRTG, 34
  Nagios, 33
  running, 35
  sar command, 34
  selecting, 34
mount command, 165
  -a option, 164
loading modules into memory, 69
mounted filesystems, displaying, 155-157
NFS shares, 534
  -o option, 158
  -ro option, 158
  -t option, 159
mount_options field
etc/fstab file, 161
mount command, 156
mount_point field
  etc/fstab file, 161
mount command, 156
mount points, 153
mounting
  filesystems
    access timestamp, 165
    automatically, 160-162, 204-207
    default options, 163-165, 181
    device files, allowing, 164
    executable files, enabling, 164
    labels, 162-163
    manually, 158-159
    mounted filesystems, displaying, 155-157
    as read-only, 164
    suid permission set, 164
    syncing, 164
    users, restricting, 164
    UUIDs, 163
NFS shares, 206-207, 534
  foreground/background, 535
  options, 535-536
  persistent mounts across reboots, 535
  READ requests maximum byte size, 536
  read-write/read-only, 536
  retrying, 535
  soft/hard options, 535
  timing out, 535
  unmounting, 535
  verifying, 534
  WRITE requests maximum byte size, 536
SAMBA shares, 520-521
mpstat command, 10
mrproper target (make command), 47
Multi Router Traffic Grapher (MRTG), 33
MSAs (Mail Submission Agents), 608
MTAs (Mail Transfer Agent), 608
procmail, 623
  as push servers, 635
mt command, 370
mtr command, 332
MUAs (Mail User Agents), 607
Multi Router Traffic Grapher (MRTG), 33
multiuser mode with/without GUI boot, 94
mydestination setting (Postfix), 612
mydomain setting (Postfix), 612
myhost setting (Postfix), 612
myorigin setting (Postfix), 612
N
  -n option
    dovecot command, 639
    lsof command, 310-311
    netstat command, 18, 309
    postconf command, 610
Nagios, 33
name-based virtual hosts, 467
name servers
  authoritative, 398, 420
  caching, 398
  configuration files, reloading, 408
  creating, 427-431
  current status, displaying, 411
  defined, 398
  dump files, creating, 410
  master, 420
  multiple, 400
  slave, 420
  SOA records, 423
  stopping, 411
  testing, 431-433
  zone files, reloading, 408
named caches, flushing, 410
named processes
  running as non-root user, 441
  starting in chrooted jail, configuring, 443
  storing data, 442
named-checkconfig command, 431
named-checkzone command, 431-432
names
  devices
    LVM, 263-264
    mapper, 13
  domains, 397
  GRUB hard disk naming convention, 116
  hostnames
    client outgoing, 612
    converting to IP addresses, 325
    displaying at login prompt, 382
    etc/exports file, 528
local, 325-326
modifying, 325
Postfix, 612
translating into IP addresses, 286
iSCSI targets, 244-245
kernel image files, 46
NIS domain, 382
partitions, 162-163
resolution, 399
  DNS queries, 402
  local networks, 323-324
  root servers, 400-401
system, 382
tape devices, 369
TTY devices, 382
NAT (Network Address Translation), 647, 658-659
nc command, 312-313, 695
negation character (!), 407
nested block action, 627
NetBIOS (Network Basic Input/Output System), 512
netfilter framework, 649
net -hosts setting (etc/auto.master file), 205
netstat command
  -at option, 309
  -au option, 309
  -c option, 18
  -e option, 309
  -i option, 309
  -l option, 18, 309
  -lt option, 18
  -lu option, 18
  network I/O monitoring, 17-18
  -n option, 18, 309
  -p option, 18, 309
  -r option, 17
  routing tables, 308
  -s option, 17, 307
Network Address Translation (NAT), 647, 658-659
Network Basic Input/Output System (NetBIOS), 512
Network File System. See NFS
NetworkManager daemon, 337-339
  command line interface, displaying, 338
  components status, 338
  current network device status, 337
  disabling, 337
  etc/resolv.conf file, populating, 323
  existence, checking for, 337
  GUI-based tool, 338
  overview, 337
  WiFi, disabling, 338
networks
  active devices, displaying, 283
  ARP, 286-287
  cards, 681
  configuration files, 321
    etc/hosts, 323-324
    etc/network/interfaces, 326
    etc/resolv.conf, 321-323
    etc/sysconfig/network-scripts directory, 327
gateways
  adding/deleting, 288
default, 288
  nonresponsive internal, 330-332
  routing table information, displaying, 287
information, 283
  primary network cards, 284-285
  temporarily modifying settings, 285
interfaces
  displaying, 306
  etc/network/interfaces configuration file, 326
  etc/sysconfig/network-scripts directory, 327
  flags, 285
  local, 309
I/O, monitoring, 6, 17-18
ip command, 289-290
ISO network model, 286
local
  bootnames, displaying, 325-326
  interface statistics, displaying, 309
  login messages, 381-382
  name resolution, 323-324
  packet information, displaying, 307
  routing tables, displaying, 308
  traffic, displaying, 313-314
ports. See ports
primary network card information, displaying, 284-285
private, 658-659
remote
  active IP addresses, displaying, 306
  availability, checking for, 301-302
  operating system types, 305
  packet loss, testing, 302
  ports, 302-304
  probing machines, 305
  UDP ports, scanning, 303
routing tables, displaying, 287, 306
runlevel, 94
settings, temporarily modifying, 285
sockets, 310
troubleshooting
  commands for, 336
  firewalls, 333
  log files for, 328-330
  NetworkManager daemon, 337-338
  nonresponsive internal gateways, 330-332
  TCP wrappers, 333
virtual private. See VPNs
wireless. See WiFi
  -new option (openssl command), 480
newline pattern matching character (\n), 626
NFS (Network File System), 525
client
  mount information, displaying, 534
  mounting NFS shares, 534
  persistent mounts across reboots, 535
  unmounting NFS shares, 535
  verifying NFS share mounts, 534
configuring, 527
etc/exports file, 527-528
NFS client mount information, displaying, 534
processes, 530-531
RPC service, 527, 531
shares
  mounting, 206-207, 534-536
  options, 535-536
  persistent mounts across reboots, 535
  resources, displaying, 533
  unmounting, 535
  verifying, 534
sharing options, 528
  UID mapping, 529-530
nfs startup script, 527
nfs-kernel-server package, 527
nfs-kernel-service startup script, 527
nfsserver startup script, 527
nfsstat command, 534
nfs-utils package, 527
Nginx, 492, 497-500
nice value (iostat command), 8
NIS domain names, 382
nmap command, 695
  -iflist option, 306
  network ports reachability, 302-303
  -O option, 305
  port scanning, 303
  probing machines, 305
  -sP option, 306
  -sU option, 303
  -sV option, 304
nmbd process, 516
nmlookup command, 518
nmcli command, 338
nm-tool command, 337
non-root users, 441
nosuid option (etc/fstab file), 164
nouser option (etc/fstab file), 164
nslookup command, 433
nullok pam_unix module option, 565
  -o option
  exportfs command, 534
  mount command, 158
  -O option (nmap command), 305
objects
  attributes, 576
  common names (CNs), 577
  defined, 576
  distinguished names (DNs), 577
OpenLDAP databases
  adding, 595
  deleting, 596
  searching, 597-600
-of option (dd command), 369
one ore more pattern matching character (+), 626

