Inhaltsverzeichnis

Vorwort zur dritten Auflage 21

Einleitung 23

I Vom Quellcode zum lauffähigen System 31

1 Installation 33

1.1 Vorbereitende Schritte 34

1.1.1 Benötigte User ermitteln und anlegen 34

1.2 Source-Code übersetzen 35

1.3 Nagios automatisch starten 39

1.4 Plugins installieren und testen 40

1.4.1 Installation 40

1.4.2 Plugin-Test 42

1.5 Konfiguration des Webinterfaces 43

1.5.1 Apache einrichten 43

1.5.2 SELinux 45

1.5.3 User-Authentifizierung 45

2 Konfiguration 49

2.1 Die Hauptkonfigurationsdatei nagios.cfg 50

2.2 Objekte – eine Übersicht 54

2.3 Zu überwachende Rechner mit host festlegen 57

2.4 Rechner gruppieren mit hostgroup 62

2.5 Zu überwachende Dienste festlegen mit service 62

2.6 Dienste mit servicegroup zusammenfassen 66

Bibliografische Informationen
http://d-nb.info/1010570137

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.7 Adressaten für Fehlermeldungen festlegen: contact 67
2.8 Die Nachrichtenempfänger: contactgroup 69
2.9 Wenn Nagios etwas tun soll: Das command-Objekt 69
2.10 Zeitfenster definieren mit timeperiod 70
2.11 Templates 71
2.12 Konfigurationshilfen für Tippfaule 73
2.12.1 Services für mehrere Rechner definieren 73
2.12.2 Eine Hostgruppe für alle Rechner 73
2.12.3 Weitere Konfigurationshilfen 74
2.12.4 Vererbung 74
2.13 CGI-Konfiguration in cgi.cfg 75
2.14 Die Ressourcen-Datei resource.cfg 77

3 Inbetriebnahme **79**
3.1 Überprüfen der Konfiguration 79
3.2 Startschuss für die Überwachung 82
3.2.1 Manueller Start 82
3.2.2 Konfigurationsänderungen wirksam werden lassen . . . 82
3.3 Übersicht über das Webinterface 83

II Im Detail **87**

4 Grundlagen **89**
4.1 Die Netzwerktopologie berücksichtigen 90
4.2 On-Demand-Host-Checks vs. regelmäßige Prüfung 93
4.3 Zustände von Hosts und Services 94

5 Service-Checks und ihre Ausführung **97**
5.1 Netzwerkdienste direkt prüfen 99
5.2 Plugins via SSH auf dem entfernten Rechner ausführen 100
5.3 Der Nagios Remote Plugin Executor 101
5.4 Überwachung via SNMP 101
5.5 Der Nagios Service Check Acceptor 102

6 Plugins für Netzwerkdienste 105

6.1 Standardoptionen 108
6.2 Erreichbarkeitstest mit Ping 108
6.2.1 check_icmp als Service-Check 111
6.2.2 check_icmp als Host-Check 112
6.3 Mailserver überwachen 113
6.3.1 SMTP überwachen mit check_smtp 113
6.3.2 POP und IMAP 116
6.4 Überwachung von FTP- und Webservern 119
6.4.1 FTP-Services 119
6.4.2 Webserverkontrolle via HTTP 120
6.4.3 Webproxies überwachen 124
6.5 Domain Name Server unter Kontrolle 127
6.5.1 DNS-Check mit nslookup 128
6.5.2 Nameserver-Überwachung mit dig 129
6.6 Secure Shell Server abfragen 131
6.7 Generische Netzwerkplugins 132
6.7.1 TCP-Ports überprüfen 133
6.7.2 UDP-Ports überwachen 135
6.8 Datenbanken überwachen 136
6.8.1 PostgreSQL 137
6.8.2 MySQL 141
6.9 LDAP-Verzeichnisdienste überwachen 144
6.10 Kontrolle eines DHCP-Servers 146
6.11 USV-Überwachung mit den Network UPS Tools 149
6.12 Gesundheitscheck eines NTP-Servers mit check_ntp_peer . . . 155

