Pro Nagios 2.0

■■■

James Turnbull

Apress®

Pro Nagios 2.0

Copyright © 2006 by James Turnbull

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN-13: 978-1-59059-609-8

ISBN-10: 1-59059-609-9

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Jim Sumser
Technical Reviewer: Justin Kulikowski
Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Jason Gilmore,
Jonathan Hassell, James Huddleston, Chris Mills, Matthew Moodie, Dominic Shakeshaft,
Jim Sumser, Matt Wade
Project Manager: Elizabeth Seymour
Copy Edit Manager: Nicole LeClerc
Copy Editor: Liz Welch
Assistant Production Director: Kari Brooks-Copony
Production Editor: Kelly Winquist
Compositor: Linda Weidemann, Wolf Creek Press
Proofreader: Nancy Sixsmith
Indexer: John Collin
Artist: Kinetic Publishing Services, LLC
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail `orders-ny@springer-sbm.com`, or visit `http://www.springeronline.com`.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail `info@apress.com`, or visit `http://www.apress.com`.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

The source code for this book is available to readers at `http://www.apress.com` in the Source Code section.

Contents

About the Author . . . xiii
About the Technical Reviewer . . . xv
Acknowledgments . . . xvii
Introduction . . . xix

■CHAPTER 1 **Installation** . . . 1

Positioning the Server. . . . 1
Choosing Software and Hardware . . . 3
Capacity Planning . . . 4
Redundancy and Backup . . . 5
Installing the Nagios Software. . . . 5
    Prerequisites for Software Installation . . . 6
    Installing the Nagios Server . . . 9
    Installing the Nagios Plug-ins . . . 17
Configuring Your Web Server for Nagios . . . 21
    Basic Configuration . . . 22
    Virtual Server Configuration . . . 24
    Configuring Your Web Server with an RPM Installation. . . . 25
    Restarting Apache . . . 26
    Testing . . . 26
Checkpoint . . . 27
Resources . . . 28
    Mailing Lists . . . 28
    Sites . . . 28

■CHAPTER 2 **Basic Object Configuration** . . . 29

How Does Nagios Work? . . . 29
How Is Nagios Configured? . . . 30
    Getting Started with Your Configuration . . . 32
    Specifying Your Configuration Files . . . 32
Defining Nagios Configuration Objects . . . 35

Defining Your First Host 36
Defining the Hostname and Address 37
Parents, Host Groups, and Contact Groups 38
Checking the Host 39
Notifications 45
Flapping 47
Event Handling 49
Retention of Status 50
State Stalking, Obsession, and Performance Data 52
Defining Services. 54
Basic Service Directives 55
Service Checking 56
Service Status and Notifications 63
Service Flapping and Event Handling 65
Service Stalking and Obsession 66
Other Directives 66
Using Templates for Objects Definition 67
Contact Objects 72
Grouping Objects. 75
Host Group Objects 76
Service Group Objects. 77
Contact Group Objects 77
Defining Time Periods. 78
Defining Commands 79
Check Commands 79
Event Handler Commands 83
Notification Commands. 84
Checkpoint 84
Resources. 85

CHAPTER 3 Security and Administration 87

General Security Guidelines. 87
Do Not Run Nagios As the root User. 88
Securing and Administering for External Commands 88
Securing the Web Console. 90
Web Console Authentication with Apache. 91
Nagios Authentication and Authorization. 97

Nagios Administration. 100
Starting and Stopping the Nagios Server. 101
Nagios init Script 106
Logging 107
Checkpoints 110
Resources. 111

CHAPTER 4 Using the Web Console 113

General 115
Monitoring. 115
Tactical Monitoring Overview 115
Service Detail 118
Host Detail. 125
Host and Service Group Views. 127
Process Information. 130
Scheduling Queue 132
Other Items in the Monitoring Menu. 133
Reporting 134
The Availability Report 134
The Event Log Report 140
Configuration 140
Checkpoints 142

CHAPTER 5 Monitoring Hosts and Services 143

Introduction to Monitoring 144
Monitoring Hosts 144
Monitoring Services. 145
Local Unix Monitoring. 147
Monitoring Network-Based Services 154
Remote Monitoring 161
Monitoring via NRPE 162
Monitoring via SSH 175
Monitoring via SMNP. 181
Monitoring Windows. 187
NSClient++ 188
Checkpoint 205
Resources. 205
Books. 205
Sites. 205

CHAPTER 6 **Advanced Commands** 207

Macros. 207
On-Demand Macros 208
Macros As Environmental Variables 209
Event Handlers 210
Notifications 213
Sending Notifications via Instant Messenger 217
Notification Aggregation and Suppression 220
External Commands 221
Processing Checks Results with External Commands. 224
External Commands for Adaptive Monitoring 225
Performance Data 227
Processing Performance Data 228
Using Performance Data. 231
Checkpoints 246
Resources 247

CHAPTER 7 **Advanced Object Configuration** 249

Host and Service Dependencies 250
Service Dependencies. 250
Service Dependency Shortcuts 253
Inheritance 254
Host Dependencies 256
Notification Escalations 258
Service Notification Escalations 259
Service Escalation Shortcuts 262
Host Escalations. 264
Extended Host and Service Information Definitions. 265
Checkpoint 267

CHAPTER 8 **Distributed Monitoring, Redundancy, and Failover** 269

Distributed Monitoring 269
Distributed Server Configuration. 271
Central Server Configuration 280
Redundancy and Failover. 289
Configuring the Master Server. 290
Configuring the Slave Server 294
Failover Process. 297

Checkpoint 298
Resources 298
Sites 298

CHAPTER 9 Integrating Nagios 299

syslog-NG and Nagios 299
Installing the Remote Host 300
Configuring the Nagios Server 309
Wrapping Up 313
Snort 313
Configuring Snort for Integration 314
Configuring syslog-NG 315
Configuring Nagios 316
Wrapping Up 317
Integrating with MRTG, Cacti, and Related Tools 317
Querying MRTG Log Files 318
Querying RRD Databases 322
SNMP Traps and Nagios 323
Receiving SNMP Traps 325
Sending SNMP Traps 336
Checkpoint 340
Resources 341
Books 341
Sites 341
MIB Files 341

CHAPTER 10 Developing Plug-ins 343

Writing Your First Plug-in 343
Writing Perl Plug-ins 350
Other Guidelines 355
Specifying Threshold Ranges 355
Specifying Performance Data 356
Commands and Files 357
Plug-in Timeouts 358
Command-Line Options 358
Other Guidelines 359

Nagios Event Broker 359
Helloworld 360
NDO Utilities 362
Other Sources of Information. 365
Checkpoints 366
Resources 366

INDEX 367