IT-Monitoring auf der Basis von Nagios

Julian Hein

NETWAYS GmbH

jhein@netways.de

Kurzvorstellung

- Julian Hein
- Geschäftsführender Gesellschafter
- Gründung 1995
- Open Source seit 1998
- Netsaint (Nagios Vorgänger) seit 1999
- NETWAYS Tätigkeitsbereiche
  - Open IT Management
  - Open Enterprise Computing
  - Managed Services

Weitere Aktivitäten

Nagios Exchange

- Offizielles 3rd Party Repository
- Ca. 7.000 registrierte User
- Ca. 1.000 registrierte Projekte
- Mehr als 1 Mio Downloads

NETWAYS Nagios Konferenz

- Konferenz 2006: 145 Teilnehmer
- Konferenz 2007: 220 Teilnehmer
- Vorträge und Workshops mit Ethan Galstad, Ton Voon, Wolfgang Bart, etc.
- Austausch der User untereinander

Sinn und Zweck von Monitoring

- Zeitnahe Benachrichtigung bei Ausfällen
- Erkennung von Problemen vor Ausfall
- Gesamtüberblick über den Zustand des Netzwerks
- Vereinfachung der Fehlersuche
- Automatisierung von Routineaufgaben
- Erkennung von langfristigen Trends
- Datensammlung für Statistiken und SLA Kontrolle

Zwei Sichten für das Monitoring

- "Kunden"-Sicht
  - Dienste: DNS, Mailversand, Internetanbindung, Webseiten, etc.
  - Prozese: Bestellung im Webshop & andere komplexe Vorgänge
- Administrator-Sicht
  - Komponenten: Datenbank, Storagesysteme, Netzwerk, etc.
  - Messwerte: Füllgrad, CPU Auslastung, etc.

Was ist Nagios

- Überwachungssystem für Devices und Services
- Server für Linux und UNIX
- Aktives Polling durch geplante Abfragen
- Plugin API für Überwachungen
- Webinterface für Präsentation
- Flexibles Benachrichtigungsystem

Grundsätzlicher Aufbau von Nagios

Nagios-Daemon

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

Nagios-Plugins

- Überwachungsaufgabe
- Executables oder Skripte
- Zustandsmeldung an Daemon
(OK, WARNING, CRITICAL)
- Zusätzliche Statusmeldung
(0 kB (0%) free on /dev/md1)

- Aktive Abfragen / Polling
  - NRPE, SSH, Windows Agents, SNMP Abfragen
  - SNMP Abfragen
- Passive Abfragen
  - NSCA, SNMP Traps

Nagios Standardüberwachungen

Windows

- Status von Windows Diensten & Prozessen
- CPU Auslastung
- Festplattenbelegung
- Speicherbelegung
- Uptime
- Events aus Logfiles
- **alle Daten des Windows Performance Monitors**

Linux & Unix

- Festplattenbelegung & CPU Auslastung
- Status und Anzahl von Prozessen
- Datenbank- & Mailserver
- Eingeloggte User
- Samba & NFS Shares
- Auslastung Swap Partition
- Syslog

Netzdienste

- DNS
- FTP
- HTTP
- LDAP
- NNTP
- PING
- SMTP
- NTP
- Real Media
- Radius
- SSH
- TCP & UDP Ports

Weitere Überwachungen (Auszugsweise)

