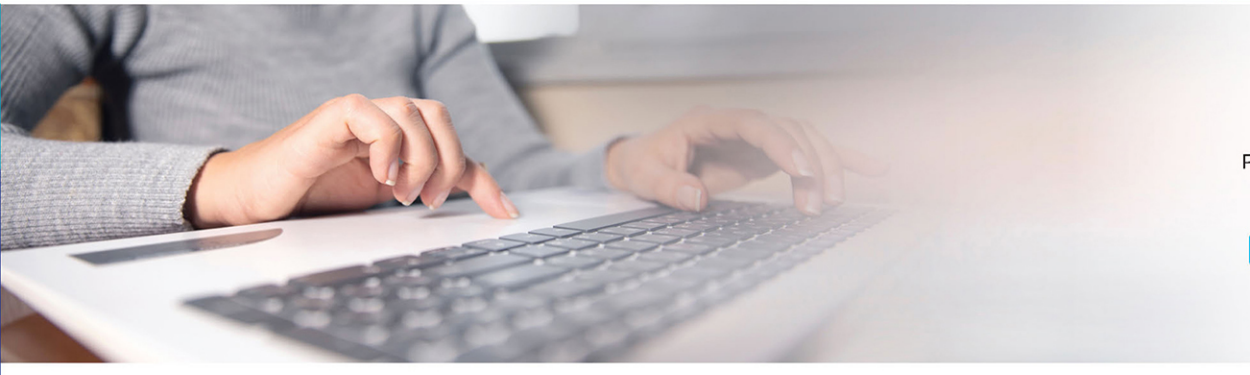
PEARSON IT CERTIFICATION



Practice Tests

Flash Cards

Labs

Study Planner

Cert Guide

Advance your IT career with hands-on learning

Red Hat RHCSA™ 10 (EX200)

SANDER VAN VUGT

FREE SAMPLE CHAPTER |

Red Hat RHCSA 10 Cert Guide: EX200

Companion Website

Access interactive study tools on this book's companion website, including review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonitcertification.com/register.
2. Enter the **print book ISBN**: 9780135576663.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

If you have any issues accessing the companion website you can contact our support team by going to **informit.com/support**.

For access to any available bonus content associated with this title, visit informit.com/register, sign in or create a new account, and register ISBN 9780135576663 by December 31, 2029.

This page intentionally left blank

Red Hat RHCSA™ 10 Cert Guide: EX200

Sander van Vugt



Red Hat RHCSA™ 10 Cert Guide: EX200

Copyright © 2026 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/global-permission-granting.html.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

$PrintCode

ISBN-13: 978-0-13-557666-3
ISBN-10: 0-13-557666-0

Library of Congress Control Number: 2026938327

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Red Hat and RHCSA are registered trademarks of Red Hat, Inc. in the United States and other countries.

Pearson IT Certification and Sander van Vugt have no affiliation with Red Hat, Inc. The RED HAT and RHCSA trademarks are used for identification purposes only and are not intended to indicate affiliation with or approval by Red Hat, Inc.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Head of IT & Professional Learning, Enterprise Learning and Skills
Julie Phifer

Acquisitions Editors
Harry Misthos
Denise Lincoln

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Chuck Hutchinson

Indexer
Timothy Wright

Proofreader
Donna E. Mulder

Technical Editors
John McDonough
Matthew Helmke

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Introduction xxx

Part I: Performing Basic System Management Tasks

CHAPTER 1 Installing Red Hat Enterprise Linux 3

CHAPTER 2 Using Essential Tools 25

CHAPTER 3 Essential File Management Tools 51

CHAPTER 4 Working with Text Files 79

CHAPTER 5 Connecting to Red Hat Enterprise Linux 99

CHAPTER 6 User and Group Management 121

CHAPTER 7 Permissions Management 145

CHAPTER 8 Configuring Networking 165

Part II: Operating Running Systems

CHAPTER 9 Managing Software 193

CHAPTER 10 Managing Processes 227

CHAPTER 11 Working with Systemd 249

CHAPTER 12 Scheduling Tasks 269

CHAPTER 13 Configuring Logging 285

CHAPTER 14 Managing Storage 309

CHAPTER 15 Managing Logical Volumes 339

Part III: Performing Advanced System Administration Tasks

CHAPTER 16 Basic Kernel Management 361

CHAPTER 17 Managing and Understanding the Boot Procedure 379

CHAPTER 18 Essential Troubleshooting Skills 395

CHAPTER 19 An Introduction to Automation with Bash Shell Scripting 413

Part IV: Managing Network Services

CHAPTER 20 Configuring SSH 433

CHAPTER 21 Managing Apache HTTP Services 447

CHAPTER 22 Managing SELinux 463

CHAPTER 23 Configuring a Firewall 489

CHAPTER 24 Accessing Network Storage 505

CHAPTER 25 Configuring Time Services 517

CHAPTER 26 Final Preparation 533

CHAPTER 27 Theoretical Pre-Assessment Exam 539

Part V: RHCSA Practice Exams

RHCSA PRACTICE EXAM A 541

RHCSA PRACTICE EXAM B 543

APPENDIX A Answers to the "Do I Know This Already?" Quizzes and Review Questions 545

APPENDIX B *Red Hat RHCSA 10 Cert Guide: EX200* Exam Updates 579

Glossary 581

Index 603

Online Elements:

RHCSA PRACTICE EXAM C

RHCSA PRACTICE EXAM D

APPENDIX C Memory Tables

APPENDIX D Memory Tables Answer Key

APPENDIX E Study Planner

Glossary

Table of Contents

Introduction xxx

Part I: Performing Basic System Management Tasks

Chapter 1 Installing Red Hat Enterprise Linux 3

"Do I Know This Already?" Quiz 3

Foundation Topics 6

Preparing to Install Red Hat Enterprise Linux 6

What Is Red Hat Enterprise Linux 10 Server? 6

Getting the Software 7

Using Red Hat Enterprise Linux 7

Using CentOS Stream 8

Other Distributions 8

Understanding Access to Repositories 8

Setup Requirements 9

Cert Guide Environment Description 10

Performing an Installation 10

Summary 21

Exam Preparation Tasks 21

Review All Key Topics 21

Define Key Terms 21

Review Questions 22

End-of-Chapter Lab 22

Lab 1.1 22

Chapter 2 Using Essential Tools 25

"Do I Know This Already?" Quiz 25

Foundation Topics 28

Basic Shell Skills 28

Understanding Commands 28

Executing Commands 28

I/O Redirection 30

Using Pipes 32

History 33

Bash Completion 35

Editing Files with vim 35
Editing Files with nano 38
Understanding the Shell Environment 39
Understanding Variables 39
Recognizing Environment Configuration Files 40
Using /etc/motd and /etc/issue 41
Finding Help 42
Using --help 42
Using man 42
Finding the Right man Page 43
Updating mandb 45
Using RHEL Lightspeed 46
Summary 47
Exam Preparation Tasks 47
Review All Key Topics 47
Complete Tables and Lists from Memory 48
Define Key Terms 48
Review Questions 48
End-of-Chapter Lab 49
Lab 2.1 49
Chapter 3 Essential File Management Tools 51
"Do I Know This Already?" Quiz 51
Foundation Topics 54
Working with the File System Hierarchy 54
Defining the File System Hierarchy 54
Understanding Mounts 55
Managing Files 60
Working with Wildcards 60
Managing and Working with Directories 60
Working with Absolute and Relative Pathnames 61
Listing Files and Directories 62
Copying Files and Directories 63
Moving Files and Directories 64
Deleting Files and Directories 65
Using Links 66

Understanding Hard Links 66
Understanding Symbolic Links 67
Creating Links 68
Removing Links 69
Working with Archives and Compressed Files 70
Managing Archives with tar 70
Creating Archives with tar 71
Monitoring and Extracting tar Files 71
Using Compression 72
Summary 74
Exam Preparation Tasks 74
Review All Key Topics 74
Complete Tables and Lists from Memory 75
Define Key Terms 75
Review Questions 75
End-of-Chapter Lab 76
Lab 3.1 76
Chapter 4 Working with Text Files 79
"Do I Know This Already?" Quiz 79
Foundation Topics 82
Using Common Text File–Related Tools 82
Doing More with less 82
Showing File Contents with cat 83
Displaying the First or Last Lines of a File with head and tail 84
Filtering Specific Columns with cut 85
Sorting File Contents and Output with sort 85
Counting Lines, Words, and Characters with wc 86
A Primer to Using Regular Expressions 87
Using Line Anchors 88
Using Escaping in Regular Expressions 89
Using Wildcards and Multipliers 89
Using Extended Regular Expressions 90
Using grep to Analyze Text 91
Working with Other Useful Text Processing Utilities 92
Summary 94

Exam Preparation Tasks 94
Review All Key Topics 94
Complete Tables and Lists from Memory 95
Define Key Terms 95
Review Questions 95
End-of-Chapter Lab 96
Lab 4.1 96

Chapter 5 Connecting to Red Hat Enterprise Linux 99

"Do I Know This Already?" Quiz 99
Foundation Topics 102
Working on Local Consoles 102
Logging In to a Local Console 102
Switching Between Terminals in a Graphical Environment 103
Working with Multiple Terminals in a Nongraphical Environment 105
Understanding Pseudo Terminal Devices 106
Booting, Rebooting, and Shutting Down Systems 107
Using SSH and Related Utilities 108
Accessing Remote Systems Using SSH 108
Securely Transferring Files Between Systems 111
Using scp to Securely Copy Files 111
Using sftp to Securely Transfer Files 112
Using rsync to Synchronize Files 113
Configuring Key-Based Authentication for SSH 113
Using Passphrases or Not? 114
Using Cockpit 114
Understanding Cockpit 115
Performing Common Tasks with Cockpit 115
Summary 116
Exam Preparation Tasks 117
Review All Key Topics 117
Complete Tables and Lists from Memory 117
Define Key Terms 117
Review Questions 117
End-of-Chapter Labs 118

Lab 5.1 118
Lab 5.2 118
Chapter 6 User and Group Management 121
"Do I Know This Already?" Quiz 121
Foundation Topics 124
Understanding Different User Types 124
Users on Linux 124
Working as Root 124
Using su 125
sudo 126
PolicyKit 128
Creating and Managing User Accounts 129
System Accounts and Normal Accounts 129
Creating Users 132
Modifying the Configuration Files 133
Using useradd 133
Home Directories 133
Default Shell 134
Managing User Properties 134
Configuration Files for User Management Defaults 135
Managing Password Properties 135
Creating a User Environment 136
Creating and Managing Group Accounts 137
Understanding Linux Groups 137
Creating Groups 138
Creating Groups with vigr 138
Using groupadd to Create Groups 139
Managing Group Properties 139
Summary 140
Exam Preparation Tasks 140
Review All Key Topics 140
Complete Tables and Lists from Memory 141
Define Key Terms 141
Review Questions 141
End-of-Chapter Labs 142

Lab 6.1 142
Lab 6.2 142
Chapter 7 Permissions Management 145
"Do I Know This Already?" Quiz 145
Foundation Topics 148
Managing File Ownership 148
Displaying Ownership 148
Changing User Ownership 149
Changing Group Ownership 149
Understanding Default Ownership 150
Managing Basic Permissions 151
Understanding Read, Write, and Execute Permissions 151
Applying Read, Write, and Execute Permissions 152
Managing Advanced Permissions 155
Understanding Advanced Permissions 155
Applying Advanced Permissions 157
Setting Default Permissions with umask 159
Working with User-Extended Attributes 160
Summary 161
Exam Preparation Tasks 162
Review All Key Topics 162
Complete Tables and Lists from Memory 162
Define Key Terms 162
Review Questions 162
End-of-Chapter Lab 163
Lab 7.1 163
Chapter 8 Configuring Networking 165
"Do I Know This Already?" Quiz 165
Foundation Topics 168
Networking Fundamentals 168
IP Addresses 168
IPv6 Addresses 169
IPv4 Network Masks 169
Binary Notation 170
MAC Addresses 171

Protocol and Ports 171
Managing Network Addresses and Interfaces 172
Validating Network Configuration 173
Validating Network Address Configuration 173
Validating Routing 176
Validating the Availability of Ports and Services 177
Managing Network Configuration with nmtui and nmcli 178
Required Permissions to Change Network Configuration 179
Configuring the Network with nmcli 180
Configuring the Network with nmtui 182
Working on Network Configuration Files 184
Setting Up Hostname and Name Resolution 185
Hostnames 185
DNS Name Resolution 187
Summary 189
Exam Preparation Tasks 189
Review All Key Topics 189
Complete Tables and Lists from Memory 190
Define Key Terms 190
Review Questions 190
End-of-Chapter Lab 191
Lab 8.1 191

Part II: Operating Running Systems

Chapter 9 Managing Software 193

"Do I Know This Already?" Quiz 193
Foundation Topics 196
Managing Software Packages with dnf 196
Understanding the Role of Repositories 196
Registering Red Hat Enterprise Linux for Support 197
Managing Subscriptions 197
Specifying Which Repository to Use 198
Understanding Repository Security 200
Creating Your Own Repository 202
Using dnf 204

