

# Netzwerkmonitoring mit Nagios & Icinga

15.11.2009 – OpenSourceExpo

*Referent: Julian Hein*

## Agenda



<i>Speisen</i>	
Currywurst	8,88 €
Curryboulette	8,88 €
Pommes Frites	8,88 €
Bockwurst	8,88 €
Rostbratwurst	8,88 €
Knacker	8,88 €
Wiener	8,88 €
Schnitzel	8,88 €
Hamburger	8,88 €
Cheeseburger	8,88 €
Hot Dog	8,88 €
Fleischspieß	8,88 €
Kartoffelsalat	8,88 €
Scharfe Zwiebeln	8,88 €
Brötchen	8,88 €
Ketchup / Mayo	8,88 €

- Kurzvorstellung
- Nagios – Eine Einführung
- AddOns – Nagios erweitern
- Was ist Icinga?
- Fragen & Antworten



NETWAYS GmbH

# Kurzvorstellung



## Allgemeine Daten

- Firmengründung 1995
- GmbH seit 2001
- Open Source seit 1997
- Nagios / Netsaint seit 1999
  
- 20 Mitarbeiter
- Sitz in Nürnberg





## Leistungsbereiche

### Open Source Systems Management

- Monitoring
- Performance Management
- Configuration Management
- Service Management
- Knowledge Management
- Asset Management
- Identity Management
- Backup & Datensicherung

### Open Source Data Center Solutions

- High Availability Lösungen
- Cluster Lösungen
- Loadbalancing
- Virtualisierung
- Speicherlösungen
- Firewalls
- Datenbanken
- Voice over IP

Managed Services

Monitoring HW

Veranstaltungen



# Konferenzen



## 4. Monitoring Conference (OSMC)

- Mehr als 260 Teilnehmer
- Parallele Tracks mit Vorträgen & Workshops
- 28. - 29. Oktober -> <http://netways.de/osmc>



## 2. Open Source Datacenter Conference (OSDC)

- Ca. 100 Teilnehmer
- Parallele Tracks mit Vorträgen & Workshops
- 26. - 27. Mai -> <http://netways.de/osdc>



# Kunden





Kurze Einführung  
**NAGIOS**



## Nagios Überblick

# Nagios®

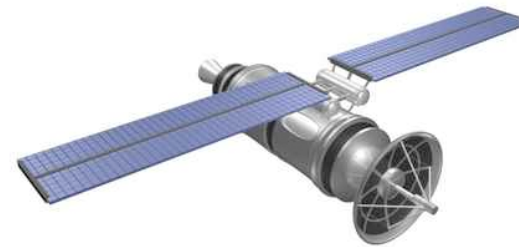
- Überwachungssystem für Devices und Dienste
- Betrieb unter Linux und UNIX möglich
- Open Source Software unter GPL
- Überwachung verschiedenster IT Komponenten
- Aktives Polling durch geplante Abfragen
- Verarbeitung passiver Events möglich
- Webinterface für Präsentation & Reporting
- Flexibles Benachrichtigungssystem

## Grundaufbau von Nagios



### Nagios Daemon

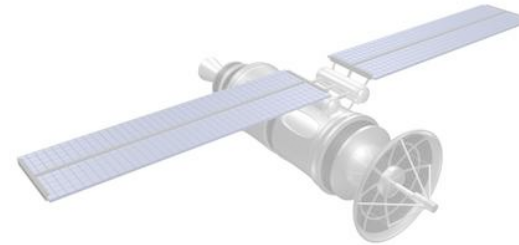
- zentrales Framework
- Konfiguration & Scheduling
- Webinterface
- Benachrichtigungen
- Logdateien & Event Handler



### Nagios Plugins

- Überwachungsaufgabe
- Exe, Skripte, Agenten
- Statusmeldung  
OK, WARNING, CRITICAL
- Zusatzinfos  
2% free on /dev/sda1

## Kommunikation



- Sehr flexible Kommunikationsmöglichkeiten
- Nagios Protokolle (NRPE, NSCA, NsClient++)
- Standardprotokolle (SSH, SNMP, WMI)
- Eigene Lösungen möglich



## Was ist alles überwachbar?

Kurze Antwort

**ALLES!\***

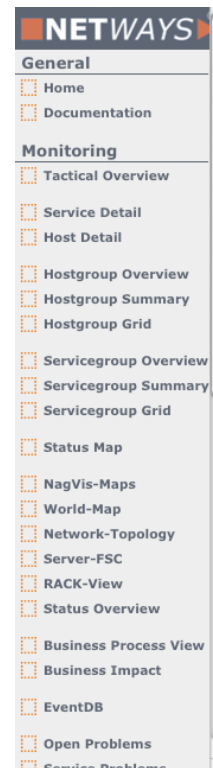
\*Plugin vorhanden: [www.monitoringexchange.org](http://www.monitoringexchange.org) oder selber schreiben



# Nagios Webinterface



- Zustand aller Objekte
- Gruppenansichten
- Historische Entwicklung
- Kartenansicht der Abhängigkeiten
- Verschiedene Reports
- Verschiedene Detailebenen



**Nagios**<sup>®</sup>  
Copyright (c) 1999-2008 Ethan Galstad

**Version 3.0.6**  
December 01, 2008  
[Read what's new in Nagios 3](#)



### Need help with Nagios?

A variety of worldwide support options are available to help you get Nagios up and running quickly. Visit [www.nagios.org/support/](http://www.nagios.org/support/) for information on:

- Installation
- Configuration
- Performance Tuning
- Integration
- Customization

**Nagios**  
Enterprises

MONITORED BY  
**Nagios**  
NETWORK MONITOR

SOURCEFORGE.NET<sup>™</sup>

Nagios and the Nagios logo are trademarks, servicemarks, registered trademarks or registered servicemarks owned by Nagios Enterprises, LLC.  
Nagios is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.