OpenLDAP databases
access control, 587-588
changes, 586-588
deleting objects, 596
passwords, 600-601
populating, 595
schemas, 584-586
searching for objects by
  Boolean operators, 599
  common names, 598
  filter expressions, 599-600
  types, 597-598
openldap-server package, 576
OpenLDAP servers, 576

openssl command
CSRs, creating, 479
RSA key file, creating, 478

OpenVAS utility, 696-698

OpenVPN (Open Virtual Private Network), 693
   configuring
       CAs, 700
       certificates, 701-705
       clients, 706-708
       servers, 705
   installing, 699

operating systems. See OSs
operators (Boolean), 599
opt directory, 363
optical media, 367
optional PAM control value, 563
option routers subdirective, 546
option subnet-mask subdirective, 546
options
-6 (nc command), 312
-a
  exportfs command, 534
  mount command, 164
  rsync command, 373
  smbpaswd command, 517
  systemctl command, 73-74
-A
  iptables command, 654
  tar command, 372
-at (netstat command), 309
-au (netstat command), 309
-b option
  free command, 10
  ldapsearch command, 598
-bs (dd command), 369
-c
  fdisk command, 176
  iostat command, 7-8
  netstat command, 18
  ping command, 301
  Pure-FTPd command line, 670
tar command, 372
-C
  Pure-FTPd command line, 670
tar command, 372
-cf (tar command), 370
-d
  arp command, 287
  bdparm command, 235
  lsusb command, 82-84
tar command, 372
-D
  ldapdelete command, 596
  ldappasswd command, 600
-delete (tar command), 372
-des3, 479
-e
  netstat command, 309
  Pure-FTPd command line, 670
-E (Pure-FTPd command line), 670
-e ssh (rsync command), 373
-f (ping command), 302
-fe (ps command), 18
free command, 10
-h
  dumpe2fs command, 179-180
  free command, 10
  shutdown command, 390
-H (smartctl command), 191
-i
Abbreviation (lsop command), 310-311
lscrcreate command, 263
netstat command, 309
smartctl command, 191
-I (hdparm command), 234
-if (dd command), 369
-iflist (nmap command), 306
iostat command, 12
-j
iptables command, 654
tar command, 330, 372
-J (mkisofs command), 199
-k
lpcicommand, 80
nc command, 312
shutdown command, 390
-key (openssl command), 480
-l
fdisk command, 176
kill command, 408
netstat command, 18, 309
Pure-FTPd command line, 670
-L
iptables command, 654
ldapsearch command, 599
smbclient command, 518
-LL (ldapsearch command), 599
-LLL (ldapsearch command), 599
-lt (netstat command), 18
-lu (netstat command), 18
-n
dovecot command, 639
lsf command, 311
netstat command, 18, 309
postconf command, 610
netstat command, 309
-new (openssl command), 480
-o
exportfs command, 534
mount command, 158
-O (nmap command), 305
-of (dd command), 369
-out (openssl command), 480
-p (netstat command), 18, 309
-P (lsf command), 311
Pure-FTPd command line, 670
-r
modprobe, 71
netstat command, 18, 308
shutdown command, 390
-R (mkisofs command), 199
-ro (mount command), 158
-s
lscrcreate command, 274
netstat command, 17, 307-309
swapon command, 166-167
-S
ldapsearch command, 600
Pure-FTPd command line, 670
sar command, 14
signreq, 482
-sP (nmap command), 306
-sU (nmap command), 303
-sV (nmap command), 304
-t
bdparm command, 235
iptables command, 654
mount command, 159
tar command, 372
telinit command, 104
xfsrestore command, 186
-T (bdparm command), 236
-tf (tar command), 370
-u
fdisk command, 176
lsf command, 14
nc command, 312
-U (smbclient command), 518
-v
lpcicommand, 78-79
lshw command, 82-84
rsync command, 373
tar command, 371
vgdisplay command, 261
-vv (lspci command), 79
-vvv (lspci command), 79
-w (nc command), 312
-W
  ldapdelete command, 596
  ldappasswd command, 600
  tar command, 372
-x
  ldapdelete command, 596
  ldappasswd command, 600
  ldapsearch command, 597
  tar command, 372
-xf (tar command), 371
-xzf (tar command), 349
-z
  nc command, 313
  tar command, 372

OSs (operating systems)
LVs, making available, 264-265
release numbers, displaying, 382
remote systems, determining, 305
sharing between. See SAMBA
versions, displaying, 382
-out option (openssl command), 480

-P option (lsof command). 310-311

packets
filtering, 650
ICMP, 302
local networks, 307
loss, 302
netfilter framework, 649
redirection (iptables utility), 657-658
PADL migration tool, 595
PAM (pluggable authentication modules), 555, 564-565
configuration file, 557
configuration types, 559-562
  account, 559
  auth, 559
  password, 560
  session, 560
current values, 562-564
currents, 558
directory contents, 558
features, 557
FTP user account access, limiting, 668
modules, 564-569
passwords, 565
user accounts
  environment, configuring, 560
  passwords, 559-560
  verifying, 559

pam.conf file, 557
pam_cracklib module, 565-566
pam_limits module, 566-567
pam_listfile module, 568
pam_unix module, 565
paper clip CD eject method, 240
Parallel ATA (PATA), 233
Parallels, 718
parameters
  boot: prompt, passing, 141
  Diffie-Hellman, 703
  initrd, 116
  kernel
    displaying, 72-73
    effects on storage devices, 239-241
    Legacy GRUB configuration, 116
  modules, 65
  root, 116
  title, 116
  wireless networks, displaying 290-291