7 Lokale Ressourcen überprüfen 157

7.1 Freie Festplattenkapazität 158
7.2 Auslastung des Swap-Bereichs 162
7.3 Systemlast prüfen 163
7.4 Prozesse überwachen 164
7.5 Logfiles unter Kontrolle 167
7.5.1 Das Standard-Plugin check_log 168

7.5.2 Die moderne Variante: check_logs.pl 169
7.5.3 Das Schweizer Taschenmesser: check_logfiles 171
7.6 Anzahl der eingeloggten User im Blick behalten 178
7.7 Systemzeit unter Kontrolle 178
7.7.1 Systemzeit via NTP überprüfen 178
7.7.2 Systemzeit mit dem Time-Protokoll kontrollieren 179
7.8 Regelmäßiger Einblick in den Zustand der Mail-Queue 181
7.9 Das Änderungsdatum einer Datei im Auge behalten 182
7.10 USVs mit apcupsd überwachen 183
7.11 Nagios kontrolliert sich selbst 184
7.11.1 Manueller Aufruf des Plugins per Skript 185
7.12 Hardware-Checks mit LM-Sensoren 185

8 Plugins für Sonderaufgaben 189
8.1 Das Dummy-Plugin für Tests 190
8.2 Plugin-Ergebnisse negieren 190
8.3 Hyperlinks einfügen mit urlize 191
8.4 Host- oder Service-Cluster als Gesamtheit prüfen 191
8.5 Checks mit check_multi zusammenfassen 194
8.5.1 Mehrzeiliger Plugin-Output 195
8.5.2 Installationsvoraussetzungen 196
8.5.3 Installation und Test 196
8.5.4 Konfigurationsdatei 197
8.5.5 Kommandozeilenparameter 198
8.5.6 Performancedaten und PNP 200
8.5.7 Einfaches Business-Prozess-Monitoring 201

9 Plugins via SSH ausführen 207
9.1 Das check_by_ssh-Plugin 208
9.2 SSH-Konfiguration 210
9.2.1 SSH-Schlüsselpaar auf dem Nagios-Server generieren . 211
9.2.2 Den User nagios auf dem Zielhost einrichten 211
9.2.3 SSH-Verbindung und check_by_ssh testen 212
9.3 Nagios-Konfiguration 213

10 Der Nagios Remote Plugin Executor (NRPE) 215

10.1 Installation 216
10.1.1 Distributionsspezifische Pakete 216
10.1.2 Installation aus dem Quellcode 217
10.2 Start via Inet-Daemon 218
10.2.1 xinetd-Konfiguration 219
10.2.2 inetd-Konfiguration 220
10.2.3 Wacht der Inet-Daemon am NRPE-Port? 220
10.3 NRPE-Konfiguration auf dem zu überwachenden Rechner . . . 221
10.3.1 Parameterübergabe an die lokalen Plugins 222
10.4 NRPE-Funktionstest 223
10.5 Nagios-Konfiguration 224
10.5.1 NRPE ohne Parameter-Übergabe 224
10.5.2 NRPE mit Parameter-Übergabe 225
10.5.3 Optimierung der Konfiguration 225
10.6 Indirekte Checks 226

11 Überwachungsrelevante Informationen sammeln mit SNMP 229

11.1 Einführung in SNMP 230
11.1.1 Die Management Information Base 231
11.1.2 SNMP-Versionen 235
11.2 NET-SNMP 237
11.2.1 Werkzeuge zur SNMP-Abfrage 237
11.2.2 Der NET-SNMP-Daemon 240
11.3 Nagios-eigene SNMP-Plugins 249
11.3.1 Das generische SNMP-Plugin check_snmp 249
11.3.2 Mehrere Interfaces gleichzeitig überprüfen 254
11.3.3 Betriebszustand einzelner Interfaces testen 256
11.4 Weitere SNMP-basierte Plugins 258
11.4.1 Festplattenplatz und Prozesse überwachen 259
11.4.2 Auslastung von Netzwerkinterfaces beobachten 260
11.4.3 Die manubulon.com-Plugins 262
11.5 SNMP-Trap-Handling mit NagTrap 267
11.5.1 Installation 267