# Nagios Webinterface Tactical Overview

**Tactical Monitoring Overview**  
 Last Updated: Tue Jun 22 23:10:37 CEST 2004  
 Updated every 90 seconds  
 Nagios® - [www.nagios.org](http://www.nagios.org)  
 Logged in as: *nagiosadmin*

**Monitoring Performance**

Service Check Execution Time: 0.02 / 4.80 / 1.241 sec  
 Service Check Latency: 0.01 / 0.64 / 0.224 sec  
 Host Check Execution Time: 0.01 / 0.49 / 0.102 sec  
 Host Check Latency: 0.00 / 0.00 / 0.000 sec  
 # Active Host / Service Checks: 84 / 444  
 # Passive Host / Service Checks: 0 / 49

**Network Outages**

0 Outages

**Network Health**

Host Health:   
 Service Health:

**Hosts**

0 Down	0 Unreachable	84 Up	0 Pending
--------	---------------	-------	-----------

**Services**

1 Critical	0 Warning	0 Unknown	492 Ok	0 Pending
1 Unhandled Problems			49 Disabled	

**Monitoring Features**

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled	Enabled	Enabled	Enabled	Enabled
34 Services Disabled 1 Service Flapping	31 Services Disabled 12 Hosts Disabled	All Services Enabled All Hosts Enabled	49 Services Disabled All Hosts Enabled	444 Services Disabled All Hosts Enabled
All Hosts Enabled No Hosts Flapping				



# Nagios Webinterface Details

## Current Network Status

Last Updated: Tue Jun 22 23:07:50 CEST 2004  
 Updated every 90 seconds  
 Nagios® - [www.nagios.org](http://www.nagios.org)  
 Logged in as: *nagiosadmin*

[View History For This Host](#)  
[View Notifications For This Host](#)  
[View Service Status Detail For All Hosts](#)

## Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0
All Problems		All Types	
0		1	

## Service Status Totals

Ok	Warning	Unknown	Critical	Pending
17	0	0	0	0
All Problems		All Types		
0		17		

## Service Status Details For Host 'net-kilogramm'

Host ↑↓	Service ↑↓	Status ↑	Last Check ↑↓	Duration ↑↓	Attempt ↑	Status Information
<a href="#">net-kilogramm</a>	<a href="#">3ware Unit 0</a>	OK	22-06-2004 22:46:30	37d 19h 29m 12s	1/2	check_3ware.pl: OK (Unit 0 at Controller 0 is OK)
	<a href="#">3ware Unit 5</a>	OK	22-06-2004 22:48:16	64d 10h 23m 24s	1/2	check_3ware.pl: OK (Unit 5 at Controller 0 is OK)
	<a href="#">CPU_LOAD</a>	OK	22-06-2004 23:06:24	64d 10h 46m 36s	1/5	load average: 0.00, 0.00, 0.00
	<a href="#">Current User</a>	OK	22-06-2004 23:06:26	36d 9h 36m 15s	1/5	USERS OK - 0 users currently logged in
	<a href="#">Disk /dev/sda1</a>	OK	22-06-2004 23:03:48	64d 10h 29m 31s	1/5	DISK OK - [1222952 kB (33%) free on /dev/sda1]
	<a href="#">Disk /dev/sda3</a>	OK	22-06-2004 23:03:48	64d 10h 27m 28s	1/5	DISK OK - [557458824 kB (61%) free on /dev/sda3]
	<a href="#">NTP</a>	OK	22-06-2004 22:46:30	37d 19h 29m 12s	1/2	OK: Time difference 0.000287 seconds
	<a href="#">PING</a>	OK	22-06-2004 23:04:11	64d 10h 23m 22s	1/5	PING OK - Packet loss = 0%, RTA = 1.90 ms
	<a href="#">Prozesse</a>	OK	22-06-2004 23:06:27	64d 10h 46m 35s	1/5	OK - 71 processes running
	<a href="#">Prozesse bacula-dir</a>	OK	22-06-2004 22:53:16	64d 10h 44m 32s	1/5	OK - 4 processes running with command name bacula-dir
	<a href="#">Prozesse bacula-fd</a>	OK	22-06-2004 22:54:07	58d 12h 40m 18s	1/5	OK - 3 processes running with command name bacula-fd
	<a href="#">Prozesse bacula-sd</a>	OK	22-06-2004 22:43:57	58d 18h 29m 59s	1/5	OK - 3 processes running with command name bacula-sd
	<a href="#">Prozesse zombie</a>	OK	22-06-2004 23:06:27	58d 1h 41m 7s	1/5	OK - 0 processes running with STATE = Z
	<a href="#">Remote Backup</a>	OK	22-06-2004 22:48:16	58d 12h 40m 8s	1/5	Bacula OK: Found 2 successful jobs
	<a href="#">SSH</a>	OK	22-06-2004 23:06:22	37d 16h 34m 12s	1/5	SSH ok - protocol version 2.0 - server version
	<a href="#">Swap Usage</a>	OK	22-06-2004 23:06:24	64d 10h 44m 30s	1/5	Swap ok - Swap used: 10% (51924992 bytes out of 509956096)
	<a href="#">Uptime</a>	OK	22-06-2004 23:03:53	23d 19h 32m 17s	1/5	Uptime o.k. - Up 120 days