P
-p option (netstat command), 18, 309
-P option (lsif command). 310-311
packages
courier-imap, 636
courier-pop, 636
DHCP servers, 543
iptables-ipv6, 650
iscsi-initiator-utils, 244
nfs-kernel-server, 527
nfs-utils, 527
openldap-server, 576
procmail, 623
SAMBA, listing of, 509
scsi-target-utils, 242
source code
downloading from original sources, 348-349
downloading on Debian-based systems, 347-348
downloading on RPM-based systems, 345-347
unpacking, 349-350
SSH, 681
parity data, 215
partitions
  adding to devices, 176
  creating, 176-177
  displaying, 176
  formatting as swap devices, 189
  IDs, 220
  labels, 162-163
  versus hard disks for RAID, 219-220
passdb backend setting (SAMBA), 512
passphrases, 202
passwd command, 121
passwd.ldif file, 595
-password option (etc/lilo.conf file), 142
passwords
  encrypted
    filesystems, 202
    GRUB 2, 130
    Legacy GRUB, 122
LDAP, 580
LILO, 142
OpenLDAP databases, 600-601
PAM
  changing, 560
  configuration type, 560
  modifying, 565
  verifying, 559
root, modifying, 121
rootdn, 580
SSH authentication, 683
PATA (Parallel ATA), 233
patching source code, 353-354
pattern matching, 626
PCI (Peripheral Component Interconnect), 77
PCI devices, listing, 77-79
Perl scripting, 461-462
PermitEmptyPasswords setting (SSH login setting), 683
PermitRootLogin keyword, 682
persistent mounts across reboots, 535
phases (boot process), 111
  BIOS/UEFI, 111
  bootloader, 111-112
  kernel, 112-113
  post-kernel, 113
PHP scripting, 459-460
physical extents (VGs), 259-260
physical filesystems, 153
physical volumes. See PVs
pid-file setting (etc/named.conf file), 406
ping command
  -c option, 301
  floods, 302
  -f option, 302
  remote systems, 301-302
pipes (|)
  logical or operator, 599
  pattern matching character, 626
platforms, determining, 352
pluggable authentication modules. See PAM
plugins, listing of website, 30
POP (Post Office Protocol), 608
  connections, 636
    Courier server, 636-637
      authdaemonrc daemon, 638
      configuration files, 637
      imap daemon, 638
      installing, 637
      POP daemon, 639
Dovecot server, 639
  clean configuration, 639-640
  data, storing, 641
  include directory, 641
  installing, 639
  interfaces for listening, 641
  mailboxes, finding, 641
  protocols, 641
  settings, 641
folders, 636
IMAP, compared, 635-636
implementing, 636
message handling, 636
populating LDAP databases, 595
Port keyword (etc/ssh/sshd_config file), 681
portmap utility
  network port numbers, 531
  RPC service, 527
  TCP wrappers, 532-533
ports
  BIND listening, configuring, 405
  connections, listening for, 313-314
defined, 310
HTTP, 494
network
reachability, 302-303
RPC-based services, 531
scanning, 303
service versions, 304
SSH connections, configuring, 681
UDP, 303
Post Office Protocol. See POP
post-kernel boot process phase, 113
postconf command
all Postfix configuration settings, 610
error checking, 611
-n option, 610
Postfix, 605
configuration file, 610-611
configuration settings
all, displaying, 610
client outgoing hostnames, 612
configuration file only, displaying, 610
destination addresses, 612
domains, 612
e-mail harvesting prevention, 612
hostnames, 612
interfaces for listening, 612
relay setting, 612
specific, displaying, 611
var/spool/postfix directory, 610
POSTROUTING filtering point, 651
PowerDNS, 399
powerfail keyword, 96
powerokwait keyword, 96
predefined addresses, 407
pre-login messages, 381-382
preparing for exams
distributions, 718-719
exam facts, 714
exam objectives, 714-716
awareness topics, 716
Key Knowledge Areas, 716
LPI.org website, 714
subtopic weight, 716
topics/subtopics, 715
immediately before, 714
question types, 719-720
choose all that apply, 721-722
choose multiple, 721
fill-in-the-blank, 723
single answer multiple choice, 720
studying, 717-718
things to remember, 724
PREROUTING filtering point, 651
primary network cards, 284-285
printers
CUPS, 512
shares, creating, 514
sharing, 513-514
printers section (SAMBA configuration file), 513-514
PrintMotd setting (SSH login setting), 683
privacy (users), violating, 682
private keys
asymmetric cryptography, 475
DNSSEC, creating, 447
file location, 484
private networks, 658-659
probing machines, 305
proc/devices file, 238
proc/diskstats file, 239
proc/dma file, 82
Process IDs, 406
processes
detailed information, displaying, 18
hijacked, 441
httpd, 457
monitoring
btop command, 22
lotop command, 22
ps command, 19
pstree command, 19
top command, 20
w command, 21
watch command, 21
named
running as non-root user, 441
starting in chrooted jail, configuring, 443
storing data, 442
nmbd, 516
relationships, displaying, 19
smbd, 516
using the filesystem, displaying, 159
protocols 817

proc filesystem
  devices file, 238
  diskstats file, 239
  filesystems file, 239
  interrupts file, 237
  partitions file, 239
  storage device information, 237-239
proc/filesystems file, 239
proc/interrupts file, 82, 237
proc/ioports file, 82