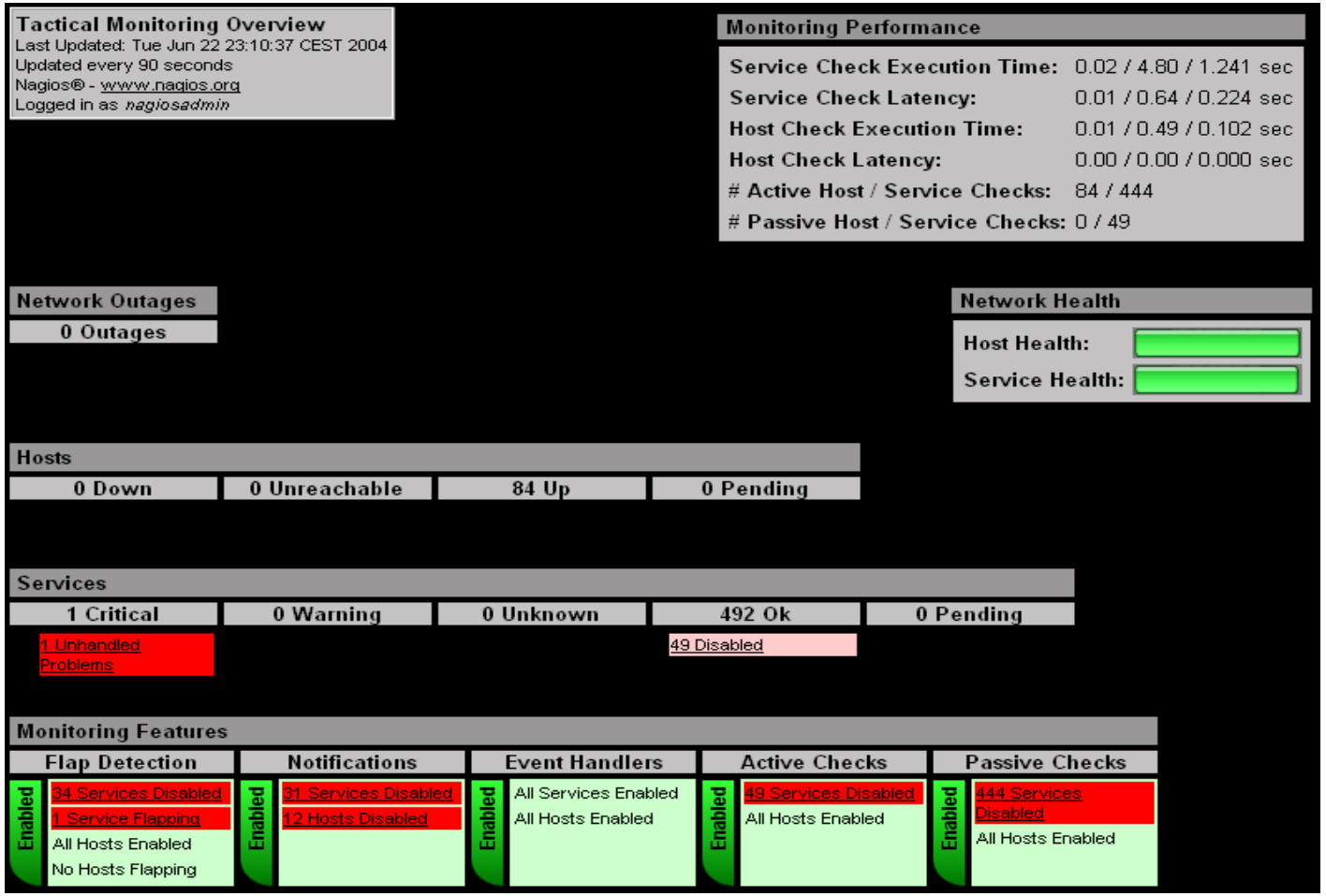
- SNMP Polling & SNMP Traps
  - Netzwerkgeräte & Storagesysteme
- Anbindung von Herstellertools
  - SAP via CCMS Schnittstelle
  - Anbindung der Agenten der HW Hersteller

- Eigene Scripte in bash, perl, VBScript, .NET
- http://www.nagiosexchange.org/

Nagios Webinterface allgemein

- Aktueller Zustand je Server & Dienst
- Zustände OK WARNING CRITICAL
- Zugriff auf Reports und Logdateien
- Unterschiedliche Detailebenen
  - Taktische Übersicht
  - Matrixansicht
  - Gruppenansicht
  - Detailansicht
- Statusmap

Nagios Webinterface Tactical Overview



Nagios Webinterface Details

Current Network Status
Last Updated: Tue Jun 22 23:07:50 CEST 2004
Updated every 90 seconds
Nagios® - 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

