

SANDER VAN VUGT

# Cert Guide

Learn, prepare, and practice for exam success



FREE SAMPLE CHAPTER

SHARE WITH OTHERS



# **Red Hat RHCSA™ 8**

## **Cert Guide**

**EX200**

Sander van Vugt



## **Red Hat RHCSA™ 8 Cert Guide: EX200**

Copyright © 2020 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. 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.

ISBN-13: 978-0-13-593813-3

ISBN-10: 0-13-593813-9

Library of Congress Control Number: 2019948460

ScoutAutomatedPrintCode

### **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.

### **Editor-in-Chief**

Mark Taub

### **Acquisitions Editor**

Denise Lincoln

### **Development Editor**

Ellie Bru

### **Managing Editor**

Sandra Schroeder

### **Senior Project Editor**

Tonya Simpson

### **Copy Editor**

Bill McManus

### **Indexer**

Cheryl Lenser

### **Proofreader**

Gill Editorial Services

### **Technical Editor**

William “Bo” Rothwell

### **Publishing Coordinator**

Cindy Teeters

### **Cover Designer**

Chuti Prasertsith

### **Compositor**

codeMantra

# **Contents at a Glance**

Introduction xxiv

## **Part I: Performing Basic System Management Tasks**

- CHAPTER 1** Installing Red Hat Enterprise Linux 3
- CHAPTER 2** Using Essential Tools 29
- CHAPTER 3** Essential File Management Tools 53
- CHAPTER 4** Working with Text Files 81
- CHAPTER 5** Connecting to Red Hat Enterprise Linux 8 99
- CHAPTER 6** User and Group Management 121
- CHAPTER 7** Permissions Management 143
- CHAPTER 8** Configuring Networking 167

## **Part II: Operating Running Systems**

- CHAPTER 9** Managing Software 197
- CHAPTER 10** Managing Processes 233
- CHAPTER 11** Working with Systemd 253
- CHAPTER 12** Scheduling Tasks 271
- CHAPTER 13** Configuring Logging 285
- CHAPTER 14** Managing Storage 309
- CHAPTER 15** Managing Advanced Storage 339

## **Part III: Performing Advanced System Administration Tasks**

- CHAPTER 16** Basic Kernel Management 367
- CHAPTER 17** Managing and Understanding the Boot Procedure 385
- CHAPTER 18** Essential Troubleshooting Skills 401
- CHAPTER 19** An Introduction to Bash Shell Scripting 423

## **Part IV: Managing Network Services**

- CHAPTER 20** Configuring SSH 443
- CHAPTER 21** Managing Apache HTTP Services 457
- CHAPTER 22** Managing SELinux 471

<b>CHAPTER 23</b>	Configuring a Firewall	497
<b>CHAPTER 24</b>	Accessing Network Storage	511
<b>CHAPTER 25</b>	Configuring Time Services	527
<b>CHAPTER 26</b>	Final Preparation	541
<b>CHAPTER 27</b>	Theoretical Pre-Assessment Exam	545

#### **Part V: RHCSA RHEL 8 Practice Exams**

RHCSA Practice Exam A 549

RHCSA Practice Exam B 551

<b>APPENDIX A</b>	Answers to the “Do I Know This Already?”	
	Quizzes and Review Questions	553

Glossary 587

Index 609

#### **Online Elements:**

RHCSA Practice Exam C

RHCSA Practice Exam D

<b>APPENDIX B</b>	Memory Tables
-------------------	---------------

<b>APPENDIX C</b>	Memory Tables Answer Key
-------------------	--------------------------

<b>APPENDIX D</b>	Study Planner
-------------------	---------------

Glossary

# Table of Contents

Introduction xxiv

## **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 8 Server? 6  
    Getting the Software 7  
    *Using Red Hat Enterprise Linux* 7  
    *Using CentOS* 7  
    *Other Distributions* 8  
    Understanding Access to Repositories 8  
    Setup Requirements 9  
    Cert Guide Environment Description 9

Performing a Manual Installation 10

Summary 24

Exam Preparation Tasks 25

Review Questions 25

End-of-Chapter Lab 26

### **Chapter 2 Using Essential Tools 29**

“Do I Know This Already?” Quiz 29

Foundation Topics 32

Basic Shell Skills 32

    Understanding Commands 32

    Executing Commands 32

    I/O Redirection 34

    Using Pipes 36

    History 37

    Bash Completion 39

Editing Files with vim 39

Understanding the Shell Environment	42
Understanding Variables	42
Recognizing Environment Configuration Files	43
Using /etc/motd and /etc/issue	43
Finding Help	44
Using --help	44
Using man	45
Finding the Right man Page	46
Updating mandb	47
Using info	48
Using /usr/share/doc Documentation Files	49
Summary	50
Exam Preparation Tasks	50
Review Questions	51
End-of-Chapter Lab	51
<b>Chapter 3 Essential File Management Tools</b>	<b>53</b>
“Do I Know This Already?” Quiz	53
Foundation Topics	56
Working with the File System Hierarchy	56
Defining the File System Hierarchy	56
Understanding Mounts	57
Managing Files	61
Working with Wildcards	62
Managing and Working with Directories	62
Working with Absolute and Relative Pathnames	63
Listing Files and Directories	64
Copying Files	65
Moving Files	66
Deleting Files	66
Using Links	68
Understanding Hard Links	68
Understanding Symbolic Links	69
Creating Links	69
Removing Links	70

Working with Archives and Compressed Files	71
Managing Archives with tar	72
<i>Creating Archives with tar</i>	72
<i>Monitoring and Extracting tar Files</i>	73
Using Compression	74
Summary	75
Exam Preparation Tasks	75
Review Questions	77
End-of-Chapter Lab	77
<b>Chapter 4 Working with Text Files</b>	<b>81</b>
“Do I Know This Already?” Quiz	81
Foundation Topics	84
Using Common Text File–Related Tools	84
Doing More with less	84
Showing File Contents with cat	85
Displaying the First or Last Lines of a File with head and tail	86
Filtering Specific Columns with cut	87
Sorting File Contents and Output with sort	87
Counting Lines, Words, and Characters with wc	88
A Primer to Using Regular Expressions	89
Using Line Anchors	90
Using Escaping in Regular Expressions	90
Using Wildcards and Multipliers	91
Using grep to Analyze Text	92
Working with Other Useful Text Processing Utilities	93
Summary	94
Exam Preparation Tasks	95
Review Questions	96
End-of-Chapter Lab	96
<b>Chapter 5 Connecting to Red Hat Enterprise Linux 8</b>	<b>99</b>
“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	104
Understanding Pseudo Terminal Devices	106
Booting, Rebooting, and Shutting Down Systems	106
Using SSH and Related Utilities	108
Accessing Remote Systems Using SSH	108
Using Graphical Applications in an SSH Environment	111
Securely Transferring Files Between Systems	111
<i>Using scp to Securely Copy Files</i>	112
<i>Using sftp to Securely Transfer Files</i>	112
<i>Using rsync to Synchronize Files</i>	113
Configuring Key-Based Authentication for SSH	114
Using Passphrases or Not?	114
Using the screen Command	115
Summary	117
Exam Preparation Tasks	117
Review Questions	118
End-of-Chapter Labs	118
<b>Chapter 6 User and Group Management</b>	<b>121</b>
“Do I Know This Already?” Quiz	121
Foundation Topics	124
Different User Types	124
Users on Linux	124
Working as Root	124
Using su	125
sudo	126
PolicyKit	126
Managing User Accounts	127
System Accounts and Normal Accounts	127
Creating Users	131
<i>Modifying the Configuration Files</i>	131

<i>Using useradd</i>	131
<i>Home Directories</i>	132
Managing User Properties	132
Configuration Files for User Management Defaults	132
Managing Password Properties	133
Creating a User Environment	134
Creating and Managing Group Accounts	135
Understanding Linux Groups	135
Creating Groups	136
<i>Creating Groups with vigr</i>	136
<i>Using groupadd to Create Groups</i>	137
Managing Group Properties	137
Summary	138
Exam Preparation Tasks	138
Review Questions	140
End-of-Chapter Lab	140
<b>Chapter 7    Permissions Management</b>	<b>143</b>
“Do I Know This Already?” Quiz	143
Foundation Topics	146
Managing File Ownership	146
Displaying Ownership	146
Changing User Ownership	147
Changing Group Ownership	148
Understanding Default Ownership	148
Managing Basic Permissions	149
Understanding Read, Write, and Execute Permissions	149
Applying Read, Write, and Execute Permissions	150
Managing Advanced Permissions	152
Understanding Advanced Permissions	152
Applying Advanced Permissions	155
Managing ACLs	156
Understanding ACLs	156
Preparing Your File System for ACLs	157
Changing and Viewing ACL Settings with setfacl and getfacl	157
Working with Default ACLs	159

Setting Default Permissions with umask	160
Working with User-Extended Attributes	162
Summary	163
Exam Preparation Tasks	163
Review Questions	164
End-of-Chapter Lab	165
<b>Chapter 8 Configuring Networking 167</b>	
“Do I Know This Already?” Quiz	167
Foundation Topics	170
Networking Fundamentals	170
IP Addresses	170
IPv6 Addresses	171
Network Masks	171
Binary Notation	172
MAC Addresses	173
Protocol and Ports	173
Managing Network Addresses and Interfaces	174
Validating Network Configuration	175
Validating Network Address Configuration	175
Validating Routing	178
Validating the Availability of Ports and Services	178
Configuring Network Configuration with nmcli and nmtui	180
Required Permissions to Change Network Configuration	180
Configuring the Network with nmcli	181
Configuring the Network with nmtui	187
Working on Network Configuration Files	189
Setting Up Hostname and Name Resolution	190
Hostnames	190
DNS Name Resolution	192
Summary	194
Exam Preparation Tasks	194
Review Questions	195
End-of-Chapter Lab	195

## Part II: Operating Running Systems

### Chapter 9 Managing Software 197

“Do I Know This Already?” Quiz	197
Foundation Topics	200
Managing Software Packages with yum	200
Understanding the Role of Repositories	200
Registering Red Hat Enterprise Linux for Support	201
Managing Subscriptions	202
Specifying Which Repository to Use	203
Understanding Repository Security	206
Creating Your Own Repository	208
Using yum	209
Using yum to Find Software Packages	210
Getting More Information About Packages	211
Installing and Removing Software Packages	212
Showing Lists of Packages	214
<i>Updating Packages</i>	215
<i>Working with yum Package Groups</i>	216
<i>Using yum History</i>	218
Managing Package Module Streams	220
Understanding Modules	220
Managing Modules	221
Managing Software Packages with rpm	225
Understanding RPM Filenames	226
Querying the RPM Database	226
Querying RPM Package Files	227
Using repoquery	228
Summary	229
Exam Preparation Tasks	229
Review Questions	230
End-of-Chapter Labs	231

**Chapter 10 Managing Processes 233**

- “Do I Know This Already?” Quiz 233
- Foundation Topics 236
  - Introduction to Process Management 236
  - Managing Shell Jobs 236
    - Running Jobs in the Foreground and Background 236
    - Managing Shell Jobs 237
    - Managing Parent-Child Relations 239
  - Using Common Command-Line Tools for Process Management 239
    - Understanding Processes and Threads 239
    - Using ps to Get Process Information 240
    - Adjusting Process Priority with nice 242
    - Sending Signals to Processes with kill, killall, and pkill 244
  - Using top to Manage Processes 246
  - Using tuned to Optimize Performance 248
  - Summary 249
  - Exam Preparation Tasks 249
  - Review Questions 250
  - End-of-Chapter Lab 251

**Chapter 11 Working with Systemd 253**

- “Do I Know This Already?” Quiz 253
- Foundation Topics 256
- Understanding Systemd 256
  - Understanding Systemd Unit Locations 256
  - Understanding Systemd Service Units 257
  - Understanding Systemd Mount Units 258
  - Understanding Systemd Socket Units 259
  - Understanding Systemd Target Units 259
- Managing Units Through Systemd 261
  - Managing Dependencies 263
  - Managing Unit Options 265
- Summary 266
- Exam Preparation Tasks 267
- Review Questions 268
- End-of-Chapter Lab 268

**Chapter 12 Scheduling Tasks 271**

- “Do I Know This Already?” Quiz 271
- Foundation Topics 274
- 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 278
  - Managing Cron Security 280
- Configuring at to Schedule Future Tasks 281

- Summary 282
- Exam Preparation Tasks 282
- Review Questions 283
- End-of-Chapter Lab 283