17 Matching Service Entries Displayed

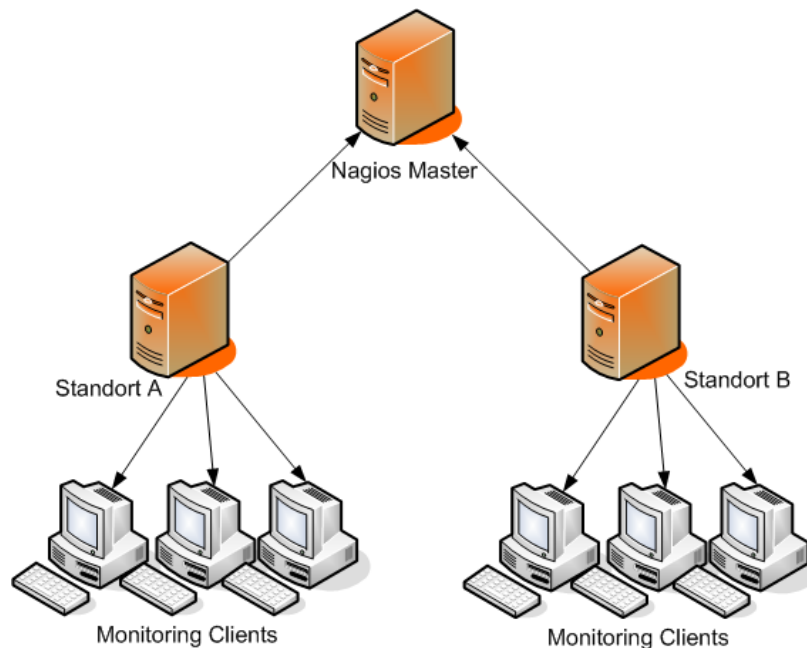
## Nagios Alarmierung

- Vielfältige Benachrichtigungskanäle
  - eMail
  - SMS, Cityruf, Pager
  - Instant Messenger & net send PopUps
  - Telefonanruf inkl. Voice Menü durch Asterisk Integration
- Eskalationen
- Personen & Gruppen
- Zeitfenster & Intervalle
- Erkennung von Folgefehlern
- Schnittstelle zu anderen Anwendungen (bsp. Ticketsysteme)



# Distributed Monitoring

- Mehrere Nagios Server überwachen Teilbereiche
- Weitermeldung der Ergebnisse an zentralen Server



## Einsatzbereiche

- Logische Netzstruktur
- Lastverteilung
- Überwachung geschützter Bereiche



## Weitere Features



- Einfache HA Implementierung
- Gegenmaßnahmen mit Event Handler
- Einfache, textbasierte Konfiguration
- Erfassung von Downtimes
- Reporting zu Verfügbarkeiten
- Generierung von Performancewerte
- Vermeidung von Fehlalarmen
- Erkennung von Ausfall vs. Nicht Erreichbarkeit



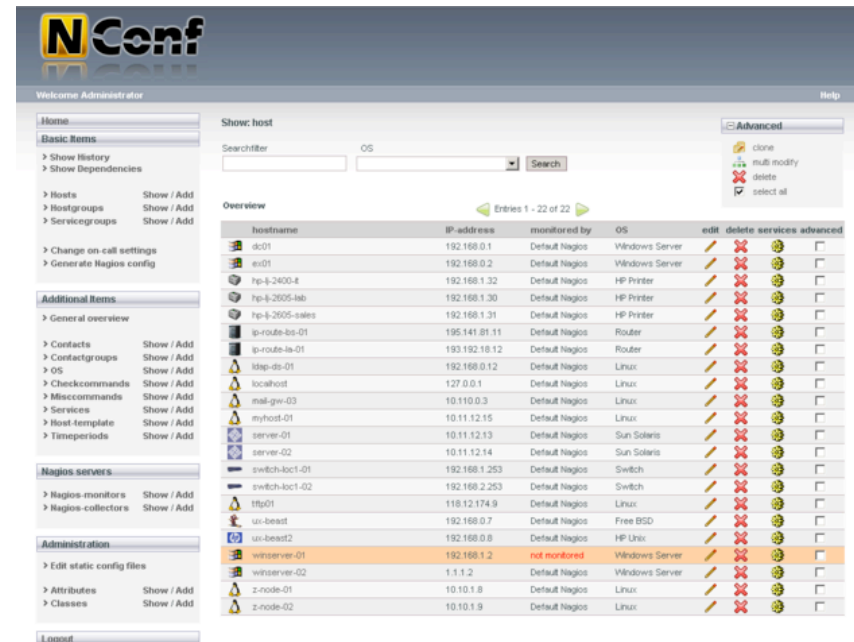
Zusatzfunktionen für Nagios

# **NAGIOS ADDONS**



# Konfigurationstools

- Beispiele NConf oder NagiosQL
- Webbasierte Konfiguration
- Bulk Updates
- Klonen von Objekten
- Generierung von Konfigurationsdateien
- Syntaktischer Config-Check
- Unterstützung von verteilten Umgebungen (NConf)