procmail utility
  advantage over MTAs, 623
  defined, 621
  global configuration, 624
  -h option, 625
  installing, 623
  lockfile, 626
  mail spool directory, choosing, 624
  MTA automatic usage, determining, 623
  rules
    actions, 626-627
    examples, 627-628
    filters, 625
    flags, 625
    pattern matching, 626
    syntax, 625
  as SPAM filter, 624
  users adding procmail to home directories, 624
proc/mounts file, 157, 534
proc/partitions file, 239
proc/sys/dev/cdrom/lock file, 240
proc/sys directory, 44-45, 73
proc/sys/net/ipv4/ip_forward file, 649
ProFTPD servers, 665, 670-671
promiscuous mode, enabling/disabling, 285
  -prompt option (etc/lilo.conf file), 139
prompts
  boot:, 141
  login, customizing, 381-382
Protocol keyword (etc/ssh/sshd_config file), 681
protocols
  CIFS, 509
  DHCP, 541
  DNS. See DNS
  Dovecot server, 641
  HTTP, 455, 494
  HTTPS, 473-475
IMAP
  connections, 636
  Courier server, 636-639
  Dovecot server, 639-641
  folders, 636
  implementing, 636
  message handling, 636
  POP, compared, 635-636
LDAP, 573
  attributes, 576
  classes, 576
  common names (CNs), 577
  configuration settings, 579-580
  directory structure, 577
  distinguished names (DNs), 577
  domains, customizing, 579-580
  objects, 576
  OpenLDAP, 576
  schemas, 576, 579
  servers, 580
NFS. See NFS
POP
  connections, 636
  Courier server, 636-639
  Dovecot server, 639-641
  folders, 636
  IMAP, compared, 635-636
  implementing, 636
  message handling, 636
SMB, 509
SMTP, 605-608
SSH, 679
  authentication, 683
  configuration file, 681
  log messages, 681
  network card connections, 681
  OpenVAS utility, 697-698
  ports, 681
  protocol connections, 681
  software, installing, 681
  user logins, 682-683
TLS, 475
protocols setting (Dovecot server), 641
proxy servers
  client configuration, 500-503
defined, 491
forward, 491
Nginx, 492, 497-500
reverse, 492
Squid, 493-497
tunneling, 491
types, 491-492
ps command, 18-19
pstree command, 19
public keys
  asymmetric cryptography, 475
  DNSSEC, 447
  SSH authentication, 683
pull servers, 635
Pure-FTPD servers, 665, 670
push servers, 635
pvchange command, 270
pvcreate command, 258
pvdisplay command, 262, 267
pvmove command, 270
pvremove command, 270
PVs (physical volumes), 258
  adding to VGs, 259
  attributes, modifying, 270
  creating, 258
  deleting from VGs, 270
  information, displaying, 262, 267
  moving data between, 270
  VG associations, displaying, 261
PXELINUX boot loader, 145-146
Q
queries (DNS), 321, 336, 406-407
question types (exam), 719-720
  choose all that apply, 721-722
  choose multiple, 721
  fill-in-the-blank, 723
  single answer multiple choice, 720
R
  -r option
    modprobe command, 71
    netstat command, 17, 308
shutdown command, 390
  -R option (mkisofs command), 199
RAID (Redundant Array of Independent Disks), 211
0, 214, 218
0+1, 217-219
1, 214, 218
4, 215, 218
5, 215, 219
10, 216, 219
50, 216, 219
deices
  creating, 221-223
  managing, 224-226
hardware, 213
levels, 213
linear, 217
partitions versus entire hard disks, 219-220
software, 213
[rangle] pattern matching character, 626
range subdirective, 546
rc script, 98
rc.sysinit script, 98
read-only NFS shares, 536
READ requests, 536
read-write NFS shares, 536
rebooting systems, 94
reconfig command, 411
record fields (zone files), 422
records
  defined, 398
  zone
    SOA, 423-425
    updating, 421
recursion setting (etc/named.conf file), 406
Red Hat-based systems
  boot scripts, 102
  configuring named processes to start in chrooted jail, 443
  etc/inittab file entries, 97
  etc/sysconfig/network-scripts directory, 327
  GRUB 2 configuration file, 125
  grub2-mkconfig command, 127
  local hostnames, displaying, 326
  repositories, 345
runlevel set, 93
static IP addresses, 327
var/log/messages file, 328
var/log/secure file, 330
redundancy (RAID) 10, 216
Redundant Array of Independent Disks. See RAID
refresh data, 424
REJECT target, 653
relatime option (etc/fstab file), 165
relay agents (DHCP), 549
relay_domains setting (Postfix), 612
relayhost setting (Postfix), 612
remember=x pam_unix module option, 565
remote storage, 367
remote systems
availability, checking for, 301-302
backing up, 373-374
network interfaces, displaying, 306
network ports reachability, 302-303
operating system types, 305
packet loss, testing, 302
ports, 304
probing machines, 305
routing tables, displaying, 306
service versions, 306
UDP ports, scanning, 303
removable media filesystems, 197
creating, 200
HFS, 197, 200
ISO9660, 197-199
UDF, 198-200
repositories
Debian-based systems, 347
files, creating, 345
Red Hat-based systems, 345
req argument (openssl command), 480
required PAM control value, 563
requisite PAM control value, 563
resolver
converting hostnames to IP addresses, 325
e tc/resolv.conf file settings, 322
respawn keyword, 97
restore command, 368
restoring
files, 368
xfs filesystems, 186-187
-restricted option (etc/lilo.conf file), 142
retrieving e-mail messages, 636
retrying NFS mounts, 535
retry value (SOA records), 424
reverse lookups, 399, 421
reverse proxy servers, 492
RFC 821, 607
ring buffer (kernel), 328
rmmod command, 71
rndc command, 408-411
-confgen option, 408
e tc/rndc.conf
creating, 408-409
permissions, 410
named server configuration files, reloading, 408
Rock Ridge extension (ISO9660 filesystem), 198-199
Ron Rivest, Adi Shamir, and Leonard Adleman (RSA), 479
-ro option (mount command), 158
root accounts, 580
root parameter (Legacy GRUB configuration), 116
root password, 121
root servers
defined, 400
displaying, 400-401
zone file listing of, 419
root users, 682
root_squash share option (NFS servers), 530
rootdn passwords, 580
rootdn setting (LDAP configuration), 580
rootpw setting (LDAP configuration), 580
Round-Robin Database tool (RRDtool), 33
route command
advantages, 288
replacing with ip command, 289
routing tables, displaying, 287
-route option (etc/resolv.conf file), 322
routers
firewalls
chains, 652
examples, 654
features, 650
filtering, 650, 654
iptables features, 650
targets, 653
iptables, 653-654
Linux system as, configuring, 649
routing tables, displaying, 287
local networks, 308
remote systems, 306
RPC-based services
NFS, 527, 531-533
port numbers, 531
rpcinfo command, 531
rpm2cpio command, 346
RPM-based systems, 345-347
RRDtool (Round-Robin Database tool), 33
RSA key files, creating, 478
RSA (Ron Rivest, Adi Shamir, and Leonard Adleman), 479
rsync command, 373-374
rules
iptables utility, 656-657
procmail utility
actions, 626-627
examples, 627-628
filters, 625
flags, 625
pattern matching, 626
syntax, 625
Squid access, 494-497
udevd daemon, 85-86
runlevel field, 95
runlevels, 93
0, 93
1, 94
2, 94
3, 94
4, 94
5, 94
6, 94
default, 96
etc/inittab file
contents, displaying, 94
fields, 95
keywords, 96-97
Red Hat-based systems typical entries, 97
features, 94
modifying, 101-104
sets, 93-94
switching, 104
rw option (etc/fstab file), 164
S
-s option
lvcreate command, 274
netstat command, 17, 307
swapon command, 166-167
-S option
ldappasswd command, 600
Pure-FTPD command line, 670
SAMBA
account data, storing, 512
client package, 509
common package, 509
configuring
corifugtion file, 510
global settings, 511-512
home directories, 512-513
printers, 513-514
verifying, 515-516
CUPS printers, sharing, 512
documentation, 510
NetBIOS workgroup, setting, 512
packages, listing of, 509
security, 512
servers
accessing, 518-520
available shares, displaying, 518
descriptions, 512
mounting shares, 520-521
specific shares, accessing, 518
starting, 516
status, 520
shares
available, displaying, 518
directory, 514
mounting, 520-521
printer, 514
security, 514
specific, accessing, 518
user accounts, creating, 516-518
SAMBA 3 documentation, 510

cmd command
  CPU monitoring, 9
  disk I/O monitoring, 14
  as monitoring tool, 34