**Chapter 13 Configuring Logging 285**

- “Do I Know This Already?” Quiz 285
- Foundation Topics 288
- Understanding System Logging 288
  - Understanding the Role of rsyslogd and journald 288
  - Reading Log Files 290
  - Understanding Log File Contents 290
  - Live Log File Monitoring 292
  - Using logger 292
- Configuring rsyslogd 293
  - Understanding rsyslogd Configuration Files 293
  - Understanding rsyslog.conf Sections 293
  - Understanding Facilities, Priorities, and Log Destinations 294
- Rotating Log Files 297
- Working with journald 299
  - Using journalctl to Find Events 299
  - Preserving the Systemd Journal 302
- Summary 304
- Exam Preparation Tasks 304
- Review Questions 305
- End-of-Chapter Lab 306

**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	314
Creating MBR Partitions with fdisk	315
Using Extended and Logical Partitions on MBR	319
Creating GPT Partitions with gdisk	320
Creating GPT Partitions with parted	324
Creating File Systems	325
Changing File System Properties	327
<i>Managing Ext4 File System Properties</i>	327
<i>Managing XFS File System Properties</i>	329
Adding Swap Partitions	329
Adding Swap Files	330
Mounting File Systems	330
Manually Mounting File Systems	331
Using Device Names, UUIDs, or Disk Labels	331
Automating File System Mounts Through /etc/fstab	332
Summary	335
Exam Preparation Tasks	335
Review Questions	336
End-of-Chapter Lab	337

**Chapter 15 Managing Advanced Storage 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	349
Creating the Logical Volumes and File Systems	351
Understanding LVM Device Naming	351
Resizing LVM Logical Volumes	353
Resizing Volume Groups	353
Resizing Logical Volumes and File Systems	354
Configuring Stratis	356
Understanding Stratis Architecture	356
Creating Stratis Storage	357
Managing Stratis	358
Configuring VDO	359
Understanding VDO	359
Setting Up VDO	360
Summary	362
Exam Preparation Tasks	362
Review Questions	363
End-of-Chapter Labs	364

### **Part III: Performing Advanced System Administration Tasks**

#### **Chapter 16 Basic Kernel Management 367**

"Do I Know This Already?" Quiz	367
Foundation Topics	370
Understanding the Role of the Linux Kernel	370
Understanding the Use of Kernel Threads and Drivers	370
Analyzing What the Kernel Is Doing	371
Working with Kernel Modules	373
Understanding Hardware Initialization	374
Managing Kernel Modules	376
Checking Driver Availability for Hardware Devices	379
Managing Kernel Module Parameters	380
Upgrading the Linux Kernel	381

Summary	381
Exam Preparation Tasks	381
Review Questions	382
End-of-Chapter Lab	383

## **Chapter 17 Managing and Understanding the Boot Procedure 385**

“Do I Know This Already?” Quiz	385
Foundation Topics	388
Managing Systemd Targets	388
Understanding Systemd Targets	388
<i>Working with Targets</i>	388
<i>Understanding Target Units</i>	389
<i>Understanding Wants</i>	390
<i>Managing Systemd Targets</i>	390
<i>Isolating Targets</i>	391
<i>Setting the Default Target</i>	393
Working with GRUB 2	394
Understanding GRUB 2	394
Understanding GRUB 2 Configuration Files	395
Modifying Default GRUB 2 Boot Options	395
Summary	396
Exam Preparation Tasks	397
Review Questions	397
End-of-Chapter Labs	398

## **Chapter 18 Essential Troubleshooting Skills 401**

“Do I Know This Already?” Quiz	401
Foundation Topics	404
Understanding the RHEL 8 Boot Procedure	404
Passing Kernel Boot Arguments	406
Accessing the Boot Prompt	406
Starting a Troubleshooting Target	407
Using a Rescue Disk	408
Restoring System Access Using a Rescue Disk	409
Reinstalling GRUB Using a Rescue Disk	411
Re-Creating the Initramfs Using a Rescue Disk	411

Fixing Common Issues	413
Reinstalling GRUB 2	413
Fixing the Initramfs	414
Recovering from File System Issues	414
Resetting the Root Password	416
Recovering Access to a Virtual Machine	416
Summary	418
Exam Preparation Tasks	418
Review Questions	419
End-of-Chapter Lab	420
<b>Chapter 19 An Introduction to Bash Shell Scripting</b>	<b>423</b>
“Do I Know This Already?” Quiz	423
Foundation Topics	426
Understanding Shell Scripting Core Elements	426
Using Variables and Input	428
Using Positional Parameters	428
Working with Variables	430
Using Conditional Loops	432
Working with if ... then ... else	432
Using    and &&	433
Applying for	434
Understanding while and until	435
Understanding case	436
Bash Shell Script Debugging	438
Summary	438
Exam Preparation Tasks	438
Review Questions	439
End-of-Chapter Lab	440

## **Part IV: Managing Network Services**

### **Chapter 20 Configuring SSH**

“Do I Know This Already?” Quiz	443
Foundation Topics	446
Hardening the SSH Server	446

Limiting Root Access	446
Configuring Alternative Ports	447
Modifying SELinux to Allow for Port Changes	447
Limiting User Access	448
Using Other Useful sshd Options	449
Session Options	450
Connection Keepalive Options	450
Configuring Key-Based Authentication with Passphrases	451
Summary	452
Exam Preparation Tasks	452
Review Questions	453
End-of-Chapter Lab	454
<b>Chapter 21 Managing Apache HTTP Services</b>	<b>457</b>
“Do I Know This Already?” Quiz	457
Foundation Topics	460
Configuring a Basic Apache Server	460
Installing the Required Software	460
Identifying the Main Configuration File	460
Creating Web Server Content	463
Understanding Apache Configuration Files	464
Creating Apache Virtual Hosts	465
Summary	468
Exam Preparation Tasks	468
Review Questions	469
End-of-Chapter Lab	469
<b>Chapter 22 Managing SELinux</b>	<b>471</b>
“Do I Know This Already?” Quiz	472
Foundation Topics	475
Understanding SELinux Working and Modes	475
Understanding Context Settings and the Policy	479
Monitoring Current Context Labels	479
Setting Context Types	481
Finding the Context Type You Need	484

Restoring Default File Contexts	485
Using Boolean Settings to Modify SELinux Settings	487
Diagnosing and Addressing SELinux Policy Violations	488
Making SELinux Analyzing Easier	490
Preparing for SELinux Coverage on the Exam	492
Summary	492
Exam Preparation Tasks	492
Review Questions	494
End-of-Chapter Lab	494
<b>Chapter 23 Configuring a Firewall</b>	<b>497</b>
“Do I Know This Already?” Quiz	497
Foundation Topics	500
Understanding Linux Firewalling	500
Understanding Previous Solutions	500
Understanding Firewalld	500
Understanding Firewalld Zones	501
Understanding Firewalld Services	502
Working with Firewalld	503
Summary	506
Exam Preparation Tasks	506
Review Questions	507
End-of-Chapter Lab	508
<b>Chapter 24 Accessing Network Storage</b>	<b>511</b>
“Do I Know This Already?” Quiz	511
Foundation Topics	514
Using NFS Services	514
Understanding NFS Security	514
RHEL 8 NFS Versions	514
Mounting the NFS Share	515
Mounting the NFS Share	516
Using CIFS Services	516
Discovering CIFS Shares	517
Mounting Samba Shares	518
Authenticating to Samba Shares	518

Configuring a Samba Server	518
Mounting Remote File Systems Through fstab	520
Mounting NFS Shares Through fstab	520
Mounting Samba Shares Through fstab	521
Using Automount to Mount Remote File Systems	521
Understanding Automount	521
Defining Mounts in Automount	522
Configuring Automount for NFS	522
Using Wildcards in Automount	523
Summary	524
Exam Preparation Tasks	524
Review Questions	525
End-of-Chapter Lab	525
<b>Chapter 25 Configuring Time Services</b>	<b>527</b>
“Do I Know This Already?” Quiz	527
Foundation Topics	530
Understanding Local Time	530
Using Network Time Protocol	531
Managing Time on Red Hat Enterprise Linux	531
Using date	532
Using hwclock	532
Using timedatectl	533
Managing Time Zone Settings	535
Configuring Time Service Clients	537
Summary	538
Exam Preparation Tasks	539
Review Questions	540
End-of-Chapter Lab	540
<b>Chapter 26 Final Preparation</b>	<b>541</b>
General Tips	541
Verifying Your Readiness	541
Registering for the Exam	541
On Exam Day	542
<i>During the Exam</i>	542
<i>The Nondisclosure Agreement</i>	544

**Chapter 27 Theoretical Pre-Assessment Exam 545****Part V: RHCSA RHEL 8 Practice Exams**

RHCSA Practice Exam A 549

RHCSA Practice Exam B 551

Appendix A Answers to the “Do I Know This Already?”

Quizzes and Review Questions 553

Glossary 587

Index 609

## 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 <http://www.sandervanvugt.com>.

## Dedication

*This book is dedicated to my family: Florence, Franck, and Alex. Together we've made great accomplishments over the past year.*

## 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 and Ellie Bruin 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 Reviewer

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

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

## 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](mailto:community@informit.com)

## Introduction

Welcome to the *Red Hat RHCSA 8 Cert Guide*. 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 20 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.

The RHCSA exam was recently updated for Red Hat Enterprise Linux 8. This book contains all you need to know to pass the RHCSA exam. As you will see, this 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 CentOS or Red Hat Enterprise Linux 8 in a virtual machine, and that is all that is required to go through the labs. You don't need to import any virtual machines; just install your own virtual machine and you'll be ready to go!

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:

- *Red Hat Certified System Administrator (RHCSA) Complete Video Course*,  
3rd Edition
- *Upgrading to Red Hat Enterprise Linux (RHEL) 8 LiveLessons*

Apart from these products, you might also appreciate my website, <http://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 ten 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 four RHCSA practice exams; these are an essential part of readying yourself for the real exam experience. You may 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 files include two extra practice exams, two hours of video from the *Red Hat Certified System Administrator (RHCSA) Complete Video Course*, 3rd Edition, 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 Server (RHEL). 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 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 8:** This chapter describes the different methods that can be used to connect to RHEL 8. 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, but 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 8. 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 on a moment that fits you best.
- **Chapter 13: Configuring Logging:** As an administrator, you need to know what's happening on your server. The rsyslogd and 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 Advanced Storage:** 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 create and manage those logical volumes. You'll also learn how to work with the new Stratis and VDO storage techniques.

### 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 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 8 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 it off, 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 8 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 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 RHEL 8 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:

- **Four practice exams:** *Red Hat RHCSA 8 Cert Guide* 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 two hours of video training:** The companion website contains more than two hours of instruction from the best-selling *Red Hat Certified System Administrator (RHCSA) Complete Video Course*, 3rd Edition.

## 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
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 8	5
Log in and switch users in multiuser targets	Connecting to Red Hat Enterprise Linux 8	5
Archive, compress, unpack, and uncompress files using tar, star, gzip, and bzip2	Essential File Management Tools	3
Create and edit text files	Working with Text Files	4

<b>Objective</b>	<b>Chapter Title</b>	<b>Chapter</b>
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
Boot, reboot, and shut down a system normally	Connecting to Red Hat Enterprise Linux 8	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
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 8	5
List, create, and delete partitions on MBR and GPT disks	Managing Storage	14
Create and remove physical volumes	Managing Advanced Storage	15
Assign physical volumes to volume groups	Managing Advanced Storage	15
Create and delete logical volumes	Managing Advanced Storage	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 non-destructively	Managing Storage	14
Create, mount, unmount, and use vfat, ext4, and xfs file systems	Managing Storage	14

<b>Objective</b>	<b>Chapter Title</b>	<b>Chapter</b>
Mount and unmount network file systems using NFS	Accessing Network Storage	24
Extend existing logical volumes	Managing Advanced Storage	15
Create and configure set-GID directories for collaboration	Permissions Management	7
Configure disk compression	Managing Advanced Storage	15
Manage layered storage	Managing Advanced Storage	15
Diagnose and correct file permission problems	Permissions Management	7
Schedule tasks using at and cron	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 Network, a remote repository, or from the local file system	Managing Software	9
Work with package module streams	Managing Software	9
Modify the system bootloader	Managing and Understanding the Boot Procedure	17
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 firewall-cmd/firewall	Configuring a Firewall	23
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 superuser access	User and Group Management	6

Objective	Chapter Title	Chapter
<b>Manage security</b>		
Configure firewall settings using firewall-cmd/firewalld	Configuring a Firewall	23
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
Use boolean settings to modify system SELinux settings	Managing SELinux	22
Diagnose and address routine SELinux policy violations	Managing SELinux	22

## Where Are the Companion Content Files?

Register this print version of *Red Hat RHCSA 8 Cert Guide* to access the bonus content online.