The screenshot shows the NConf web interface. The main content area displays a table of hosts with the following columns: hostname, IP address, monitored by, OS, edit, delete, services, and advanced. The table contains 22 entries, with the first one highlighted in orange.

hostname	IP address	monitored by	OS	edit	delete	services	advanced
dc01	192.168.0.1	Default Nagios	Windows Server				
eu01	192.168.0.2	Default Nagios	Windows Server				
hp-6-2400-4	192.168.1.32	Default Nagios	HP Printer				
hp-6-2605-lab	192.168.1.30	Default Nagios	HP Printer				
hp-6-2605-sales	192.168.1.31	Default Nagios	HP Printer				
ip-route-ba-01	195.141.81.11	Default Nagios	Router				
ip-route-la-01	193.192.18.12	Default Nagios	Router				
istp-ds-01	192.168.0.12	Default Nagios	Linux				
localhost	127.0.0.1	Default Nagios	Linux				
mail-gw-03	10.110.0.3	Default Nagios	Linux				
myhost-01	10.11.12.15	Default Nagios	Linux				
server-01	10.11.12.13	Default Nagios	Sun Solaris				
server-02	10.11.12.14	Default Nagios	Sun Solaris				
switch-lac1-01	192.168.1.253	Default Nagios	Switch				
switch-lac1-02	192.168.2.253	Default Nagios	Switch				
tfp01	118.12.174.9	Default Nagios	Linux				
ux-beast	192.168.0.7	Default Nagios	Free BSD				
ux-beast2	192.168.0.8	Default Nagios	HP Unix				
winsrvr-01	192.168.1.2	not monitored	Windows Server				
winsrvr-02	1.1.1.2	Default Nagios	Windows Server				
z-node-01	10.10.1.8	Default Nagios	Linux				
z-node-02	10.10.1.9	Default Nagios	Linux				

