Contents

Foreword to the second edition **21**

Introduction **25**

I From Source Code to a Running Installation 35

1 Installation **37**

1.1 Preparations 38

1.1.1 Determining and setting up the required users 38

1.2 Compiling Source Code 39

1.3 Starting Nagios Automatically 43

1.4 Installing and Testing Plugins 43

1.4.1 Installation 44

1.4.2 Plugin test 45

1.5 Configuration of the Web Interface 47

1.5.1 Setting up Apache 47

1.5.2 SELinux 48

1.5.3 User authentication 49

2 Nagios Configuration **53**

2.1 The Main Configuration File `nagios.cfg` 55

2.2 Objects—an Overview 59

2.3 Defining the Machines to Be Monitored, with `host` 62

2.4 Grouping Computers Together with `hostgroup` 65

2.5 Defining Services to Be Monitored with `service` 66

2.6 Grouping Services Together with `servicegroup` 69

2.7 Defining Addressees for Error Messages: `contact` 70
2.8 The Message Recipient: `contactgroup` 72
2.9 When Nagios Needs to Do Something: The `command` Object . . 72
2.10 Defining a Time Period with `timeperiod` 74
2.11 Templates 75
2.12 Configuration Aids for Those Too Lazy to Type 76
2.12.1 Defining services for several computers 76
2.12.2 One host group for all computers 77
2.12.3 Other configuration aids 77
2.13 CGI Configuration in `cgi.cfg` 77
2.14 The Resources File `resource.cfg` 79

3 Startup **81**
3.1 Checking the Configuration 81
3.2 Getting Monitoring Started 84
3.2.1 Manual start 84
3.2.2 Making configuration changes come into effect 84
3.3 Overview of the Web Interface 85

II In More Detail . . . **89**

4 Nagios Basics **91**
4.1 Taking into Account the Network Topology 92
4.2 On-Demand Host Checks vs. Periodic Reachability Tests 95
4.3 States of Hosts and Services 96

5 Service Checks and How They Are Performed **99**
5.1 Testing Network Services Directly 101
5.2 Running Plugins via Secure Shell on the Remote Computer . . 102
5.3 The Nagios Remote Plugin Executor 102
5.4 Monitoring via SNMP 103
5.5 The Nagios Service Check Acceptor 104

6 Plugins for Network Services **105**
6.1 Standard Options 108

6.2 Reachability Test with Ping 108
6.2.1 check_icmp as a Service Check 111
6.2.2 check_icmp as a Host Check 111
6.3 Monitoring Mail Servers 113
6.3.1 Monitoring SMTP with check_smtp 113
6.3.2 POP and IMAP 115
6.4 Monitoring FTP and Web Servers 118
6.4.1 FTP services 119
6.4.2 Web server control via HTTP 119
6.4.3 Monitoring Web proxies 123
6.5 Domain Name Server Under Control 127
6.5.1 DNS check with nslookup 128
6.5.2 Monitoring the name server with dig 129
6.6 Querying the Secure Shell Server 131
6.7 Generic Network Plugins 132
6.7.1 Testing TCP ports 132
6.7.2 Monitoring UDP ports 135
6.8 Monitoring Databases 136
6.8.1 PostgreSQL 137
6.8.2 MySQL 141
6.9 Monitoring LDAP Directory Services 143
6.10 Checking a DHCP Server 146
6.11 Monitoring UPS with the Network UPS Tools 149
6.12 Health Check of an NTP Server with check_ntp_peer 154

7 Testing Local Resources 157

7.1 Free Hard Drive Capacity 158
7.2 Utilization of the Swap Space 162
7.3 Testing the System Load 162
7.4 Monitoring Processes 163
7.5 Checking Log Files 167
7.5.1 The standard plugin check_log 168
7.5.2 The modern variation: check_logs.pl 169
7.5.3 The Swiss Army knife: check_logfiles 170