This print version of this title comes with a website of companion content. You have online access to these files by following these steps:

1. Go to [www.pearsonITcertification.com/register](http://www.pearsonITcertification.com/register) and log in or create a new account.
2. Enter the ISBN: **9780135938133**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of the companion content files can be very large, especially image and video files.

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

## Figure Credits

Chapter opener images by Charlie Edwards/ Photodisc/Getty Images

Figures 1-1 through 1-15 © 2019 Red Hat, Inc

Figures 2-1 and 2-2 © 2019 Red Hat, Inc

Figures 5-1 and 5-2 © 2019 Red Hat, Inc

Figures 8-1 through 8-5 © 2019 Red Hat, Inc

Figure 10-1 © 2019 Red Hat, Inc

Figures 18-1 through 18-5 © 2019 Red Hat, Inc

*This page intentionally left blank*

# Managing and Understanding the Boot Procedure

## “Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows 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 17-1 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 17-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Working with Systemd	1–7
Working with GRUB 2	8–10

1. Which of the following is the most efficient way to define a system want?
  - a. Use the **systemctl enable** command.
  - b. Define the want in the unit file [Service] section.
  - c. Create a symbolic link in the /usr/lib/system/system directory.
  - d. Create a symbolic link in the unit wants directory in the /etc/system/system directory.
2. Which target is considered the normal target for servers to start in?
  - a. graphical.target
  - b. server.target
  - c. multi-user.target
  - d. default.target

3. Which of the following is *not* an example of a system target?
  - a. rescue.target
  - b. restart.target
  - c. multi-user.target
  - d. graphical.target
4. Where do you define which target a unit should be started in if it is enabled?
  - a. The target unit file
  - b. The wants directory
  - c. The systemctl.conf file
  - d. The [Install] section in the unit file
5. To allow targets to be isolated, you need a specific statement in the target unit file. Which of the following describes that statement?
  - a. AllowIsolate
  - b. Isolate
  - c. SetIsolate
  - d. Isolated
6. An administrator wants to change the current multi-user.target to the rescue.target. Which of the following should she do?
  - a. Use **systemctl isolate rescue.target**
  - b. Use **systemctl start rescue.target**
  - c. Restart the system, and from the GRUB boot prompt specify that rescue.target should be started
  - d. Use **systemctl enable rescue.target --now**
7. To which System V runlevel does multi-user.target correspond?
  - a. 2
  - b. 3
  - c. 4
  - d. 5

8. What is the name of the file where you should apply changes to the GRUB 2 configuration?
  - a. /boot/grub/menu.lst
  - b. /boot/grub2/grub.cfg
  - c. /etc/sysconfig/grub
  - d. /etc/default/grub
9. After applying changes to the GRUB 2 configuration, you need to write those changes. Which of the following commands will do that for you?
  - a. grub2 -o /boot/grub/grub.cfg
  - b. grub2-mkconfig > /boot/grub2/grub.cfg
  - c. grub2 > /boot/grub2/grub.cfg
  - d. grub2-install > /boot/grub2/grub.cfg
10. What is the name of the GRUB2 configuration file that is generated on a UEFI system?
  - a. /boot/efi/redhat/grub.cfg
  - b. /boot/efi/EFI/redhat/grub.cfg
  - c. /boot/EFI/grub.cfg
  - d. /boot/EFI/efi/grub.cfg

## Foundation Topics

### Managing Systemd Targets

Systemd is the service in Red Hat Enterprise Linux 8 that is responsible for starting all kinds of things. Systemd goes way beyond starting services; other items are started from Systemd as well. In Chapter 11, “Working with Systemd,” you learned about the Systemd fundamentals; this chapter looks at how Systemd targets are used to boot your system into a specific state.

#### Understanding Systemd Targets

A Systemd *target* is basically just a group of units that belong together. Some targets are just that and nothing else, whereas other targets can be used to define the state a system is booting in, because these targets have one specific property that regular targets don’t have: they can be isolated. Isolatable targets contain everything a system needs to boot or change its current state. Four targets can be used while booting:

- **emergency.target:** In this target only a minimal number of units are started, just enough to fix your system if something is seriously wrong. You’ll find that it is quite minimal, as some important units are not started.
- **rescue.target:** This target starts all units that are required to get a fully operational Linux system. It doesn’t start nonessential services though.
- **multi-user.target:** This target is often used as the default target a system starts in. It starts everything that is needed for full system functionality and is commonly used on servers.
- **graphical.target:** This target also is commonly used. It starts all units that are needed for full functionality, as well as a graphical interface.

#### Working with Targets

Working with targets may seem complicated, but it is not. It drills down to three common tasks:

- Adding units to be automatically started
- Setting a default target
- Running a nondefault target to enter troubleshooting mode

In Chapter 11 you learned how to use the **systemctl enable** and **systemctl disable** commands to add services to or remove services from targets. In this chapter you'll learn how to set a default target and how to run a nondefault target to enter troubleshooting mode. But first we'll take a closer look at the working of targets under the hood.

## Understanding Target Units

Key Topic

Behind a target there is some configuration. This configuration consists of two parts:

- The target unit file
- The “wants” directory, which contains references to all unit files that need to be loaded when entering a specific target

Targets by themselves can have dependencies to other targets, which are defined in the target unit file. Example 17-1 shows the definition of the `multi-user.target` file, which defines the normal operational state of a RHEL server.

### Example 17-1 The `multi-user.target` File

```
[root@localhost ~]# systemctl cat multi-user.target
# /usr/lib/systemd/system/multi-user.target
# SPDX-License-Identifier: LGPL-2.1+
#
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it
# under the terms of the GNU Lesser General Public License as
# published by
# the Free Software Foundation; either version 2.1 of the License,
# or
# (at your option) any later version.

[Unit]
Description=Multi-User System
Documentation=man:systemd.special(7)
Requires=basic.target
Conflicts=rescue.service rescue.target
After=basic.target rescue.service rescue.target
AllowIsolate=yes
```

You can see that by itself the target unit does not contain much. It just defines what it requires and which services and targets it cannot coexist with. It also defines load ordering, by using the **After** statement in the [Unit] section. The target file does not contain any information about the units that should be included; that is in the individual unit files and the wants (explained in the upcoming section “Understanding Wants”).

Systemd targets look a bit like runlevels used in previous versions of RHEL, but targets are more than that. A target is a group of units, and there are multiple different targets. Some targets, such as the multi-user.target and the graphical.target, define a specific state that the system needs to enter. Other targets just bundle a group of units together, such as the nfs.target and the printer.target. These targets are included from other targets, such as multi-user.target or graphical.target.

## Understanding Wants

Understanding the concept of a want simply requires understanding the verb *want* in the English language, as in “I want a cookie.” Wants in Systemd define which units Systemd wants when starting a specific target. Wants are created when Systemd units are enabled using **systemctl enable**, and this happens by creating a symbolic link in the /etc/systemd/system directory. In this directory, you’ll find a subdirectory for every target, containing wants as symbolic links to specific services that are to be started.

## Managing Systemd Targets



As an administrator, you need to make sure that the required services are started when your server boots. To do this, use the **systemctl enable** and **systemctl disable** commands. You do not have to think about the specific target a service has to be started in. Through the [Install] section in the service unit file, the services know for themselves in which targets they need to be started, and a want is created automatically in that target when the service is enabled. The following procedure walks you through the steps of enabling a service:

1. Type **systemctl status vsftpd**. If the service has not yet been enabled, the Loaded line will show that it currently is disabled:

```
[root@server202 ~]# systemctl status vsftpd
vsftpd.service - Vsftpd ftp daemon
    Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled)
    Active: inactive (dead)
```

2. Type **ls /etc/systemd/system/multi-user.target.wants**. You’ll see symbolic links that are taking care of starting the different services on your machine. You can also see that the vsftpd.service link does not exist.

3. Type **systemctl enable vsftpd**. The command shows you that it is creating a symbolic link for the file /usr/lib/systemd/system/vsftpd.service to the directory /etc/systemd/system/multi-user.target.wants. So basically, when you enable a Systemd unit file, in the background a symbolic link is created.

**TIP** On the RHCSA exam, you are likely to configure a couple of services. It is a good idea to read through the exam questions, identify the services that need to be enabled, and enable them all at once to make sure that they are started automatically when you restart. This prevents your being so focused on configuring the service that you completely forget to enable it as well.

## Isolating Targets

As already discussed, on Systemd machines there are several targets. You also know that a target is a collection of units. Some of those targets have a special role because they can be isolated. These are also the targets that you can set as the targets to get into after system start.

By isolating a target, you start that target with all of its dependencies. Only targets that have the **isolate** option enabled can be isolated. We'll explore the **systemctl isolate** command later in this section. Before doing that, let's take a look at the default targets on your computer.

To get a list of all targets currently loaded, type **systemctl --type=target**. You'll see a list of all the targets currently active. If your server is running a graphical environment, this will include all the dependencies required to install the graphical.target also. However, this list shows only the active targets, not all the targets. Type **systemctl --type=target --all** for an overview of all targets that exist on your computer. You'll now see inactive targets also (see Example 17-2).

### Example 17-2 Showing System Targets

```
root@localhost ~]# systemctl --type=target --all
UNIT           LOAD   ACTIVE   SUB    DESCRIPTION
basic.target    loaded  active   active  Basic System
bluetooth.target loaded  active   active  Bluetooth
cryptsetup.target loaded  active   active  Local Encrypted
                           Volumes
dbus.target     not-found  inactive  dead    dbus.target
emergency.target loaded  inactive  dead    Emergency Mode
getty-pre.target loaded  active   active  Login Prompts
                           (Pre)
getty.target    loaded  active   active  Login Prompts
```

graphical.target	loaded	active	active	Graphical Interface
initrd-fs.target	loaded	inactive	dead	Initrd File Systems
initrd-root-device.target	loaded	inactive	dead	Initrd Root Device
initrd-root-fs.target	loaded	inactive	dead	Initrd Root File System
initrd-switch-root.target	loaded	inactive	dead	Switch Root
initrd.target	loaded	inactive	dead	Initrd Default Target
local-fs-pre.target	loaded	active	active	Local File Systems (Pre)
local-fs.target	loaded	active	active	Local File Systems
multi-user.target	loaded	active	active	Multi-User System
network-online.target	loaded	active	active	Network is Online
network-pre.target	loaded	active	active	Network (Pre)
network.target	loaded	active	active	Network
nfs-client.target	loaded	active	active	NFS client services
nss-lookup.target	loaded	inactive	dead	Host and Network Name Lookups
nss-user-lookup.target	loaded	active	active	User and Group Name Lookups
paths.target	loaded	active	active	Paths
remote-fs-pre.target	loaded	active	active	Remote File Systems (Pre)
remote-fs.target	loaded	active	active	Remote File Systems
rescue.target	loaded	inactive	dead	Rescue Mode
rpc_pipefs.target	loaded	active	active	rpc_pipefs. target
rpcbind.target	loaded	active	active	RPC Port Mapper
shutdown.target	loaded	inactive	dead	Shutdown
slices.target	loaded	active	active	Slices
sockets.target	loaded	active	active	Sockets
sound.target	loaded	active	active	Sound Card
sshd-keygen.target	loaded	active	active	sshd-keygen. target
swap.target	loaded	active	active	Swap
sysinit.target	loaded	active	active	System Initialization

Of the targets on your system, a few have an important role because they can be started (isolated) to determine the state your server starts in. These are also the targets that can be set as the default targets. These targets also roughly correspond to runlevels used on earlier versions of RHEL. These are the following targets:

```
poweroff.target    runlevel 0
rescue.target      runlevel 1
multi-user.target  runlevel 3
graphical.target   runlevel 5
reboot.target      runlevel 6
```

If you look at the contents of each of these targets, you'll also see that they contain the AllowIsolate=yes line. That means that you can switch the current state of your computer to either one of these targets using the **systemctl isolate** command. Exercise 17-1 shows you how to do this.

### Exercise 17-1 Isolating Targets

Key Topic

1. From a root shell, go to the directory /usr/lib/systemd/system. Type **grep Isolate \*.target**. This shows a list of all targets that allow isolation.
2. Type **systemctl isolate rescue.target**. This switches your computer to rescue.target. You need to type the root password on the console of your server to log in.
3. Type **systemctl isolate reboot.target**. This restarts your computer.

### Setting the Default Target

Setting the default target is an easy procedure that can be accomplished from the command line. Type **systemctl get-default** to see the current default target and use **systemctl set-default** to set the desired default target.