11.5.2 Konfiguration und Datenbank 268
11.5.3 Interaktion mit Nagios 270
11.5.4 Das NagTrap-Webfrontend 273

12 Das Nagios-Benachrichtigungssystem 277
12.1 Wer soll wann wie informiert werden? 278
12.2 Wann entsteht eine Nachricht? 279
12.3 Die Nachrichtenfilter 279
12.3.1 Benachrichtigungen systemweit ein- und abschalten . . 281
12.3.2 Rechner- und dienstbezogene Nachrichten 281
12.3.3 Personenbezogene Filtermöglichkeiten 284
12.3.4 Fallbeispiele 285
12.4 Externe Benachrichtigungsprogramme 288
12.4.1 Benachrichtigung per E-Mail 289
12.4.2 Nachricht per SMS 291
12.5 Eskalationsmanagement 294
12.6 Abhängigkeiten zwischen Hosts und Services berücksichtigen . 298
12.6.1 Der Standardfall: Service Dependencies 298
12.6.2 Nur für Ausnahmefälle: Host Dependencies 302

13 Passive Tests über das External Command File 305
13.1 Die Schnittstelle für externe Kommandos 306
13.2 Passive Service-Checks 307
13.3 Passive Host-Checks 308
13.4 Auf veraltete Informationen passiver Checks reagieren 309

14 Der Nagios Service Check Acceptor (NSCA) 313
14.1 Installation 314
14.2 Konfiguration des Nagios-Servers 315
14.2.1 Die Konfigurationsdatei nsca.cfg 315
14.2.2 Konfiguration des Inet-Daemons 317
14.3 Konfiguration auf Clientseite 318
14.4 Testergebnisse an den Server schicken 319
14.5 Anwendungsbeispiel I: Syslog und Nagios integrieren 321
14.5.1 syslog-ng für den Einsatz mit Nagios vorbereiten 321

14.5.2 Nagios-Konfiguration: Volatile Services 323
14.5.3 Fehlerzustände manuell aufheben 325
14.6 Anwendungsbeispiel II: Verarbeitung von SNMP-Traps 326
14.6.1 Traps empfangen mit snmptrapd 326
14.6.2 Traps an NSCA übergeben 328
14.6.3 Die passende Service-Definition 330

15 Verteiltes Monitoring **331**
15.1 Den OCSP/OCHP-Mechanismus einschalten 332
15.2 OCSP/OHCP-Kommandos definieren 333
15.3 Einsatzszenarien 335
15.3.1 Redundanz bei Konfigurationsdateien vermeiden 335
15.3.2 Templates definieren 336

16 Mod Gearman **339**
16.1 Funktionsweise 340
16.2 Szenarien 340
16.2.1 Load Balancing 340
16.2.2 Verteiltes Monitoring 341
16.3 Installation 341
16.3.1 Gearman aus dem Quellcode übersetzen 341
16.3.2 Mod Gearman aus dem Quellcode übersetzen 342
16.4 Konfiguration 342

III Webinterface und Visualisierungsmöglichkeiten **345**

17 Die klassische Weboberfläche **347**
17.1 Probleme erkennen und behandeln 350
17.1.1 Kommentare zu problembehafteten Rechnern 351
17.1.2 Verantwortung für Probleme übernehmen 353
17.2 Die einzelnen CGI-Programme im Überblick 354
17.2.1 Statusanzeige in Variationen: status.cgi 354
17.2.2 Zusatzinformationen und Steuerzentrale: extinfo.cgi . . 358
17.2.3 Schnittstelle für externe Kommandos: cmd.cgi 363
17.2.4 Das Wichtigste auf einen Blick: tac.cgi 366