Using dnf to Find Software Packages 204
Getting More Information About Packages 206
Installing and Removing Software Packages 207
Showing Lists of Packages 209
Updating Packages 210
Working with dnf Package Groups 212
Using dnf History 214
Managing Software Packages with rpm 215
Understanding RPM Filenames 216
Querying the RPM Database 216
Querying RPM Package Files 217
Managing Software with Flatpak 219
Understanding Flatpak 219
Installing Flatpak 220
Managing Flatpak Applications 220
Summary 221
Exam Preparation Tasks 222
Review All Key Topics 222
Complete Tables and Lists from Memory 222
Define Key Terms 222
Review Questions 223
End-of-Chapter Lab 223
Lab 9.1 223
Chapter 10 Managing Processes 227
"Do I Know This Already?" Quiz 227
Foundation Topics 230
Introducing Process Management 230
Managing Shell Jobs 230
Running Jobs in the Foreground and Background 230
Managing Shell Jobs 231
Understanding Parent–Child Relations 233
Using Common Command-Line Tools for Process Management 233
Understanding Processes and Threads 234
Using ps to Get Process Information 235
Understanding Process Priorities 237

Exploring Relations Between Slices 237
Managing Process Priorities 238
Sending Signals to Processes with kill, killall, and pkill 239
Killing Zombies 241
Using top to Manage Processes 242
Using tuned to Optimize Performance 244
Summary 245
Exam Preparation Tasks 246
Review All Key Topics 246
Complete Tables and Lists from Memory 246
Define Key Terms 246
Review Questions 246
End-of-Chapter Lab 247
Lab 10.1 247
Chapter 11 Working with Systemd 249
"Do I Know This Already?" Quiz 249
Foundation Topics 252
Understanding Systemd 252
Understanding Systemd Unit Locations 252
Understanding Systemd Service Units 253
Understanding Systemd Mount Units 254
Understanding Systemd Socket Units 255
Understanding Systemd Target Units 256
Managing Units Through Systemd 257
Managing Dependencies 260
Managing Unit Directives 262
Summary 265
Exam Preparation Tasks 265
Review All Key Topics 265
Complete Tables and Lists from Memory 266
Define Key Terms 266
Review Questions 266
End-of-Chapter Lab 266
Lab 11.1 267

Chapter 12 Scheduling Tasks 269

"Do I Know This Already?" Quiz 269

Foundation Topics 272

Understanding Task Scheduling Options in RHEL 272

Using Systemd Timers 272

Configuring cron to Automate Recurring Tasks 274

Managing the crond Service 274

Understanding cron Timing 276

Managing cron Configuration Files 276

Understanding the Purpose of anacron 279

Managing cron Security 280

Configuring at to Schedule Future Tasks 281

Summary 281

Exam Preparation Tasks 282

Review All Key Topics 282

Define Key Terms 282

Review Questions 282

End-of-Chapter Lab 283

Lab 12.1 283

Chapter 13 Configuring Logging 285

"Do I Know This Already?" Quiz 285

Foundation Topics 288

Understanding System Logging 288

Understanding the Role of systemd-journald and rsyslogd 288

Reading Log Files 290

Understanding Log File Contents 291

Live Log File Monitoring 292

Working with systemd-journald 292

Using journalctl to Find Events 292

Preserving the Systemd Journal 296

Configuring rsyslogd 298

Understanding rsyslogd Configuration Files 298

Understanding rsyslog.conf Sections 298

Understanding Facilities, Priorities, and Log Destinations 298

Rotating Log Files 302
Using logger 304
Summary 305
Exam Preparation Tasks 305
Review All Key Topics 305
Complete Tables and Lists from Memory 305
Define Key Terms 306
Review Questions 306
End-of-Chapter Lab 306
Lab 13.1 307
Chapter 14 Managing Storage 309
"Do I Know This Already?" Quiz 309
Foundation Topics 312
Understanding MBR and GPT Partitions 312
Understanding the MBR Partitioning Scheme 312
Understanding the Need for GPT Partitioning 313
Understanding Storage Measurement Units 314
Managing Partitions and File Systems 315
Creating MBR Partitions with fdisk 316
Using Extended and Logical Partitions on MBR 318
Creating GPT Partitions with fdisk 320
Creating GPT Partitions with parted 322
Creating File Systems 323
Changing File System Properties 325
Managing Ext4 File System Properties 325
Managing XFS File System Properties 327
Adding Swap Partitions 327
Adding Swap Files 328
Mounting File Systems 329
Manually Mounting File Systems 329
Using Device Names, UUIDs, or Disk Labels 330
Automating File System Mounts Through /etc/fstab 331
Using Systemd Mounts 334
Summary 335

Exam Preparation Tasks 335
Review All Key Topics 336
Complete Tables and Lists from Memory 336
Define Key Terms 336
Review Questions 336
End-of-Chapter Lab 337
Lab 14.1 337

Chapter 15 Managing Logical Volumes 339

"Do I Know This Already?" Quiz 339
Foundation Topics 342
Understanding LVM 342
LVM Architecture 342
LVM Features 343
Creating LVM Logical Volumes 344
Creating the Physical Volumes 346
Creating the Volume Groups 350
Creating the Logical Volumes and File Systems 351
Understanding LVM Device Naming 352
Resizing LVM Logical Volumes 354
Resizing Volume Groups 354
Resizing Logical Volumes and File Systems 354
Reducing Volume Groups 356
Summary 357
Exam Preparation Tasks 357
Review All Key Topics 358
Complete Tables and Lists from Memory 358
Define Key Terms 358
Review Questions 358
End-of-Chapter Labs 359
Lab 15.1 359

Part III: Performing Advanced System Administration Tasks

Chapter 16 Basic Kernel Management 361

"Do I Know This Already?" Quiz 361
Foundation Topics 364

Understanding the Role of the Linux Kernel 364
Understanding the Use of Kernel Threads and Drivers 364
Analyzing What the Kernel Is Doing 366
Working with Kernel Modules 368
Understanding Hardware Initialization 368
Managing Kernel Modules 370
Checking Driver Availability for Hardware Devices 373
Managing Kernel Module Parameters 374
Upgrading the Linux Kernel 375
Summary 375
Exam Preparation Tasks 376
Review All Key Topics 376
Complete Tables and Lists from Memory 376
Define Key Terms 376
Review Questions 376
End-of-Chapter Lab 377
Lab 16.1 377
Chapter 17 Managing and Understanding the Boot Procedure 379
"Do I Know This Already?" Quiz 379
Foundation Topics 382
Managing Systemd Targets 382
Understanding Systemd Targets 382
Working with Targets 382
Understanding Target Units 383
Understanding Wants 384
Managing Systemd Targets 384
Isolating Targets 385
Setting the Default Target 387
Working with GRUB 2 388
Understanding GRUB 2 388
Understanding GRUB 2 Configuration Files 390
Modifying Default GRUB 2 Boot Options 390
Summary 391
Exam Preparation Tasks 391

Review All Key Topics 391
Define Key Terms 392
Review Questions 392
End-of-Chapter Labs 393
Lab 17.1 393
Lab 17.2 393

Chapter 18 Essential Troubleshooting Skills 395

"Do I Know This Already?" Quiz 395
Foundation Topics 398
Understanding the RHEL 10 Boot Procedure 398
Passing Kernel Boot Arguments 400
Accessing the Boot Prompt 400
Starting a Troubleshooting Target 401
Using a Rescue Disk 403
Restoring System Access Using a Rescue Disk 403
Reinstalling GRUB Using a Rescue Disk 405
Re-creating the Initramfs Using a Rescue Disk 405
Fixing Common Issues 406
Reinstalling GRUB 2 406
Fixing the Initramfs 406
Recovering from File System Issues 407
Resetting the Root Password 407
Summary 409
Exam Preparation Tasks 409
Review All Key Topics 409
Complete Tables and Lists from Memory 410
Define Key Terms 410
Review Questions 410
End-of-Chapter Lab 411
Lab 18.1 411

Chapter 19 An Introduction to Automation with Bash Shell Scripting 413

"Do I Know This Already?" Quiz 413
Foundation Topics 416
Understanding Shell Scripting Core Elements 416
Using Variables and Input 418

Using Positional Parameters 418
Working with Variables 420
Using Conditional Loops 422
Working with if … then … else 422
Using || and && 423
Applying for 424
Understanding while and until 425
Understanding case 426
Bash Shell Script Debugging 427
Summary 428
Exam Preparation Tasks 428
Review All Key Topics 428
Define Key Terms 429
Review Questions 429
End-of-Chapter Lab 429
Lab 19.1 430

Part IV: Managing Network Services

Chapter 20 Configuring SSH 433

"Do I Know This Already?" Quiz 433
Foundation Topics 436
Hardening the SSH Server 436
Limiting Root Access 436
Configuring Alternative Ports 437
Modifying SELinux to Allow for Port Changes 437
Limiting User Access 438
Using Other Useful sshd Options 439
Session Options 440
Connection Keepalive Options 440
Configuring Key-Based Authentication with Passphrases 441
Summary 442
Exam Preparation Tasks 442
Review All Key Topics 442
Complete Tables and Lists from Memory 443

Define Key Terms 443
Review Questions 443
End-of-Chapter Lab 444
Lab 20.1 444
Chapter 21 Managing Apache HTTP Services 447
"Do I Know This Already?" Quiz 447
Foundation Topics 450
Configuring a Basic Apache Server 450
Installing the Required Software 450
Identifying the Main Configuration File 450
Creating Web Server Content 453
Understanding Apache Configuration Files 454
Creating Apache Virtual Hosts 456
Summary 458
Exam Preparation Tasks 458
Review All Key Topics 458
Define Key Terms 459
Review Questions 459
End-of-Chapter Lab 459
Lab 21.1 460
Chapter 22 Managing SELinux 463
"Do I Know This Already?" Quiz 464
Foundation Topics 467
Understanding SELinux Working Modes 467
Understanding Context Settings and the Policy 471
Monitoring Current Context Labels 471
Setting Context Types 473
Finding the Context Type You Need 476
Restoring Default File Contexts 477
Managing Port Access 479
Using Boolean Settings to Modify SELinux Settings 479
Diagnosing and Addressing SELinux Policy Violations 481
Making SELinux Analyzing Easier 483
Summary 485

Exam Preparation Tasks 485
Review All Key Topics 485
Complete Tables and Lists from Memory 485
Define Key Terms 486
Review Questions 486
End-of-Chapter Lab 486
Lab 22.1 487

Chapter 23 Configuring a Firewall 489

"Do I Know This Already?" Quiz 489
Foundation Topics 493
Understanding Linux Firewalling 493
Understanding Previous Firewalling Solutions 493
Understanding Firewalld 493
Understanding Firewalld Zones 494
Understanding Firewalld Services 495
Working with Firewalld 496
Summary 500
Exam Preparation Tasks 500
Review All Key Topics 500
Complete Tables and Lists from Memory 501
Define Key Terms 501
Review Questions 501
End-of-Chapter Lab 502
Lab 23.1 502

Chapter 24 Accessing Network Storage 505

"Do I Know This Already?" Quiz 505
Foundation Topics 508
Using NFS Services 508
Understanding NFS Security 508
Setting Up NFS 508
Mounting the NFS Share 509
Mounting Remote File Systems Through fstab 510
Mounting NFS Shares Through fstab 510

Using Autofs to Mount Remote File Systems 511
Understanding Autofs 512
Defining Mounts in Autofs 512
Configuring Autofs for NFS 512
Using Wildcards in Autofs 513
Summary 514
Exam Preparation Tasks 514
Review All Key Topics 514
Define Key Terms 514
Review Questions 515
End-of-Chapter Lab 515
Lab 24.1 515

Chapter 25 Configuring Time Services 517

"Do I Know This Already?" Quiz 517
Foundation Topics 520
Understanding Local Time 520
Using Network Time Protocol 521
Managing Time on Red Hat Enterprise Linux 521
Using date 522
Using hwclock 522
Using timedatectl 523
Managing Time Zone Settings 525
Configuring Time Service Clients 527
Summary 528
Exam Preparation Tasks 529
Review All Key Topics 529
Complete Tables and Lists from Memory 529
Define Key Terms 529
Review Questions 530
End-of-Chapter Lab 530
Lab 25.1 530

Chapter 26 Final Preparation 533

General Tips 533

Verifying Your Readiness 533

Registering for the Exam 533

On Exam Day 534

During the Exam 535

The Nondisclosure Agreement 536

Chapter 27 Theoretical Pre-Assessment Exam 539

Part V: RHCSA Practice Exams

RHCSA Practice Exam A 541

RHCSA Practice Exam B 543

Appendix A Answers to the "Do I Know This Already?" Quizzes and Review Questions 545

Appendix B *Red Hat RHCSA 10 Cert Guide: EX200* Exam Updates 579

Glossary 581

Index 603

Online Elements:

RHCSA Practice Exam C

RHCSA Practice Exam D

Appendix C Memory Tables

Appendix D Memory Tables Answer Key

Appendix E Study Planner

Glossary

About the Author

Sander van Vugt is an independent Linux trainer, author, and consultant living in the Netherlands. Sander is the author of the best-selling *Red Hat Certified System Administrator (RHCSA) Complete Video Course* and the *Red Hat Certified Engineer (RHCE) Complete Video Course*. He has also written numerous books about different Linux-related topics and many articles for Linux publications around the world. Sander has been teaching Red Hat, Linux+, and LFCS classes since 1994. As a consultant, he specializes in Linux high-availability solutions and performance optimization. You can find more information about Sander on his website at https://www.sandervanvugt.com.

For more information about RHCSA certification and additional resources, visit the author's Red Hat Certification page at https://www.rhatcert.com/.