To set the graphical.target as the default target, you need to make sure that the required packages are installed. If this is not the case, you can use the **yum group list** command to show a list of all RPM package groups. The “server with gui” and “GNOME Desktop” package groups both apply. Use **yum group install "server with gui"** to install all GUI packages on a server where they have not been installed yet.

## Working with GRUB 2

The GRUB 2 boot loader is one of the first things that needs to be working well to boot a Linux server. As an administrator, you will sometimes need to apply modifications to the GRUB 2 boot loader configuration. This section explains how to do so. The RHEL 8 boot procedure is discussed in more detail in Chapter 18, where troubleshooting topics are covered as well.

### Understanding GRUB 2

The GRUB 2 boot loader makes sure that you can boot Linux. GRUB 2 is installed in the boot sector of your server's hard drive and is configured to load a Linux kernel and the initramfs:



- The kernel is the heart of the operating system, allowing users to interact with the hardware that is installed in the server.
- The initramfs contains drivers that are needed to start your server. It contains a mini file system that is mounted during boot. In it are kernel modules that are needed during the rest of the boot process (for example, the LVM modules and SCSI modules for accessing disks that are not supported by default).

Normally, GRUB 2 works just fine and does not need much maintenance. In some cases, though, you might have to change its configuration. To apply changes to the GRUB 2 configuration, the starting point is the /etc/default/grub file, which has options that tell GRUB what to do and how to do it. Example 17-3 shows the contents of this file after an installation with default settings of RHEL 8.



#### Example 17-3 Contents of the /etc/default/grub File

```
[root@localhost ~]# cat /etc/default/grub
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto resume=/dev/mapper/rhel-swap
    rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
```

As you can see, the /etc/default/grub file does not contain much information. The most important part that it configures is the GRUB\_CMDLINE\_LINUX option. This line contains boot arguments for the kernel on your server.

**TIP** For the RHCSA exam, make sure that you understand the contents of the /etc/default/grub file. That is the most important part of the GRUB 2 configuration anyway.

Apart from the configuration in /etc/default/grub, there are a few configuration files in /etc/grub.d. In these files, you'll find rather complicated shell code that tells GRUB what to load and how to load it. You typically do not have to modify these files. You also do not need to modify anything if you want the capability to select from different kernels while booting. GRUB 2 picks up new kernels automatically and adds them to the boot menu automatically, so nothing has to be added manually.

## Understanding GRUB 2 Configuration Files

Based on the configuration files mentioned previously, the main configuration file is created. If your system is a BIOS system, the name of the file is /boot/grub2/grub.cfg. On a UEFI system the file is written to /boot/efi/EFI/redhat. After making modifications to the GRUB 2 configuration, you'll need to regenerate the relevant configuration file, which is why you should know the name of the file that applies to your system architecture. Do *not* edit it, as this file is automatically generated.

## Modifying Default GRUB 2 Boot Options

To apply modifications to the GRUB 2 boot loader, the file /etc/default/grub is your entry point. The most important line in this file is GRUB\_CMDLINE\_LINUX, which defines how the Linux kernel should be started. In this line, you can apply permanent fixes to the GRUB 2 configuration. Some likely candidates for removal are the options **rhgb** and **quiet**. These options tell the kernel to hide all output while booting. That is nice to hide confusing messages for end users, but if you are a server administrator, you probably just want to remove these options.

**TIP** On the exam, you want to know immediately if something does not work out well. To accomplish this, it is a good idea to remove the **rhgb** and **quiet** boot options. Without these you will not have to guess why your server takes a long time after a restart; you'll just be able to see.

Another interesting parameter is GRUB\_TIMEOUT. This defines the amount of time your server waits for you to access the GRUB 2 boot menu before it continues booting automatically. If your server runs on physical hardware that takes a long time to get through the BIOS checks, it may be interesting to increase this time a bit.

While working with GRUB 2, you need to know a bit about kernel boot arguments. There are many of them, and most of them you'll never use, but it is good to know where you can find them. Type **man 7 bootparam** for a man page that contains an excellent description of all boot parameters that you may use while starting the kernel.

To write the modified configuration to the appropriate files, you use the **grub2-mkconfig** command and redirect its output to the appropriate configuration file. On a BIOS system, the command would be **grub2-mkconfig -o /boot/grub2/grub.cfg**, and on a UEFI system the command would be **grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg**.

In Exercise 17-2, you learn how to apply modifications to the GRUB 2 configuration and write them to the `/boot/grub2/grub.cfg` configuration file.

**TIP** You should know how to apply changes to the GRUB configuration, but you should also know that the default GRUB 2 configuration works fine as it is for almost all computers. So, you will probably never have to apply any changes at all!

## Key Topic

### Exercise 17-2 Applying Modifications to GRUB 2

1. Open the file `/etc/default/grub` with an editor and remove the `rhgb` and `quiet` options from the `GRUB_CMDLINE_LINUX` line.
2. From the same file, set the `GRUB_TIMEOUT` parameter to 10 seconds. Save changes to the file and close the editor.
3. From the command line, type **grub2-mkconfig > /boot/grub2/grub.cfg** to write the changes to GRUB 2. (Note that instead of using the redirector `>` to write changes to the `grub.cfg` file, you could use the `-o` option. Both methods have the same result.)
4. Reboot and verify that while booting you see boot messages scrolling by.

## Summary

In this chapter you learned how Systemd and GRUB 2 are used to bring your server into the exact state you desire at the end of the boot procedure. You also learned how Systemd is organized, and how units can be configured for automatic start with the use of targets. Finally, you read how to apply changes to the default GRUB 2 boot loader. In the next chapter, you learn how to troubleshoot the boot procedure and fix some common problems.

## 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 B; 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 outer margin of the page. Table 17-2 lists a reference of these key topics and the page number on which each is found.

**Table 17-2** Key Topics for Chapter 17

Key Topic Element	Description	Page	Key Topic
Section	Understanding target units	389	
Section	Managing Systemd targets	390	
Exercise 17-1	Isolating targets	393	
List	Explanation of the role of kernel and initramfs	394	
Example 17-3	Contents of the /etc/default/grub file	394	
Exercise 17-2	Applying modifications to GRUB 2	396	

## Define Key Terms

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

unit, wants, target, Systemd, dependencies, initramfs, kernel, boot loader, GRUB

## 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. What is a unit?
2. Which command enables you to make sure that a target is no longer eligible for automatic start on system boot?

3. Which configuration file should you modify to apply common changes to GRUB 2?
4. Which command should you use to show all service units that are currently loaded?
5. How do you create a want for a service?
6. How do you switch the current operational target to the rescue.target?
7. Why can it happen that you get the message that a target cannot be isolated?
8. You want to shut down a Systemd service, but before doing that you want to know which other units have dependencies to this service. Which command would you use?
9. What is the name of the GRUB 2 configuration file where you apply changes to GRUB 2?
10. After applying changes to the GRUB 2 configuration, which command should you run?

## End-of-Chapter Labs

You have now learned how to work with Systemd targets and the GRUB 2 boot loader. Before continuing, it is a good idea to work on some labs that help you ensure that you can apply the skills that you acquired in this chapter.

### Lab 17.1

1. Set the default target to multi-user.target.
2. Reboot to verify this is working as expected.

### Lab 17.2

1. Change your GRUB 2 boot configuration so that you will see boot messages upon startup.

*This page intentionally left blank*

# Index

## SYMBOLS

& (ampersand) command, 237–238

\ (backslash) escape character, 433

~/.bash\_profile, 43

~/.bashrc, 43

/boot directory, 56–57

/dev directory, 56

. (dot), 553, 91

/etc directory, 56

/etc/anacrontab, 278–279

/etc/bashrc, 43

/etc/crontab file, managing, 276–278

/etc/default/grub, 395

/etc/default/useradd, 132–133

/etc/dracut.conf, 412–413

/etc/fstab, 332–335

NFS share mounting, 520–521

Samba share mounting, 521

/etc/group, 136–137

/etc/gshadow, 137

/etc/hosts, 191–192

/etc/httpd, 464–465

/etc/httpd/conf/httpd.conf, 460–463

/etc/issue, 43

/etc/login.defs, 133

/etc/logrotate.conf, 298

/etc/motd, 43

/etc/passwd, 89

fields, 128–129

modifying, 131

/etc/profile, 43

/etc/shadow

fields, 129–130

modifying, 131

/etc/sysconfig/selinux, 476

/etc/systemd/journald.conf, 303

--help option, 44–45

/home directory, 56, 58

&& (logical AND), 553, 433

|| (logical OR), 564, 433

/media directory, 56

/mnt directory, 56

/opt directory, 56

\$PATH, 553, 33

/proc directory, 56, 372

/ (root) directory, 56

/root directory, 56

/run directory, 56

#! (shebang), 569, 426

/srv directory, 56

/sys directory, 56

/tmp directory, 57

/usr directory, 57–58

/usr/share/doc documentation files, 49

/var directory, 57–58

/var/log, list of log files, 290

/var/log/messages, 290–292

\* (wildcard), 573

## A

absolute filenames

defined, 553

overview, 63–64

accessing repositories, 8

- accounts. *See* group accounts; user accounts
- ACLs (access control lists), 156–160  
  changing/viewing settings, 157–159  
  default ACLs, 159–160  
  defined, 553  
  file system preparation, 157  
  support for, 156–157
- advanced permissions, 152–156
- aliases, 33
- alternative port configuration, 447
- ampersand (&) command, 237–238
- anacron  
  configuring, 278–279  
  defined, 553
- AND, 553, 433
- Apache servers  
  configuration files, 460–465  
  content creation, 463–464  
  software requirements, 460  
  verifying availability, 464  
  virtual hosts, 465–467
- Application profile, 553
- Application Stream, 553, 220
- apropos command, 47
- archiving  
  defined, 554  
  files  
    extracting tar files, 73  
    with tar, 72
- arguments  
  defined, 33  
  in shell scripts, 428–429
- asterisk (\*) wildcard, 573
- at command, 281  
  defined, 554  
  task scheduling, 281
- atq command, 281
- atrm command, 281
- attributes  
  defined, 554  
  user-extended, 162–163
- audit log
- defined, 554  
  SELinux messages in, 488–490
- audited, 554
- authentication  
  key-based, 114–115, 451–452  
  to Samba shares, 518
- autofs, 521–523  
  configuring, 522  
  defined, 554  
  defining mounts, 522  
  overview, 521  
  wildcards in, 523
- automount, 521–523  
  configuring, 522  
  defined, 554  
  defining mounts, 522  
  overview, 521  
  wildcards in, 523
- awk command, 93–94

## B

- background processes  
  defined, 554  
  running, 236–237  
  types of, 239
- backslash (\) escape character, 433
- backups  
  of ACLs, 157  
  defined, 554
- Bash. *See also* shell scripting  
  commands  
    command-line completion, 39  
    executing, 33  
    help with, 44–49  
    history, 37–38  
    I/O redirection, 34–35  
    pipes, 36  
    syntax, 32–33  
  defined, 554, 32  
  escaping, 90
- bash -x command, 438
- bash-completion, 39
- Basic Input Output System (BIOS), 554

batch command, 281  
bg command, 237, 238  
binary, 554  
binary notation  
  for IP addresses, 172  
BIOS (Basic Input Output System), 554  
blkid command, 331–332  
Boolean settings for SELinux, 487–488  
boot loaders, 554  
boot process  
  GRUB 2, 394–397  
    changing configuration, 394–395  
    configuration files, 395–396  
    modifying default options, 396–397  
  steps in, 404–405  
systemd targets  
  enabling services, 390–391  
  isolating, 391–394  
  setting default, 394  
  target units, 389–390  
  tasks of, 388–389  
  types of, 388  
  viewing, 391–393  
  wants, 390  
troubleshooting  
  accessing boot prompt, 406–407  
  file system issues, 414–415  
  overview, 405  
  recovering virtual machine access,  
    416–418  
  re-creating initramfs image, 414  
  reinstalling GRUB 2, 413–414  
  rescue disk usage, 408–413  
  resetting root password, 416  
  starting troubleshooting targets,  
    407–408  
boot prompt, accessing, 406–407  
broadcast addresses, 171  
Btrfs, 554  
bunzip2 command, 74  
bzip2 command, 74