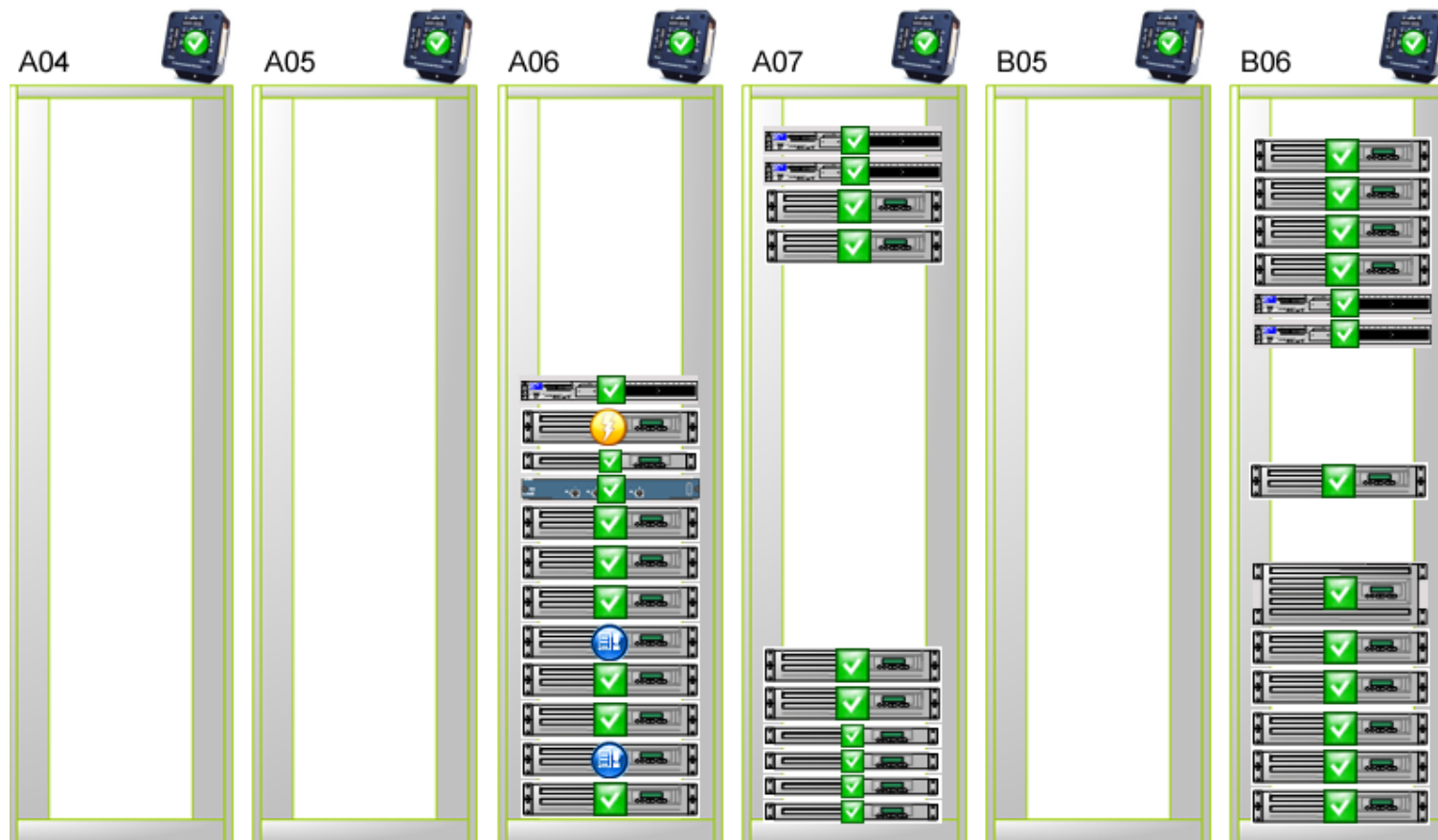
## Visualisierung

- NagVis zur grafischen Darstellung von Nagios Daten
- Eigene Grafiken + Nagios Status
- Einzelne Objekte
- Objektgruppen
- Hierarchische Maps mit Drill-Down
- Integration in Nagios Webinterface
- Drag`n`Drop im Webinterface