Acknowledgments

This book could not have been written without the help of all the people who contributed to it. I want to thank the people at Pearson—Denise Lincoln, Harry Misthos, and Ellie Bru in particular. We've worked a lot together over the years, and this book is another milestone on our road to success!

About the Technical Reviewers

John McDonough has more than 35 years of development experience; currently, John is a cloud security architect for Fortinet. As a cloud security architect, John writes code to automate the deployment and management of secure cloud infrastructure and security policy. John is a regular presenter and blogger about automating cloud infrastructure deployment and configuration. John has presented at multiple Fortinet, Microsoft, and Cisco events. Additionally John has presented at AI Networking Summit (ONUG), HashiConf, SXSW, AnsibleFest, Developer Week, and other industry events. John's career has varied from product engineer to custom application developer, technical marketing engineer, and now cloud security architect.

Matthew Helmke got his first computer in 1981 and started using UNIX in 1987 while studying LISP. Today he works as a technical writer for Chainguard.dev and in the past has written about Linux and other topics for a diverse set of companies, including for a while as a technical writer at Red Hat. He is the author of several books, including *Ubuntu Unleashed*, *The Official Ubuntu Book*, and *VMware Cookbook*. You can find Matthew on LinkedIn at https://www.linkedin.com/in/matthewhelmke/.

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 email 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 email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *Red Hat RHCSA 10 Cert Guide: EX200* 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 9780135576663 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

Welcome to the *Red Hat RHCSA 10 Cert Guide: EX200*. The Red Hat exams are some of the toughest in the business, and this guide will be an essential tool in helping you prepare to take the Red Hat Certified System Administrator (RHCSA) exam.

As an instructor with more than 30 years of experience teaching Red Hat Enterprise Linux, I have taken the RHCSA exam (and the RHCE exam) numerous times so that I can keep current on the progression of the exam, what is new, and what is different. I share my knowledge with you in this comprehensive Cert Guide so that you get the guidance you need to pass the RHCSA exam.

This book contains everything you need to know to pass the 2025 version of the RHCSA exam. As you will see, the Cert Guide covers every objective in the exam and comprises 27 chapters, more than 80 exercises, 4 practice exams, an extensive glossary, and hours of video training. This Cert Guide is the best resource you can get to prepare for and pass the RHCSA exam.

Goals and Methods

To learn the topics described in this book, it is recommended that you create your own testing environment. You cannot become an RHCSA without practicing a lot. Within the exercises included in every chapter of the book, you will find all the examples you need to understand what is on the exam and thoroughly learn the material needed to pass it. The exercises in the chapters provide step-by-step procedures that you can follow to find working solutions so that you can get real experience before taking the exam.

Each chapter also includes one or more end-of-chapter labs. These labs ask questions that are similar to the questions that you might encounter on the exam. Solutions are not provided for these labs, and that is on purpose, because you need to train yourself to verify your work before you take the exam. On the exam, you also have to be able to verify for yourself whether the solution is working as expected. Please be sure to also go to this book's companion website, which provides additional practice exams, appendixes, and video training—all key components to studying for and passing the exam.

To make working with the assignments in this book as easy as possible, the complete lab environment is Bring Your Own. In Chapter 1, you'll learn how to install Red Hat Enterprise Linux 10 in a virtual machine, and that is all that is required to go through the labs.

This book contains everything you need to pass the exam, but if you want more guidance and practice, I have a number of video training titles available to help you study, including the following:

- *Linux Fundamentals*, Third Edition
- *Red Hat Certified System Administrator (RHCSA) RHEL 10*

Apart from these products, you might also appreciate my website, https://rhatcert.com. Through this website, I provide updates on anything that is useful to exam candidates. I recommend that you register on the website so that I can send you messages about important updates that I've made available. Also, you'll find occasional video updates on my YouTube channel, rhatcert. I hope that all these resources provide you with everything you need to pass the Red Hat Certified System Administrator exam in an affordable way. Good luck!

Who Should Read This Book?

This book is written as an RHCSA exam preparation guide. That means that you should read it if you want to increase your chances of passing the RHCSA exam. A secondary use of this book is as a reference guide for Red Hat system administrators. As an administrator, you'll like the explanations and procedures that describe how to get things done on Red Hat Enterprise Linux.

So, why should you consider passing the RHCSA exam? That question is simple to answer: Linux has become a very important operating system, and qualified professionals are in demand all over the world. If you want to work as a Linux professional and prove your skills, the RHCSA certificate really helps and is one of the most sought-after certificates in IT. Having this certificate dramatically increases your chances of becoming hired as a Linux professional.

How This Book Is Organized

This book is organized as a reference guide to help you prepare for the RHCSA exam. If you're new to the topics, you can just read it cover to cover. You can also read the individual chapters that you need to fine-tune your skills in this book. Every chapter starts with a "Do I Know This Already?" quiz that asks questions about 10 topics that are covered in that chapter and provides a simple tool to check whether you're already familiar with the topics covered in the chapter.

The book also provides two RHCSA practice exams; these are an essential part of readying yourself for the real exam experience. You might be able to provide the right answer to the multiple-choice chapter questions, but that doesn't mean that you can create the configurations when you take the exam. The companion website includes two extra practice exams, two hours of video from the *Red Hat Certified*

System Administrator (RHCSA) RHEL 10, and additional appendixes. The following outline describes the topics that are covered in the chapters:

Part I: Performing Basic System Management Tasks

- **Chapter 1: Installing Red Hat Enterprise Linux:** In this chapter, you learn how to install Red Hat Enterprise Linux (RHEL) Server. It also shows how to set up an environment that can be used for working on the labs and exercises in this book.
- **Chapter 2: Using Essential Tools:** This chapter covers some of the Linux basics, including working with the shell and Linux commands. This chapter is particularly important if you're new to working with Linux.
- **Chapter 3: Essential File Management Tools:** In this chapter, you learn how to work with tools to manage the Linux file system. This is an important skill because everything on Linux is very file system oriented.
- **Chapter 4: Working with Text Files:** In this chapter, you learn how to work with text files. The chapter teaches you not only how to create text files but also how to look for specific content in the different text files.
- **Chapter 5: Connecting to Red Hat Enterprise Linux:** This chapter describes the different methods that can be used to connect to RHEL 10. It explains both local login and remote login and the different terminal types used for this purpose.
- **Chapter 6: User and Group Management:** On Linux, users are entities that can be used by people or processes that need access to specific resources. This chapter explains how to create users and make user management easier by working with groups.
- **Chapter 7: Permissions Management:** In this chapter, you learn how to manage Linux permissions through the basic read, write, and execute permissions and also through the special permissions and access control lists.
- **Chapter 8: Configuring Networking:** A server is useless if it isn't connected to a network. In this chapter, you learn the essential skills required for managing network connections.

Part II: Operating Running Systems

- **Chapter 9: Managing Software:** Red Hat offers an advanced system for managing software packages. This chapter teaches you how it works.
- **Chapter 10: Managing Processes:** As an administrator, you need to know how to work with the different tasks that can be running on Linux. This chapter shows how to do this, by sending signals to processes and by changing process priority.

- **Chapter 11: Working with Systemd:** Systemd is the standard manager of services and more in RHEL 10. In this chapter, you learn how to manage services using Systemd.
- **Chapter 12: Scheduling Tasks:** In this chapter, you learn how to schedule a task for execution at a time that fits you best.
- **Chapter 13: Configuring Logging:** As an administrator, you need to know what's happening on your server. The rsyslogd and systemd-journald services are used for this purpose. This chapter explains how to work with them.
- **Chapter 14: Managing Storage:** Storage management is an important skill to master as a Linux administrator. This chapter explains how hard disks can be organized in partitions and how these partitions can be mounted in the file system.
- **Chapter 15: Managing Logical Volumes:** Dividing disks in partitions isn't very flexible. If you need optimal flexibility, you need LVM logical volumes, which are used by default while you're installing Red Hat Enterprise Linux. This chapter shows how to manage those logical volumes.

Part III: Performing Advanced System Administration Tasks

- **Chapter 16: Basic Kernel Management:** The kernel is the part of the operating system that takes care of handling hardware. This chapter explains how that works and what an administrator can do to analyze the current configuration and manage hardware devices in case the automated procedure doesn't work well.
- **Chapter 17: Managing and Understanding the Boot Procedure:** Many things are happening when a Linux server boots. This chapter describes the boot procedure in detail and zooms in on vital aspects of the boot procedure, including the GRUB 2 boot loader and the Systemd service manager.
- **Chapter 18: Essential Troubleshooting Skills:** Sometimes a misconfiguration can cause your server to no longer boot properly. This chapter teaches you some of the techniques that can be applied when normal server startup is no longer possible.
- **Chapter 19: An Introduction to Automation with Bash Shell Scripting:** Some tasks are complex and need to be performed repeatedly. Such tasks are ideal candidates for optimization through shell scripts. In this chapter, you learn how to use conditional structures in shell scripts to automate tasks efficiently.

Part IV: Managing Network Services

- **Chapter 20: Configuring SSH:** Secure Shell (SSH) is one of the fundamental services that is enabled on RHEL 10 by default. Using SSH allows you to connect to a server remotely. In this chapter, you learn how to set up an SSH server.
- **Chapter 21: Managing Apache HTTP Services:** Apache is the most commonly used service on Linux. This chapter shows how to set up Apache web services, including the configuration of Apache virtual hosts.
- **Chapter 22: Managing SELinux:** Many Linux administrators only know how to switch off SELinux, because SELinux is hard to manage and is often why services cannot be accessed. In this chapter, you learn how SELinux works and what to do to configure it so that your services are still working and will be much better protected against possible abuse.
- **Chapter 23: Configuring a Firewall:** Apart from SELinux, RHEL 10 comes with a firewall as one of the main security measures, which is implemented by the firewalld service. In this chapter, you learn how this service is organized and what you can do to block or enable access to specific services.
- **Chapter 24: Accessing Network Storage:** While you're working in a server environment, managing remote mounts is an important skill. A remote mount allows a client computer to access a file system offered through a remote server. These remote mounts can be made through a persistent mount in /etc/fstab, or by using the automount service. This chapter teaches how to set up either of them and shows how to configure an FTP server.
- **Chapter 25: Configuring Time Services:** For many services, such as databases and Kerberos, it is essential to have the right time. That's why as an administrator you need to be able to manage time on Linux. This chapter teaches you how.
- **Chapter 26: Final Preparation:** In this chapter, you get some final exam preparation tasks. It contains many tips that help you maximize your chances of passing the RHCSA exam.
- **Chapter 27: Theoretical Pre-Assessment Exam:** This chapter provides an RHCSA theoretical pre-assessment exam to help you assess your skills and determine the best route forward for studying for the exam.

Part V: RHCSA Practice Exams

This part supplies two RHCSA practice exams so that you can test your knowledge and skills further before taking the exams. Two additional exams are on the companion website.

How to Use This Book

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **"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 and the specific topics that you need to focus on.
- **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:** Following the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section lists a series of study activities that you should complete. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include the following:
  - **Review All Key Topics:** The Key Topic icon is shown next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter and their corresponding 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.
  - **Complete Tables and Lists from Memory:** To help you exercise your memory and memorize some facts, many of the more important lists and tables from the chapter are included in a document on the companion website. This document offers only partial information, allowing you to complete the table or list.
  - **Define Key Terms:** This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of this book.
- **Review Questions:** These questions at the end of each chapter measure insight into the topics that were discussed in the chapter.
- **End-of-Chapter Labs:** Real labs give you the right impression of what an exam assignment looks like. The end-of-chapter labs are your first step in finding out what the exam tasks really look like.

Other Features

In addition to the features in each of the core chapters, this book, as a whole, has additional study resources on the companion website, including the following:

- **Two practice exams:** *Red Hat RHCSA 10 Cert Guide: EX200* comes with four practice exams. You will find two in the book and two additional exams on the companion website; these are provided as PDFs so you can get extra practice testing your skills before taking the exam in the testing facility.
- **More than an hour of video training:** The companion website contains more than an hour of instruction from the best-selling *Red Hat Certified System Administrator (RHCSA) RHEL 10 Complete Video Course*.

Exam Objective to Chapter Mapping

Table 1 details where every objective in the RHCSA exam is covered in this book so that you can more easily create a successful plan for passing the exam.