## C

cache, 555  
cache tier, 356  
capabilities, 555  
case statement, 436–437  
cat command, 84–85  
CentOS  
  defined, 555  
  installing, 10–24  
  obtaining, 7  
Cert Guide environment setup, 9–10  
certificate authority (CA), 555  
certificates, 555  
chage command, 133–134  
characters  
  counting, 88–89  
  escaping, 433  
chattr command, 163  
chcon command, 481  
chgrp command, 148  
chmod command, 150–152, 155  
chown command  
  group ownership, 148  
  user ownership, 147–148  
chrony  
  defined, 555  
  time service client configuration,  
    537–538  
chroot, 555  
chroot /mnt/sysimage command,  
  409–410, 414  
chvt command, 105  
CIFS (Common Internet File System)  
  defined, 555  
  history of, 516–517  
  mounting through fstab, 521  
  server configuration, 518–519  
  shares  
    authentication, 518  
    discovering, 517–518, 520  
    mounting, 518, 520

cloud, 555  
 command mode (vim), 40  
 command-line completion, 39  
 commands  
     command-line completion, 39  
     executing, 33  
     help with, 44–49  
         /usr/share/doc documentation files, 49  
         --help option, 44–45  
     info command, 48–49  
     man command, 45–48  
     mandb command, 47–48  
     history, 37–38  
     I/O redirection, 34–35  
     LVM management, 353  
     pipes, 36  
     syntax, 32–33  
     vim editor, 40–41

Common Internet File System. *See CIFS*  
 (Common Internet File System)

compression  
     defined, 555  
     overview, 73–74

conditional loops, 432–437  
     case statement, 436–437  
     defined, 555  
     for loops, 429, 434–435  
     if.then.else construction, 432–434  
     until loops, 435–436  
     while loops, 435–436

configuration files  
     for Apache servers, 460–465  
     GRUB 2, 395–396  
     ifcfg, 189  
     modifying, 131  
     rsyslogd, 293, 297  
     in shell environment, 43  
     for user management, 132–133

connections  
     defined, 555  
     devices versus, 180  
     fixed and dynamic IP addresses for, 189  
     SSH server options, 450  
     viewing properties, 182–185  
     viewing status, 181

consoles  
     defined, 555, 102  
     local consoles  
         logging in, 102–103  
         pseudo terminals, 106  
         switching terminals, 103–105

remote access  
     with Secure Shell, 108–110, 112  
     transferring files, 111–112

context labels, 479–481

context switches, 556

context types, 481–485  
     defined, 556  
     finding via man pages, 484–485  
     restoring defaults, 485–486  
     setting, 481–484

contexts, 556

Coordinated Universal Time (UTC), 556, 530

copying files  
     cp command, 65–66  
     scp command, 112

counting words/lines/characters, 88–89

cp command, 65–66

createrepo command, 208

credentials files, 556

cron  
     anacron service, 278–279  
     components of, 274  
     configuration file management, 276–278  
     crond management, 274–275  
     defined, 556  
     exercise, 280  
     security, 280  
     timing, 276

crond, managing, 274–275

crontab command, 277

cryptography, 556  
cut command, 84, 87

## D

daemons, 236  
date command, 532  
daylight saving time, 530  
debugging shell scripts, 438  
deduplication, 556  
default ACLs, 159–160  
default boot options, modifying, 396–397  
default file contexts, restoring, 485–486  
default ownership, 148–149  
default permissions, 160–161  
default routes, 556  
default targets, setting, 394  
default zones in firewalld, 501  
deleting files, 66  
dependencies  
    defined, 556  
    of units, managing, 263–264  
dependency hell, 556, 225  
destinations  
    defined, 556  
    in rsyslogd, 294–296  
device files, 557, 35  
device mappers, 557  
devices  
    connections versus, 180  
    defined, 557  
    mounting, 57–61, 331–332  
    naming, 351–352  
df -hT command, 61  
df -Th command, 59  
dictionary attacks, 446  
direct write logging, 288  
directories. *See also* files  
    defined, 557  
    in FSH, 56–57  
    home, 132  
    listing, 64–65  
    managing, 62–63

mounting, 57–58  
ownership  
    changing groups, 148  
    changing users, 147–148  
    default ownership, 148–149  
    viewing, 146–147  
permissions  
    ACLs, 156–160  
    advanced, 152–156  
    basic, 149–152  
    default, 160–161  
    user-extended attributes, 162–163

disabled mode, 557

disabling  
    root login, 446  
    SELinux, 478–479

disk device types, 315  
disk labels, mounting with, 331–332  
distributions, 557

dmesg  
    analyzing kernel activity, 371–372  
    defined, 557

dnf command, yum command and, 200  
DNS name resolution, 192–193  
documentation files, 49  
dot (), 553, 91  
downloading GPG keys, 206–207  
dracut command  
    defined, 557

re-creating initramfs image, 411–413,  
    414

drivers, 371, 374–375  
    checking availability, 379–380  
dynamic IP addresses, 174, 189  
dynamic routes, 557

## E

echo command, 43  
editing files with vim, 39–41  
elevated permissions  
    running tasks with, 125  
    PolicyKit, 126

- su command, 125
- sudo command, 126
- emergency reset, 108
- emergency.target, 388
- enabling
  - modules, 223
  - SELinux, 475–476
  - services, 390–391
- enforcing mode, 557
- entitlements, 201
- env command, 42
- environments, 557
- EPEL (Extra Packages for Enterprise Linux) repositories, 201
- epoch time, 557, 532
- escaping
  - characters, 433
  - defined, 557
  - regular expressions, 90
- exam preparation, 541–544
  - nondisclosure agreement (NDA), 544
  - registering for exam, 541–542
  - SELinux coverage, 492
  - theoretical pre-assessment exam, 545–547
  - tips for taking exam, 542–544
  - verifying readiness, 541
  - what to bring to exam, 542
- examples
  - /etc/crontab file, 277
  - /etc/default/grub, 395
  - /etc/default/useradd, 132–133
  - /etc/dracut.conf, 412–413
  - /etc/fstab, 333
  - /etc/group, 136
  - /etc/hosts, 191–192
  - /etc/httpd, 464
  - /etc/httpd/conf/httpd.conf, 461–463
  - /etc/logrotate.conf, 298
  - /etc/passwd, 89, 128
  - /etc/shadow, 129
  - /etc/sysconfig/selinux, 476
- /etc/systemd/journald.conf, 303
- /var/log/messages, 291
- anacron configuration, 279
- analyzing kernel activity, 372
- arguments in shell scripts, 428
- basic script example, 426
- blkid command, 332
- case statement, 437
- chage command, 134
- CIFS share discovery, 517
- connection properties, 182–185
- connection status, 181
- context label viewing, 480
- counting with wc command, 89
- cron job in /etc/cron.d, 278
- current environment display, 42
- debugging shell scripts, 438
- df -hT command, 61
- file ownership display, 147
- file system formatting with XFS, 326–327
- filtering with cut command, 87
- findmnt command, 59–60
- firewall configuration, 504
- firewalld services, 502
- for loops, 434
- ftp service file, 503
- GPG key downloads, 206–207
- group ACL changes, 158
- hostname configuration, 190–191
- hostnamectl status command, 373
- id command, 124
- ifcfg configuration files, 189
- if.then.else construction, 433
- ip addr show command, 176
- ip link show command, 177
- ip route show command, 178–179
- journalctl -o verbose command, 301–302
- kernel thread viewing, 239–240
- line anchors, 90
- link properties, 70

listing kernel threads, 370  
log file viewing from journald, 299–300  
log file viewing with systemctl status  
    command, 289  
logging in with Secure Shell, 110  
lsblk command, 349  
lsmod command, 376  
lspci command, 379–380  
LVM device naming, 352  
modinfo command, 377–378  
monitoring time synchronization  
    status, 534–535  
mount command, 58–59  
mount units, 258  
multi-user.target, 389  
newgrp command, 149  
permissions checking, 158  
physical volume verification, 348  
ps aux command, 88  
ps -ef command, 240–241  
ps fax command, 241–242  
pvcreate command, 345  
pvdisplay command, 348  
read command in shell scripts, 430  
regular expression necessity, 89–90  
repository availability verification, 209  
repository file, 204–205  
RULES section of rsyslog.conf, 294  
screen command, 115–116  
sealert command, 490–491  
searching man pages, 46  
SELinux messages in audit.log, 489  
semanage fcontext usage, 483  
service units, 257  
sestatus command, 477  
socket units, 259  
ss -lt command, 179  
systemctl list-dependencies command,  
    263–264  
systemctl show command, 265  
systemctl status command, 262  
systemctl status crond -l command, 275  
systemd mount units for VDO,  
    360–361  
systemd targets, 391–393  
target units, 260  
time zone settings, 536–537  
timedatectl command, 533  
tune2fs command, 327–328  
udevadm monitor command, 375  
unit types in systemd, 256  
until loops, 436  
uptime command, 247  
vgdisplay command, 350  
volume groups resizing verification,  
    354  
web server availability verification, 464  
while loops, 435  
yum groups info command, 218  
yum groups list command, 217  
yum history command, 219  
yum info nmap command, 211–212  
yum install nmap command, 212–213  
yum list command, 214  
yum list kernel command, 215  
yum module info command, 223  
yum module list command, 221–222  
yum module list perl command, 223  
yum search command, 210  
yum update command, 215–216  
execute permissions, 149–152  
executing commands, 33  
exercises  
    ACLs (access control lists), 160  
    advanced permissions, 156  
    Apache virtual host configuration,  
        466–467  
    at task scheduling, 281  
    automount configuration for NFS, 522  
    bash-completion, 39  
    basic permission management, 152  
    connection parameter changes with  
        nmcli, 186  
    context label setting, 483–484

cron task scheduling, 280  
directory management, 62–63  
file management, 67–68  
file system creation, 327  
firewall management with  
  firewall-cmd, 503–505  
GPT partition creation with gdisk,  
  321–324  
GPT partition creation with  
  parted, 325  
grep options, 93  
group account management, 137  
GRUB 2 modifications, 397  
head command, 86  
history (in Bash), 38  
if.then.else construction, 434  
info command, 49  
input in shell scripts, 431  
internal and external commands, 34  
I/O redirection and pipes, 36–37  
isolating targets, 394  
journalctl command, 300–301  
kernel module management, 378  
kernel modules with parameters, 380  
less command, 85  
live log file monitoring, 292  
load average management, 248  
local time management, 534  
logging in with Secure Shell, 109–110  
logical partition creation, 319–320  
logical volume resizing, 355–356  
man -k command, 48  
MBR partition creation with fdisk,  
  316–318  
module management, 224–225  
mounting partitions through /etc/fstab,  
  335  
mounts overview, 60  
network configuration validation, 177  
network connections management with  
  nmcli, 186  
network settings verification, 179–180  
NFS share mounting, 516  
NFS share offering, 515  
package management with yum, 219  
physical volume creation, 346–347  
positional parameters, 429  
preserving systemd journal, 303  
process management from command  
  line, 245  
pseudo terminals, 106  
remote access with public/private keys,  
  114–115  
remote access with Secure Shell, 112  
repository creation, 208–209  
rescuing system, 410–411  
restorecon command, 486  
RPM queries, 228–229  
rsyslog.conf rule changes, 297  
Samba server configuration, 519  
SELinux Boolean settings, 488  
SELinux mode manipulation, 478  
SELinux-specific man pages, 485  
shell environment management, 44  
shell job management, 238  
simple shell script creation, 427  
SMB share discovery and mounting,  
  520  
SSH security option configuration, 449  
Stratis volume management, 358–359  
swap partition creation, 330  
switching terminals, 104  
switching user accounts, 127  
symbolic links and hard links, 71  
tail command, 86  
tar, 75  
time service client configuration, 538  
troubleshooting targets, 408  
tuned, 249  
unit configuration changes, 266  
unit management with systemctl, 261  
user account creation, 135  
VDO storage management, 361  
vim practice, 41

volume group and logical volume creation, 352  
 web server setup, 463  
 wildcard automount configuration, 523  
 exit command, 427  
 exports, 557  
 Ext2, 557  
 Ext3, 557  
 Ext4  
   defined, 557  
   property management, 327–329  
 extended partitions  
   defined, 557  
   on MBR, 319–320  
 external commands, 558, 33  
 Extra Packages for Enterprise Linux (EPEL) repositories, 201  
 extracting tar files, 73

## F

facilities  
   defined, 558  
   in rsyslogd, 294–296  
 fdisk command, 315–320  
 Fedora  
   defined, 558  
   obtaining, 8  
 fg command, 237, 238  
 FHS (Filesystem Hierarchy Standard)  
   defined, 558  
   mounts, 57–61  
   overview, 56–57  
 file command, 73  
 file descriptors, 558  
 file systems. *See also* storage  
   ACL preparation, 157  
   automount, 521–523  
     configuring, 522  
     defining mounts, 522  
     overview, 521  
     wildcards in, 523