SATA (Serial AT Attachment), 116, 233

sbin directory, 363

scanning ports
  nmap command, 303
  service versions, 304
  UDP, 303

schemas
  defined, 576
  LDAP, importing, 579
  OpenLDAP, 584-586

scp command, 687

scripts
  Apache Web Server, enabling
    Perl, 461-462
    PHP, 459-460
  boot, 98-102
  build-key, 703
  build-key-server, 701-703
  CA.pl, 482
  configuration, 244
  configure, 350-351
  nfs, 527
  nfs-kernel-service, 527
  nfsserver, 527

SCSI devices, 236

scsi_id command, 246

scsi-target-utils package, 242

sdparm command, 236

Secure Shell. See SSH

Secure Sockets Layer. See SSL

security
  access control, 587-588
  alerts
    monitoring, 695
    services, 698
  Apache Web Server, 463-464
  asymmetric cryptography, 475
  attacks
    bijack, 441
    man-in-the-middle, 477

authentication. See authentication

chroot jail
  configuring named process to start in chrooted jail, 443
  copying files to directories, 442-443
  creating directories, 442
defined, 441

DNS cache poisoning, 447

DINSSEC
  BIND configuration settings, 406
  public/private keys, creating, 447
e-mail harvesting prevention, 612

firewalls. See firewalls

GRUB 2, 128-130

iptables utility, 695
  chains, 652
  examples, 653-656
  features, 650
  filtering, 650, 654
  options, 654
  packet redirection, 657-658
  rules, saving, 656-657
  targets, 653

Legacy GRUB, 122-124

LILO, 142

OpenVPN, 699

passwords. See passwords

permissions, 410

potential holes, monitoring, 695

SAMBA, 512-514

software updates, 695

SSH, 687-689

SSL, 476-477

TSIG, 406, 447

utilities, 695
  fail2ban, 696-697
  iptables, 695
  nc, 695
  nmap, 695
  OpenVAS, 696-698
  Snort, 696-698
  telnet, 695

VPNs
  CAs, configuring, 700
  client certificates, creating, 703-705
server certificates, creating, 701-703
server configuration, 705
zone transfer limitations, 446
security setting (SAMBA), 512
selecting
collectd daemon statistics for monitoring, 30
data for backups, 361-363
directories, 362-363
filesystems, 362-363
kernel configuration file options, 51-52
BIND, configuring, 403-406
certificates, creating, 701-703
Courier, 636-637
authdaemons daemon, 638
collection files, 637
imap daemon, 638
installing, 637
Maildir format, 638
POP daemon, 639
as SMTP server, 636
descriptions in SAMBA, 512
DHCP
configuration file, 543-544
DDNS updates, 545
IP information for, 545-546
log files, 548-549
packages, 543
relay agents, 549
rogue, 543
static hosts, 547-548
virtual machines, 543
djbdns, 399
DNS. See DNS, servers
dnsmasq, 399
Dovecot, 639-641
exim, 605, 615
FTP, 665
active versus passive mode, 671-674
configuration file, 665
ProFTPd, 665, 670-671
Pure-FTPd, 665, 670
vsftpd, 665-669
LDAP, 580-584
name
authoritative, 398, 420
 caching, 398
configuration files, reloading, 408
current status, displaying, 411
defined, 398
dump files, creating, 410
master, 420
multiple, 400
slave, 420
SOA records, 423
stopping, 411
zone files, reloading, 408
servers
Apache Web
authentication, 465-466
configuration file, 455-456
directives, 456-457
implementing SSL with mod_ssl module, 477-478
killing off extra servers, 464
log files, 458
maximum number of clients, 464
modules, loading, 460
Perl scripting, enabling, 461-462
PHP scripting, enabling, 459-460
security, 463-464
SSL directives, 484-485
starting, 457-458
verifying, 457
versions, 457
virtual hosts, 466-467
Self-Monitoring, Analysis, and Reporting
Technology (SMART) devices, 190-191
Self-Monitoring, Analysis, and Reporting
Technology (SMART) devices, 190-191
SELinux, 442
sending e-mail messages, 608
sendmail e-mail server, 605
Serial AT Attachment (SATA), 116, 233
mail spool directory, 624
monitoring tools, 34
servers
Apache Web
authentication, 465-466
configuration file, 455-456
directives, 456-457
implementing SSL with mod_ssl module, 477-478
killing off extra servers, 464
log files, 458
maximum number of clients, 464
modules, loading, 460
Perl scripting, enabling, 461-462
PHP scripting, enabling, 459-460
security, 463-464
SSL directives, 484-485
starting, 457-458
verifying, 457
versions, 457
virtual hosts, 466-467
servers
BIND, configuring, 403-406
certificates, creating, 701-703
Courier, 636-637
authdaemons daemon, 638
collection files, 637
imap daemon, 638
installing, 637
Maildir format, 638
POP daemon, 639
as SMTP server, 636
descriptions in SAMBA, 512
DHCP
configuration file, 543-544
DDNS updates, 545
IP information for, 545-546
log files, 548-549
packages, 543
relay agents, 549
rogue, 543
static hosts, 547-548
virtual machines, 543
djbdns, 399
DNS. See DNS, servers
dnsmasq, 399
Dovecot, 639-641
exim, 605, 615
FTP, 665
active versus passive mode, 671-674
configuration file, 665
ProFTPd, 665, 670-671
Pure-FTPd, 665, 670
vsftpd, 665-669
LDAP, 580-584
name
authoritative, 398, 420
caching, 398
configuration files, reloading, 408
current status, displaying, 411
defined, 398
dump files, creating, 410
master, 420
multiple, 400
slave, 420
SOA records, 423
stopping, 411
zone files, reloading, 408
servers
BIND, configuring, 403-406
certificates, creating, 701-703
Courier, 636-637
authdaemons daemon, 638
collection files, 637
imap daemon, 638
installing, 637
Maildir format, 638
POP daemon, 639
as SMTP server, 636
descriptions in SAMBA, 512
DHCP
configuration file, 543-544
DDNS updates, 545
IP information for, 545-546
log files, 548-549
packages, 543
relay agents, 549
rogue, 543
static hosts, 547-548
virtual machines, 543
djbdns, 399
DNS. See DNS, servers
dnsmasq, 399
Dovecot, 639-641
exim, 605, 615
FTP, 665
active versus passive mode, 671-674
configuration file, 665
ProFTPd, 665, 670-671
Pure-FTPd, 665, 670
vsftpd, 665-669
LDAP, 580-584
name
authoritative, 398, 420
caching, 398
configuration files, reloading, 408
current status, displaying, 411
defined, 398
dump files, creating, 410
master, 420
multiple, 400
slave, 420
SOA records, 423
stopping, 411
zone files, reloading, 408
NFS
access, 532-533
e/etc/exports, 527-528
NFS client mount information, displaying, 534
NFS software, installing, 527
processes, 530-531
RPC services, 527, 531
shared resources, displaying, 533
sharing options, 528
UID mapping, 529-530
Postfix, 605
all configuration settings, displaying, 610
client outgoing hostnames, 612
configuration file, 610-611
destination addresses, 612
domains, 612
e-mail harvesting prevention, 612
hostnames, 612
interfaces for listening, 612
relay setting, 612
specific settings only, displaying, 611
/var/spool/postfix directory, 610
proxy
client configuration, 500-503
defined, 491
forward, 491
Nginx, 492, 497-500
reverse, 492
Squid, 493-497
tunneling, 491
types, 491-492
pull, 635
push, 635
root
defined, 400
displaying, 400-401
zone file listing, 419
SAMBA
accessing, 518-520
available shares, displaying, 518
mounting shares, 520-521
specific shares, accessing, 518
starting, 516
status, 520
sendmail, 605, 615
SMTP, 636
SSH
authentication, 683
configuration file, 681
log messages, 681
network card connections, 681
ports, 681
protocol connections, 681
user logins, 682-683
VPN, configuring, 705
ServerSignature directive, 485
ServerTokens directive, 485
services
accessing, 333
directories, 204-207
directory, 573
libwrapped
blocking access, 334
displaying, 333
ports, 304
resolver, 325
RPC
NFS, 527, 531-533
port numbers, 531
session-keyfile setting (etc/named.conf file), 406
session keys, 406
session PAM configuration type, 560
sftp command, 687
sha256 pam_unix module option, 565
shares
custom, 514
NFS
mounting, 206-207, 534-536
persistent mounts across reboots, 535
unmounting, 535
verifying, 534
SAMBA
available, displaying, 518
mounting, 520-521
specific, accessing, 518
sharing
between operating systems. See SAMBA
home directories, 512-513
printers, 512-514
resources from NFS servers to NFS clients
directories, 527-528
NFS server processes, 530-531
options, 528
UIDs, mapping, 529-530
showmount command, 534
shutdown command, 96, 389-390
shutdown messages, 389-390
shutting down systems, 96
signatures
digital, 476
transaction (TSIG), 406, 447
-sigsreq option, 482
Simple Mail Transfer Protocol (SMTP),
605-608, 636
single answer multiple choice exam questions,
720
single character pattern matching character
(,), 626
single drive systems, 257-258
single user mode
GRUB 2, 128
Legacy GRUB, booting, 120-122
LILO, booting, 141
runlevel, 94
size
blocks, 181
filesystems, 272-273
LVs, 271-274
physical extents, 259-260
VGs, 270
slapadd command, 577
slapcat command, 587, 595
slapd.conf file, 576-581
slapindex command, 587
slappasswd command, 580
slave name servers, 420
slave servers (DNS), 420
SMART (Self-Monitoring, Analysis, and
Reporting Technology) devices, 190-191
smartctl command, 191
smartd daemon, 190
SMB (Server Message Block), 509
smbclient command, 518
smbd process, 516
smbpasswd command, 517
SMB sharing. See SAMBA
smbstatus command, 520
SMTP (Simple Mail Transfer Protocol),
605-608, 636
snapshots (LVM), 256, 274-277
sniffers, 313-314, 698
Snort utility, 696-698
SOA (Start of Authority) records, 423-425
sockets, 310
software
RAID, 213
updates, 695
source code
building
configure script, executing, 350-351
directory storage, 352
Makefile, 352-353
platforms, determining, 352
downloading
Debian-based systems, 347-348
from original sources, 348-349
RPM-based systems, 345-347
finding, 345
kernel, downloading, 47
patching, 353-354
unpacking, 349-350
source command, 701
source files, 349-350
SPAM filters, 624
splashimages, 115
split BIND configuration, 443-445
forwarders, 445
internal/external network example, 444-445
techniques, 444
-sP option (nmap command), 306
Squid, 493
access settings, 494
client authentication, 494
configuration file, 493
as HTTP forward proxy server, 494
HTTP port requests, 494
installing, 493
static data, caching, 493
squid.conf file, 493
statistics, displaying 825