Table 1 Coverage of RHCSA Objectives

Objective	Chapter Title	Chapter
Understand and use essential tools		
Access a shell prompt and issue commands with correct syntax	Using Essential Tools	2
Use input-output redirection (>, >>, |, 2>, etc.)	Using Essential Tools	2
Use grep and regular expressions to analyze text	Working with Text Files	4
Access remote systems using SSH	Connecting to Red Hat Enterprise Linux	5
Log in and switch users in multiuser targets	Connecting to Red Hat Enterprise Linux	5
Archive, compress, unpack, and uncompress files using tar, gzip, and bzip2	Essential File Management Tools	3
Create and edit text files	Working with Text Files	4
Create, delete, copy, and move files and directories	Essential File Management Tools	3
Create hard and soft links	Essential File Management Tools	3
List, set, and change standard ugo/rwx permissions	Permissions Management	7
Locate, read, and use system documentation including man, info, and files in /usr/share/doc	Using Essential Tools	2

Objective	Chapter Title	Chapter
Create simple shell scripts		
Conditionally execute code (use of: if, test, [], etc.)	An Introduction to Automation with Bash Shell Scripting	19
Use looping constructs (for, etc.) to process file, command-line input	An Introduction to Automation with Bash Shell Scripting	19
Process script inputs ($1, $2, etc.)	An Introduction to Automation with Bash Shell Scripting	19
Processing output of shell commands within a script	An Introduction to Automation with Bash Shell Scripting	19
Operate running systems		
Boot, reboot, and shut down a system normally	Connecting to Red Hat Enterprise Linux	5
Boot systems into different targets manually	Essential Troubleshooting Skills	18
Interrupt the boot process in order to gain access to a system	Essential Troubleshooting Skills	18
Identify CPU/memory intensive processes and kill processes	Managing Processes	10
Adjust process scheduling	Managing Processes	10
Manage tuning profiles	Managing Processes	10
Locate and interpret system log files and journals	Configuring Logging	13
Preserve system journals	Configuring Logging	13
Start, stop, and check the status of network services	Configuring Networking	8
Securely transfer files between systems	Connecting to Red Hat Enterprise Linux	5
Configure local storage		
List, create, and delete partitions on MBR and GPT disks	Managing Storage	14
Create and remove physical volumes	Managing Logical Volumes	15
Assign physical volumes to volume groups	Managing Logical Volumes	15
Create and delete logical volumes	Managing Logical Volumes	15
Configure systems to mount file systems at boot by universally unique ID (UUID) or label	Managing Storage	14
Add new partitions and logical volumes, and swap to a system nondestructively	Managing Storage	14

Objective	Chapter Title	Chapter
Create and configure file systems		
Create, mount, unmount, and use vfat, ext4, and xfs file systems	Managing Storage	14
Mount and unmount network file systems using NFS	Accessing Network Storage	24
Configure autofs	Accessing Network Storage	24
Extend existing logical volumes	Managing Logical Volumes	15
Diagnose and correct file permission problems	Permissions Management	7
Deploy, configure, and maintain systems		
Schedule tasks using at cron and systemd timer units	Scheduling Tasks	12
Start and stop services and configure services to start automatically at boot	Working with Systemd	11
Configure systems to boot into a specific target automatically	Managing and Understanding the Boot Procedure	17
Configure time service clients	Configuring Time Services	25
Install and update software packages from Red Hat Content Delivery Network, a remote repository, or from the local file system	Managing Software	9
Modify the system bootloader	Managing and Understanding the Boot Procedure	17
Manage basic networking		
Configure IPv4 and IPv6 addresses	Configuring Networking	8
Configure hostname resolution	Configuring Networking	8
Configure network services to start automatically at boot	Configuring Networking	8
Restrict network access using firewalld and firewall-cmd	Configuring a Firewall	23
Manage users and groups		
Create, delete, and modify local user accounts	User and Group Management	6
Change passwords and adjust password aging for local user accounts	User and Group Management	6
Create, delete, and modify local groups and group memberships	User and Group Management	6
Configure privileged access	User and Group Management	6

Objective	Chapter Title	Chapter
Manage security		
Configure firewall settings using firewall-cmd/ firewalld	Configuring a Firewall	23
Manage default file permissions	Permissions Management	7
Configure key-based authentication for SSH	Configuring SSH	20
Set enforcing and permissive modes for SELinux	Managing SELinux	22
List and identify SELinux file and process context	Managing SELinux	22
Restore default file contexts	Managing SELinux	22
Manage SELinux port labels	Managing SELinux	22
Use Boolean settings to modify system SELinux settings	Managing SELinux	22

Figure Credits

Cover image: ARAMYAN/Adobe Stock

Figure 1-1 through Figure 1-12, Figure 5-1 through Figure 5-3, Figures 8-1, 8-2, 8-4 and 8-5, Figure 10-1, Figure 11-1, Figure 18-1 through Figure 18-5: Red Hat, Inc.

Figure 2-1, Figure 2-2: Linux

Figure 8-3: GNOME Project

Working with Text Files

Since the early days of UNIX, working with text files has been an important administrator skill. Even on modern Linux versions such as Red Hat Enterprise Linux 10, working with text files is still an important skill, as everything you do on Linux is stored as a text file. By applying the correct tools, you'll easily find and modify the configuration of everything. This chapter is about these tools. Make sure that you master them well, because good knowledge of these tools really will make your work as a Linux administrator a lot easier. At the same time, it will increase your chances of passing the RHCSA exam.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 4-1 lists the major headings in this chapter and their 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 and Review Questions."

Table 4-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Using Common Text File–Related Tools	1–5
A Primer to Using Regular Expressions	6–8
Using **grep** to Analyze Text	10
Working with Other Useful Text Processing Utilities	9

1. Which command was developed to show only the first couple of lines in a text file?
   a. **head**
   b. **top**
   c. **first**
   d. **cat**

2. Which command enables you to count the number of words in a text file?

   a. **count**
   b. **list**
   c. **ls -l**
   d. **wc**

3. Which key on your keyboard do you use in **less** to go to the last line of the current text file?

   a. End
   b. Page Down
   c. q
   d. G

4. Which option is missing (…) from the following command, assuming that you want to filter the first field out of the /etc/passwd file and assuming that the character that is used as the field delimiter is a :?

```
cut ... : -f 1 /etc/passwd
```

   a. **-d**
   b. **-c**
   c. **-t**
   d. **-x**

5. Which option is missing (…) if you want to sort the third column of the output of the command **ps aux**?

```
ps aux | sort ...
```

   a. **-k3**
   b. **-s3**
   c. **-k f 3**
   d. **-f 3**

6. Which of the following commands would only show lines in the file /etc/passwd that start with the text *anna*?

   a. **grep anna /etc/passwd**
   b. **grep -v anna /etc/passwd**
   c. **grep $anna /etc/passwd**
   d. **grep ^anna /etc/passwd**

7. Which regular expression do you use to make the previous character optional?

   a. ?

   b. .

   c. *

   d. &

8. Which regular expression do you use if you want the preceding character to occur at least one time?

   a. ?

   b. .

   c. *

   d. +

9. Assuming that the field delimiter : is used, which command prints the fourth field of a line in the /etc/passwd file if the text *user* occurs in that line?

   a. **awk '/user/ { print $4 }' /etc/passwd**

   b. **awk -d : '/user/ { print $4 }' /etc/passwd**

   c. **awk -F : '/user/ $4' /etc/passwd**

   d. **awk -F : '/user/ { print $4 }' /etc/passwd**

10. Which option would you use with **grep** to show only lines that do *not* contain the regular expression that was used?

    a. **-x**

    b. **-v**

    c. **-u**

    d. **-q**

Foundation Topics

Using Common Text File–Related Tools

Before we start talking about the best possible way to find text files containing specific text, let's take a look at how you can display text files in an efficient way. Table 4-2 provides an overview of some common commands often used for this purpose.

Key Topic

Table 4-2 Essential Tools for Managing Text File Contents

Command	Explanation
less	Opens the text file in a pager, which allows for easy reading
cat	Dumps the contents of the text file on the screen
head	Shows the top of the text file
tail	Shows the bottom of the text file
cut	Used to filter specific columns or characters from a text file
sort	Sorts the contents of a text file
wc	Counts the number of lines, words, and characters in a text file

Apart from their use on a text file, these commands may also prove very useful when used with pipes. You can use the command **less /etc/passwd**, for example, to open the contents of the /etc/passwd file in the **less** ***pager***, but you can also use the command **ps aux | less**, which sends the output of the command **ps aux** to the **less** pager to allow for easy reading.

Doing More with less

In many cases, as a Linux administrator you'll need to read the contents of text files. The **less** utility offers a convenient way to do so. To open the contents of a text file in **less**, just type **less** followed by the name of the file you want to see, as in **less /etc/passwd**.

From **less**, you can use the Page Up and Page Down keys on your keyboard to browse through the file contents. Seen enough? Then you can press **q** to quit **less**. Also very useful is that you can easily search for specific contents in **less** using **/sometext** for a forward search and **?sometext** for a backward search. Repeat the last search by using **n**.

If you think this sounds familiar, it should. You have seen similar behavior in **vim** and **man**. The reason is that all of these commands are based on the same code.

NOTE Once upon a time, **less** was developed because it offered more features than the classical UNIX tool **more,** which was developed to go through file contents page by page. So, the idea was to do more with **less**. The **more** developers did not like that, so they enhanced the features of the **more** command as well. The result is that both **more** and **less** offer many features that are similar, and which tool you use doesn't really matter that much anymore. There is one significant difference, though, and that is the **more** utility ends if the end of the file is reached. To prevent this behavior, you can start **more** with the **-p** option. Another difference is that the **more** tool is a standard part of any Linux and UNIX installation. This is not the case for **less**, which may have to be installed separately.

In Exercise 4-1, you apply some basic **less** skills to work with file contents and command output.

Exercise 4-1 Applying Basic less Skills

1. From a terminal, type **less /etc/passwd**. This opens the /etc/passwd file in the **less** pager.
2. Type **/root** to look for the text *root*. You'll see that all occurrences of the text *root* are highlighted.
3. Press **G** to go to the last line in the file.
4. Press **q** to quit **less**.
5. Type **ps aux | less**. This sends the output of the **ps aux** command (which shows a listing of all processes) to **less**. Browse through the list.
6. Press **q** to quit **less**.

Showing File Contents with cat

The **less** utility is useful to read long text files. If a text file is not that long, you are probably better off using **cat**, which just dumps the contents of the text file on the terminal it was started from. This is convenient if the text file is short. If the text file is long, however, you'll see all contents scrolling by on the screen, and only the lines that fit on the terminal screen are displayed. Using **cat** is simple. Just type **cat** followed by the name of the file you want to see. For instance, use **cat /etc/passwd** to show the contents of this file on your computer screen.

TIP The **cat** utility dumps the contents of a file to the screen from the beginning to the end, which means that for a long file you'll see the last lines of the file only. If you are interested in the first lines, you can use the **tac** utility, which gives the inversed result of **cat**.

Displaying the First or Last Lines of a File with head and tail

If a text file contains much information, it can be useful to filter the output a bit. You can use the **head** and **tail** utilities to do that. Using **head** on a text file will show by default the first ten lines of that file. Using **tail** on a text file shows the last ten lines by default. You can adjust the number of lines that are shown by adding **-n** followed by the number you want to see. So, **tail -n 5 /etc/passwd** shows the last five lines of the /etc/passwd file.

TIP With older versions of **head** and **tail**, you had to use the **-n** option to specify the number of lines you wanted to see. With current versions of both utilities, you may also omit the **-n** option. So, using either **tail -5 /etc/passwd** or **tail -n 5 /etc/passwd** gives you the exact same results.

Another useful option that you can use with **tail** is **-f**. This option starts by showing you the last ten lines of the file you've specified, but it refreshes the display as new lines are added to the file. This is convenient for monitoring log files. The command **tail -f /var/log/messages** (which has to be run as the root user) is a common command to show in real time messages that are written to the main log file /var/log/messages. To end this command, press Ctrl-C.

By combining **tail** and **head**, you can do smart things as well. Suppose, for instance, that you want to see line number 11 of the /etc/passwd file. To do that, use **head -n 11 /etc/passwd | tail -n 1**. The command before the pipe shows the first 11 lines from the file. The result is sent to the pipe, and on that result **tail -n 1** is used, which leads to only line number 11 being displayed. In Exercise 4-2, you apply some basic **head** and **tail** operations to get the exact results that you want.

Exercise 4-2 Using Basic head and tail Operations

1. From a root shell, type **tail -f /var/log/messages**. You'll see the last lines of /var/log/messages being displayed. The file doesn't close automatically.
2. Press Ctrl-C to quit the previous command.
3. Type **head -n 5 /etc/passwd** to show the first five lines in /etc/passwd.
4. Type **tail -n 2 /etc/passwd** to show the last two lines of /etc/passwd.
5. Type **head -n 5 /etc/passwd | tail -n 1** to show only line number 5 of the /etc/passwd file.

Filtering Specific Columns with cut

When you're working with text files, it can be useful to filter out specific fields. Imagine that you need to see a list of all users in the /etc/passwd file. In this file, several fields are defined, of which the first contains the name of the users who are defined. To filter out a specific field, the **cut** command is useful. To do this, use the **-d** option to specify the field delimiter followed by **-f** with the number of the specific field you want to filter out. So, the complete command is **cut -d : -f 1 /etc/passwd** if you want to filter out the first field of the /etc/passwd file. You can see the result in Example 4-1.

Example 4-1 Filtering Specific Fields with **cut**

```
[root@localhost ~]# cut -d : -f 1 /etc/passwd
root
bin
daemon
adm
lp
sync
shutdown
halt
...
```

Sorting File Contents and Output with sort

Another very useful command to use on text files is **sort**. As you can probably guess, this command sorts text. If you type **sort /etc/passwd**, for instance, the content of the /etc/passwd file is sorted in byte order. You can use the **sort** command on the output of a command also, as in **cut -f 1 -d : /etc/passwd | sort**, which sorts the contents of the first column in the /etc/passwd file.

By default, the **sort** command sorts in byte order, which is the order in which the characters appear in the ASCII text table. Notice that this looks like alphabetical order, but it is not, as all capital letters are shown before lowercase letters. So *Zoo* would be listed before *apple*. In some cases, that is not convenient because the content that needs sorting may be numeric or in another format. The **sort** command offers different options to help sorting these specific types of data. Type, for instance, **cut -f 3 -d : /etc/passwd | sort -n** to sort the third field of the /etc/passwd file in numeric order. It can be useful also to sort in reverse order; if you use the command **du -h | sort -rn**, you get a list of files sorted with the biggest file in that directory listed first.

