

Das Nagios Ökosystem

Alexander Wirt
und
Mike Liebsch

2011-08-21



Inhaltsverzeichnis

- 1 Allgemein
- 2 Konfigurationsmanagement
- 3 Graphing & Reporting
- 4 Core Erweiterung
- 5 LB & HA
- 6 Alternative Frontends & Erweiterungen



Nagios

- Weit verbreitet
- Große Community
- Verschiedene Rewrites (Icinga, Shinken)
- Leicht Erweiterbar



Nagios

- Weit verbreitet
- Große Community
- Verschiedene Rewrites (Icinga, Shinken)
- Leicht Erweiterbar

Aber...

Nagios alleine ist langweilig!



Nagios Konfiguration

- Dateibasiert
- Teilbar in viele Dateien
- Automatisch erzeugbar
- Gerade in großen Umgebungen unhandlich
- Strukturierung schwierig
- Überblick nur im laufenden Setup eindeutig



LDAP

- Speicherung der Konfiguration in LDAP
- Verschiedene Frontends verfügbar
 - Idapvi
 - Apache Directory Studio
 - viele weitere
- Script-bar (Libraries verfügbar)
- Infrastruktur hierarchisch abbildbar
- Export in Nagios Konfigurationsdateien notwendig (LConf)
 - Bietet ein Schema
 - Nutzung von Vererbung möglich



Wato

- Konfigurationstool for check_mk
- Python basiert
- setzt auf Livestatus auf
- erzeugt check_mk Konfigurationen



Wato Host anlegen

Hostname	<input type="text"/>
Alias <i>(optional)</i>	<input type="text"/>
IP-Address <i>Leave empty for automatic IP address lookup via DNS</i>	<input type="text"/>
Productivity	Production System ▾
Bulkwalk (SNMP v2c)	Simple walk (SNMP v1) ▾
Operating System	Linux ▾
<input type="button" value="Save & Finish"/> <input type="button" value="Save & got to Services"/>	



NagiosQL

- PHP basierte Webanwendung
- Erzeugt Nagios und Icinga Konfiguration
- Speicherung in MySQL
- Automatische Backup Funktion
- Aktivierung der Konfiguration über Webfrontend
- Eingebaute Konsistenz Prüfung der Werte



NagiosQL Host editieren

Verwaltung

[Verwaltung](#) -> [Überwachung](#) -> [Host](#)

- Hauptseite
- Überwachung**
 - Host
 - Services
 - Hostgruppen
 - Servicegruppen
 - Hostvorlagen
 - Servicevorlagen
- Alarmierung
- Befehle
- Spezialitäten
- Werkzeuge
- Verwaltung

[Menu ausblenden]

Host definieren

Allgemeine Einstellungen | Prüfeinstellungen | Alarmeinstellungen | Zusatzeinstellungen | Serviceeinstellungen

Allgemeine Einstellungen

Hostname*	10.100.1.1 (1) (2) (1) ?	Beschreibung*	10.100.1.1 ?
Hostadresse*	10.100.1.1 ?	Anzeigename	
Vorgeschaltete Hosts	<ul style="list-style-type: none">10.100.1.110.100.1.1 (1) (2) (2)10.100.1.1 (1) (3)10.100.1.1 (1) (3) (1) ?	Hostgruppen	<ul style="list-style-type: none">aaaacentralClaimtoolCostingTool ?
Prüfbefehl	check-host-alive ?	Aktiv	<input checked="" type="checkbox"/>
Befehlsübersicht			
\$ARG1\$		\$ARG5\$	
\$ARG2\$		\$ARG6\$	
\$ARG3\$		\$ARG7\$	
\$ARG4\$		\$ARG8\$	