7.6 Keeping Tabs on the Number of Logged-In Users 177
7.7 Checking the System Time 177
7.7.1 Checking the system time via NTP 177
7.7.2 Checking system time with the time protocol 178
7.8 Regularly Checking the Status of the Mail Queue 180
7.9 Keeping an Eye on the Modification Date of a File 181
7.10 Monitoring UPSs with `apcupsd` 182
7.11 Nagios Monitors Itself 183
7.11.1 Running the plugin manually with a script 184
7.12 Hardware Checks with LM Sensors 184

8 Plugins for Special Tasks 187
8.1 The Dummy Plugin for Tests 188
8.2 Negating Plugin Results 188
8.3 Inserting Hyperlinks with `urlize` 189
8.4 Checking Host or Service Clusters as an Entity 189
8.5 Summarizing Checks with `check_multi` 191
8.5.1 Multiple-line plugin output 193
8.5.2 Installation requirements 194
8.5.3 Installation and testing 194
8.5.4 Configuration file 195
8.5.5 Command-line parameters 196
8.5.6 Performance data and PNP 198
8.5.7 Simple business process monitoring 199

9 Executing Plugins via SSH 205
9.1 The `check_by_ssh` Plugin 206
9.2 Configuring SSH 208
9.2.1 Generating SSH key pairs on the Nagios server 208
9.2.2 Setting up the user `nagios` on the target host 209
9.2.3 Checking the SSH connection and `check_by_ssh` . . . 209
9.3 Nagios Configuration 210

10 The Nagios Remote Plugin Executor (NRPE) 213
10.1 Installation 214

10.1.1 Distribution-specific packages 214
10.1.2 Installation from the source code 215
10.2 Starting via the inet Daemon 216
10.2.1 `xinetd` configuration 216
10.2.2 `inetd` configuration 217
10.2.3 Is the Inet daemon watching on the NRPE port? 218
10.3 NRPE Configuration on the Computer to Be Monitored 218
10.3.1 Passing parameters on to local plugins 220
10.4 NRPE Function Test 221
10.5 Nagios Configuration 222
10.5.1 NRPE without passing parameters on 222
10.5.2 Passing parameters on in NRPE 223
10.5.3 Optimizing the configuration 223
10.6 Indirect Checks 224

11 Collecting Information Relevant for Monitoring with SNMP 227
11.1 Introduction to SNMP 228
11.1.1 The Management Information Base 229
11.1.2 SNMP protocol versions 233
11.2 NET-SNMP 234
11.2.1 Tools for SNMP requests 235
11.2.2 The NET-SNMP daemon 238
11.3 Nagios's Own SNMP Plugins 246
11.3.1 The generic SNMP plugin `check_snmp` 246
11.3.2 Checking several interfaces simultaneously 252
11.3.3 Testing the operating status of individual interfaces . . . 254
11.4 Other SNMP-based Plugins 255
11.4.1 Monitoring hard drive space and processes with `nagios-snmp-plugins` 256
11.4.2 Observing the load on network interfaces with `check-iftraffic` 257
11.4.3 The `manubulon.com` plugins for special application purposes 259

12 The Nagios Notification System 265

12.1 Who Should be Informed of What, When? 266

12.2 When Does a Message Occur? 267

12.3 The Message Filter 267

12.3.1 Switching messages on and off systemwide 268

12.3.2 Enabling and suppressing computer and service-related messages 269

12.3.3 Person-related filter options 272

12.3.4 Case examples 273

12.4 External Notification Programs 275

12.4.1 Notification via e-mail 276

12.4.2 Notification via SMS 278

12.5 Escalation Management 282

12.6 Accounting for Dependencies between Hosts and Services . . . 285

12.6.1 The standard case: service dependencies 285

12.6.2 Only in exceptional cases: host dependencies 289

13 Passive Tests with the External Command File 291

13.1 The Interface for External Commands 292

13.2 Passive Service Checks 293

13.3 Passive Host Checks 294

13.4 Reacting to Out-of-Date Information of Passive Checks 295

14 The Nagios Service Check Acceptor (NSCA) 299

14.1 Installation 300

14.2 Configuring the Nagios Server 301

14.2.1 The configuration file `nsca.cfg` 301

14.2.2 Configuring the inet daemon 303

14.3 Client-side Configuration 304

14.4 Sending Test Results to the Server 305

14.5 Application Example I: Integrating syslog and Nagios 306

14.5.1 Preparing `syslog-ng` for use with Nagios 307

14.5.2 Nagios configuration: volatile services 309

14.5.3 Resetting error states manually 310

14.6 Application Example II: Processing SNMP Traps 312

14.6.1 Receiving traps with `snmptrapd` 312
14.6.2 Passing on traps to NSCA 314
14.6.3 The matching service definition 315