You can also use the **sort** command and specify which column you want to sort. To do this, use **sort -k3 -t : /etc/passwd**, for instance, which uses the field separator : to sort the third column of the /etc/passwd file. Add **-n** to the command to sort in a numeric order, and not in an alphabetic order.

Another example is shown in Example 4-2, where the output of the **ps aux** command is sorted. This command gives an overview of processes running on a Linux system. The fourth column indicates memory usage percentage, and by applying a numeric sort to the output of the command, you can see that the processes are sorted by memory usage, such that the process that consumes the most memory is listed last.

Example 4-2 Using **ps aux** to Find the Busiest Processes on a Linux Server

```
[root@localhost ~]# ps aux | sort -k 4 -n
root          897  0.3  1.1 348584 42200 ?         v  08:12   0:00
   /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid
student      2657  1.0  1.1 2936188 45200 ?        Ssl  08:14   0:00
   /usr/bin/gjs /usr/share/org.gnome.Characters/org.gnome.Characters.
BackgroundService
student      2465  0.3  1.3 143976 52644 ?         S    08:14   0:00
   /usr/bin/Xwayland :0 -rootless -noreset -accessx -core -auth /
   run/user/1000/.mutter-Xwaylandauth.0SRUV1 -listenfd 4 -listenfd 5
   -displayfd 6 -initfd 7
student      2660  1.9  1.4 780200 53412 ?         Ssl  08:14   0:00
   /usr/libexec/gnome-terminal-server
root         2480  2.1  1.6 379000 61568 ?         Ssl  08:14   0:00
   /usr/bin/python3 /usr/libexec/rhsm-service
student      2368  0.9  1.6 1057048 61096 ?        Sl   08:14   0:00
   /usr/libexec/evolution-data-server/evolution-alarm-notify
root         1536  0.6  1.8 555908 69916 ?         Ssl  08:12   0:00
   /usr/libexec/packagekitd
student      2518  0.6  1.8 789408 70336 ?         Ssl  08:14   0:00
   /usr/libexec/gsd-xsettings
student      2540  0.5  1.8 641720 68828 ?         Sl   08:14   0:00
   /usr/libexec/ibus-x11 --kill-daemon
student      2381  4.7  1.9 1393476 74756 ?        Sl   08:14   0:00
   /usr/bin/gnome-software --gapplication-service
student      2000 16.0  7.8 3926096 295276 ?       Ssl  08:14   0:03
   /usr/bin/gnome-shell
```

Counting Lines, Words, and Characters with wc

When working with text files, you sometimes get a large amount of output. Before deciding which approach to handling the large amount of output works best in a

specific case, you might want to have an idea about the amount of text you are dealing with. In that case, the **wc** command is useful. In its output, this command gives three different results: the number of lines, the number of words, and the number of characters.

Consider, for example, the **ps aux** command. This command gives a list of all processes running on a server. One solution to count how many processes there are exactly is to pipe the output of **ps aux** through **wc**, as in **ps aux | wc**. You can see the result of the command in Example 4-3, which shows that the total number of lines is 90 and that there are 1,045 words and 7,583 characters in the command output.

Example 4-3 Counting the Number of Lines, Words, and Characters with **wc**

```
[root@localhost ~]# ps aux | wc
     90       1045    7583
```

A Primer to Using Regular Expressions

Working with text files is an important skill for a Linux administrator. You must know not only how to create and modify existing text files, but also how to find the text file that contains specific text.

It will be clear sometimes which specific text you are looking for. Other times, it might not. For example, are you looking for *color* or *colour*? Both spellings might give a match. This is just one example of why using flexible patterns while looking for text can prove useful. In Linux these flexible patterns are known as ***regular expressions***, often also referred to as *regex*.

To understand regular expressions a bit better, let's take a look at a text file example, shown in Example 4-4. This file contains the last six lines from the /etc/passwd file. (This file is used for storing Linux accounts; see Chapter 6, "User and Group Management," for more details.)

Example 4-4 Sample Lines from **/etc/passwd**

```
[root@localhost ~]# tail -n 6 /etc/passwd
anna:x:1000:1000::/home/anna:/bin/bash
rihanna:x:1001:1001::/home/rihanna:/bin/bash
annabel:x:1002:1002::/home/annabel:/bin/bash
anand:x:1003:1003::/home/anand:/bin/bash
joanna:x:1004:1004::/home/joanna:/bin/bash
joana:x:1005:1005::/home/joana:/bin/bash
```

Now suppose that you are looking for the user anna. In that case, you could use the general regular expression parser **grep** to look for that specific string in the file/tc/passwd by using the command **grep anna /etc/passwd**. Example 4-5 shows the results of that command, and as you can see, way too many results are shown, as the string *anna* occurs in other strings as well.

Example 4-5 Example of Why You Need to Know About Regular Expressions

```
[root@localhost ~]# grep anna /etc/passwd
anna:x:1000:1000::/home/anna:/bin/bash
rihanna:x:1001:1001::/home/rihanna:/bin/bash
annabel:x:1002:1002::/home/annabel:/bin/bash
joanna:x:1004:1004::/home/joanna:/bin/bash
```

Key Topic

A *regular expression* is a search pattern that enables you to look for specific text in an advanced and flexible way.

Using Line Anchors

In Example 4-5, suppose that you wanted to specify that you are looking for lines that start with the text *anna*. The type of regular expression that specifies where in a line of output the result is expected is known as a ***line anchor***.

To show only lines that start with the text you are looking for, you can use the regular expression ^ (in this case, to indicate that you are looking only for lines where *anna* is at the beginning of the line; see Example 4-6).

Example 4-6 Looking for Lines Starting with a Specific Pattern

```
[root@localhost ~]# grep ^anna /etc/passwd
anna:x:1000:1000::/home/anna:/bin/bash
annabel:x:1002:1002::/home/annabel:/bin/bash
```

Another regular expression that relates to the position of specific text in a specific line is $, which states that the line ends with some text. For instance, the command **grep ash$ /etc/passwd** shows all lines in the /etc/passwd file that end with the text *ash*. This command shows all accounts that have a shell and are able to log in (see Chapter 6 for more details).

Using Escaping in Regular Expressions

Although not mandatory, when you're using regular expressions, it is a good idea to use ***escaping*** to prevent regular expressions from being interpreted by the shell. When a command line is entered, the Bash shell parses the command line, looking for any special characters like *, $, and ?. It will next interpret these characters. The point is that regular expressions use some of these characters as well, and to make sure the Bash shell doesn't interpret them, you should use escaping.

In many cases, it is not really necessary to use escaping, as often no special characters occur; in some cases, the regular expression fails without escaping. To prevent this from ever happening, it is a good idea to put the regular expression between single quotes. So, instead of typing **grep ^anna /etc/passwd**, it is better to use **grep '^anna' /etc/passwd**, even if in this case both examples work.

Using Wildcards and Multipliers

In some cases, you might know which text you are looking for, but you might not know how the specific text is written. Or you might just want to use one regular expression to match different patterns. In those cases, wildcards and multipliers come in handy.

To start with, there is the dot (.) regular expression. This is used as a ***wildcard*** character to look for one specific character. So, the regular expression **r.t** would match the strings *rat*, *rot*, and *rut* and any other string of three characters that starts with *r* and ends with *t*.

In some cases, you might want to be more specific about the characters you are looking for. If that is the case, you can specify a range of characters that you are looking for. For instance, the regular expression **r[aou]t** matches the strings *rat*, *rot*, and *rut* but it wouldn't match *rit* and *ret* or any other string of three characters that starts with *r* and ends with *t*.

Another useful regular expression is the ***multiplier*** *. This matches zero or more of the previous character. That does not seem to be very useful, but indeed it is, as you will see in the examples at the end of this section.

If you know exactly how many of the previous character you are looking for, you can specify a number also, as in **re\{2\}d**, which would match *reed*, but not *red*. The last regular expression that is useful to know about is ?, which matches zero or one of the previous character. Table 4-3 provides an overview of the most important regular expressions.

Key Topic

Table 4-3 Most Significant Regular Expressions

Regular Expression	Use
^text	Matches line that starts with specified text.
text$	Matches line that ends with specified text.
.	Wildcard. (Matches any single character.)
[abc]	Matches *a*, *b*, or *c*.
?	Extended regular expression that matches zero or one of the preceding character.
+	Extended regular expression that matches one or more of the preceding character.
*	Matches zero to an infinite number of the previous character.
\{2\}	Matches exactly two of the previous character.
\{1,3\}	Matches a minimum of one and a maximum of three of the previous character.
colou?r	Matches zero or one of the previous character. This makes the previous character optional, which in this example would match both *color* and *colour*.
(…)	Used to group multiple characters so that the regular expression can be applied to the group.

Using Extended Regular Expressions

What makes regular expressions sometimes a bit hard to understand is the fact that there are different sets of regular expressions. The base regular expressions as discussed so far are supported by tools like **grep**. There is also a set of extended regular expressions, which is not supported by default. When used with **grep**, you'll have to add the **-E** option to indicate it is an extended regular expression. The + can be used to indicate that a character should occur one or more times, and the ? is used to indicate that a character should occur zero or one times. When used in **grep**, don't forget to use **grep -E** to ensure that these are interpreted as extended regular expressions! Alternatively, use the **egrep** utility while dealing with extended regular expressions.

Let's take a look at an example of a regular expression that comes from the man page semanage-fcontext and relates to managing SELinux (see Chapter 22, "Managing SELinux"). The sample line contains the following regular expression:

```
"web(/.*)?"
```

In this regular expression, the text */web* is referred to. This text string can be followed by the regular expression (/.*)?. To understand the regular expression, start with the ?, which refers to the part between braces and indicates that the part between braces may occur zero times or one time. Within the braces, the pattern starts with a slash, which is just a slash, followed by a dot, which represents one character, which on its turn is followed by an *, which indicates zero or more characters of the preceding. So this means that just the directory name gives a match, but also the directory name followed by just a slash, or a slash that is followed by a filename.

What makes regular expressions difficult is that there is not just one set of regular expressions; there are also extended regular expressions. And to make the concept more complex, the extended regular expressions need specific commands. The well-known command **grep** (covered next) by default deals with base regular expressions. If you want to use extended regular expressions, you need **grep -E** or **egrep**.

Two common extended regular expressions are + and ?. The + will look for a pattern where the preceding character occurs one or more times, and the ? looks for a pattern where the preceding character does not occur or occurs one time. Use the following procedure to find out how these extended regular expressions can be confusing:

Step 1. Create a text file with the name **regex.txt** and the following contents:

```
bat
boot
boat
bt
```

Step 2. Use **grep 'b.*t' regex.txt** to see any line that starts with a *b* and ends with a *t*.

Step 3. Use **grep 'b.+t' regex.txt**. You might expect to see only lines that have at least three characters, but you don't, because you are using an extended regular expression, and without using any additional options, **grep** doesn't recognize the extended regular expression.

Step 4. Use **grep -E 'b.+t' regex.txt**. Now you see that the extended regular expression does work as expected.

Using grep to Analyze Text

The ultimate utility to work with regular expressions is **grep**, which stands for "general regular expression parser." Quite a few examples that you have seen already were based on the **grep** command. The **grep** command has a couple of useful options to make it even more efficient. Table 4-4 describes some of the most useful options.

Key Topic

Table 4-4 Most Useful **grep** Options

Option	Use
-i	Matches upper- and lowercase letters (i.e., not case sensitive).
-v	Shows only lines that do *not* contain the regular expression.
-r	Searches files in the current directory and all subdirectories.
-e	Searches for lines matching more than one regular expression. Use **-e** before each regular expression you want to use.
-E	Interprets the search pattern as an extended regular expression.
-A <number>	Shows <number> of lines after the matching regular expression.
-B <number>	Shows <number> of lines before the matching regular expression.

In Exercise 4-3, you work through some examples using these **grep** options.

Exercise 4-3 Using Common grep Options

1. Type **grep '^#' /etc/services**. This shows that the file /etc/services contains a number of lines that start with the comment sign, #.
2. To view the configuration lines that really matter, type **grep -v '^#' /etc/services**. This shows only lines that do not start with a #.
3. Type **grep -v '^#' /etc/services -B 5**. This shows lines that do not start with a # sign but also the five lines that are directly before each of those lines, which is useful because in the preceding lines you'll typically find comments on how to use the specific parameters. However, you'll also see that many blank lines are displayed.
4. Type **grep -v -e '^#' -e '^$' /etc/services**. This excludes all blank lines and lines that start with #.

Working with Other Useful Text Processing Utilities

The **grep** utility is a powerful utility that allows you to work with regular expressions. It is not the only utility, though. Some even more powerful utilities exist, like **awk** and **sed**, both of which are extremely rich and merit a book by themselves. The utilities were developed in the time that computers did not commonly have screens attached, and for that reason they do a good job of treating text files in a scripted way.

As a Linux administrator in the twenty-first century, you do not have to be a specialist in using these utilities anymore. It does make sense, however, to know how

to perform some common tasks using these utilities. The most useful use cases are summarized in the following examples.

This command shows the fourth field from /etc/passwd:

```
awk -F :   '{ print $4 }'  /etc/passwd
```

This is something that can be done by using the **cut** utility as well, but the **awk** utility is more successful in distinguishing the fields that are used in command output of files. The bottom line is that if **cut** does not work, you should try the **awk** utility.