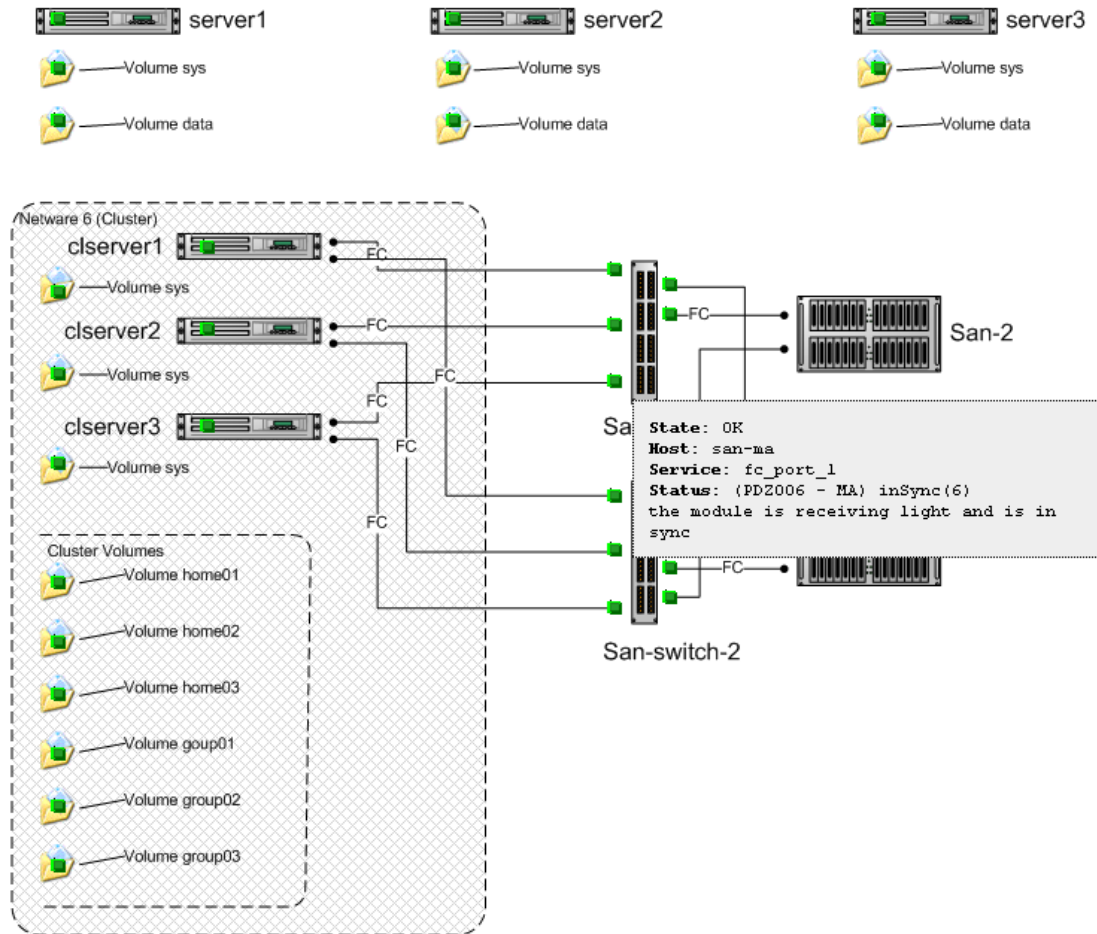




# NagVis Rack Ansicht

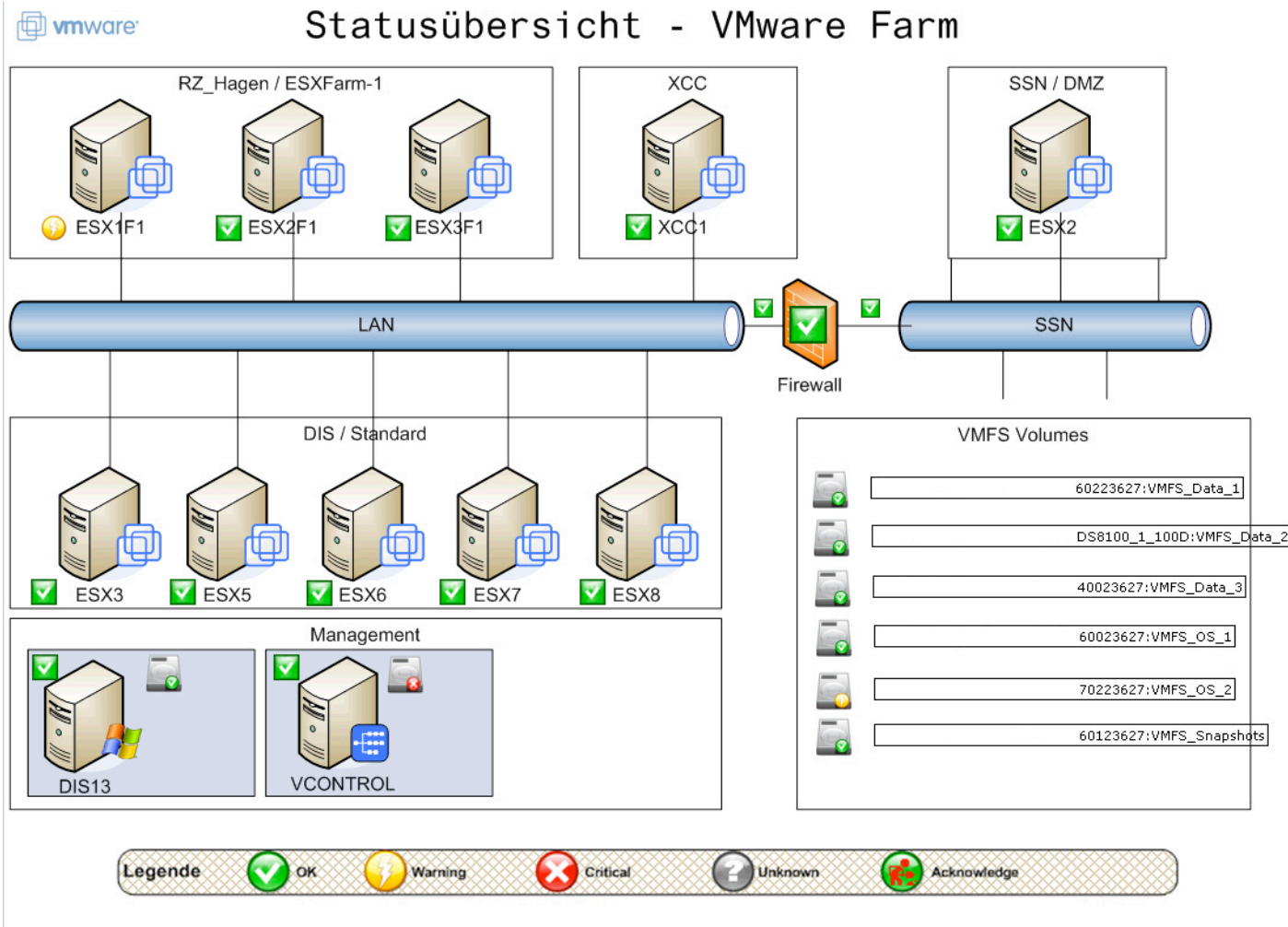


# NagVis SAN Ansicht





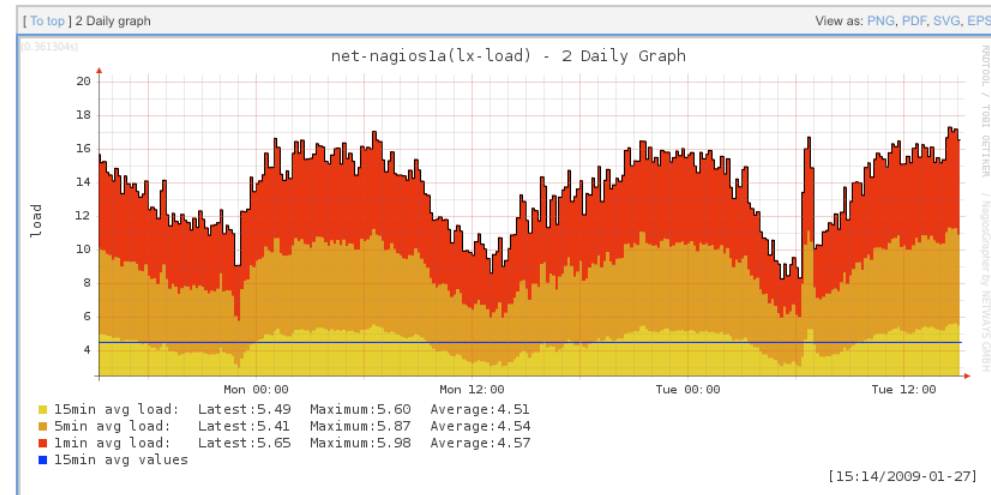
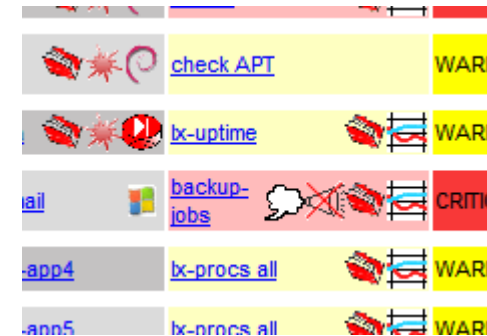
# NagVis Netzwerkstruktur