15 Distributed Monitoring **317**
15.1 Switching On the OCSP/OCHP Mechanism 318
15.2 Defining OCSP/OCHP Commands 319
15.3 Practical Scenarios 321
15.3.1 Avoiding redundancy in configuration files 321
15.3.2 Defining templates 322

III The Web Interface and Other Ways to Visualize Nagios Data **325**

16 The Classical Web Interface **327**
16.1 Recognizing and Acting On Problems 330
16.1.1 Comments on problematic hosts 330
16.1.2 Taking responsibility for problems 332
16.2 An Overview of the Individual CGI Programs 334
16.2.1 Variations in status display: `status.cgi` 334
16.2.2 Additional information and control center: `extinfo.cgi` 339
16.2.3 Interface for external commands: `cmd.cgi` 343
16.2.4 The most important things at a glance: `tac.cgi` 345
16.2.5 The topological map of the network: `statusmap.cgi` 346
16.2.6 Navigation in 3D: `statuswrl.cgi` 348
16.2.7 Querying the status with a cell phone: `statuswml.cgi` 350
16.2.8 Analyzing disrupted partial networks: `outages.cgi` . 350
16.2.9 Querying the object definition with `config.cgi` 351
16.2.10 Availability statistics: `avail.cgi` 351
16.2.11 What events occur, how often?—`histogram.cgi` . . . 353
16.2.12 Filtering log entries after specific states: `history.cgi` 354
16.2.13 Who was told what, when?—`notifications.cgi` . . 355

16.2.14 Showing all log file entries: `showlog.cgi` 356
16.2.15 Evaluating whatever you want: `summary.cgi` 357
16.2.16 Following states graphically over time: `trends.cgi` . . 358
16.3 Planning Downtimes 359
16.3.1 Maintenance periods for hosts 360
16.3.2 Downtime for services 361
16.4 Additional Information on Hosts and Services 362
16.4.1 Extended host information 363
16.4.2 Extended service information 366
16.5 Configuration Changes through the Web Interfaces: the Restart Problem 367
16.6 Modern Layout with the Nuvola Style 368

17 Flexible Web Interface with the NDOUtils 375
17.1 The Event Broker 376
17.2 The Database Interface 378
17.3 The Installation 380
17.3.1 Compiling the source code 381
17.3.2 Preparing the MySQL database 381
17.3.3 Upgrading the database design 383
17.4 Configuration 383
17.4.1 Adjusting the Event Broker configuration 384
17.4.2 Configuring database access 385
17.4.3 Starting the `ndo2db` daemon 386
17.4.4 Loading the Event Broker module in Nagios 386

18 NagVis 389
18.1 Installation 391
18.1.1 Installing the source code 392
18.1.2 Initial configuration 393
18.1.3 User authentication 396
18.2 Creating NagVis Maps 396
18.2.1 Editing the configuration in text form 400
18.2.2 Adding NagVis maps to the Nagios Web interface 401