Zusätzliche Vorlagen

Vorlagename



check_mk

- Metasprache zur Konfiguration von Nagios mit Filtern und Tags
- Agent (kann auch NRPE ersetzen)
- Leicht erweiterbar (Python)
- durch Inventarisierung können Systeme selbst neue Checks erzeugen
- Erstellung von Nagios Konfiguration
- Integration von Cluster Checks und Business Process View
- Integration von pnp4nagios für Performance Visualisierung



check_mk Beispiel

```
ignored_services = [
    ( ALL_HOSTS, [ "NIC_.*vnet.*" ] ),
    ( ALL_HOSTS, [ ".*chroot.*" ] ),
]

all_hosts = [
    'monitoring.grml.org|web|hostw-guest',
    'deb.grml.org|web|hostw-guest',
    'misc.grml.org|hostw-guest' ]

parents = [
    ( "father.grml.org", ["hostw-guest"], ALL_HOSTS )
]

legacy_checks = [
    ( ( "check_ssh", "ssh_service", False), ALL_HOSTS ),
    ( ( "check_smtp", "smtp_service", False), [ "mail.grml.org" ] ),
]
```



Nutzung von Leistungsdaten

- Checks geben perfdata zurück
- Keine extra Checks notwendig
 - Munin, Ganglia, Cacti
 - Weniger Load
 - Speziell bei Netzwerkhardware
- Speicherung in RRD oder DB
- Darstellung im Frontend
- Exportierbar zur weiteren Nutzung
- Für erweiterte Reports nutzbar

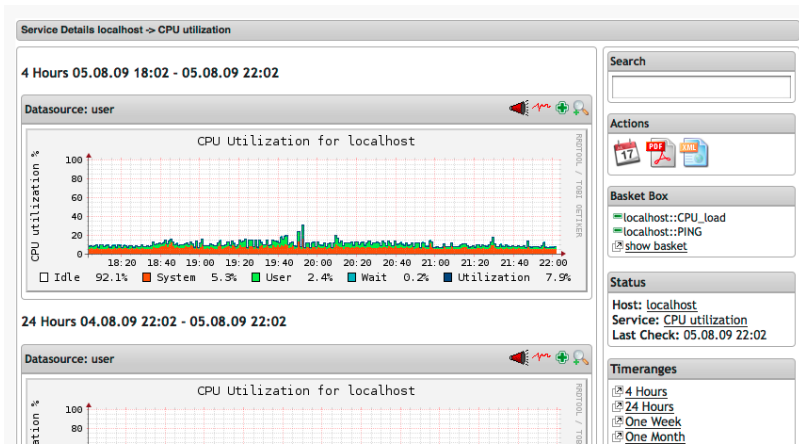


pnp4nagios

- Verschiedene Verarbeitungsmodi
 - Service/Host-Command
 - Broker Module
- PHP Frontend
- Hübsche Übersichtsseiten
- Popups im Nagios Frontend
- Zoomable
- Einfaches Troubleshooting
- Exportfunktionen
- Nutzung von RRD als Backend
- Template für jeden Command



pnp4nagios Screen

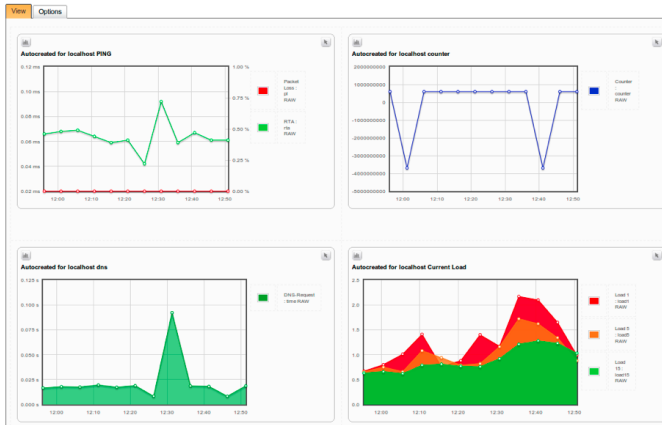


NETWAYSGrapherV2

- Früher nagiosgrapher - heute v2
- AppKit Frontend (PHP und Adobe Flex)
- Collector Backend Daemon
- Speicherung in MySQL Datenbank
- Automatische Erkennung neuer Dienste
- Komplette Konfiguration via Webfrontend