SSH (Secure Shell), 679
  authentication, 683
  client commands, 684-687
  configuration file, 681
  log messages, 681
  network card connections, 681
  OpenVAS utility, 697-698
  ports, 681
  protocol connections, 681
  security, 687-689
  software, installing, 681
  user logins, 682-683
ssh command, 687
ssh_config file, 684-685
ssh-keygen command, 683
SSL (Secure Sockets Layer), 475
  Apache directives, 484-485
  asymmetric cryptography, 475
  CA chains, 484
  certificates
    creating, 478-483
    CSRs, 479-481
    directory, 484
    file location, 484
    RSA key file, creating, 478
    self-signing, 480
    signing requests, 482
    storing, 483
ciphers, 485
  client authentication, 484
  header response information, 485
  implementing, 477-478
  private key file location, 484
  protocol, specifying, 485
  security concerns, 476-477
  self-signed certificates, 477
  traces, 485
  turning on/off, 484
SSLCACertificateFile directive, 484
SSLCACertificatePath directive, 484
SSLCertificateChainFile directive, 484
SSLCertificateFile directive, 484
SSLCertificateKeyFile directive, 484
SSLCipherSuite directive, 485
SSLEngine directive, 484

SSLProtocol directive, 485
SSSD (System Security Services Daemon), 577
start argument (update-rc.d command), 102-103
Start of Authority (SOA) records, 423-425
starting
  Apache Web Server, 457-458
  iscsid daemon, 244
  LDAP servers, 582-584
  runlevels, 102-104
  SAMBA server, 516
  system. See boot process
tgtd daemon, 242
StartServers setting (Apache Web Server), 464
startup. See boot process
stat command, 183
static hosts (DHCP), 547-548
statements
  acl, 494
  auth_param, 494
  cache_dir, 493
  http_access, 494
  http_port, 494
  view, 444
static data, 493
static IP addresses, assigning, 327
statistics, displaying
  collectd daemon, 30
  CPU
    iostat command, 7-9
    mpstat command, 10
    sar command, 9
device I/O, 12-13
disk I/O
  iostat command, 12-13
  losetup command, 14-17
  sar command, 14
memory
  free command, 10
  vmstat command, 11-12
network I/O, 17-18
processes
  btop command, 22
  lstop command, 22
statistics, displaying

ps command, 18-19
ps tree command, 19
top command, 20
w command, 21
watch command, 21

status
name servers, displaying, 411
network devices, 337
NetworkManager components, 338
SAMBA servers, displaying, 520