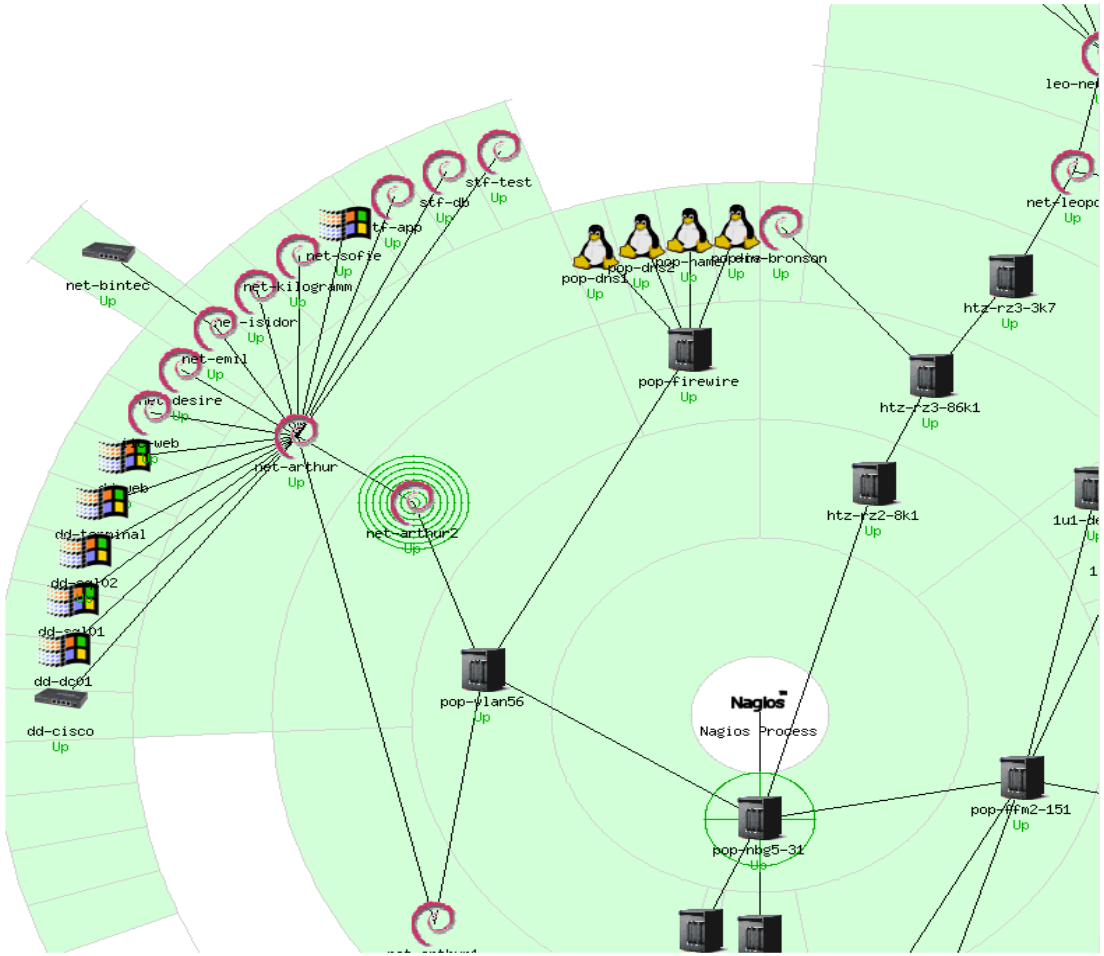
All Problems	All Types
0	17

Service Status Details For Host 'net-kilogramm'

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



Nagios Reporting

- Statusänderungen
- Statustrends
- Benachrichtigungen
- Verfügbarkeit %
- Verfügbarkeit Zeit
- Performancewerte via Schnittstelle