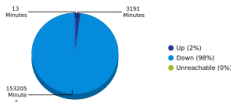
NETWAYSGrapher Beispiel



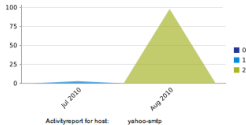
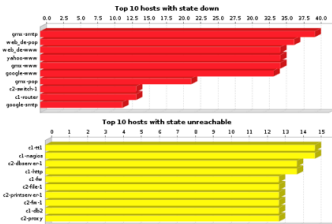
Icinga Reporting

- Vordefinierte Reporting Templates
- Top10 Reports
- Verfügbarkeits- und SLA Reports
- JasperServer als Backend (tomcat)
- Speicherung in Datenbank
- Verschiedene Outputs (PDF, HTML, Excel, CSV, RTF)

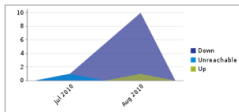




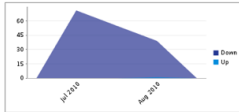
Top 10 Host Report



This graph displays the state history for given host



This graph displays the notifications for given host



Broker

- Nagios Event Broker (NEB)
- Core Interne Funktionen aus externen Bibliotheken abrufen
- Call-back Routinen
- Aufruf bei speziellen Events im Core
- Vielseitig verwendbar



Broker

- Nagios Event Broker (NEB)
- Core Interne Funktionen aus externen Bibliotheken abrufen
- Call-back Routinen
- Aufruf bei speziellen Events im Core
- Vielseitig verwendbar

Integration

```
event_broker_options
```

```
broker_module=/somewhere/module.o arg1 arg2=foo debug=0
```



Livestatus

- Broker
- Interaktion via Unix Socket
 - Gruppierungen
 - Filter
- Remote Verfügbarkeit via SSH oder xinetd
- Ausgabe in CSV, JSON oder Python
- Auch für Frontends nutzbar (siehe Multisite, Nagvis)



Livestatus Beispiel

```
root@linux\# echo 'GET hosts' | unixcat /var/lib/nagios/rw/live
acknowledged;action_url;address;alias;check_command;check_period;checks_enabled;contacts;in_check_period;in_notification_period;is_flapping;last_check;last_state_change;name;notes;notes_url;notification_period;scheduled_downtime_depth;state;total_services
0;/nagios/pnp/index.php?host=$HOSTNAME$;127.0.0.1;Acht;check-mk-ping;;1;check_mk,hh;1;1;0;1256194120;1255301430;Acht;;;24X7;0;0;7
0;/nagios/pnp/index.php?host=$HOSTNAME$;127.0.0.1;DREI;check-mk-ping;;1;check_mk,hh;1;1;0;1256194120;1255301431;DREI;;;24X7;0;0;1
0;/nagios/pnp/index.php?host=$HOSTNAME$;127.0.0.1;Drei;check-mk-ping;;1;check_mk,hh;1;1;0;1256194120;1255301435;Drei;;;24X7;0;0;4
```



Livestatus Beispiel

```
root@linux\# cat query
GET services
Stats: state = 0
Stats: state = 1
Stats: state = 2
Stats: state = 3
root@linux\# unixcat /var/lib/nagios/rw/live < query
4297;13;9;0
```



- Darstellung der Monitoring Objekte im Dateisystem
- Jeder Host ist ein Verzeichnis
- Jeder Service eine Datei
- Grepable
- Übersicht über das derzeitige Monitoring



Verteilung

- Große und/oder komplexe Setups
- Ein Server nicht mehr ausreichend
 - Lastverteilung
 - Ausfallsicherheit
 - Verschiedene Rollen
 - Verschiedene Netze