CIFS  
   authentication, 518  
   discovering shares, 517–518, 520  
   history of, 516–517  
   mounting shares, 518, 520  
   mounting through fstab, 521  
   server configuration, 518–519  
   creating, 325–327  
   defined, 558  
   mounting, 330–335  
     automating with /etc/fstab, 332–335  
     with device name/UUID/disk label, 331–332  
     manually, 331  
 NFS  
   automount configuration, 522  
   mounting shares, 515–516  
   mounting through fstab, 520–521  
   security, 514  
   versions, 514–515  
   property management, 327–329  
   troubleshooting, 414–415  
   types of, 326  
 files. *See also* directories; text files  
   absolute and relative filenames, 63–64  
   archiving  
     extracting tar files, 73  
     with tar, 72  
   compressing, 73–74  
   copying  
     cp command, 65–66  
     scp command, 112  
   deleting, 66  
   editing with vim, 39–41  
   links  
     creating, 69–70  
     hard links, 68–69, 71  
     removing, 70–71  
     symbolic links, 69, 71  
   listing, 64–65  
   moving, 66  
   ownership

- changing groups, 148
- changing users, 147–148
- default ownership, 148–149
- viewing, 146–147
- permissions
  - ACLs, 156–160
  - advanced, 152–156
  - basic, 149–152
  - default, 160–161
  - user-extended attributes, 162–163
- synchronizing, 112
- transferring securely, 111–112
- wildcards, 61–62
- Filesystem Hierarchy Standard.** *See FHS (Filesystem Hierarchy Standard)*
- filtering text files
  - with `cut` command, 87
  - with `head` command, 86
  - with `tail` command, 86
- `find` command, 147
- finding
  - context types, 484–485
  - packages, 210–211
- `findmnt` command, 59–60
- `firewall-cmd` command, 503–506
- `firewalld`, 500–503
  - defined, 558
  - services, 502–503
  - zones, 501
- firewalls
  - defined, 558
  - `firewall-cmd` command, 503–506
  - `firewalld`, 500–503
    - services, 502–503
    - zones, 501
  - `netfilter`, 500
    - viewing configuration, 504
- first lines of text files, viewing, 86
- fixed IP addresses, 174, 189
- folders, 558. *See also* directories
- foreground processes
  - defined, 559
  - running, 236–237
- for loops, 429, 434–435
- `fsck` command, 414
- `fstab`, 559, 332–335
  - NFS share mounting, 520–521
  - Samba share mounting, 521

## G

- `gdisk` command, 320–324
- GECOS**, 559
- `getenforce` command, 476
- `getfacl` command, 157–159
- `getsebool` command, 487
- GiB, 9
- global unique ID (GUID), 559
- PGP keys, downloading, 206–207
- GPT (GUID Partition Table)**
  - creating
    - with `gdisk` command, 320–324
    - with `parted` command, 324–325
  - defined, 559
  - overview, 313
- graphical applications with Secure Shell, 111
- `graphical.target`, 388
- `grep` command, 242
  - options, 92–93
- group accounts
  - creating, 136–137
  - `groupadd` command, 137
  - `vigr` command, 136–137
  - membership checking, 137
  - property management, 137
  - types of, 135–136
- group owners
  - changing, 148
  - defined, 559
- `groupadd` command, 137

groupmems command, 137  
groupmod command, 137  
groups  
  defined, 559  
  of packages, 216–218  
groups command, 148  
GRUB 2, 394–397  
  accessing boot prompt, 406–407  
  changing configuration, 394–395  
  configuration files, 395–396  
  defined, 559  
  modifying default options, 396–397  
  reinstalling, 411, 413–414  
grub2-install command, 413–414  
grub2-mkconfig command, 396–397  
GUID (global unique ID), 559  
GUID Partition Table. *See GPT (GUID Partition Table)*  
gunzip command, 74  
gzip command, 559, 74

## H

hard links  
  defined, 560  
  exercise, 71  
  overview, 68–69  
hardware clock, 530  
hardware initialization, 371, 374–375  
  checking driver availability, 379–380  
hardware time, 560  
head command, 84, 86  
help with commands, 44–49  
  /usr/share/doc documentation files, 49  
  --help option, 44–45  
  info command, 48–49  
  man command, 45–48  
  mandb command, 47–48  
hexadecimal, 560  
history  
  in Bash, 37–38  
  of CIFS, 516–517  
  of packages, 218–219

home directories, 132  
hostnamectl set-hostname command, 190  
hostnamectl status command, 190, 373  
hostnames, 190–192  
hosts, 170. *See also* virtual hosts  
httpd package, 460  
hwclock command, 532  
hypervisors, 560

## I

id command, 124  
ifcfg configuration files, 189  
ifconfig command, 175  
if.then.else construction, 432–434  
info command, 48–49  
inheritance, 560  
init, 560  
initramfs  
  defined, 560  
  re-creating from rescue disk, 411–414  
inodes, 560, 68  
input in shell scripts, 430–431  
input mode (vim), 40  
input modules, 560  
insmod command, 378  
installing  
  modules, 224  
  packages, 212–213  
RHEL  
  advantages of subscription, 6  
  Cert Guide environment, 9–10  
  free alternatives, 7  
  manual installation, 10–24  
  obtaining, 7  
  repository access, 8  
  setup requirements, 9  
interfaces, 560  
internal commands, 561, 33  
Internet Protocol (IP), 561  
I/O redirection, 34–35  
IP (Internet Protocol), 561  
ip addr command, 175

ip addr show command, 175–176  
 ip command, 175–177  
 ip link command, 175  
 ip link show command, 177  
 ip route command, 175  
 ip route show command, 178  
 iptables command, 561, 500  
 IPv4 addresses  
     binary notation, 172  
     defined, 561, 170  
     fixed versus dynamic, 174  
     overview, 170–171  
     subnet masks, 171  
     validating configuration, 175–177  
 IPv6 addresses  
     defined, 561, 170  
     overview, 171  
 isolating systemd targets, 391–394  
 iterations, 561

## J

jobs  
     defined, 561  
     shell jobs. *See* shell jobs  
 jobs command, 237–238  
 journalctl command, 561, 288, 299–302  
 journalctl -o verbose command, 301–302  
 journald, 299–303  
     defined, 561, 288  
     journalctl command, 299–302  
     overview, 288–289  
     preserving systemd journal, 302–303

## K

kernel  
     analyzing activity, 371–373  
     defined, 561, 370  
     drivers, 371, 374–375  
     upgrading, 381  
 kernel modules, 373, 376–380  
     drivers, checking availability, 379–380  
     listing, 376

loading/unloading, 378  
 parameter management, 380  
 viewing information about, 377–378  
 kernel ring buffer, 561  
 kernel space, 561  
 kernel threads  
     defined, 236  
     listing, 370  
     showing, 239–240  
 Kernel-based Virtual Machine (KVM), 561  
 key-based authentication, 114–115, 451–452  
 key-based logins, 562  
 kill command, 562, 239, 244–245  
 killall command, 245  
 KVM (Kernel-based Virtual Machine), 561

## L

labels, 562  
 last lines of text files, viewing, 86  
 less command, 84–85  
 line anchors, 562, 90  
 lines, counting, 88–89  
 links  
     creating, 69–70  
     hard links, 68–69, 71  
     removing, 70–71  
     symbolic links, 69, 71  
 Linux, 562  
 listing  
     directories, 64–65  
     files, 64–65  
     firewalld services, 502  
     kernel modules, 376  
     kernel threads, 370  
     modules, 221–223  
     packages, 214–215  
 live log file monitoring, 292  
 ln command, 69–70  
 load average for processes, 247

loading kernel modules, 378  
local consoles  
  logging in, 102–103  
  pseudo terminals, 106  
  switching terminals, 103–105  
local time  
  defined, 530  
  managing, 534  
  time zone settings, 535–537  
log files  
  journald, 299–303  
    journalctl command, 299–302  
    overview, 288–289  
    preserving systemd journal, 302–303  
  rotating, 297–299  
  rsyslogd, 293–297  
    configuration files, 293, 297  
    facilities/priorities/destinations,  
      294–296  
    overview, 288–289  
for SELinux  
  in audit log, 488–490  
  sealert command, 490–491  
types of, 288  
viewing  
  with journalctl -o verbose command,  
    301–302  
  from journald, 299–300  
  live monitoring, 292  
  sample content, 290–292  
  with systemctl status command, 289  
  in /var/log, 290  
log rotation  
  defined, 562  
  overview, 297–299  
logger command, 292  
logging in  
  disabling root login, 446  
  with key-based authentication, 114–115  
  to local consoles, 102–103  
  to remote servers, 108–110, 112  
logical AND (`&&`), 553, 433  
logical extent, 562  
logical OR (`||`), 564, 433  
logical partitions  
  defined, 562  
  on MBR, 319–320  
Logical Volume Manager. *See* LVM  
  (Logical Volume Manager)  
logical volumes  
  creating, 344–345, 351–352  
  defined, 562  
  resizing, 353–356  
login shells, 562  
loopback interfaces, 176  
loops. *See* conditional loops  
ls command, 64–65, 70  
ls -l command, 146–147  
lsblk command, 348–349  
lscpu command, 247  
lsmod command, 376  
lspci command, 379–380  
lvcreate command, 353  
lvdisplay command, 353  
lvextend command, 354  
LVM (Logical Volume Manager)  
  advantages of, 343–344  
  architecture, 342–343  
  commands, 353  
  defined, 562  
  device naming, 351–352  
  logical volumes  
    creating, 344–345,  
      351–352  
    resizing, 353–356  
  partitions, creating, 347  
  physical volumes  
    creating, 346–349  
    verifying, 348  
  volume groups  
    creating, 349–350, 352  
    resizing, 353–354

`lvremove` command, 353  
`lvresize` command, 354–355  
`lvs` command, 353

## M

MAC addresses, 173  
`man` command, 45–48  
`man -k` command, 46–48  
`man` pages  
  finding context types, 484–485  
  searching, 46  
  for `semanage` command, 482–483  
`mandb` command, 47–48  
masquerading, 563  
MBR (Master Boot Record)  
  creating with `fdisk`, 315–318  
  defined, 563  
  extended and logical partitions, 319–320  
  overview, 312–313  
measurement units for storage, 314  
`mkfs` command, 326–327  
`modinfo` command, 377–378  
`modprobe` command, 378  
modular kernel. *See* kernel modules  
modules  
  defined, 563, 220  
  enabling, 223  
  information about, 223  
  installing, 224  
  listing, 221–223  
  managing, 221–225  
  terminology, 220  
more command, 85  
mount command, 58–59, 331, 518  
mounting  
  file systems, 330–335  
    automating with `/etc/fstab`, 332–335  
    with device name/UUID/disk label, 331–332  
    manually, 331  
  NFS shares, 515–516, 520–521  
  Samba shares, 518, 520–521

mounts, 57–61  
  defined, 563  
  defining in `automount`, 522  
  in `systemd`, 258  
  for VDO, 360–361  
  wildcard configuration, 523  
moving files, 66  
multiplier, 563  
multi-user.target, 388, 389  
`mv` command, 66

## N

naming devices, 351–352  
nano editor in `systemd`, 266  
NAT (Network Address Translation), 171.  
  *See also* masquerading  
NDA (nondisclosure agreement), 544  
netfilter  
  defined, 563  
  overview, 500  
netmask. *See* subnet masks  
netstat command, 178  
Network Address Translation (NAT), 171.  
  *See also* masquerading  
Network File System. *See* NFS (Network File System)  
network masks. *See* subnet masks  
network time, 563  
Network Time Protocol (NTP)  
  defined, 563  
  overview, 531  
networking  
  configuring, 180–189  
  with `nmcli` command, 181–187  
  with `nmtui` command, 187–189  
  permissions for, 180–181  
DNS name resolution, 192–193  
hostnames, 190–192  
IPv4 addresses, 170–171  
  binary notation, 172  
  fixed versus dynamic, 174  
  subnet masks, 171  
  validating configuration, 175–177

IPv6 addresses, 170, 171  
 MAC addresses, 173  
 port addresses, 173  
     validating, 178–179  
 protocols, 173  
 routing, validating, 178  
 verifying settings, 179–180  
**newgrp** command, 149  
**NFS** (Network File System)  
     automount configuration, 522  
     defined, 563  
     mounting shares, 515–516  
     mounting through fstab, 520–521  
     security, 514  
     versions, 514–515  
**nftables** command, 564, 500  
**nice** command, 564, 242–244  
**nmcli** command, 180–187  
**nm-connection-editor** command, 188  
**nmtui** command, 180, 187–189  
**nodes**, 170  
**nohup** command, 239  
**nondisclosure agreement (NDA)**, 544  
**normal user accounts**, system accounts  
     versus, 127–130  
**NTP** (Network Time Protocol)  
     defined, 563  
     overview, 531