You can also use the **awk** utility to do tasks that you might be used to using **grep** for. Consider the following example:

```
awk -F : '/user/ { print $4 }' /etc/passwd
```

This command searches the /etc/passwd file for the text *user* and will print the fourth field of any matching line.

In this example, the "stream editor" **sed** is used to print the fifth line from the /etc/passwd file:

```
sed -n 5p /etc/passwd
```

The **sed** utility is a very powerful utility for filtering text from text files (like **grep**), but it has the benefit that it also allows you to apply modifications to text files, as shown in the following example:

```
sed -i s/old-text/new-text/g ~/myfile
```

In this example, the **sed** utility is used to search for the text *old-text* in ~/myfile and replace all occurrences with the text *new-text*. Notice that the default **sed** behavior is to write the output to STDOUT, but the option **-i** will write the result directly to the file. Make sure that you know what you are doing before using this command, because it might be difficult to revert file modifications that are applied in this way.

You'll like the following example if you've ever had a utility containing a specific line in a file that was erroneous:

```
sed -i -e '2d' ~/myfile
```

With this command, you can delete a line based on a specific line number. You can also make more complicated references to line numbers. Use, for instance, **sed -i -e '2d;20,25d' ~/myfile** to delete lines 2 and 20 through 25 in the file ~/myfile.

TIP Do not focus on **awk** and **sed** too much. These are amazing utilities, but many of the things that can be accomplished using them can be done using other tools as well. The **awk** and **sed** tools are very rich, and you can easily get lost in them if you are trying to dig too deep.

Summary

In this chapter, you learned how to work with text files. You acquired some important skills like searching text files with **grep** and displaying text files or part of them with different utilities. You also learned how regular expressions can be used to make the search results more specific. Finally, you learned about the very sophisticated utilities **awk** and **sed**, which allow you to perform more advanced operations on text files.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have several choices for exam preparation: the end-of-chapter labs; the memory tables in Appendix C; Chapter 26, "Final Preparation"; and the practice exams.

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the margin of the page. Table 4-5 lists a reference for these key topics and the page number on which each is found.

Key Topic

Table 4-5 Key Topics for Chapter 4

Key Topic Element	Description	Page
Table 4-2	Essential Tools for Managing Text File Contents	82
Paragraph	Definition of a regular expression	88
Table 4-3	Most Significant Regular Expressions	90
Table 4-4	Most Useful **grep** Options	92

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Tables Answer Key," includes completed tables and lists to check your work.

Define Key Terms

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

pager, regular expression, line anchor, escaping, wildcard, multiplier

Review Questions

The questions that follow are meant to help you test your knowledge of concepts and terminology and the breadth of your knowledge. You can find the answers to these questions in Appendix A.

1. Which command enables you to see the results of the **ps aux** command in a way that you can easily browse up and down in the results?
2. Which command enables you to show the last five lines from ~/samplefile?
3. Which command do you use if you want to know how many words are in ~/samplefile?
4. After opening command output using **tail -f ~/mylogfile**, how do you stop showing output?
5. Which **grep** option do you use to exclude all lines that start with either a **#** or a ;?
6. Which regular expression do you use to match one or more of the preceding characters?
7. Which **grep** command enables you to see *text* as well as *TEXT* in a file?
8. Which **grep** command enables you to show all lines starting with *PATH*, as well as the five lines just before that line?
9. Which **sed** command do you use to show line 9 from ~/samplefile?
10. Which command enables you to replace all occurrences of the word *user* with the word *users* in ~/samplefile?

End-of-Chapter Lab

In this end-of-chapter lab, you work with some of the most significant text processing utilities.

Lab 4.1

1. Describe two ways to show line 5 from the /etc/passwd file.
2. How would you locate all text files on your server that contain the current IP address? Do you need a regular expression to do this?
3. You have just used the **sed** command that replaces all occurrences of the text *Administrator* with *root*. Your Windows administrators do not like that very much. How do you revert?
4. Assuming that in the **ps aux** command the fifth line contains information about memory utilization, how would you process the output of that command to show the process that has the heaviest memory utilization first in the results list?
5. Which command enables you to filter the sixth column of **ps aux** output?
6. How do you delete the sixth line from the file ~/myfile?

Index

A

absolute filename, 61
administrative access, granting to a non-root user, 126–127
administrator user, 15–16
advanced permissions
  applying, 157–158
  SGID (set group ID), 155–156
  sticky bit, 156–157
  SUID (set user ID), 155
alias, 29
AlmaLinux, 8
ampersand (&), starting background processes, 231
anacron, 279–280
analyzing SELinux messages, 483–485
Apache web service
  configuration files, 455
    chroot environment, 455
    DocumentRoot parameter, 450
    main configuration file, 455
    ServerRoot parameter, 450
  configuring a basic Apache server, 450
  creating web server content, 453–454
  installing the required software, 450
  virtual hosts, 456–457
applications, Flatpak, 220–221
applying
  advanced permissions, 157–158
  permissions, 152–154
architecture, LVM (Logical Volume Manager), 342–343
archives, 70–72
arguments
  command, 28
  script, 418–419
asterisk (*), 60
at command, 281
atd service, 281
atq command, 281
attributes, user-extended, 160–161
audit log, SELinux messages, retrieving, 481–483
auditd service, 289, 483–485
[auo], 60
authentication
  passphrases, 114
  SSH, 113
autofs, 511–512
  configuring for NFS, 512
  using wildcards, 513–514
automating file system mounts, 331–333
awk command, 92–93

B

background processes, terminating, 233
backslash (\), 423
Bash history, 33–35
Bash shell, C02.xref shell, 28
  command-line completion, 35
bash shell scripting. *See* scripting
batch command, 281
bg command, 231–232
BIOS (Basic Input/Output System), 312
BIOS device names, 172–173

blkid command, 330
Boolean settings, SELinux policies, 479–481
boot loader, C17.xref GRUB 2
boot options, GRUB 2, 390–391
boot procedure, 398–399
  resetting the root password, 407–409
  starting a troubleshooting target, 401–402
  troubleshooting, 399
    using a rescue disk, 403–404
boot prompt
  accessing, 400
  entering boot arguments, 401
bzip2, 72

C

c command, 46
caret (^), 88
case statement, 426–427
cat command, 83
cd command, 61
Centos Stream, 8
Cert Guide environment, 10
cgroups, 237. *See also* slices
chage command, 135–136
changing
  group ownership, 149–150
  ownership, 149
chattr command, 161
chcon command, 473
chgrp command, 150
chmod command, 153–154, 157–158
chown command, 149
chrony service, 527–528
chroot environment, 455
chvt command, 105–106
ClientAliveCountMax option, SSH (Secure Shell), 440
ClientAliveInterval option, SSH (Secure Shell), 440
closed source drivers, 365
Cockpit, 114–115
  administrative access, 115
  performing common tasks, 115–116
  user interface, 115
command mode, vim, 36
command-line completion, 35
commands, 29–30. *See also* options; tools; utilities
  alias, 29
  arguments, 28
  at, 281
  atq, 281
  awk, 92–93
  batch, 281
  bg, 231–232
  blkid, 330
  c, 46
  cat, 83
  cd, 61
  chage, 135–136
  chattr, 161
  chcon, 473
  chgrp, 150
  chmod, 153–154, 157–158
  chown, 149
  chvt, 105–106
  cp, 63–64
  crontab, 277–278
  cut, 85
  date, 522
  df -Th, 58, 59
  dnf, 196–197, 204
  dnf group info, 213
  dnf group list, 212–213
  dnf history, 214
  dnf info, 206–207
  dnf install map, 208–209
  dnf list, 209–210
  dnf search, 205
  dnf update, 210–211
  dnf upgrade, 375
  echo, 40

egrep, 90–91
exit, 417
external, 29
fg, 231–232
findmnt, 58
Flatpak, 220–221
foreground jobs, 230–231
fsck, 407
FTP, 112
getenforce, 469
getent hosts, 189
grep, 90–92
groupadd, 139
groupmems, 139–140
groupmod, 139–140
head, 84
--help option, 42
hostnamectl status, 367–368
hwclock, 522
id, 124
ifconfig, 178
internal, 29
ip addr show, 174–175
ip link show, 175–176
ip route show, 176–177
jobs, 231–233
journalctl, 288–289, 292–296, 483
kill, 233, 239–240
killall, 240–241
less, 82–83
ln, 68
logger, 304
ls, 62–63, 68–69
ls -l, 148–149, 157
lsblk, 58, 315, 349
lsmod, 371
lspci, 373–374
lvextend, 354–355
lvresize, 355
man, 42
man -f, 45
man -k, 42–46
mkdir, 61
modinfo, 371–373
more, 83
mount, 56–58, 329
mv, 64–65
newgrp, 150–151
nice, 239
nmcli, 178–179, 180–182, 187–189
nmtui, 178–179, 182–184
nohup, 233
options, 28
passwd, 135–136
pipes, 32
pkexec, 128
pkill, 240–241
ps, 235–236
ps aux, 86, 234, 364–365
pv, 345
pvcreate --help, 345–346
pvdisplay, 348–349
renice, 239
restorecon, 477–479
rm, 65
rmdir, 61
rpm, 215, 216–217
rsync, 113
scp, 111–112
sealert, 484
sed, 93–94
semanage, 473–475
semanage port, 479
sestatus, 469–470
sftp, 112
showmount, 509–510
sort, 85–86
ss -lt, 177
ssh, 108–111
ssh-copy-id, 114
ssh-keygen, 114
su, 125–126
su -, 104
subscription-manager, 197–198

sudo, 103, 104, 125, 126–127
syntax, 28
systemctl cat, 254–255, 264, 383
systemctl disable, 384
systemctl edit, 263
systemctl enable, 254, 384
systemctl halt, 108
systemctl isolate, 387
systemctl list-dependencies, 260–262
systemctl poweroff, 108
systemctl status, 258–260, 274–275, 289–290
systemctl -t target, 385–387
tail, 84
tail -f, 292
tar, 70–74
timedatectl, 522, 523–524
top, 242–243
tuned-adm, 245
type, 29
tzselect, 526–527
udevadm monitor, 369–370
umount, 329
uname, 367
usermod, 139–140
vgcreate, 350
vgdisplay, 350–351
vigr, 138
vimtutor, 36
visudo, 127
wc, 86–87
xfs_admin, 327
comments, script, 416–417
community distributions, 8
compression programs, 72
conditional loops, scripting, 419, 422
configuration files, 35
/etc/anacrontab, 279–280
/etc/default/useradd, 135
/etc/fstab, 331–333
/etc/hosts, 185–187
/etc/login.defs, 135
/etc/NetworkManager/system-connections/, 184–185
/etc/passwd, 129–131
/etc/shadow, 131–132
Apache, 455
DocumentRoot parameter, 450–453
main configuration file, 455
ServerRoot parameter, 450
virtual hosts, 456–457
chrony, 527–528
cron, 276–279
environment, 40
GRUB 2, 390
logrotate.conf, 303
modifying, 133
repository, 199–200
rsyslogd, 298, 301–302
console, 102–103. *See also* logging in
context labels, SELinux, 471
finding the context type you need, 476–477
monitoring, 471–473
restoring default file contexts, 477–479
setting context types, 473–475
setting on a nondefault Apache DocumentRoot, 475
copying files and directories, 63–64, 111–112
counting, lines, words, and characters, 86–87
cp command, 63–64
creating
file systems, 323–325, 351
groups, 138
using groupadd, 139
with vigr, 138
links, 68–69
logical volumes, 344–346, 351
MBR partitions, 316–318
physical volumes, 346–349
repositories, 202–203
user accounts, 136–137

user environment, 136
users, 132–133
modifying the configuration file, 133
using useradd, 133
VG (volume group), 350–351
cron
anacron, 279–280
configuration files, 276–279
cron jobs
directories, 278–279
environment variables, 278
starting, 277–278
security, 280
time and date fields, 276
crond service, 274–275
crontab command, 277–278
/etc/crontab, 276–279
Ctrl-C, stopping jobs, 231
Ctrl-D, stopping jobs, 231
Ctrl-Z, stopping jobs, 231
cut command, 85

D

daemons, 230, 274. *See also* cron
date command, 522
debugging, scripts, 427–428
decompressing files, 72
dedicated mounts, 55–56
default ownership, 150–151
default permissions, 159–160
default shell, 134
deleting files and directories, 65
dependencies, 196–197, 215
managing, 260–262
target, 383
targets, 257
desktop virtualization, Cert Guide environment, 10
device mapper, 352
device names (LVM), 352–353
devices
dedicated mounts, 55–56
mounts, 55, 58
df -Th command, 58, 59
DHCP (Dynamic Host Configuration Protocol), 172
diagnosing SELinux policy violations, 481–483
dictionary attacks, 436
direct write, 288
directories, C03.xref mounts, 60–61
copying, 63–64
cron job, 278–279
deleting, 65
listing, 62–63
moving, 64–65
disk devices, 315–316
disk labels, 330–331
displaying
contents of text files, 83
kernel information, 371–373
/proc file system, 367
hostnamectl status command, 367–368
uname command, 367
lists of packages, 209–210
ownership, 148–149
running process information, 235–236
dmesg utility, displaying kernel information, 366–367
dnf command, 196–197, 204
dnf config-manager tool, 199
dnf group info command, 213
dnf group list command, 212–213
dnf history command, 214
dnf info command, 206–207
dnf install map command, 208–209
dnf list command, 209–210
dnf search command, 205
dnf update command, 210–211
dnf upgrade command, 375
DNS name resolution, 187–189
dollar sign ($), 88
dot (.) regular expression, 89

drivers, 365
  checking availability, 373–374
  hardware initialization, 368–370
dumb terminal, 106
dump utility, 333
dynamically assigned IP addresses, 172