17.2.5 Topologische Netzwerkkarte mit statusmap.cgi 367
17.2.6 Navigation in 3D: statuswrl.cgi 369
17.2.7 Statusabfrage via Handy: statuswml.cgi 370
17.2.8 Gestörte Teilnetze analysieren: outages.cgi 371
17.2.9 Objektdefinition abfragen mit config.cgi 371
17.2.10 Verfügbarkeitsstatistik: avail.cgi 372
17.2.11 Wie oft tritt welches Ereignis ein? – histogram.cgi 374
17.2.12 Logeinträge nach Zuständen filtern: history.cgi 375
17.2.13 Nachrichten verfolgen mit notifications.cgi 376
17.2.14 Anzeige aller Logfile-Einträge: showlog.cgi 377
17.2.15 Auswertung nach Wunsch: summary.cgi 377
17.2.16 Zustände über die Zeit verfolgen: trends.cgi 379
17.3 Wartungszeiten planen 380
17.3.1 Wartungszeiträume für Hosts 381
17.3.2 Wartungsfenster für Services 382
17.4 Zusatzinformationen über Rechner und Dienste 383
17.4.1 Erweiterte Host-Informationen 384
17.4.2 Erweiterte Service-Informationen 387
17.5 Das Neustart-Problem bei Konfigurationsänderungen 388
17.6 Modernes Outfit mit dem Nuvola-Style 389

18 Flexible Weboberfläche mit den NDOUtils 395

18.1 Der Event-Broker 396
18.2 Die Datenbankschnittstelle 398
18.3 Die Installation 400
18.3.1 Den Quellcode übersetzen 401
18.3.2 Vorbereiten der MySQL-Datenbank 401
18.3.3 Upgrade des Datenbank-Designs 403
18.4 Konfiguration 403
18.4.1 Anpassen der Event-Broker-Konfiguration 404
18.4.2 Konfiguration des Datenbankzugriffs 405
18.4.3 Den ndo2db-Daemon starten 406
18.4.4 Das Event-Broker-Modul in Nagios laden 406

19 Live-Zugriff auf die Statusdaten mit MK_Livestatus 409

19.1 Installation 410

19.2 Zugriff über Netzwerk 411

19.3 Die Livestatus Query Language 412

20 NagVis 415

20.1 Installation 418

20.1.1 Den Quellcode einspielen 418

20.1.2 Initiale Konfiguration 419

20.1.3 Benutzer-Authentifikation 422

20.2 NagVis-Maps erstellen 423

20.2.1 Konfiguration in Textform bearbeiten 429

20.2.2 Die Nagios-Weboberfläche um NagVis-Maps erweitern . 429

21 Grafische Darstellung von Performancedaten 431

21.1 Plugin-Performancedaten mit Nagios verarbeiten 432

21.1.1 Der Template-Mechanismus 433

21.1.2 Externe Kommandos zur Verarbeitung einsetzen 435

21.2 Graphen fürs Web mit Nagiosgraph 436

21.2.1 Basis-Installation 436

21.2.2 Konfiguration 437

21.3 Performancedaten mit Perf2rrd zur Auswertung vorbereiten . . 443

21.3.1 Installation 444

21.3.2 Nagios-Konfiguration 445

21.3.3 Perf2rrd in der Praxis 446

21.4 Der Grafik-Spezialist drraw 448

21.4.1 Installation 448

21.4.2 Konfiguration 449

21.4.3 Praktische Anwendung 450

21.5 Reibungsloses Plotten mit PNP 454

21.5.1 Installation 455

21.5.2 Die Standardkonfiguration 455

21.5.3 Die PNP-Weboberfläche 457

21.5.4 Massenverarbeitung von Performancedaten 460

21.5.5 Wie soll die Grafik aussehen? 462
21.6 inGraph – Performancedaten visualisieren 464
21.6.1 Installation und Konfiguration 465
21.6.2 Das Datenbank-Backend 467
21.6.3 Nagios-Konfiguration 467
21.6.4 inGraph-Webfrontends 469
21.6.5 Anomalien finden mit dem Check Plugin 471
21.7 Weitere Tools und die Grenzen grafischer Auswertung 472