status command, 411
steal value (iostat command), 8
stop command, 411

storage
backup data, 367
bootloaders, 112
certificates, 483
deVICES
information, displaying, 237-239
kernel parameter affects, 239-241
Dovecot server data, 641
e-mail messages, 610, 628-629
kernel modules, 113
parity data, 215
SAMBA account data, 512
source files, 349
TSIG session keys, 406
zone files, 419

strace, 336
stripes, 263
striping, 214
studying for exams, 717-718
subdomains, 398
subnet 192.168.0.0 netmask 255.255.255.0
subdirective, 546
subnet directive, 544-546
subtopic weight, 716
sufficient PAM control value, 563
suffix setting (LDAP configuration), 580
suid option (etc/fstab file), 164
-sU option (nmap command), 303
superuser accounts, creating, 129
-sV option (nmap command), 304
swap devices, 189-190
swapon command, 166, 189
swap space, 166-167, 189
sync command, 166
syncing, 164
syntax
/etc/exports file, 527
/etc/hosts.allow file, 335
/etc/hosts.deny file, 335
multiple-line directives, 457
procmail rules, 625
SAMBA configuration file, verifying, 515-516
SOA records, 423
zone files, 421-422
sysctl command, 73-74
sysinit keyword, 96
SYSLINUX boot loader, 143-144
syslinux.cfg file, 144
System Security Services Daemon (SSSD), 577
system value (iostat command), 8
systems
architecture, displaying at login prompt, 382
base state, booting, 98
files, limiting access. See chroot jail
halting, 93
initialization technologies, 93
monitoring, 6
names, displaying at login prompt, 382
probing machines, 305
rebooting, 94
remote
active IP addresses, displaying, 306
availability, checking for, 301-302
backing up, 373-374
network interfaces, displaying, 306
network ports reachability, 302-303
operating system types, 305
packet loss, testing, 302
port service versions, 304
routing tables, displaying, 306
UDP ports, scanning, 303
shutting down, 96
single drives, 257-258
startup. See boot process
storage devices
displaying, 237-239
kernel parameter affects, 239-241
TCP wrappers
827

SysV-init system runlevels, 93-940, 93
1, 94
2, 94
3, 94
5, 94
6, 94
default, 96
etc/inittab file, 94-97
features, 94
sets, 93-94

SysV-init system runlevels, 93-94
0, 93
1, 94
2, 94
3, 94
5, 94
6, 94
boot scripts, 98-102
default, 96
etc/init.d directory, 101-102
etc/inittab file, 94-97
features, 94
runlevels, 101-104
sets, 93-94

T

-t option
hdparm command, 235
iptables command, 654
mount command, 159
tar command, 372
telinit, 104
xfsrestore command, 186

-T option (hdparm command), 236
table of contents (tar balls), 372
tables
ARP
deleting entries from, 287
displaying, 286
routing, displaying
local networks, 308
remote systems, 306
tape archive command. See tar command
tape backups, 367
tape devices, 369-370
tar balls
appending to existing, 372
compressing, 372
contents
displaying, 370-371
extracting, 371-372
partial restore, 372
creating, 370-372
current directory, setting, 372
deleting files from, 372
differences, displaying, 372
table of contents, displaying, 372
verifying, 372
tar command
backups, 369-372
filenames, listing at end, 372
options
-A, 372
-cf, 370
-c, 372
-C, 372
-delete, 372
-d, 372
-j, 350, 372
-ef, 370
-t, 372
-v, 371
-W, 372
-zf, 371
-z, 372
-xzf, 349
-xz, 372
source code, unpacking, 349