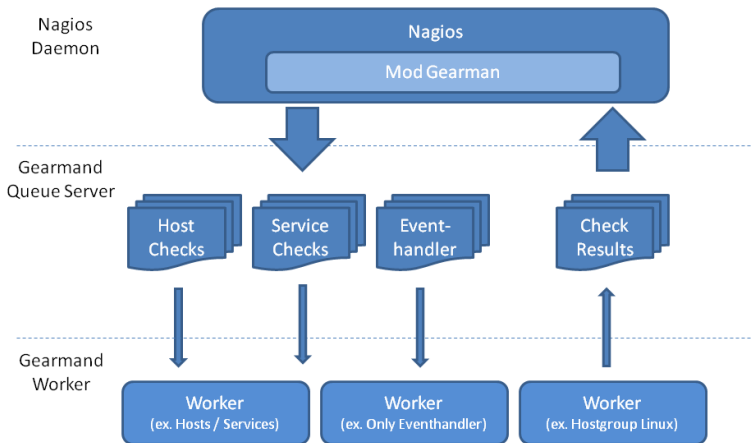


mod_gearman

- Broker
- Erstellung von Jobs für jeden Check
- Verteilung von Jobs auf Worker
- Worker auf verschiedenen Systemen (dynamisch oder fix)
- asynchron und parallel (kein blocking)
- pnp4nagios worker
- Build-In AES256 Verschlüsselung der Pakete



mod gearman Aufbau

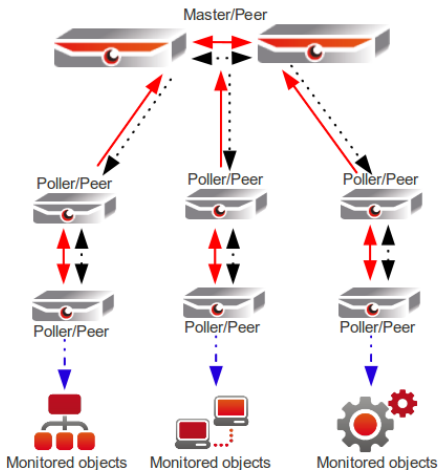


Merlin

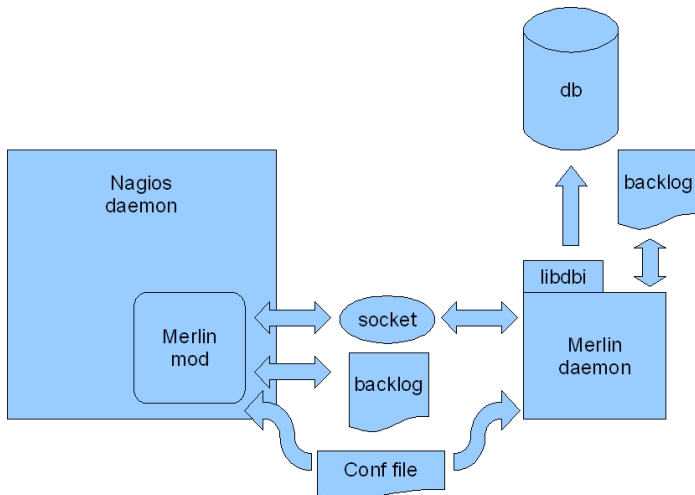
- Broker von op5 entwickelt
- Zusätzlicher Dienst (merlind)
- Steuerung durch Master und Verteilung auf Peers und Poller
- Redundanz und Load Balancing
- Status Informationen in DB Speicherbar
- Intelligente oder festgelegte Verteilung



Merlin Aufbau



Merlin Backend

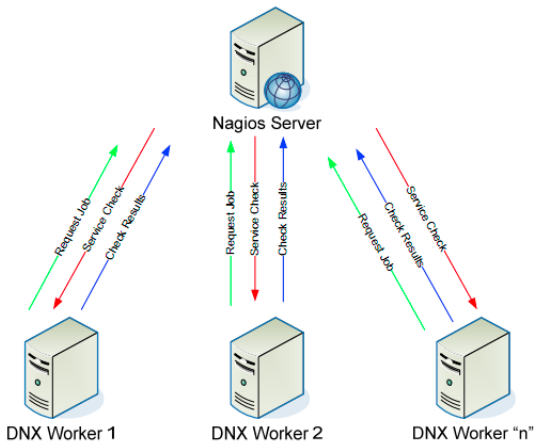


DNX

- Broker
- Distributed Nagios eXecutor
- Master-Slave Architektur
- Reine Lastverteilung
- Speziell bei zeitaufwendigen Checks



DNX Aufbau



Default Frontends

- Nagios C CGI
 - Unhandlich
 - Schwerer zu warten
 - Irgendwie sehr 90er
- Icingaweb
 - PHP und DB basiert
 - Multisitefähig
 - imho nicht geeignet für den produktiven Einsatz



Default Frontends

- Nagios C CGI
 - Unhandlich
 - Schwerer zu warten
 - Irgendwie sehr 90er
- Icingaweb
 - PHP und DB basiert
 - Multisitefähig
 - imho nicht geeignet für den produktiven Einsatz

Default ist nett aber...