19 Graphic Display of Performance Data 403

19.1 Processing Plugin Performance Data with Nagios 404

19.1.1 The template mechanism 405

19.1.2 Using external commands to process performance data 407

19.2 Graphs for the Web with Nagiosgraph 408

19.2.1 Basic installation 408

19.2.2 Configuration 409

19.3 Preparing Performance Data for Evaluation with Perf2rrd . . . 415

19.3.1 Installation 416

19.3.2 Nagios configuration 417

19.3.3 Perf2rrd in practice 418

19.4 The Graphics Specialist `drraw` 420

19.4.1 Installation 420

19.4.2 Configuration 421

19.4.3 Practical application 423

19.5 Automated to a Large Extent: NagiosGrapher 426

19.5.1 Installation 427

19.5.2 Configuration 430

19.6 Smooth Plotting with PNP 446

19.6.1 Installation 447

19.6.2 The standard configuration 447

19.6.3 The PNP Web interface 449

19.6.4 Bulk processing of performance data 452

19.6.5 How should the graphic appear? 454

19.7 Other Tools and the Limits of Graphic Evaluation 456

IV Special Applications 459

20 Monitoring Windows Servers 461

20.1 Agent-less Checks via WMI 463

20.2 Installing and Configuring the Additional Services 464

20.2.1 NSClient 464

20.2.2 NC_Net 465

20.2.3 NSClient++ 465

20.2.4 OpMon Agent 469
20.2.5 Rectifying problems with port 1248 471
20.3 The `check_nt` Plugin 472
20.3.1 Generally supported commands 473
20.3.2 Advanced functions of NC_Net 480
20.3.3 Installing the `check_ncnet` plugin 480
20.4 NRPE for Windows 488
20.4.1 NRPE_NT, the classic tool 488
20.4.2 Plugins for NRPE in Windows 490
20.4.3 NRPE with NSClient++ 493
20.4.4 Internal NSClient++ functions 495

21 Monitoring Room Temperature and Humidity 505
21.1 Sensors and Software 506
21.1.1 The `PCMeasure` software for Linux 506
21.1.2 The query protocol 507
21.2 The Nagios Plugin `check_pcmeasure2.pl` 507

22 Monitoring SAP Systems 511
22.1 Checking without a Login: `sapinfo` 512
22.1.1 Installation 512
22.1.2 First test 512
22.1.3 The plugin `check_sap.sh` 514
22.1.4 More up to date and written in Perl: `check_sap.pl` . . 516
22.2 Monitoring with SAP's Own Monitoring System CCMS 519
22.2.1 A short overview over the alert monitor 519
22.2.2 Obtaining the necessary SAP usage permissions for Nagios 521
22.2.3 Monitors and templates 523
22.2.4 The CCMS plugins 525
22.2.5 Performance optimization 530

23 Processing Events with the EventDB 531
23.1 How the EventDB Works 532
23.2 Installation 533

23.2.1 Installation requirements 534
23.2.2 Preparing the MySQL database 534
23.2.3 Sending events to the database with `syslog-ng` 536
23.3 Using the Web Interface 538
23.3.1 Preselection of the filter with URL parameters 540
23.4 The Nagios Plugin for the EventDB 542
23.5 Maintenance 544
23.6 Sending Windows Events to Syslog 545
23.7 Making the Incomprehensible Legible with SNMPTT 546
23.7.1 The configuration file `snmptt.ini` 547
23.7.2 Converting MIBs 548

V Development 551

24 Writing Your Own Plugins 553
24.1 Programming Guidelines for Plugins 554
24.1.1 Return values 554
24.1.2 Information for the administrator on the standard output 555
24.1.3 Onboard online help? 556
24.1.4 Reserved options 557
24.1.5 Specifying thresholds 557
24.1.6 Timeout 558
24.1.7 Performance data 559
24.1.8 Copyright 559
24.2 The Perl Module `Nagios::Plugin` 560
24.2.1 Installation 560

25 Determining File and Directory Sizes 563
25.1 Splitting up the Command Line With `Getopt::Long` 565
25.2 The Perl Online Documentation 566
25.2.1 The module `Pod::Usage` 568
25.3 Determining Thresholds 570
25.4 Implementing Timeouts 571

25.5 Displaying Performance Data 572
25.6 Configuration Files for Plugins 572

26 Monitoring Oracle with the Instant Client 575
26.1 Installing the Oracle Instant Client 576
26.2 Establishing a Connection to the Oracle Database 577
26.3 A Wrapper Plugin for `sqlplus` 578
26.3.1 How the wrapper works 578
26.3.2 The Perl plugin in detail 579