**O**

**octal**, 564  
**optimization with tuned**,  
     248–249  
**options**, 32  
**OR**, 564, 433  
**output modules**, 564  
**ownership**  
     changing groups, 148  
     changing users, 147–148  
     default, 148–149  
     defined, 564  
     viewing, 146–147

**P**

**package groups**, 564  
**Package Module Streams**, 220  
**packages**  
     defined, 564  
     finding, 210–211  
     groups of, 216–218  
     history of, 218–219  
     information about, 211–212  
     installing, 212–213  
     listing, 214–215  
     managing, 219  
     modules. *See* modules  
**Package Module Streams**, 220  
     removing, 213–214  
**repoquery** command, 228  
**repositories**. *See* repositories  
**rpm** command, 225  
     database queries, 226  
     filename parts, 226  
     package file queries, 227–228  
     query usage, 228–229  
     updating, 215–216  
**pagers**, 564  
**parent shells**, 565  
**parent-child relations for shell jobs**, 239  
**parted** command, 324–325, 347  
**partitions**  
     advantages of multiple, 312  
     defined, 565  
     disk device types, 315  
     GPT (GUID Partition Table), 313  
         gdisk command, 320–324  
         parted command, 324–325  
     LVM partition creation, 347  
     MBR (Master Boot Record), 312–313  
         creating with fdisk, 315–318  
         extended and logical partitions,  
             319–320  
     swap files, 330  
     swap partitions, 329–330  
     utilities for, 314–315

- partprobe command, 320
- passphrases
  - configuring, 451–452
  - defined, 565
  - overview, 114
- passwd command, 133–134
- passwords
  - defined, 565
  - dictionary attacks, 446
  - resetting root password, 416
  - user account properties, 133–134
- paths, 565
- performance optimization with tuned, 248–249
- permissions
  - ACLs, 156–160
    - changing/viewing settings, 157–159
    - default ACLs, 159–160
    - file system preparation, 157
    - support for, 156–157
  - advanced, 152–156
  - basic, 149–152
  - default, 160–161
  - defined, 565
  - elevating, 125
    - PolicyKit, 126
    - su command, 125
    - sudo command, 126
  - networking configuration changes, 180–181
  - user-extended attributes, 162–163
- permissive mode, 565
- physical extent, 565
- physical volumes
  - creating, 346–349
  - defined, 565
  - verifying, 348
- PID (process identification number), 566
- pinfo command, 48–49
- pipes
  - defined, 565
  - less command, 84
  - overview, 36
- pkill command, 245
- PolicyKit, 125–126
- pools
  - creating, 357
  - defined, 356
  - managing, 358–359
- port addresses, 173
  - validating, 178–179
- port forwarding, 565
- port scans, avoiding, 447
- Portable Operating System Interface (POSIX), 566
- portmappers, 566
- ports
  - alternative port configuration, 447
  - changing SELinux labels, 447–448
  - defined, 565
- positional parameters in shell scripts, 428–429
- POSIX (Portable Operating System Interface), 566
- preparation for exam, 541–544
  - nondisclosure agreement (NDA), 544
  - registering for exam, 541–542
  - theoretical pre-assessment exam, 545–547
  - tips for taking exam, 542–544
  - verifying readiness, 541
  - what to bring to exam, 542
- primary groups
  - changing, 149
  - defined, 566, 131
- primary partition, 566
- priorities
  - defined, 566
  - of processes, adjusting, 242–244
    - in rsyslogd, 294–296
- private keys, 566
- private network addresses, 170–171
- privileged users. *See* root
- proc, 566
- process identification number (PID), 566

process management  
from command line, 245  
kill command, 244–245  
nice command, 242–244  
performance optimization, 248–249  
processes versus threads, 239–240  
ps command, 240–242  
shell jobs  
    managing, 237–239  
    parent-child relations, 239  
    running in foreground/background,  
        236–237  
top command, 246–248  
types of processes, 236  
processes  
    adjusting priority, 242–244  
    defined, 566  
    information about, 240–242  
    load average, 247  
    sending signals to, 244–245  
    states of, 247  
    threads versus, 239–240  
    types of, 236  
profiles  
    defined, 566, 220  
    tuned, 248  
programmatic API in Stratis, 356  
protocols  
    defined, 566  
    for networking, 173  
ps aux command, 88, 239–240  
ps command, 240–242  
Pseudo Root File System, 566  
pseudo rout mount, 567  
pseudo terminals, 106  
public keys, 567  
pvcreate command, 345, 353  
pvdisplay command, 348, 353  
pvremove command, 353  
pvs command, 353  
pwd command, 63

## Q

querying  
    exercise, 228–229  
    repositories, 228  
    RPM database, 226  
    RPM package files, 227–228  
queues, 567

## R

read command, 430  
read permissions, 149–152  
real-time clock, 567, 530  
reboot  
    defined, 567  
    during exam, 544  
    overview, 106–108  
Red Hat Customer Portal, 567  
Red Hat Enterprise Linux. *See RHEL*  
    (Red Hat Enterprise Linux)  
Red Hat Package Manager, 567  
redirectors, 34–35  
reference clock, 567  
registering  
    for exam, 541–542  
    RHEL, 201  
regular expressions, 89–92  
    awk and sed commands, 93–94  
    defined, 567  
    escaping, 90  
    grep options, 92–93  
    line anchors, 90  
    wildcards, 91–92  
reinstalling GRUB 2, 411, 413–414  
relative filenames  
    defined, 568  
    overview, 63–64  
remote access  
    with key-based authentication,  
        114–115  
    with Secure Shell, 108–110, 112  
    transferring files, 111–112

- rsync command, 112
- scp command, 112
- sftp command, 112
- Remote Procedure Calls (RPC), 568
- removing
  - links, 70–71
  - packages, 213–214
- renice command, 242–244
- repoquery command, 228
- repositories
  - accessing, 8
  - creating, 208–209
  - defined, 568
  - querying, 228
  - role of, 200–201
  - security, 206–207
  - specifying, 202–205
- repository files
  - example, 204–205
  - options, 205
- requirements for RHEL, 9
- rescue disks, 408–413
  - re-creating initramfs image, 411–413, 414
  - reinstalling GRUB 2, 411, 413–414
  - restoring system access, 409–411
- rescue.target, 388
- resident memory, 568
- resizing
  - logical volumes, 353–356
  - volume groups, 353–354
- resolver, 568
- restorecon command, 482, 485–486
- restoring
  - default file contexts, 485–486
  - system access with rescue disk, 409–411
- RHEL (Red Hat Enterprise Linux)
  - defined, 6–7, 567
  - installing manually, 10–24
  - preparation for installation
    - advantages of subscription, 6
    - Cert Guide environment, 9–10
  - free alternatives, 7
  - obtaining, 7
  - repository access, 8
  - setup requirements, 9
  - registering, 201
- rich rules, 568
- rm command, 66
- rmmmod command, 378
- root
  - defined, 568
  - disabling login, 446
  - overview, 124–125
  - PolicyKit, 126
  - resetting password, 416
  - su command, 125
  - sudo command, 126
- root directory, 568
- rotating log files, 297–299
- routing, validating, 178
- RPC (Remote Procedure Calls), 568
- rpm command, 225
  - database queries, 226
  - downloading GPG keys, 206
  - filename parts, 226
  - package file queries, 227–228
  - query usage, 228–229
- RPM packages. *See* packages
- rpm -q --scripts, 227
- rpm -qa command, 226, 228
- rpm -qc command, 226–227
- rpm -qd command, 226–227
- rpm -qf command, 226–227
- rpm -qi command, 226–227
- rpm -ql command, 226–227
- rpm -qp command, 227–228
- rpm -qR command, 227
- rpm -V command, 228
- rpm -Va command, 228
- rsync command, 112
- rsyslogd, 293–297
  - configuration files, 293, 297
  - defined, 568, 288

facilities/priorities/destinations, 294–296  
overview, 288–289  
RULES section of rsyslog.conf, 294  
running processes, 247

## S

Samba  
defined, 568  
history of CIFS, 516–517  
server configuration, 518–519  
shares  
authentication, 518  
discovering, 517–518, 520  
mounting, 518, 520  
mounting through fstab, 521  
SAN (storage-area network), 570  
scheduler, 568  
scheduling tasks  
at, 281  
cron  
anacron service, 278–279  
components of, 274  
configuration file management, 276–278  
crond management, 274–275  
exercise, 280  
security, 280  
timing, 276  
Scientific Linux  
defined, 568  
obtaining, 8  
scp command, 112  
screen command, 115–116  
scripts. *See* shell scripting  
sealert command, 490–491  
searching  
man pages, 46  
text files, 89–92  
secondary groups, 569, 131

Secure Shell. *See* SSH (Secure Shell)  
Secure Sockets Layer (SSL). *See*  
Transport Layer Security (TLS)  
security  
cron, 280  
for NFS, 514  
repositories, 206–207  
SSH server hardening, 446–449  
alternative port configuration, 447  
disabling root login, 446  
limiting user access, 448–449  
SELinux port labels, 447–448  
sed command, 93–94, 110  
SELinux  
Boolean settings, 487–488  
changing port labels, 447–448  
context labels, 479–481  
context types, 481–485  
finding via man pages, 484–485  
restoring defaults, 485–486  
setting, 481–484  
defined, 569  
disabling, 478–479  
elements of, 475  
enabling, 475–476  
exam preparation for, 492  
log files  
in audit log, 488–490  
sealert command, 490–491  
modes, 475–479  
SELinux Policy, 569  
semanage command, 481–483  
semanage port command, 447–448  
Server Message Block. *See* SMB (Server Message Block)  
services  
defined, 569, 256  
enabling, 390–391  
in firewalld, 502–503  
in systemd, 257–258  
session options for SSH server, 450

sestatus command, 476–477  
 set group ID (SGID) permission, 153–155  
 set user ID (SUID) permission, 152–153, 155  
 setenforce command, 476  
 setfacl command, 157–159  
 setroubleshoot-server package, 491  
 setsebool command, 488  
 setup requirements for RHEL, 9  
 sftp command, 112  
 SGID (set group ID) permission, 153–155  
 shares  
 CIFS  
   authentication, 518  
   discovering, 517–518, 520  
   mounting, 518, 520  
   mounting through fstab, 521  
 defined, 569  
 NFS  
   mounting, 515–516  
   mounting through fstab, 520–521  
 shebang (#!), 569, 426  
 shell environment  
   /etc/motd and /etc/issue, 43  
   configuration files, 43  
   variables, 42–43  
 shell jobs  
   defined, 236  
   managing, 237–239  
   parent-child relations, 239  
   running in foreground/background, 236–237  
 shell metacharacters, 569  
 shell scripting  
   arguments, 428–429  
   conditional loops, 432–437  
     case statement, 436–437  
     for loops, 429, 434–435  
     if.then.else construction, 432–434  
   until loops, 435–436  
   while loops, 435–436  
 debugging scripts, 438  
 elements of, 426–427  
 variables, 430–431  
 shells, 569, 32. *See also* Bash; shell scripting  
 showmount command, 516  
 signals  
   defined, 569  
   sending to processes, 244–245  
 sleeping processes, 247  
 SMB (Server Message Block)  
   defined, 569  
   history of CIFS, 516–517  
   server configuration, 518–519  
 shares  
   authentication, 518  
   discovering, 517–518, 520  
   mounting, 518, 520  
   mounting through fstab, 521  
 smbclient command, 517–518  
 snapshots  
   defined, 569, 344  
   managing, 358  
   in Stratis, 356  
 sockets in systemd, 259  
 soft links. *See* symbolic links  
 software clock, 530  
 software management. *See also* yum command  
 modules  
   enabling, 223  
   information about, 223  
   installing, 224  
   listing, 221–223  
   managing, 221–225  
   terminology, 220  
 packages  
   finding, 210–211  
   groups of, 216–218

history of, 218–219  
 information about, 211–212  
 installing, 212–213  
 listing, 214–215  
 managing, 219  
 Package Module Streams, 220  
 removing, 213–214  
 updating, 215–216  
 registering RHEL, 201  
 repoquery command, 228  
 repositories  
   creating, 208–209  
   querying, 228  
   role of, 200–201  
   security, 206–207  
   specifying, 202–205  
 rpm command, 225  
   database queries, 226  
   filename parts, 226  
   package file queries, 227–228  
   query usage, 228–229  
   subscription management, 201  
 software requirements for Apache servers, 460  
 software time. *See* system time  
 sort command, 84, 87–88  
 sorting, text files with sort command, 87–88  
 source context, 569  
 special permissions. *See also* advanced permissions  
 ss -lt command, 178–179  
 SSH (Secure Shell)  
   connection options, 450  
   defined, 569, 108  
   graphical applications with, 111  
   key-based authentication, 114–115, 451–452  
   list of configuration options, 451  
   remote access with, 108–110, 112  
   server hardening, 446–449  
 alternative port configuration, 447  
 disabling root login, 446  
 limiting user access, 448–449  
 SELinux port labels, 447–448  
 session options, 450  
 transferring files, 111–112  
   rsync command, 112  
   scp command, 112  
   sftp command, 112  
 ssh command, 108–110, 111  
 ssh-add command, 452  
 ssh-agent command, 452  
 ssh-copy-id command, 114  
 sshd. *See* SSH (Secure Shell)  
 ssh-keygen command, 114  
 SSL (Secure Sockets Layer). *See also* Transport Layer Security (TLS)  
 star command, 73  
 static routes, 570  
 STDERR (standard error)  
   defined, 570  
   overview, 34  
 STDIN (standard input)  
   defined, 570  
   overview, 34  
 STDOUT (standard output)  
   defined, 570  
   overview, 34  
 sticky bit, 154–155  
 stopped processes, 247  
 storage. *See also* file systems  
   LVM  
     advantages of, 343–344  
     architecture, 342–343  
     commands, 353  
     device naming, 351–352  
     logical volume creation, 344–345, 351–352  
     logical volume resizing, 353–356  
     partition creation, 347