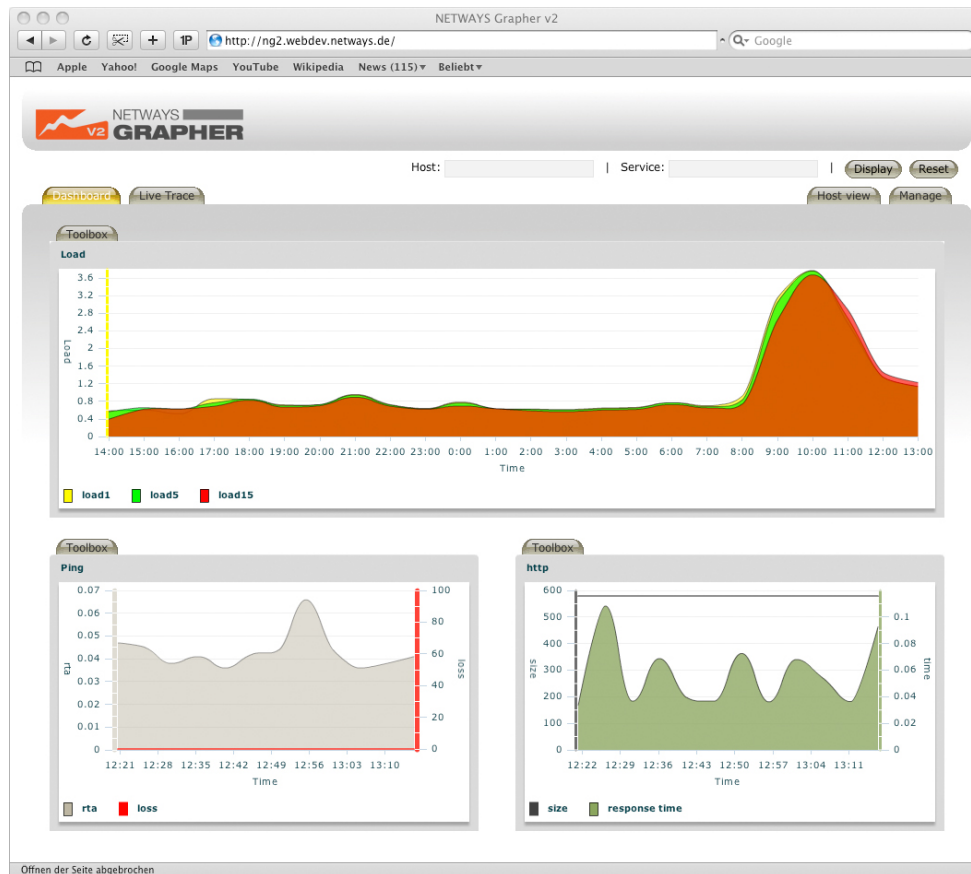
# Performanceanalyse

- NagiosGrapher & PNP
- Erzeugung von Performancecharts
- Hoher Automatisierungsgrad
- Direkte Einbindung in Nagios Webfrontend
- RRD Backend für Datenspeicherung
- Erstellung der Graphen in Echtzeit
- Umfangreiche Features
  - Berechnungen
  - Multigraphen
  - Datenkonsolidierung
  - Housekeeping





# Performanceanalyse 2.0



- NETWAYS Grapher V2
- Flashbasierte Graphen
- Aktualisierung in Realtime
- Ajax Webinterface
- Dashboards
- Multigraphen
- Zentrales Data Warehouse
- Aktuell RC1
- Final dieses Jahr



# Geschäftsprozesse

- Business Process View
- Aggregation von Einzelüberwachungen zu Geschäftsprozessen
- Hierarchischer Treeview
- And / Or Verknüpfungen
- Drilldown zum Service
- Ausfallsimulationen

## Übersicht: Alle Business Prozesse

### Priorität 1

Alarmierung rund um die Uhr (24 x 7)

Business Process	Status	Status Information
<a href="#">WebShop</a>	CRITICAL	currently 48 user sessions, 17 anonymous sessions
<a href="#">WebSite</a>	CRITICAL	Please note: This afternoon maintenance on WebServer1, Production only on WebServer2