E

echo command, 40
egrep command, 90–91
elif statement, 422
emergency reset, 108
end-of-chapter labs, 10
enforcing mode, SELinux, 467–468
epoch time, 522
escaping, 89
essential commands
  LVM (Logical Volume Manager), 353
  vim, 36–37
exam. *See* RHCSA exam
execute permissions, 152
  applying, 152–154
  script, 417
exit command, 417
exit statement, scripting, 417
Ext4, managing system properties, 325–327
extended partitions, 318–320
extended regular expressions, 90–91
external commands, 29
extracting, tar files, 71–72

F

facilities, 298, 300
fdisk utility, 315, 316–318
  creating GPT partitions, 320–322
  creating logical partitions, 318–320
Fedora, 8
fg command, 231–232
FHS (Filesystem Hierarchy Standard), 54–55
file and directory ownership, 148
file descriptors, 31
file management, C03.xref mounts, 60, 65–66. *See also* ownership; permissions
  absolute filename, 61
  archives, 70–72
  compression, 72
  copying files and directories, 63–64
  deleting files and directories, 65
  directories, 60–61
  hard links, 66–67
  hidden files, 63
  links, 66
    creating, 68–69
    removing, 69
    symbolic, 67, 69–70
  listing files and directories, 62–63
  moving files and directories, 64–65
  relative filename, 62
  symbolic links, 67
  synchronizing files, 113
  using sftp command, 112
  wildcards, 60
file permissions, 463
file systems
  creating, 323–325, 351
  Ext4, managing system properties, 325–327
  mounting, 329
    automatic, 331–333
    manual method, 329
    Systemd, 334–335
    using device names, UUIDs, or disk labels, 330–331
  resizing, 354–356
  root directory, 55
  troubleshooting, 407
  XFS, managing system properties, 327
filtering, text files, 85
final preparation. *See also* RHCSA exam
  during the exam, 535–536
  exam day, 534–535

registering for the exam, 533–534
verifying your readiness, 533
finding, software packages, 204–206
findmnt command, 58
firewall-cmd tool, 496–500
Firewalld, 493
configuring, 496–500
services, 495–496
zones, 494
firewalling
iptables, 493
netfilter, 493
nftables, 493
fixed IP address, 172
Flatpak, 219–220
applications, 220–221
installing, 220
remotes, 220
for conditional statement, 424–425
for loops, scripting, 419
forcing a reset, 108
foreground jobs, 230–231
forking, 409
formatting a partition, 324–325
fsck command, 407
/etc/fstab, 331–333
FTP commands, 112

G

GB, 9
gdisk utility, 315
getenforce command, 469
getent hosts command, 189
GiB, 9
GNOME, 183–184
GPG key, 200–202
GPT (GUID Partition Table) partitions, 313
creating with fdisk, 320–322
creating with parted, 322–323
granting administrator permissions, 126–127
graphical environment, switching between terminals, 103–104
grep command, 90–92
group ownership, changing, 149–150
groupadd command, 139
groupmems command, 139–140
groupmod command, 139–140
groups
creating, 138
using groupadd, 139
with vigr, 138
primary, 137
properties, 139–140
secondary, 138
GRUB 2, 388–389
boot options, 390–391
boot prompt
accessing, 400
entering boot arguments, 401
starting a troubleshooting target, 401–402
configuration files, 390
reinstalling, 405, 406
gzip, 72

H

hard drive, partitions. *See also* partitions; storage
GPT, 313
MBR, 312–313
hard links, 69–70
hardening the SSH server, 436
configuring alternative ports, 437
limiting root access, 436–437
limiting user access, 438–439
modifying SELinux to allow for port changes, 437–438
hardware
drivers, checking availability, 373–374
initialization, 368–370
head command, 84
--help option, 41–42

hexadecimal addresses, 169
hidden files, 63
history, Bash shell, 33–35
home directory, 133–134
host, 168
hostnamectl status command, 367–368
hostnames, 185–187
/etc/hosts, 185–187
hwclock command, 522

I

id command, 124
ifconfig command, 178
if...then...else statement, 422–423
if...then...else...fi statement, scripting, 420–421
initramfs, 388
  recreating using the rescue disk, 405–406
  troubleshooting, 406
input mode, vim, 36
installing
  Apache web service software, 450
  Flatpak, 220
  Red Hat Enterprise Linux, 10–11
    create the storage configuration, 18–19
    creating an administrator user, 15–16
    DVD ISO, 7
    preparation, 6
    reboot to finalize the installation, 19–21
    root user account, 15
    selecting date and time, 14–15
    selecting language and keyboard setting, 11–12
    selecting the installation source, 16–17
    Server with GUI option, 16–18
    set up networking, 19
    setup requirements, 9
    specifying the complete configuration of your server, 12–14
    starting the installation, 19–20
  SELinux-specific man pages, 477
  software packages, 207–209
interface
  Cockpit, 115
  networking, 172
  nmtui, 183–184
internal commands, 29
interpreting, log files, 291–292
I/O redirection, C02.xref redirection, 30–32
ip addr show command, 174–175
IP addresses, 168
  host, 168
  validating, 173–176
ip link show command, 175–176
ip route show command, 176–177
iptables, 493
IPv4 addresses, 168
  binary notation, 170–171
  network masks, 169–170
IPv6 addresses, 168
isolating, targets, 385–387
/etc/issue, 41

J

jobs, stopping, 231. *See also* process management
jobs command, 231–233
journal. *See* Systemd, journal
journalctl command, 288–289, 292–295, 483

K

kernel, 364. *See also* process management
  displaying information about
    /proc file system, 367
    dmesg utility, 366–367
    uname command, 367–368
  drivers, 365
    checking availability, 373–374
    hardware initialization, 368–370

modules, 368
displaying detailed information, 371–373
loading/unloading, 373
managing, 370–371, 373
parameters, 374–375
tainted, 365
threads, 230, 234, 364–365
upgrading, 375
key-based authentication, SSH, 113
kill command, 233, 239–240
killall command, 240–241
killing zombies, 241–242

L

labels, 330–331
less command, 82–83
line anchors, 88
links, 66
creating, 68–69
hard, 66–67, 69–70
removing, 69
symbolic, 67, 69–70
Linux distributions
AlmaLinux, 8
Centos Stream, 8
Fedora, 8
Rocky Linux, 8
listing files and directories, 62–63
lists of packages, displaying, 209–210
ln command, 68
load average, 243–244
loading kernel modules, 373
local time, 524–525
log files, 290–291
interpreting, 291–292
monitoring, 292
rotating, 302–304
logger command, 304
logging
auditd service, 289
journalctl command, 292–296
rsyslogd, 289, 298
configuration files, 298
destination, 299–300
facilities, 298, 300
priority, 298, 301
RULES section, 299
systemd-journald, 288–289
logging in, 111
to a local console, 102–103
to a remote server, 109–111
logical AND (&&), 423–424
logical extent, 355
logical operators, scripting, 423–424
logical OR (||), 423–424
logical partitions, 318–320
logical volumes
creating, 344–346, 351
resizing, 354–356
login shell, 40, 41
/etc/login.defs, 135
loops
case statement, 426–427
conditional, 422
while, 425–436
ls command, 62–63, 68–69
ls -l command, 148–149, 157
lsblk command, 58, 315, 349
lsmod command, 371
lspci command, 373–374
LUNs (logical units), 342
lvextend command, 354–355
LVM (Logical Volume Manager), 342
architecture, 342–343
creating logical volumes, 344–346, 351
creating physical volumes, 346–349
creating the volume group, 350–351
device names, 352–353
essential commands, 353
features, 343–344
file system, creating, 351
logical extent, 355
reducing volume groups, 356

resizing logical volumes, 354–356
resizing volume groups, 354
snapshots, 344
lvresize command, 355

M

MAC addresses, 171
machine slice, 237
man 7 file-hierarchy, 54
man command, 42
man -f command, 45
man -k command, 42–46
man pages, SELinux-specific, installing, 477
man Systemd.directives, 263
managing
dependencies, 260–262
kernel modules, 370–371, 373
permissions, 154
port access, 479–487
shell jobs, 231–233
software, 219
subscriptions, 197–198
targets, 384–385
mandb, updating, 45
MaxSessions option, SSH (Secure Shell), 440
MB (megabyte), 311–314
MBR (Master Boot Record), 312–313
creating extended and logical partitions, 318–320
creating partitions with fdisk, 316–318
managing partitions, 315–316
messages
login, 41
SELinux
analyzing, 483–485
retrieving, 481–483
meta key, 39
MiB (mebibyte), 311–314
mkdir command, 61
modinfo command, 371–373
modules
kernel, 368
displaying detailed information, 371–373
managing, 370–371, 373
parameters, 374–375
loading/unloading, 373
/etc/modules-load.d, 370
monitoring
context labels, 471–473
log files, 292
tar files, 71–72
more command, 83
/etc/motd, 41
mount command, 56–58, 329
mount units, 254–255
mounting file systems, 329
automatic, 331–333
manual method, 329
NFS, 509–510
using fstab, 510–511
NFS (Network File System), using autofs, 511–514
Systemd, 334–335
using device names, UUIDs, or disk labels, 330–331
mounts, 55
dedicated, 55–56
overview, 58
moving files and directories, 64–65
multipliers, 89–90
mv command, 64–65

N

nano, 38–39, 264
NAT (Network Address Translation), 169
netfilter, 493
netstat command, 177
network cards, 172–173
network masks, 169–170
networking

configuring the network with nmtui, 182–184
DHCP (Dynamic Host Configuration Protocol), 172
DNS name resolution, 187–189
hexadecimal addresses, 169
hostnames, 185–187
interfaces, 172
IP addresses, 168
dynamically assigned, 172
fixed, 172
host, 168
IPv4 addresses
binary notation, 170–171
network masks, 169–170
IPv6 addresses, 169
MAC addresses, 171
managing network configuration, 178–179
managing network connections with nmcli, 181–182
NAT (Network Address Translation), 169
network cards, 172–173
permissions required to change configuration, 179
ports, 171–172, 177
private network addresses, 169
protocol, 172
router, 168
validating network address configuration, 173–176
validating routing, 176–177
verifying network settings, 177–178
newgrp command, 150–151
NFS (Network File System), 508
mounting
using autofs, 511–514
using fstab, 510–511
mounting the NFS share, 509–510
security, 508
setting up, 508–509
nftables, 493
nice command, 239
NIS (Network Information Service), 508
nmcli command, 178–179, 180–182, 187–189
nmtui command, 178–179, 182–184
nohup command, 233
nondisclosure agreement, RHCSA exam, 536–537
nongraphical environment, switching between terminals, 105–106
NTP (Network Time Protocol), 521
NVMe devices, 316

O

open source drivers, 365
options
chgrp command, 150
chown command, 149
command, 28
cut command, 85
firewall-cmd, 499–500
grep command, 92
head and tail commands, 84
journalctl command, 296
ls command, 63
mount command, 332
rsync command, 113
sort command, 85–86
ssh, 111
SSH (Secure Shell), 440–441
systemctl command, 258
Systemd timers, 273
tar command, 72–74
output
df -hT command, 59
dmesg utility, 366–367
dnf info map command, 206–207
dnf install map, 208–209
dnf list command, 209
dnf search user, 205
hostnamectl status command, 367–368

ip addr show command, 174
ip link show command, 175
ip route show command, 176
journalctl command, 294–295
lsblk command, 349
lspci command, 374
modinfo command, 372–373
nmcli command, 180
ps aux command, 234, 364–365
ps command, 235–236
pvcreate --help command, 345–346
pvdisplay command, 349
sealert command, 484
semanage command, 475
sestatus command, 469–470
sorting, 85–86
systemctl cat command, 254–255, 383
systemctl list-dependencies command, 260–261
systemctl status command, 275, 289–290
udevadm monitor command, 369–370
verbose, 294
ownership
changing, 149
default, 150–151
displaying, 148–149
file and directory, 148
group, changing, 149–150

P

package dependencies, 196–197
package files, RPM queries, 217–218
package groups, 212–213
packages
finding using dnf command, 204–206
getting more information, 206–207
installing, 207–209
showing lists of, 209–210
updating, 210–211
using dnf for package management, 214
using rpm for package management, 215
parameters
GRUB 2, 390–391
kernel module, 374–375
positional, 418–419
parent-child relations, processes, 233, 239–240
parted utility, 315
creating GPT partitions, 322–323
partitions. *See also* LVM (Logical Volume Manager)
formatting, 324–325
GPT, 313
creating with fdisk, 320–322
creating with parted, 322–323
MBR, 312–313, 315–316
creating extended and logical partitions, 318–320
creating with fdisk, 316–318
swap, adding, 327–328
passphrases, 114
passwd command, 135–136
/etc/passwd, 129–131
passwords, properties, 135–136
$PATH variable, 29
performance, tuned profiles, 244–245
permissions
advanced, 155–157
applying, 157–158
SGID, 155–156
sticky bit, 156–157
SUID, 155–157
applying, 152–154
for changing network configuration, 179
default, 159–160
execute, 152
file, 463
managing, 154
read, 151–152
user-extended attributes, 160–161
write, 152
permissive mode, SELinux, 467–468
physical volumes, 342, 346–349