IV Spezielle Einsatzzwecke 475

22 Windows-Server überwachen 477
22.1 Agentenlose Checks via WMI 479
22.2 Installation und Konfiguration der Zusatzdienste 480
22.2.1 NSClient 480
22.2.2 NC_Net 481
22.2.3 NSClient++ 481
22.2.4 OpMon Agent 485
22.2.5 Probleme mit Port 1248 beheben 486
22.3 Das check_nt-Plugin 487
22.3.1 Generell unterstützte Kommandos 489
22.4 Die erweiterten Funktionen von NC_Net 496
22.4.1 Installation des Plugins check_ncnet 496
22.4.2 Windows-Performance-Counter 497
22.5 NRPE für Windows 503
22.5.1 NRPE_NT, der Klassiker 504
22.5.2 Plugins für NRPE unter Windows 505
22.5.3 NRPE mit NSClient++ 508
22.5.4 Interne NSClient++-Funktionen 510

23 Raumtemperatur und Luftfeuchtigkeit überwachen 521
23.1 Sensoren und Software 522
23.1.1 Die messpc-Software für Linux 522
23.1.2 Das Abfrageprotokoll 523

23.2 Das Nagios-Plugin check_pcmeasure2.pl 523

24 Überwachung von SAP-Systemen **527**

24.1 Überprüfung ohne Login: sapinfo 528
24.1.1 Installation 528
24.1.2 Erster Test 528
24.1.3 Das Plugin check_sap.sh 530
24.1.4 Aktueller und in Perl geschrieben: check_sap.pl 532
24.2 Überwachung mit SAP CCMS 534
24.2.1 Der Alert-Monitor im Überblick 535
24.2.2 Nagios die nötigen SAP-Nutzungsrechte verschaffen . . 537
24.2.3 Monitore und Templates 539
24.2.4 Die CCMS-Plugins 541
24.2.5 Performance-Optimierung 545

25 Ereignisse verarbeiten mit der EventDB **547**

25.1 Funktionsweise der EventDB 548
25.2 Installation 549
25.2.1 Installationsvoraussetzungen 550
25.2.2 Vorbereiten der MySQL-Datenbank 551
25.2.3 Events an die Datenbank schicken mit syslog-ng 552
25.3 Das Webinterface nutzen 554
25.3.1 Vorauswahl des Filters mit URL-Parametern 556
25.4 Das Nagios-Plugin für die EventDB 558
25.5 Maintenance 560
25.6 Windows-Events an Syslog senden 561
25.7 Unverständliches lesbar machen mit SNMPTT 562
25.7.1 Die Konfigurationsdatei snmptt.ini 563
25.7.2 MIBs konvertieren 565

26 Überwachung von Geschäftsprozessen **567**

26.1 Das Nagios Business Process Addon 568
26.1.1 Installation 568
26.1.2 Konfiguration 569
26.1.3 Integration in Nagios 573

26.1.4 Alarmierung durch Nagios 574
26.2 Nagios Business Process Intelligence 577
26.2.1 Installation und Konfiguration 577
26.2.2 Einrichten der Geschäftsprozesse 579
26.2.3 Einbinden in Nagios 580

V Entwicklung 583

27 Plugins selbst schreiben 585
27.1 Programmierrichtlinien für Plugins 586
27.1.1 Rückgabewerte 586
27.1.2 Informationen für den Admin auf der Standardausgabe 587
27.1.3 Online-Hilfe an Bord? 588
27.1.4 Reservierte Optionen 589
27.1.5 Schwellwertangaben 590
27.1.6 Abbruch nach Zeit 591
27.1.7 Performancedaten 591
27.1.8 Copyright 591
27.2 Das Perl-Modul Nagios::Plugin 592
27.2.1 Installation 592

28 Datei- und Verzeichnisgrößen ermitteln 595
28.1 Die Kommandozeile mit Getopt::Long zerlegen 597
28.2 Die Perl-Online-Dokumentation 598
28.2.1 Das Modul Pod::Usage 600
28.3 Schwellwerte ermitteln 602
28.4 Timeouts implementieren 603
28.5 Performancedaten ausgeben 603
28.6 Konfigurationsdateien für Plugins 604