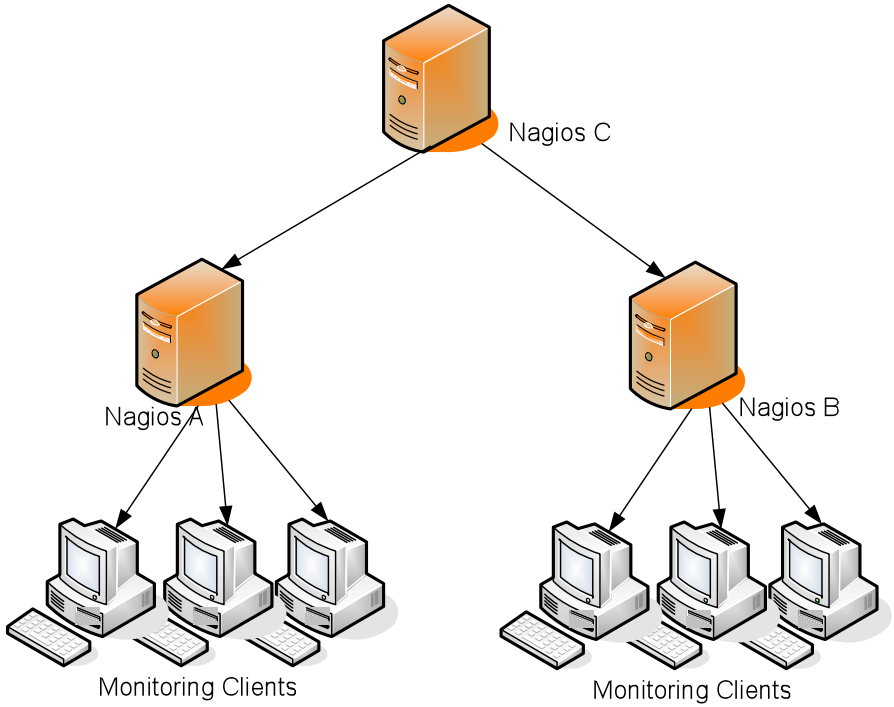
State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	17d 13h 32m 6s	99.996%	100.000%
	Scheduled	0d 0h 59m 30s	0.235%	0.235%
	Total	**17d 14h 31m 36s**	**99.996%**	**100.000%**
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
Undetermined	Nagios Not Running	0d 0h 1m 2s	0.004%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 1m 2s	0.004%	
All	Total	17d 14h 32m 38s	100.000%	100.000%

Nagios Alarmierung

- Flexible Benachrichtigungskanäle durch Shellscripts
  - eMail
  - SMS, Cityruf, Pager
  - Instant Messanger & net send PopUps
  - Telefonanruf inkl. Voice Menü
- Eskalation der Benachrichtigung
- Umfangreiche Benachrichtigungseinstellungen
- Schnittstelle zu anderen Anwendungen
- Keine Benachrichtigungen bei Folgefehlern

Spezielle Features: Distributed Monitoring

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



Einsatzbereiche

- Logische Netzstruktur
- Lastverteilung
- Überwachung geschützter Bereiche
- End2End Monitoring

Weitere Features

- Einfache HA Implementierung
- Automatisierte Gegenmaßahmen durch Event Handler
- Einfache, textbasierte Konfiguration durch Templates
- Erfassung von Downtimes
- Generierung von Performancewerte
- Vermeidung von Fehlalarmen durch Re-Checks & Flap-Detection
- Erkennung von Ausfall vs. Nicht Erreichbarkeit

Nagios 3.0

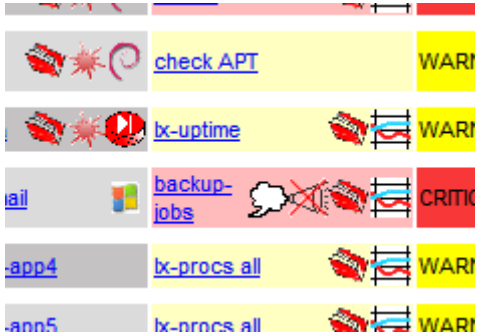
- Status: 3.0 RC1, aber bereits stabil, produktiv im Einsatz
- Erweiterung der Plugin API
- Verbesserungen am Embedded Perl Interpreter
- Custom Variables
- Flexiblere Konfigurationsoptionen
- Flexiblere Timeperiods
- Flexiblere Benachrichtigungen
- **Dramatische Performanceverbesserungen**
- => für große Netze einsetzen