PID (process identification number), 234
pipes, 32–33
pkexec command, 128
pkill command, 240–241
plus sign (+), 91
policies, SELinux, 467
  Boolean settings, 479–481
  diagnosing and addressing violations, 481–483
PolicyKit, 128
ports, 171–172
  managing access, 479–487
  validating availability, 177
positional parameters, scripting, 418–419
primary group, 137
priority
  process, 238–239
  rsyslogd, 298, 301
private key, 113, 114
private network addresses, 169
privileged users, 124
/proc file system, displaying kernel information, 367
process management, 230. *See also* services; Systemd
  cgroups, 237
  from the command line, 241
  displaying running process information, 235–236
  kernel threads, 234
  load average, 243–244
  parent-child relations, 233, 239–240
  PID (process identification number), 234
  process priorities, 238–239
  process states, 242–243
  shell jobs, 230
    background, 231
    foreground, 230–231
    managing, 231–233
    stopping, 231
  signals, 239–241
  slices, 237–238
  threads, 234
  tuned, 244–245
  zombies, killing, 241–242
properties
  group, 139–140
  password, 135–136
  user, 134
protocol, 172
ps aux command, 86, 234
ps command, 235–236
pseudo terminals, 106–107
public key, 113, 114
pv command, 345
pvcreate --help command, 345–346
pvdisplay command, 348–349

Q-R

queries, RPM, 216–219
question mark (?), 60, 91

read permissions, 151–154
reading, text files, 82–83
rebooting, 107–108
Red Hat
  Centos Stream, 7
  Fedora, 7
  free developer program, 7
Red Hat Enterprise Linux 10
  free alternatives, 7
  free subscription, 6
  installing
    create the storage configuration, 18–19
    creating an administrator user, 15–16
    DVD ISO, 7
    reboot to finalize the installation, 19–21
    root user account, 15
    selecting date and time, 14–15
    selecting language and keyboard setting, 11–12

selecting the installation source, 16–17
Server with GUI option, 16–18
set up networking, 19
setup requirements, 9
specifying the complete configuration of your server, 12–14
starting the installation, 19–20
paid subscription, benefits, 6
Red Hat Customer Portal, 7
registering for support, 197
repositories, 8–9
setup requirements, 9
Red Hat Network, 7
redirection, 31–33
reducing volume groups, 356
regular expressions, 87–88
dot (.), 89
escaping, 89
extended, 90–91
line anchors, 88
multipliers, 89–90
wildcards, 89–90
reinstalling, GRUB 2, 405, 406
relative filename, 62
remote access, SSH, 109–111, 114
remotes, Flatpak, 220
removing, links, 69
removing zombies, 241–242
renice command, 239
repositories, 8–9, 196–197
creating, 202–203
security, 200–202
specifying, 198–200
repository configuration files, 199–200
rescue disk, 403
options, 404
recreating the initramfs, 405–406
reinstalling GRUB 2, 405
restoring system access, 403
resetting the root password, 407–409
resizing
file systems, 354–356
logical volumes, 354–356
volume groups, 354
restorecon command, 477–479
RHCSA exam
nondisclosure agreement, 536–537
registering, 533–534
updates, 579–580
RHEL Lightspeed, 46–47
RHSM (Red Had Subscription Management) tools, 197
rm command, 65
rmdir command, 61
Rocky Linux, 8
root directory, 55
root password, resetting, 407–409
root user account, 15, 124–125
rotating, log files, 302–304
routers, 168
routing, validating, 176–177
rpm command, 215, 216–217
RPM database, querying, 216–217
RPM filename, 216
RPM queries, 217–218
rsync command, 113
rsyslog.conf, 301–302
rsyslogd, 288, 289, 298
configuration files, 298
destination, 299–300
facilities, 298, 300
priority, 298, 301
RULES section, 299
RTC (real-time clock), 520
RULES section, rsyslogd, 299

S

scp command, 111–112
scripting, 416
arguments, 418–419
body script, 417
case statement, 426–427
comments, 416–417

conditional loops, 419, 422
debugging, 427–428
elif statement, 422
execute permission, 417
exit statement, 417
for conditional statement, 424–425
if...then...else statement, 422–423
if...then...else...fi statement, 420–421
logical operators, 423–424
positional parameters, 418–419
shebang, 416
storage, 417
until statement, 425–436
variables, 420–421
while statement, 425–436
sealert command, 484
secondary group, 138
securely copying files, 111–112
security. *See also* SELinux
cron, 280
file permissions, 463
NFS (Network File System), 508
repositories, 200–202
SSH (Secure Shell), 436
configuring alternative ports, 437
configuring key-based authentication, 441–442
limiting root access, 436–437
limiting user access, 438–439
modifying SELinux to allow for port changes, 437–438
sed command, 93–94
SELinux
context labels, 467, 471
finding the context type you need, 476–477
monitoring, 471–473
restoring default file contexts, 477–479
setting context types, 473–475
setting on a nondefault Apache DocumentRoot, 475
core elements, 467
enabled/disabled modes, 467
enforcing mode, 467–468
managing port access, 479–487
permissive mode, 467–468
policies, 467
Boolean settings, 479–481
diagnosing and addressing violations, 481–483
setting the default mode, 468–469
source domain, 467
-specific man pages, installing, 477
target domain, 467
working with different modes, 470–471
semanage command, 473–475
semanage port command, 479
server
NFS, setting up, 508–509
rebooting, 107–108
remote access using SSH, 108–109
ServerAliveCountMax option, SSH (Secure Shell), 440
ServerAliveInterval option, SSH (Secure Shell), 440
ServerRoot parameter, context labels, setting on a nondefault Apache DocumentRoot, 475
service units, 253–254
services, 252. *See also* Apache web service
anacron, 279–280
atd, 281
chrony, 527–528
crond, 274–275
Firewalld, 495–496
sestatus command, 469–470
setting default permissions, 159–160
setup requirements, 9
sftp command, 112
SGID permission, 155–156
shebang, 416
shell, 28
command-line completion, 35

commands, 29–30. *See also* commands; options
environment, 39
configuration files, 40
variables, 39–40
history, 33–35
login, 40
redirection, 31–33
scripting. *See* scripting
subshell, 40
shell jobs, 230, 238–239
showmount command, 509–510
signals, process, 239–241
skeleton directory, 134
slices, 236–238
snapshots, LVM, 344
sockets, 255–256
software, managing with Flatpak, 219–220. *See also* Flatpak
software packages. *See also* packages
finding using dnf command, 204–206
getting more information, 206–207
installing, 207–209
package groups, 212–213
showing lists of, 209–210
updating, 210–211
sort command, 85–86
sorting, text files, 85–86
specifying which repository to use, 198–200
ss -lt command, 177
SSH (Secure Shell), 108
accessing remote systems, 108–109
configuring key-based authentication, 113, 441–442
connection keepalive options, 440
dictionary attacks, 436
hardening the server, 436
configuring alternative ports, 437
limiting root access, 436–437
limiting user access, 438–439
modifying SELinux to allow for port changes, 437–438
logging in to a remote server, 109
MaxSessions option, 440
public/private keys, 114
UseDNS option, 440
ssh command, 108–111
ssh-copy-id command, 114
ssh-keygen command, 114
STDERR, 31
STDIN, 31
STDOUT, 30, 31
sticky bit, 156–157
stopping jobs, 231
storage. *See also* LVM (Logical Volume Manager); partitions
disk devices, 315–316
disk size specifications, 314
MB (megabyte), 314
MiB (mebibyte), 311–314
partitions, 315–316
creating with fdisk, 316–318
GPT, 320–323
MBR, 315–320
physical volumes, 342
script, 417
stratum, 521
su - command, 104
su command, 125–126
subnet mask, 169–170
subscription-manager command, 197–198
subscriptions, managing, 197–198
subshell, 40, 103
sudo command, 103, 104, 125, 126–127
SUID permission, 155–157
superuser, 124–125
swap files, adding, 328–329
swap partitions, adding, 327–328
switching between terminals
in a graphical environment, 103–104
in a nongraphical environment, 105–106
switching user accounts, 126, 128–129

symbolic links, 67, 69–70, 257
symbols, redirection, 31
synchronizing files, 113
syntax
  case statement, 427
  commands, 28
system accounts, 129
system properties, managing
  Ext4, 325–327
  XFS, 327
system slice, 237
system time, 520
/etc/NetworkManager/
    system-connections, 184–187
systemctl cat command, 254–255,
    264, 383
systemctl disable command, 384
systemctl edit command, 263
systemctl enable command, 254, 384
systemctl halt command, 108
systemctl isolate command, 387
systemctl list-dependencies command,
    260–262
systemctl poweroff command, 108
systemctl status command, 258–260,
    274–275, 289–290
systemctl -t target command, 385–387
Systemd, 252, 288, 382
  creating a mount file, 334–335
  directives
    managing, 262–264
    modifying with systemctl edit, 263
  journal, 288–289, 294–295
    customizing, 297
    finding events, 292–296
    log rotation, 296–297
    making permanent, 297
    preserving, 296
  managing dependencies, 260–262
  mount units, 254–255
  process, 107
  service units, 253–254
  socket units, 255–256
  target units, 256–257, 383–384
  targets, 382–383, 384
    isolating, 385–387
    managing, 384–385
    setting the default, 387–388
    wants, 384
  timers, 272–273
  unit files, 252–253
  units, 252
    requesting current status, 258–259
    starting and stopping, 257–258
systemd-udevd process, 368–369

T

tail command, 84
tail -f command, 292
tainted kernel, 365
tar command, 70–74
tar files, monitoring and extracting, 71–72
target units, 256–257, 383–384
targets
  dependencies, 383
  isolating, 385–387
  managing, 384–385
  setting the default, 387–388
  Systemd, 382–383, 384
  wants, 384
TCPKeepAlive option, SSH
    (Secure Shell), 440
terminal, 102
terminals
  dumb, 106
  pseudo, 106–107
  switching between
    in a graphical environment, 103–104
    in a nongraphical environment,
      105–106
text editors
  nano, 38–39, 264
  vim, 35–36, 37–38, 264
    command mode, 36

essential commands, 36–37
input mode, 36
text files, 79
analyzing text, 91–92
counting lines, words, and characters, 86–87
displaying the contents, 83
displaying the first or last lines, 84
filtering specific columns, 85
reading the contents of, 82–83
sorting file contents and output, 85–86
tools, 82
theoretical pre-assessment exam, 540
threads, 230, 234, 364–365
time, C25.xref NTP (Network Time Protocol)
Linux time, 520
local, 524–525
managing on Red Hat Enterprise Linux, 521, 522
system time, 520
time and date fields, cron, 276
time service clients, configuring, 527–528
time synchronization, 521
time zones, 525–527
timedatectl command, 522, 523–524
timers, 272–273
managing on Red Hat Enterprise Linux, epoch time, 522
options, 273
tools
dnf config-manager, 199
firewall-cmd, 496–500
RHSM (Red Had Subscription Management), 197
tuned, 244–245
top command, 242–243
troubleshooting
boot procedure, 399
starting a troubleshooting target, 401–402
using a rescue disk, 403–404
file system issues, 407
initramfs, 406
scripts, 427–428
tuned, 244–245
tuned-adm command, 245
type command, 29
tzselect command, 526–527

U

udevadm monitor command, 369–370
UEFI (Unified Extensible Firmware Interface), 313
umask setting, 159–160
umount command, 329
uname command, 367
unit files, 252–253
units, 252. *See also* Systemd
directives, 262–264
starting and stopping, 257–258
unloading kernel modules, 373
unprivileged users, 124
until statement, scripting, 425–436
updating
mandb, 45
packages, 210–211
upgrading, Linux kernel, 375
UseDNS option, SSH, 440
user accounts. *See also* configuration files; ownership; permissions
creating, 132–133, 136–137
modifying the configuration file, 133
using useradd, 133
granting administrator permissions, 126–127
home directory, 133–134
normal, 129
properties, 134
root, 124–125
switching, 126, 128–129
system, 129
user environment, creating, 136
user interface, Cockpit, 115

user slice, 237
useradd utility, 133, 418
/etc/default/useradd, 135
user-extended attributes, 160–161
usermod command, 139–140
UTC (Coordinated Universal Time), 520
utilities
  dmesg, 366–367
  dump, 333
  fdisk, 316–320
  useradd, 418
UUIDs (universally unique IDs), 330–331

V

validating network address configuration, 173–176
variables
  program, 39–40
  scripting, 420–421
/var/log, 289. *See also* log files
verifying
  network settings, 177–178
  port availability, 177
VG (volume group), creating, 350–351
vgcreate command, 350
vgdisplay command, 350–351
vigr command, 138
vim, 35–36, 37–38, 264
  command mode, 36
  essential commands, 36–37
  input mode, 36
vimtutor command, 36
virtual hosts, Apache web service, 456–457
visudo command, 127
volume groups. *See also* LVM (Logical Volume Manager)
  reducing, 356
  resizing, 354

W

wants, 257, 384
wc command, 86–87
web server, Apache, creating, 453–454
while statement, scripting, 425–436
wildcards, 60, 89–90, 513–514
write permissions, 152–154

X-Y-Z

XFS, managing system properties, 327
xfs_admin command, 327

zombies, 241–242
zones, Firewalld, 494