29 Oracle-Überwachung mit dem Instant-Client 607
29.1 Den Oracle-Instant-Client installieren 608
29.2 Verbindung zur Oracle-Datenbank herstellen 609
29.3 Ein Wrapper-Plugin für sqlplus 609
29.3.1 Die Funktionsweise des Wrappers 610

29.3.2 Das Perl-Plugin im Detail 611

Anhang **615**

A Nagios-Konfigurationsparameter **617**

A.1 Die Hauptkonfigurationsdatei nagios.cfg 618

A.2 CGI-Konfiguration in cgi.cfg 639

A.2.1 Authentifikationsparameter 639

A.2.2 Sonstige Parameter 641

B Schnell wechselnde Zustände: Flapping **645**

B.1 Flap Detection bei Services 646

B.1.1 Nagios-Konfiguration 647

B.1.2 Historienspeicher 648

B.1.3 Darstellung in der Weboberfläche 649

B.2 Flap Detection bei Hosts 651

C Eventhandler **653**

C.1 Ausführungszeitpunkte für Eventhandler 654

C.2 Eventhandler in der Service-Definition festlegen 655

C.3 Das Handler-Skript 656

C.4 Beachtenswertes beim Umgang mit Eventhandlern 657

D Makros **659**

D.1 Standardmakros 660

D.1.1 Host-Makros 661

D.1.2 Service-Makros 662

D.1.3 Gruppen-Makros 662

D.1.4 Kontakt-Makros 663

D.1.5 Benachrichtigungsmakros 664

D.1.6 Makros für Zeit- und Datumsangaben 664

D.1.7 Statistikmakros 665

D.1.8 Standardmakros über das Environment verwenden . . . 665

D.2 On-Demand-Makros 666

D.3 Makros für selbstdefinierte Variablen 667

D.4 Makro-Inhalte: Nicht alles ist erlaubt 669

E Single-Sign-On für die Nagios-Weboberfläche 671

E.1 HTTP-Authentifikation für Single-Sign-On 672

E.2 Kerberos-Authentifikation mit mod_auth_kerb 674

E.2.1 Installation 675

E.2.2 Service-Ticket für Apache erstellen 675

E.2.3 Kerberos-Konfiguration 676

E.2.4 Apache-Konfiguration 677

E.2.5 Definition eines Nagios-Kontakts 678

E.3 Single-Sign-On mit mod_auth_ntlm_winbind 679

E.3.1 Installation 679

E.3.2 Samba vorbereiten 680

E.3.3 Apache-Konfiguration 682

E.3.4 Definition eines Nagios-Kontakts 683

E.4 Mozilla Firefox als Webclient 684

E.4.1 Firefox und NTLM 685

E.5 Microsoft Internet Explorer als Webclient 685

F Tipps zur Performance-Optimierung 687

F.1 Nagios-interne Statistiken 688

F.1.1 Das Kommandozeilentool nagiostats 688

F.1.2 Nagios-Performance im grafischen Verlauf 692

F.1.3 Ein Plugin zur Überwachung der Latenz 694

F.2 Maßnahmen zur Performance-Verbesserung 696

F.2.1 Service-Checks – so oft wie nötig, so wenig wie möglich 696

F.2.2 Performancedaten intelligent verarbeiten 697

F.2.3 Plugins in interpretierten Sprachen vermeiden 698

F.2.4 Host-Checks optimieren 699

F.2.5 Die Sache mit dem Reaper 699

F.2.6 Passive Checks bevorzugen 700

F.2.7 Optimierung großer Nagios-Umgebungen 701

F.2.8 NDOUtils-Datenbank optimieren 701

F.3 Neustart 702

G Der Embedded Perl-Interpreter **705**

G.1 Anforderungen an ein ePN-taugliches Plugin 706

G.2 ePN verwenden 708

G.2.1 ePN einkompilieren 708

G.2.2 Interpreter-spezifische Parameter in der nagios.cfg . . . 708

G.2.3 ePN auf Plugin-Basis deaktivieren 709

G.3 Das Testwerkzeug new_mini_epn 709