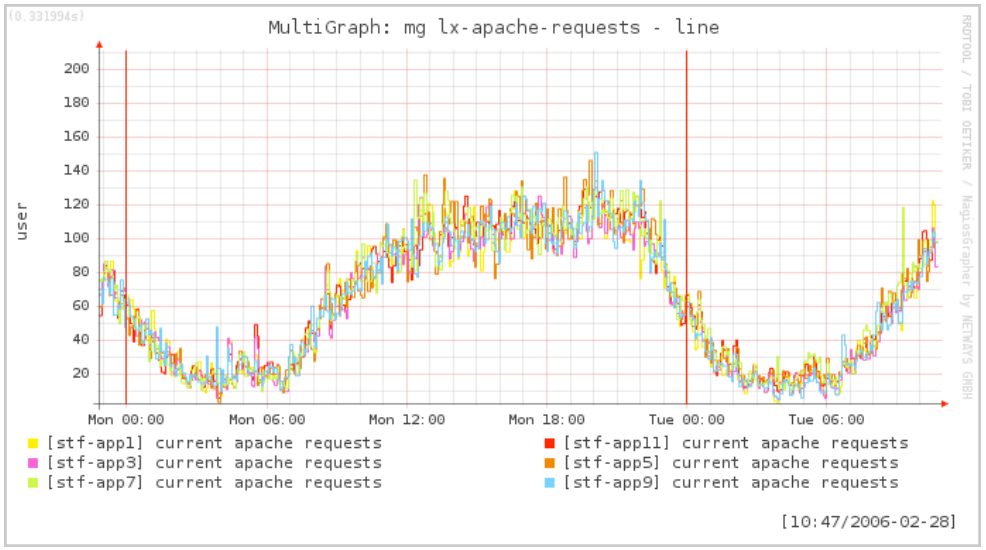
Weitere Gründe für Nagios

- Sehr große Verbreitung
- Sehr aktive Community
- Konstante und konservative Weiterentwicklung
- Professionellen Support
- Viel Erfahrung auch in großen Projekten
- Einfache Erweiterbarkeit durch Plugins
- Hohe Anzahl von AddOns (GPL)

1. NagiosGrapher

- Hoher Automatisierungsgrad
- Einfaches Handling im Webfrontend
- RRD Backend für Datenspeicherung
- Umfangreiche Zusatzfeatures





2. NagVis

- Visualisierung beliebiger Sachverhalte durch eigene Grafiken
- Anzeige von einzelnen Hosts oder Services
- Anzeige kompletter Gruppen oder Submaps
- Direkte Verbindung mit Nagios Webinterface
- Konfiguration per Drag'n'Drop im Webinterface

3. Wiki

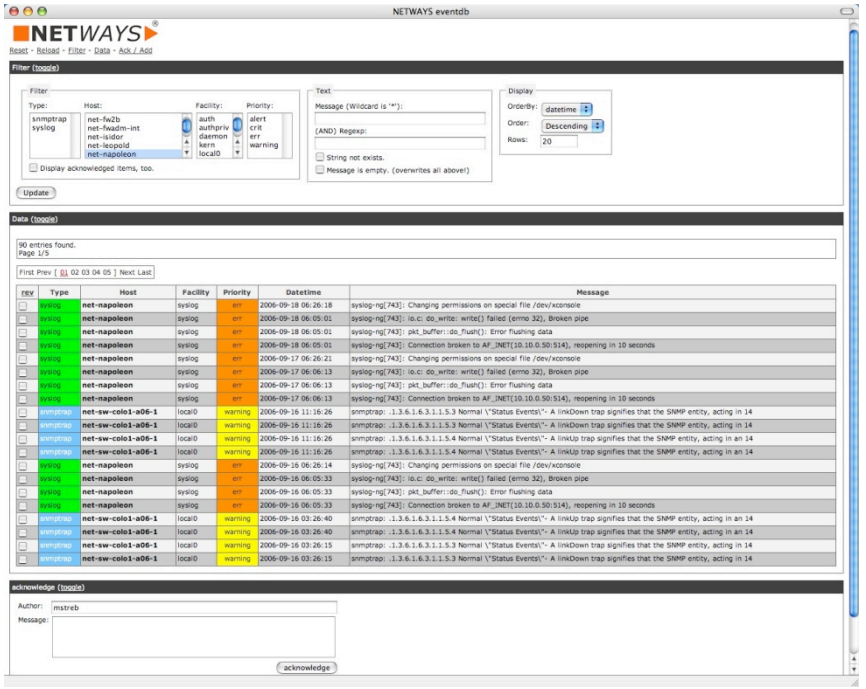
- Ablage von Dokumentation
- Einfache Integration in Nagios Frontend
- Schnell und unkompliziert durch Webzugriff
- Einfache Dokumentationssyntax
- Verfolgung von Änderungen und Diffs
- Ablage von Binärdateien