Unzureichend für viele Setups

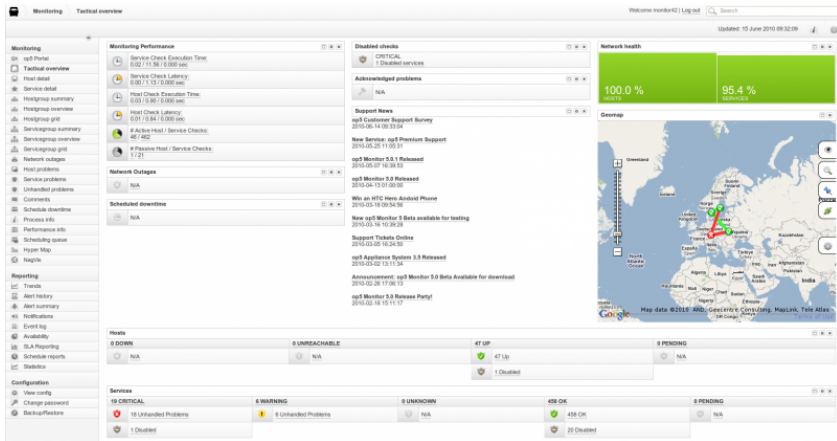


Ninja

- Entwickelt von op5
- Datenbank Backend
- MVC in PHP
- Leichte Integration von Distributed Setups (Merlin)
- Module wie Google Maps verfügbar
- API für Scripting



Ninja Dashboard



Thruk

- Perl Catalyst
- Dank Livestatus Echtzeitansicht
- Viele Sonderfunktionen
- Suche und Filterung der Ergebnisse
- Multisitefähig
 - Verschiedene Backends
 - Einzel und Zusammen (NICHT korreliert)
 - Nagios, Icinga und Shinken



Thruk Screenshot

The screenshot displays the Thruk interface for monitoring Nagios services. The main content area shows 'Service Status Details For Host 'n0_test_host_001''. A table lists various services with their current status, last check time, duration, and attempt count. The first service, 'n0_test_critical_08', is in a 'CRITICAL' state, while others are 'OK' or 'WARNING'.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
n0_test_host_001	n0_test_critical_08	CRITICAL	2011-03-29 18:36:44	473d 1h 30m 15s	3/3	n0_test_host_001 (checked by barney) CRITICAL: critical n0_test_critical_08
	n0_test_ok_04	OK	2010-01-08 13:15:51	473d 1h 28m 35s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_04
	n0_test_ok_05	OK	2010-01-08 13:17:31	473d 1h 26m 54s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_05
	n0_test_ok_09	OK	2010-01-08 13:19:11	473d 1h 25m 14s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_09
	n0_test_ok_10	OK	2010-01-08 13:20:53	473d 1h 23m 33s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_10
	n0_test_ok_11	OK	2010-01-08 13:22:34	473d 1h 21m 53s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_11
	n0_test_ok_15	OK	2010-01-08 12:54:16	473d 1h 20m 9s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_15
	n0_test_ok_16	OK	2010-01-08 12:55:53	473d 1h 18m 32s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_16
	n0_test_ok_17	OK	2010-01-08 12:57:33	473d 1h 16m 52s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_17
	n0_test_ok_19	OK	2010-01-08 12:59:14	473d 1h 15m 11s	1/3	n0_test_host_001 (checked by barney) OK: ok n0_test_ok_19
	n0_test_random_00	OK	2010-01-08 13:00:54	473d 1h 13m 31s	1/3	n0_test_host_001 (checked by barney) OK: random n0_test_random_00 ok
	n0_test_random_02	OK	2010-01-08 13:02:34	473d 1h 11m 51s	1/3	n0_test_host_001 (checked by barney) OK: random n0_test_random_02 ok
	n0_test_random_06	OK	2010-01-08 13:04:15	473d 1h 10m 10s	1/3	n0_test_host_001 (checked by barney) OK: random n0_test_random_06 ok
	n0_test_random_07	OK	2010-01-08 13:05:55	473d 1h 8m 30s	1/3	n0_test_host_001 (checked by barney) OK: random n0_test_random_07 ok
	n0_test_random_12	WARNING	2011-01-18 12:00:44	473d 1h 6m 49s	3/3	n0_test_host_001 (checked by barney) WARNING: random n0_test_random_12 unchanged
	n0_test_random_13	OK	2010-01-08 13:08:16	473d 1h 5m 9s	1/3	n0_test_host_001 (checked by barney) OK: random n0_test_random_13 ok