tar.gz files, 349
targets, 57
defined, 48
iptables, 653
isCSI
creating, 242
defined, 241
local devices, 244-247
verifying configuration, 243
tcpdump command, 313-314
TCP wrappers, 333, 532-533
blocking access, 334
libwrapped services, displaying, 333
telinit command, 104
telnet utility, 616, 695
testing
  anonymous FTP settings, 666
  benchmarking, 235-236
  DNS servers, 431-433
  OpenVPN server configuration, 705
  VPNs, 705
testparm command, 515-516
-tf option (tar command), 370
tgt-admin --show command, 243
tgtd daemon, starting, 242
third-party backup utilities, 374-375
thrashing, 164
time, displaying at login prompt, 382
timeout option (etc/lilo.conf file), 139
timeouts
  etc/resolv.conf file, 322
  Legacy GRUB configuration, 115
  NFS mounts, 535
Time To Live. See TTL
title parameter (Legacy GRUB configuration), 116
titles (GRUB 2), 127
TLS (Transport Layer Security), 475
top command, 20
top-level domains, 397
Tower of Hanoi backup strategy, 366
TraceEnable directive, 485
ttraceroute command, 330-331
traces (SSL), 485
traffic (local network), displaying, 313-314
Transaction SIGnatures (TSIG), 406, 447
tunneling proxy servers, 491
types
  filesystems, listing of, 154-155
  PAM configuration, 559-562
    account, 559
    auth, 559
    password, 560
    session, 560
  proxy servers, 491-492
    forward, 491
    reverse, 492
    tunneling, 491
  zone records, 423-425
U
-u option
  fdisk command, 176
  lsof command, 14
  nc command, 312
-U option (smbclient command), 518
UATA (Ultra Advanced Technology Attachment), 233
udevd monitor command, 86
udevd daemon, 85-86, 246
UDP ports, scanning, 303
UDF (Universal Disk Format) filesystems, 198
  creating, 200
  defined, 155
UEFI (Unified Extensible Firmware Interface), 111
UIDs, mapping, 529-530
uname command
  current kernel, displaying, 65
  platforms, determining, 352
uncompressing files, 368
undeleting files, 183
Uniform Resource Locators (URLs), 402
Universally Unique Identifiers (UUIDs), 163
Unix style comments (#), 405
unloading modules from memory, 71
unmount command, 155
unmounting
  filesystems, 155, 159-160
  NFS shares, 535
unpacking
  kernel, 47
  source code, 349-350
unzip command, 368
unzipping source files, 349-350
update-rc.d command, 102-103
updates
  software, 695
  source code, 353-354
  zone records, 421
uptime command, 7
URLs (Uniform Resource Locators), 402
USB devices, 82-84
US-CERT, 698
user value (iostat command), 8
userlist_deny directive, 668
userlist_enable directive, 668
userlist_file directive, 668
username maps, 517-518
users
  accounts
    adding to etc/vsftpd.ftpusers file, 668
    FTP server access, limiting, 667-669
  anonymous, 666
  authentication. See authentication
  filesystem mounting restrictions, 164
  home directories
    backing up, 362
    procmail utility, adding, 624
    sharing, 512-513
  logged in
    displaying at login prompt, 382
    monitoring, 21
  messages
    shutdown, 389-390
    wall, 387-389
  non-root, 441
  PAM accounts, 559-560
  privacy violations, 682
  root, 682
  SAMBA accounts, creating, 516-518
  SSH logins, 682-683
  superusers, 129, 181
usr directory, 362
usr/share/doc/kernel-doc-2.6.32/
  Documentation/sysctl/fs.txt file, 44
usr/share/doc/kernel-doc/Documentation
  directory, 43
  html directory, 510
usr/share/easy-rsa directory, 700
usr/src directory, 47, 349
usr/src/linux/Documentation directory, 43
utilities. See also commands
  apachectl, 457
  backup
    dd command, 368-369
    selecting, 367
    tar command, 369-372
    creating/restoring files, 368
dhclient, 323
fail2ban, 696-697
dnsmasq, 312-313
iptables, 695
  chains, 652
  examples, 653-656
  features, 650
  filtering, 650, 654
  packet redirection, 657-658
  rules, saving, 656-657
  targets, 653
nc, 312-313, 695
nmap, 695
OpenVAS, 696-698
PADL migration, 595
portmap
  network port numbers, 531
  RPC service, 527
  TCP wrappers, 532-533
procmail
  advantage over MTA's, 623
defined, 621
global configuration, 624
installing, 623
lockfile, 626
mail spool directory, choosing, 624
MTA automatic usage, determining, 623
rules, 625-627
as SPAM filter, 624
users adding procmail home directories, 624
rndc, 410
SAMBA client, 509
security, 695
fail2ban, 696-697
iptables, 695
nc, 695
nmap, 695
OpenVAS, 696-698
Snort, 696-698
telnet, 695
Snort, 696-698
telnet, 616, 695
third-party backup, 374-375
UUIDs (Universally Unique Identifiers), 163
v
  -v option
lspci command, 78-79
lsusb command, 82-84
rsync command, 373
tar command, 371
tgdisplay command, 261
values
  blocks in/out, 11-12
  etc/collectd/collectd.conf file, 29-30
  etc/issue file, 382
  file-max file, 45
  free command, 10
  iostat command, 8
  PAM control, 562-564
var directory, 363
var/log/auth.log file, 330
var/log/boot.log file, 330
var/log/messages file, 84, 328
var/log/SAMBA directory, 516
var/log/secure file, 330
var/log/syslog file, 84, 328
var/named directory, 419
var/named/named.ca file, 419
var/named/named.localhost file, 419
var/spool/postfix directory, 610
var/www/html directory, 458
verifying
  Apache Web Server, 457
  NFS share mounts, 534
  PAM passwords/user accounts, 559
  SAMBA configuration file, 515-516
  scripting
    Perl, 462
    PHP, 460
tar balls, 372
target configuration, 243
versions
  Apache Web Server, 457
  kernel image filenames, 46
  OSs, displaying at login prompt, 382
Very Secure FTP daemon. See vsftpd servers
vfat filesystems, 69-70
vgchange command, 270
vgdisplay command, 260-261
  after LV creation, 265-267
  -v option, 261
vgextend command, 270
VGs (volume groups), 259
  activating, 270
  information, displaying, 260-261, 265-267
  LVs
    associations, displaying, 261
    creating, 262-263
    physical extents, 259-260
  PVs
    adding, 259
    associations, displaying, 261
    deleting, 270
    size, extending, 270
  visual representation, 259
view statement, 444
VirtualBox, 718
virtual domains (Postfix), 614
virtual filesystems
/ directory, 153
defined, 153
example, 154
mount points, 153
virtual hosts, 466, 477
virtual machines
DHCP servers, 543
studying for exams, 718
virtual memory, 10
Virtual Private Networks. See VPNs
vmlinux file, 139
vmstat command, 11-12
VMWare, 718
volume groups. See VGs
VPNs (Virtual Private Networks), 699
CA, 700
clients
  certificates, creating, 703-705
  configuring, 706-708
OpenVPN, 699
servers
  certificates, creating, 701-703
  configuration, 705
vsftpd servers (Very Secure FTP daemon), 665
anonymous FTP, 665
  access not permitted, 667
  settings, 666
  testing, 666
  user accounts, limiting, 669
anonymous users uploading content, 666
banners, 669
chroot jailing local user accounts, 669
configuration file, 665
directives, 669
file uploads, disabling, 669
FTP client connections, 669
installing, 665
pre-login messages, 669
transfer rates, 669
user accounts, limiting, 667-668
-vv option (lspci command), 79
-vvv option (lspci command), 79
W
w command, 21
w flag (procmail utility), 625
W flag (procmail utility), 625
-w option (nc command), 312
-W option
  ldapdelete command, 596
  ldappasswd command, 600
  tar command, 372
wait keyword, 96
wall command, 387-389
wall messages, 387-389
watch command, 21
websites
df plugin, 30
disk plugin, 30
dns plugin, 30
GitHub, 348
kernel.org, 43
LPI Marketplace, 717
LPI.org, 714
PADL migration tool, 595
plugins, listing of, 30
tools for displaying collectd daemon data, 31
US-CERT, 698
VMWare, 718
white listing IP addresses, 697
wildcard filter expression, (*), 599
WiFi
disabling, 338
interface parameters, displaying, 290-291
wireless routers available, listing, 291-293
Windows accounts, mapping, 517
wireless routers available, displaying, 291-293
wireshark, 336
workgroup setting (SAMBA), 512
write_enable directive, 669
WRITE requests, 536
WWIDs (World Wide Identifiers), 241
X
-x option
  ldapdelete command, 596
ldappasswd command, 600
ldapsearch command, 597
tar command, 372
X11Forwarding setting (SSH login setting), 683
XEN, 718
-xf option (tar command), 371
xfs-based filesystems, 184
   backing up/restoring
      xfsdump command, 184-186
      xfsrestore command, 186-187
   information, displaying, 187
   problems, checking for, 189
   unmounted, fixing, 188-189
xfs_check command, 189
xfsdump command, 184-186
xfs filesystems, 154, 175
xfs_info command, 187
xfs_repair command, 188-189
xfsrestore command, 186-187
{x.y} pattern matching character, 626
-z option
   nc command, 313
   tar command, 372
Y
YUM, source code, downloading, 345-347
yumdownloader command, 346
Z
zero or more pattern matching character (*), 626
zImage files, 46
zip command, 368
zone files
   @ (current origin) character, 422
   comments, 421
   creating, 421
   defined, 398
   DNSSEC, 448-449
   etc/named.conf file, 407, 420-421
   forward, 420
   local host file, 419
   record fields, 422
   reloading, 408
   reverse lookup, 421
   root servers, listing of, file, 419
   storage location, 419
   storing in chroot directory, 442
   syntax, 421-422
   transferring, 421, 446
   TTL, 422
zone records
   SOA, 423-425
   updating, 421
-x option
   nc command, 313
   tar command, 372