- physical volume creation, 346–349
- physical volume verification, 348
- volume group creation, 349–350, 352
- volume group resizing, 353–354
- measurement units, 314
- partitions
  - advantages of multiple, 312
  - disk device types, 315
  - formatting with file system, 326–327
  - GPT (GUID Partition Table), 313, 320–325
  - LVM partition creation, 347
  - MBR (Master Boot Record), 312–313, 315–320
  - swap files, 330
  - swap partitions, 329–330
  - utilities for, 314–315
- Stratis
  - architecture, 356–357
  - features of, 356
  - pool creation, 357
  - pool management, 358–359
- VDO
  - configuring, 360–361
  - overview, 359–360
- storage-area network (SAN), 570
- Stratis
  - architecture, 356–357
  - defined, 570
  - features of, 356
  - pools
    - creating, 357
    - managing, 358–359
  - stratis blockdev command, 358
  - stratis filesystem command, 358
  - stratis pool add-data command, 358
  - stratis pool command, 358
  - stratum, 570
  - streams, 220
  - su command, 125
- subnet masks
  - defined, 570
  - overview, 171
- subscription management, 201
- subscription-manager tool, 201
- subshells, 570
- sudo command, 125, 126
- SUID (set user ID) permission, 152–153, 155
- superuser. *See* root
- swap files, 330
- swap partitions, 329–330
- switching
  - terminals, 103–105
  - user accounts, 127
- symbolic links
  - defined, 570
  - exercise, 71
  - overview, 69
- synchronizing
  - files, 112
  - time, 534–535
- sysfs, 570
- system accounts, normal user accounts
  - versus, 127–130
- system logging. *See* log files
- system time, 570, 530
- systemctl command, 256, 261–263
- systemctl disable command, 390
- systemctl edit command, 265
- systemctl enable command, 260, 390
- systemctl get-default command, 394
- systemctl halt command, 107
- systemctl isolate command, 393
- systemctl list-dependencies command, 260, 263–264
- systemctl poweroff command, 107
- systemctl set-default command, 394
- systemctl show command, 265
- systemctl status command, 262, 289, 464

- systemctl status crond -l command, 274–275
- systemctl status -l chronyd command, 534–535
- systemctl status NetworkManager command, 180
- systemd
  - defined, 570
  - preserving journal, 302–303
  - rebooting, 107
  - units
    - configuration changes, 266
    - dependency management, 263–264
    - locations, 256–257
    - managing, 261–263
    - mounts, 258, 360–361
    - option management, 265–266
    - services, 257–258
    - sockets, 259
    - targets, 259–260
    - types of, 256
  - systemd targets
    - enabling services, 390–391
    - isolating, 391–394
    - setting default, 394
    - target units, 389–390
    - tasks of, 388–389
    - types of, 388
    - viewing, 391–393
    - wants, 390
  - systemd-udevd, 374
- T**
  - tac command, 85
  - tail command, 84, 86
  - tail -f command, 292
  - tainted kernel, 571, 371
  - Tape ARchiver (*tar*) utility. *See tar*, 71–73
    - compressing files, 73–74
    - creating archives, 72
    - defined, 571
- exercise, 75
- extracting files, 73
- options, 74
- target context, 571
- targets
  - defined, 571
  - starting for troubleshooting, 407–408
- in systemd, 259–260
  - enabling services, 390–391
  - isolating, 391–394
  - setting default, 394
  - target units, 389–390
  - tasks of, 388–389
  - types of, 388
  - viewing, 391–393
  - wants, 390
- task scheduling
  - at, 281
  - cron
    - anacron service, 278–279
    - components of, 274
    - configuration file management, 276–278
    - crond management, 274–275
    - exercise, 280
    - security, 280
    - timing, 276
- terminals
  - defined, 571, 102
  - pseudo, 106
  - screen command, 115–116
  - switching, 103–105
    - virtual, 104–105
- test command, 430–431, 432
- text files
  - counting words/lines/characters with
    - wc command, 88–89
  - filtering
    - with cut command, 87
    - with head command, 86
    - with tail command, 86

- regular expressions, 89–92
  - awk and sed commands, 93–94
  - escaping, 90
  - grep options, 92–93
  - line anchors, 90
  - wildcards, 91–92
  - sorting with sort command, 87–88
  - tools for, 80–84
  - viewing
    - with cat command, 85
    - first/last lines of, 86
    - with less command, 84–85
  - theoretical pre-assessment exam, 545–547
  - thin allocation, 571
  - thin provisioning, 356
  - threads
    - defined, 571, 236
    - processes versus, 239–240
  - time
    - date command, 532
    - epoch time, 532
    - hwclock command, 532
    - local time management, 534
    - monitoring synchronization status, 534–535
    - NTP (Network Time Protocol), 531
    - time service clients, 537–538
    - time zone settings, 535–537
    - timedatectl command, 532, 533
    - types of, 530
  - time service clients, configuring, 537–538
  - time stamps, 571
  - time synchronization, 571
  - time zone settings, 535–537
  - timedatectl command, 532–533
  - timers, 571
  - timing in cron, 276
  - TLS (Transport Layer Security), 571
  - top command, 246–248
  - transferring, files securely, 111–112
  - Transport Layer Security (TLS), 571
  - troubleshooting boot process
    - accessing boot prompt, 406–407
    - file system issues, 414–415
    - overview, 405
    - recovering virtual machine access, 416–418
    - re-creating initramfs image, 414
    - reinstalling GRUB 2, 413–414
    - rescue disk usage, 408–413
    - resetting root password, 416
    - starting troubleshooting targets, 407–408
  - TTY, 571
  - tune2fs command, 327–329
  - tuned
    - defined, 571
    - performance optimization, 248–249
    - profile overview, 248
  - tuned-adm command, 249
  - tzselect command, 536–537
- U**
- udev, 572
  - udevadm monitor command, 374–375
  - UEFI (Unified Extensible Firmware Interface), 572
  - umask
    - defined, 572
    - setting default permissions, 160–161
  - umount command, 572, 331
  - uname command, 373
  - Unified Extensible Firmware Interface (UEFI), 572
  - uninterruptable sleep processes, 247
  - units
    - configuration changes, 266
    - defined, 572
    - dependency management, 263–264
    - locations, 256–257
    - managing, 261–263
    - mounts, 258, 360–361
    - option management, 265–266
    - services, 257–258

sockets, 259  
 targets, 259–260, 389–390  
 types of, 256  
**universally unique ID (UUID)**  
 defined, 572  
 mounting with, 331–332  
 unloading kernel modules, 378  
 unprivileged users, 572  
 until loops, 435–436  
 updating  
   `mandb` database, 47–48  
   packages, 215–216  
 upgrading kernel, 381  
 uptime command, 247  
 user accounts  
   creating, 131–132, 135  
     home directories, 132  
     modifying configuration files, 131  
     `useradd` command, 131  
   `id` command, 124  
   limiting SSH server access, 448–449  
   password properties, 133–134  
   property management, 132–134  
   root, 124–125  
     PolicyKit, 126  
     `su` command, 125  
     `sudo` command, 126  
   switching, 127  
   system versus normal accounts, 127–130  
     user environment, creating, 134  
   user environments, creating, 134  
   user ownership, changing, 147–148  
   user space, 572  
   `useradd` command, 131  
   `userdel` command, 131  
   user-extended attributes, 162–163  
   `usermod` command, 132  
   users, 572  
**UTC (Coordinated Universal Time),**  
 556, 530

**UUID (universally unique ID)**  
 defined, 572  
 mounting with, 331–332

**V**

validating  
 IPv4 address configuration, 175–177  
 port availability, 178–179  
 routing, 178  
 values, 572  
 variables  
 defined, 572  
 in shell environment, 42–43  
 in shell scripts, 430–431  
**VDO (Virtual Data Optimizer)**  
 configuring, 360–361  
 defined, 572  
 overview, 359–360  
 verifying  
 exam readiness, 541  
 network settings, 179–180  
 physical volumes, 348  
 web server availability, 464  
**VFAT, 572**  
**vgcreate command, 349–350, 353**  
**vgdisplay command, 350, 353**  
**vgextend command, 353–354**  
**vgreduce command, 353–354**  
**vgremove command, 353**  
**vgs command, 353, 354**  
 viewing  
 ACL settings, 157–159  
 connection properties, 182–185  
 connection status, 181  
 context labels, 480  
 firewall configuration, 504  
 hostname configuration, 190–191  
 kernel module information, 377–378  
 log files

- with `journalctl -o verbose` command, 301–302
  - from `journald`, 299–300
  - live monitoring, 292
  - sample content, 290–292
  - with `systemctl status` command, 289
  - in `/var/log`, 290
  - ownership, 146–147
  - systemd targets, 391–393
  - text files
    - with `cat` command, 85
    - first/last lines of, 86
    - with `less` command, 84–85
  - `vigr` command, 136–137
  - `vim` editor
    - commands, 40–41
    - overview, 39–41
    - in `systemd`, 266
  - `vimtutor` command, 40
  - `vipw` command, 131
  - virtual console `tty1`, 105
  - Virtual Data Optimizer. *See* VDO (Virtual Data Optimizer)
  - virtual hosts
    - for Apache servers, 465–467
    - defined, 572
  - virtual machines (VMs), recovering access, 416–418
  - virtual memory, 572
  - virtual terminals, 104–105
  - `visudo` command, 126
  - VMs (virtual machines), recovering access, 416–418
  - volume groups
    - creating, 349–350, 352
    - defined, 572
    - resizing, 353–354
  - volume-managing file systems, 356
- W**
- `want`, 573
  - wants, 573, 390
  - `wc` command, 84, 88–89
- web servers. *See* Apache servers
  - while loops, 435–436
  - wildcards
    - in `automount`, 523
    - defined, 573
    - file management, 61–62
    - regular expressions, 91–92
  - words, counting, 88–89
  - write permissions, 149–152
- X**
- `X forwarding`, 111
  - `XFS`
    - defined, 573
    - property management, 329
  - `xfs_admin` command, 329
- Y**
- `YUM` (Yellowdog Update, Modified)
    - defined, 573, 200
    - repositories, role of, 200–201
  - `yum` command
    - common tasks, 209–210
    - `dnf` command and, 200
    - modules
      - enabling, 223
      - information about, 223
      - installing, 224
      - listing, 221–223
      - managing, 221–225
    - packages
      - finding, 210–211
      - groups of, 216–218
      - history of, 218–219
      - information about, 211–212
      - installing, 212–213
      - listing, 214–215
      - managing, 219
      - removing, 213–214
      - updating, 215–216
  - `yum group` command, 216
  - `yum groupinstall` command, 216

yum groups info command, 217–218  
yum groups list command, 216–217  
yum history command, 218–219  
yum info command, 211–212  
yum install command, 212–213, 225  
yum install kernel command, 381  
yum list command, 214–215  
yum localinstall command, 225  
yum module enable command, 223  
yum module info command, 223  
yum module install command, 224  
yum module list command, 221–223  
yum provides command, 211

yum remove command, 213–214  
yum repolist command, 209  
yum search command, 210–211  
yum update command, 215–216  
yum upgrade kernel command, 381  
yum whatprovides command, 211

## Z

zombie processes, 247  
zombies, 573  
zones  
    defined, 573  
    in firewalld, 501