Multisite

- Python basiertes Webfrontend mit Livestatus Backend
- konfigurierbare Views
- Multisitefähig
- pnp integration
- graphische Repräsentation von perfddata
- rollenbasiertes Authorisationsmodell



Multisite Screenshot

The screenshot displays the Nagios Multisite v1.1.0rc3 interface. The main content area shows the 'Hostgroups (Summary)' page for 'nagiosadmin (admin)' at 20:24. The interface includes a sidebar with navigation options and a main table of hostgroup data.

Tactical Overview

Hosts	Problems	Unhandled
99	0	0
2463	45	45

Master control

Rechenzentrum Franken

- Hostgroups: disabled
- Service checks: enabled
- Host checks: enabled
- Event handlers: enabled
- Performance data: enabled

Linuxcluster Bayern

- Hostgroups: enabled
- Service checks: enabled
- Host checks: enabled
- Event handlers: enabled
- Performance data: enabled

Site status

- Rechenzentrum Franken: online
- Linuxcluster Bayern: online

Views

- Hosts
 - All hosts
 - All hosts (Min)
 - All hosts (Max)
 - Host search
- Hostgroups
 - Hostgroups
 - Hostgroups (Grid)
 - Hostgroups (Summary)
- Services
 - All services
 - Recently changed services
 - Services by host groups
 - Service search
- Servicegroups
 - Servicegroups (Grid)
 - Servicegroups (Summary)
 - Services by group
- Problems
 - Host problems

Hostgroups (Summary)

Name	Alias	Min	Max	OK	Warn	Crit	Unk	Down	Uptime
check_mk	Fallback hostgroup of check_mk	2	0	0	0	16	1	1	117
linux-prod	Linux Server (Produktiv)	10	0	0	0	700	18	7	13.7
linux-test	Linux Server (Test)	7	0	0	0	399	1	8	8.0
windows-prod	Windows Server (Produktiv)	8	0	0	0	85	3	2	1.6
windows-test	Windows Server (Test)	8	0	0	0	69	1	2	1.6

Linuxcluster Bayern

Name	Alias	Min	Max	OK	Warn	Crit	Unk	Down	Uptime
alle	alle	66	0	0	0	831	1	1	1
linux-test	linux-test	1	0	0	0	12	1	1	1

refresh: 30 secs



Multisite Screenshot

multisite check v1.1.6rc3 Services of Host Rechenzentrum Franken, avms35 nagiosadmin (admin) 20:20

Quicksearch: avms35

Tactical Overview: 1831 OK 45 Unhandled 45

Rechenzentrum Franken: Hosts OK, Service checks OK, Host checks OK, Event handlers OK, Performance data OK

Views: Hosts, Hostgroups, Services, Servicegroups, Problems, Alerts, Other

Host history | Host downtimes | Hoststatus | Problems of host | Host & service history | PHP graphs | Complete site

Filter: Commands | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 30 2 | 30 2 | 90 2 | = | Edit