4. Ticketsystem

- Weiterbearbeitung von Nagios-Alarmen
  - Unkritische Probleme erzeugen Tickets statt E-Mail
  - Zuweisen der Störung zu einem Mitarbeiter
  - Tracking des Bearbeitungsfortschritts
  - Automatisches Schließen möglich
- Überwachung des Ticketsystems
  - Grundsätzliche Verfügbarkeit
  - Überwachung der Reaktions- oder Lösungszeit
  - Eskalation von hochpriorisierten Anfragen
- Vorhandene Integrationslösungen
  - Request Tracker
  - OTRS

5. EventDB

- Zentrale Schnittstelle für ereignisbezogene Meldungen
  - Logfiles von Servern und Anwendungen
  - E-Mail Benachrichtigungen
  - SNMP Traps
- Vorteile
  - Verbesserte Analysemöglichkeiten
  - Einfache Integration in Nagios

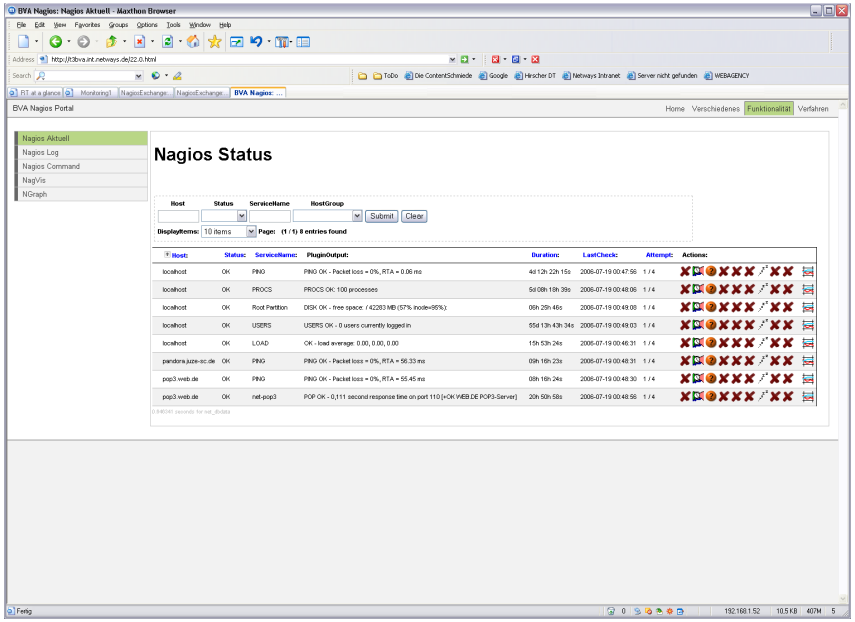


6. Notification Manager

- Externe Verwaltung von Benachrichtigungen
  - Webbasierte Konfiguration
  - Definition von Arbeitszeiten, Urlauben und Vertretungsregelungen
- Zentrale Schnittstelle für Benachrichtigungskanäle
  - E-Mail
  - SMS
  - Instant Messenger
  - Telefonanrufe
- Benachrichtigungszentrale für mehrere Nagios Server

7. Nagios Portal

- Alternatives Webinterface für Nagios mit erweiterten Funktionen
  - Design komplett durch Templates steuerbar
  - Integrierte Benutzerverwaltung mit Anbindung an LDAP, ADS oder NDS
  - Freie Konfiguration aller Ansichten
  - Datenanzeige als Listen, Grafiken oder sogar Tachometer
- Datenquellen
  - Alle Daten aus Nagios
  - Charts von NagiosGrapher
  - Maps aus NagVis
  - Ticketdaten
  - Inhalte aus Wikisystemen
  - SQL Datenbanken
  - Anwendungen durch Proxy



Fazit

- Nagios bietet nicht alle Features out-of-the-box
- Nagios stabile und getestete Grundlage für das Monitoring
- Framework für alle möglichen Überwachungsanforderungen
- Funktionserweiterung mit freien AddOns einfach
- Erfahrung und Support im Markt vorhanden

- **=> Nagios einsetzen**

- Eine Schwachstelle: Reporting

Q&A

- Hier und Jetzt
- NETWAYS Lounge im 2. Stock
- http://www.netways.de
- http://blog.netways.de
- jhein@netways.de