### Priorität 2

Alarmierung Montag bis Sonntag 7:00 bis 22:00 Uhr

Business Process	Status	Status Information
<a href="#">eMail</a>	WARNING	Please note: This Saturday from 19:00 till 23:00 maintenance on the MailGateway1

### Priorität 3

Alarmierung Montag bis Donnerstag 7:00 bis 17:00 Uhr, Freitag 7:00 bis 15:00 Uhr

Business Process	Status	Status Information
<a href="#">Intranet Portal</a>	OK	currently 61 user sessions
<a href="#">ERP System</a>	OK	system resource usage 34%

### Priorität 4

Abnahme-, Entwicklungs- und Testsysteme -- keine Alarmierung

Business Process	Status	Status Information
<a href="#">Testsystem 1</a>	OK	Dummyhosts with Dummieservices
<a href="#">Testsystem 2</a>	OK	The System is relocation in the new RZ
<a href="#">Testsystem 3</a>	OK	The System is relocation in the new RZ

[\[Ampel einblenden\]](#)



# Business Process View Ebenen

Status: Details für WebShop

Host	Service	Status	Status Information
	<a href="#">Internet Connection</a>	OK	
	<a href="#">Loadbalancer Cluster</a>	OK	
and	<a href="#">DNS Cluster</a>	OK	
	<a href="#">WebShop Frontend Servers</a>	CRITICAL	
	<a href="#">ERP System</a>	OK	



Status: Details für WebShop Frontend Servers

\* Die Anwendung ist für den Kunden ver

Host	Service	Status	Status Information
or	<a href="#">WebShop Frontend Servers Line1</a>	CRITICAL	
	<a href="#">WebShop Frontend Servers Line2</a>	CRITICAL	



Status: Details für WebShop Frontend Servers Line2

Host	Service	Status	Status Information
and	<a href="#">nbp_webserver2</a>	CRITICAL	HTTPS: CRITICAL, HTTPS/1.0 200 - 3000 bytes in 3000 seconds
	<a href="#">nbp_webserver2</a>	CRITICAL	HTTP: CRITICAL, HTTP OK HTTP/1.0 200 OK - 2000 bytes in 477.981 seconds
	<a href="#">nbp_appserver2</a>	OK	HTTP: OK, HTTP OK HTTP/1.0 200 OK - 0 bytes in 0 seconds

\* Die Anwendung ist für den Kunden verfügbar, wenn keine der Komponenten im Status CRITICAL ist.



## Integrationslösungen

- Dokumentation: Twiki, MediaWiki, FOSWiki
- End2End Monitoring: AutoIT
- Helpdesk: RT, OTRS
- CMDB: i-doit
- Reporting: Jasper & Pentahoo

... Und viele weitere AddOns



Was war nochmal Icinga?

**ICINGA**



## Was ist Icinga

- Community Fork von Nagios
- 4 Komponenten & Teams
  - Icinga-core (RC1)
  - Icinga-api (Alpha)
  - Icinga-web (Alpha)
  - Icinga-docs (Stable)
- Abwärtskompatibel zu Nagios
  - Plugins
  - Konfigurationssyntax
  - AddOns
  - Datenbankschema (teilweise)



## Icinga Docs

- Eigenes Dokumentationsteam
- Verfügbare Sprachen: Englisch & Deutsch
- Spanische Übersetzung in Arbeit
- Erstellung der Docu im Docbook Format & Ausgabe in
  - HTML (<http://docs.icinga.org>)
  - PDF (<http://docs.icinga.org>)
  - Manpages
  - Andere Formate



## Icinga Core

- Bisherige Nagios
- Alle aktuellen Patches und Bugfixes
- Datenbankbindung (IDOUtils) bereits integriert
- Datenbankabstraktion libdbi & ocilib eingebaut
- SSL Verschlüsselung für IDOUtils
- Unterstützung für MySQL, PostgreSQL & Oracle
- Performanceoptimierungen



## Icinga API

- Liest die Daten aus Icinga
- Sendet Daten an Icinga
- Zugriff auf IDO DB (Icinga Kernel geplant)
- Ausgabeformat PHP-PDO (JSON geplant)
- Keine Kenntnis der darunterliegenden Strukturen notwendig
- PHP aber keine Abhängigkeiten zu Libraries
- Basis für Webservice (geplant)



## Icinga Web

- Modernes Web 2.0 Interface basierend auf
  - icinga-api
  - PHP, ExtJS, Agavi MVC
- Komplette Anpassbarkeit durch Cronks (Widgets)
- Individuelle Sichten auf alle Monitoring-Objekte
- Event Viewer
- Leistungsfähige Suche
- Schnittstelle für AddOns



# LIVE DEMO



## Fragen & Antworten

- Jetzt und hier & am Icinga Stand

### ICINGA

- Website: [www.icinga.org](http://www.icinga.org)

### NETWAYS

- Website: [www.netways.de](http://www.netways.de)
- E-Mail: [jhein@netways.de](mailto:jhein@netways.de)
- Blog [blog.netways.de](http://blog.netways.de)
- Twitter [twitter.com/netways](https://twitter.com/netways)

[netways.de/osmc](http://netways.de/osmc)