STATUS	Service	Output detail	Age	Checked	Icons	Perf-O-Meter
OK	Check_MK	OK - Agent Version 2.2-1, processed 19 host info	2010-05-28 15:42:46	42 sec		
OK	CPU_loadok	OK - user: 1%, system: 3%, wait: 0% (1 CPU)	2010-05-28 15:42:46	42 sec	★	4%
OK	n_DSA101	OK - 28% used (8.46 of 30.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	28%
OK	n_DSA102	OK - 29% used (15.75 of 54.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	29%
OK	n_DSA103	OK - 17% used (9.43 of 54.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	17%
OK	n_DSA104	OK - 25% used (13.45 of 60.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	25%
OK	n_DSA105	OK - 17% used (8.49 of 54.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	17%
OK	n_DSA106	OK - 25% used (14.00 of 54.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	25%
OK	n_DSA107	OK - 36% used (6.65 of 18.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	36%
OK	n_DSA108	OK - 0% used (0.16 of 18.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	0%
OK	n_DSA109	OK - 49% used (12.39 of 25.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	49%
OK	n_DSA110	OK - 39% used (6.44 of 18.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	39%
OK	n_DSA111	OK - 53% used (9.70 of 18.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	53%
OK	n_DSA112	OK - 39% used (7.14 of 18.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	39%
OK	n_DSA113	OK - 33% used (10.11 of 30.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	33%
OK	n_DSA114	OK - 62% used (11.28 of 18.00 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	62%
OK	n_DSA20	OK - 46% used (7.92 of 16.96 GB) (levels at 80.0% 0%)	2010-05-28 15:42:46	42 sec	★	46%
OK	Memory used	OK - 59.4% of RAM (5.05 of 8.50 GB) used by processes	2010-05-28 15:42:46	42 sec	★	
OK	MC 60	OK - packets: 0.00 in / 0.00 out	2010-05-28 15:44:46	42 sec	★	
OK	shadowsets	OK - 15 shadowsets in normal state	2010-05-28 15:42:46	42 sec	★	

refresh: 60 secs



NagVis

- Visualisierung von Nagios Strukturen
- Leicht aber auch komplex Erweiterbar
- Mit Nagios verknüpfte Widgets
- Extrem flexibel
- Einfache Erstellung von Schaubildern



Nagvis Screenshot I

NagVis

Wähle Map: **Standort 1** Diese Map bearbeiten Hilfe?

NagVis Map Liste

Standort 1 ❌ 	Standort 2 ✅ 	Standort 3 ✅ 	Standort 4 ❌
Standort 5 ✅ 	Standort 6 ✅ 	Netzwerk ❌ 	VPN-Übersicht ❌



Nagvis Screenshot II



Business Process View

- Abbildung von Clustersystemen in Nagios
- Simulation von Ausfällen und deren Auswirkungen auf das Gesamtsystem
- Überwachung von Dienst SLAs
- Logische Verknüpfung von Diensten



Business Process View

Short Summary: All Business Processes



Priority 1

Alerting round the clock (24 x 7)

Business Process	Status	Status Information
WebShop	 OK 	currently 48 user sessions, 17 anonymous sessions
WebSite	 OK 	Please note: This afternoon maintenance on WebServer1, Production only on WebServer2


Priority 2

Alerting Monday to Sunday 7:00 to 22:00

Business Process	Status	Status Information
eMail	 OK 	Please note: This Saturday from 19:00 till 23:00 maintenance on the MailGateway1




Priority 3

Alerting Monday to Thursday 7:00 to 17:00, Friday 7:00 to 15:00

Business Process	Status	Status Information
Intranet Portal	 OK 	currently 61 user sessions
ERP System	 OK 	system resource usage 34%

Priority 4

Testsystems -- no Alerting

Business Process	Status	Status Information
Testsystem 1	 OK	Dummyhosts with Dummyservices
Testsystem 2	 OK	The System is relocation in the new RZ
Testsystem 3	 OK	The System is relocation in the new RZ



Links

DNX <http://dnx.sourceforge.net>

Nagios Exchange <http://exchange.nagios.org> (Plugins)

NagiosQL <http://www.nagiosql.org>

mod_gearman

<http://labs.consol.de/lang/de/nagios/mod-gearman/>

Nagios Wiki <http://www.nagios-wiki.de> (Viel Doku in deutsch)

netways <http://www.netways.org> (netways grapher v2)

MK <http://www.mathias-kettner.de> (Livestatus, check_mk, Multisite, wato)

op5 <http://www.op5.com> (Ninja, Merlin, Plugins)

pnp4nagios <http://www.pnp4nagios.org>

Thruk <http://www.thruk.org>