Appendixes 583

A An Overview of the Nagios Configuration Parameters 585
A.1 The Main Configuration File `nagios.cfg` 586
A.2 CGI Configuration in `cgi.cfg` 606
A.2.1 Authentication parameters 606
A.2.2 Other Parameters 608

B Rapidly Alternating States: Flapping 611
B.1 Flap Detection with Services 612
B.1.1 Nagios configuration 613
B.1.2 The history memory and the chronological progression of the changes in state 614
B.1.3 Representation in the Web interface 615
B.2 Flap Detection for Hosts 616

C Event Handlers 619
C.1 Execution Times for the Event Handler 620
C.2 Defining the Event Handler in the Service Definition 621
C.3 The Handler Script 622
C.4 Things to Note When Using Event Handlers 623

D Macros 625
D.1 Standard Macros 627
D.1.1 Host macros 627
D.1.2 Service macros 628

D.1.3 Group macros 628
D.1.4 Contact macros 629
D.1.5 Notification macros 630
D.1.6 Macros to specify time and date 630
D.1.7 Statistics macros 631
D.1.8 Using standard macros about the environment 631
D.2 On-Demand Macros 632
D.3 Macros for User-defined Variables 633
D.4 Macro Contents: Not Everything Is Allowed 635

E Single Sign-On for the Nagios Web Interface 637
E.1 HTTP Authentication for Single Sign-On 638
E.2 Kerberos Authentication with `mod_auth_kerb` 640
E.2.1 Installation 641
E.2.2 Creating a service ticket for Apache 641
E.2.3 Kerberos configuration 642
E.2.4 Apache configuration 643
E.2.5 Definition of a Nagios contact 644
E.3 Single Sign-On with `mod_auth_ntlm_winbind` 645
E.3.1 Installation 645
E.3.2 Preparing Samba 646
E.3.3 Apache configuration 648
E.3.4 Defining a Nagios contact 649
E.4 Mozilla Firefox as a Web Client 650
E.4.1 Firefox and NTLM 651
E.5 Microsoft Internet Explorer as a Web Client 651

F Tips on Optimizing Performance 653
F.1 Internal Statistics of Nagios 654
F.1.1 The command-line tool `nagiostats` 654
F.1.2 Showing Nagios performance graphically 658
F.1.3 A plugin to monitor latency 660
F.2 Measures for Improving Performance 662
F.2.1 Service checks: as often as necessary, as few as possible 662

F.2.2 Processing performance data intelligently 663
F.2.3 Avoiding plugins in interpreted languages 664
F.2.4 Optimizing host checks 664
F.2.5 The matter of the Reaper 666
F.2.6 Preferring passive checks 666
F.2.7 Optimizing large Nagios environments 667
F.2.8 Optimizing the NDOUtils database 667

G The Embedded Perl Interpreter 669
G.1 Requirements of an ePN-capable Plugin 670
G.2 Using ePN 672
G.2.1 Compiling ePN 672
G.2.2 Interpreter-specific parameters in `nagios.cfg` 673
G.2.3 Disabling ePN on a per-plugin basis 673
G.3 The Testing Tool `new_mini_epn` 674

H What's New in Nagios 3.0? 677
H.1 Changes in Object Definitions 678
H.1.1 The `host` object 678
H.1.2 The `service` object 680
H.1.3 Group objects 681
H.1.4 The `contact` object 681
H.1.5 Time definitions 682
H.1.6 Dependency descriptions 683
H.1.7 Escalation objects 683
H.1.8 Inheritance 684
H.2 Variable and Macros 685
H.3 Downtime, Comments, and Acknowledgments 687
H.4 Rapidly Changing States 687
H.5 External Commands 687
H.6 Embedded Perl 688
H.7 A New Logic for Host Checks 689
H.8 Restart 690
H.9 Performance Optimization 691

H.10 Extended Plugin Output 692
H.11 CGI 692
H.12 Miscellaneous 692
H.13 Upgrade from Nagios 2.x to 3.0 693