Nagios Monitoring & Systems Management

Julian Hein

Agenda

- Vorstellung NETWAYS
- Nagios Einführung
- Nagios AddOns
- Integrationsmöglichkeiten
- Fragen & Antworten

Kurzvorstellung

NETWAYS GmbH

Allgemeine Daten

- Gründung 1995
- Open Source seit 1997
- Nagios / Netsaint seit 1999

- 19 festangestellte Mitarbeiter

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

Nagios Aktivitäten

3rd NETWAYS Nagios Konferenz

- Veranstalter der Nagios Konferenz
- Teilnehmer: 145 (06), 220 (07), 250 (08)
- 5 Tracks mit Vorträgen & Workshops

Nagios® Enterprises Partner

- Nagios Enterprises Preferred Partner
- Einer von 4 Partnern weltweit

Nagios® Enterprises

- Nagios Community Advisory Board

NagiosExchange Portal

Nagios EXCHANGE

- Offizielles 3rd Party Repository
- 10.000 User, 1.400 Projects
- 1 Mio Downloads

Nagios FORGE

- Entwicklungsplattform für AddOns
- Versionsverwaltung, Mailinglists, usw.

Nagios WIKI

- Englischsprachiges Wikisystem
- HowTos, Best Practices, Code Snippets

Kunden

GfK
StayFriends
Kabel Deutschland
MESSE MÜNCHEN INTERNATIONAL
HappyDigits
BOSCH
Audi
BERU
KEIPER
DAIMLER
T-Mobile
T-Systems
arvato BERTELSMANN
FUJITSU
SUSE
DekaBank
LVM Versicherungen
Postbank
Deutsche Bausparkasse BADENIA
Banque LBLux
PUMA
SWAROVSKI
LIDL
neckermann.de
Bayer HealthCare
GEBERIT
BRENNTAG
Linde
SIEMENS
BLACK & DECKER
osce
BVA
Auswärtiges Amt
Bundesamt für Güterverkehr
Lufthansa Technik Logistik
REWE TOURISTIK
DACHSER Intelligente Logistik
Köln Bonn Airport
ALFRED TALKE Logistic Services

Einführung

NAGIOS

Sinn und Zweck von Monitoring

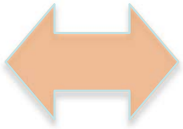
- Zeitnahe Benachrichtigung
- Erkennung drohender Probleme
- Gesamtüberblick über Netzwerk
- Vereinfachung der Fehlersuche
- Routineaufgaben automatisieren
- Erkennung von langfristigen Trends
- Datensammlung für SLA Überwachung

Nagios Überblick

Nagios®

- Überwachungssystem für Geräte und Dienste
- Nagios Server für Linux und UNIX
- Plugin API für Überwachungen
- Aktives Polling durch geplante Abfragen
- Webinterface für Präsentation & Reporting
- Flexibles Benachrichtigungsystem

Grundaufbau von Nagios



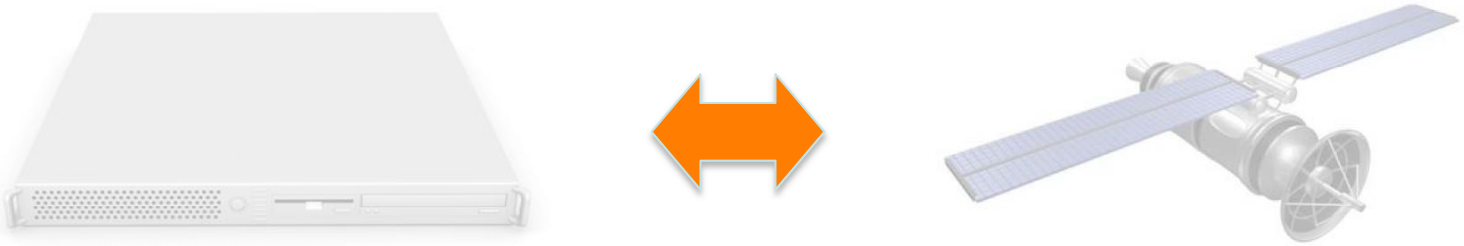
Nagios Daemon

- 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)

Kommunikation



- Flexible Server Client Kommunikation
- Eigene Nagios Protokolle (NRPE, NSCA, NsClient++)
- Standardprotokolle (SSH, SNMP, WMI)
- Eigene Lösungen
- Aktive Abfragen & passive Kommunikation

Was ist alles überwachbar?

Kurze Antwort

ALLES!

Mögliche Überwachungen

Hardware

- Netzwerkhardware durch SNMP
- Serverhardware durch Integration der Herstellertools (bsp. OpenManage, ServerView, IBM Director)
- Umweltmonitoring

Betriebssysteme

- CPU, Memory, Disk Auslastungen
- Prozesse und Dienste
- Windows Performance Monitor
- Alle Logfiles

Netzdienste

- Alle gängigen Netzwerkdienste (wie bsp. DNS, FTP, HTTP, LDAP, SMTP, SSH) durch Simulation eines Clientzugriffs
- TCP und UDP Ports

Applikationen

- SAP
- Alle Datenbanken
- Alle gängigen Messaging Systeme
- Web- & Application Server
- Verzeichnisdienste (AD, LDAP, NDS)

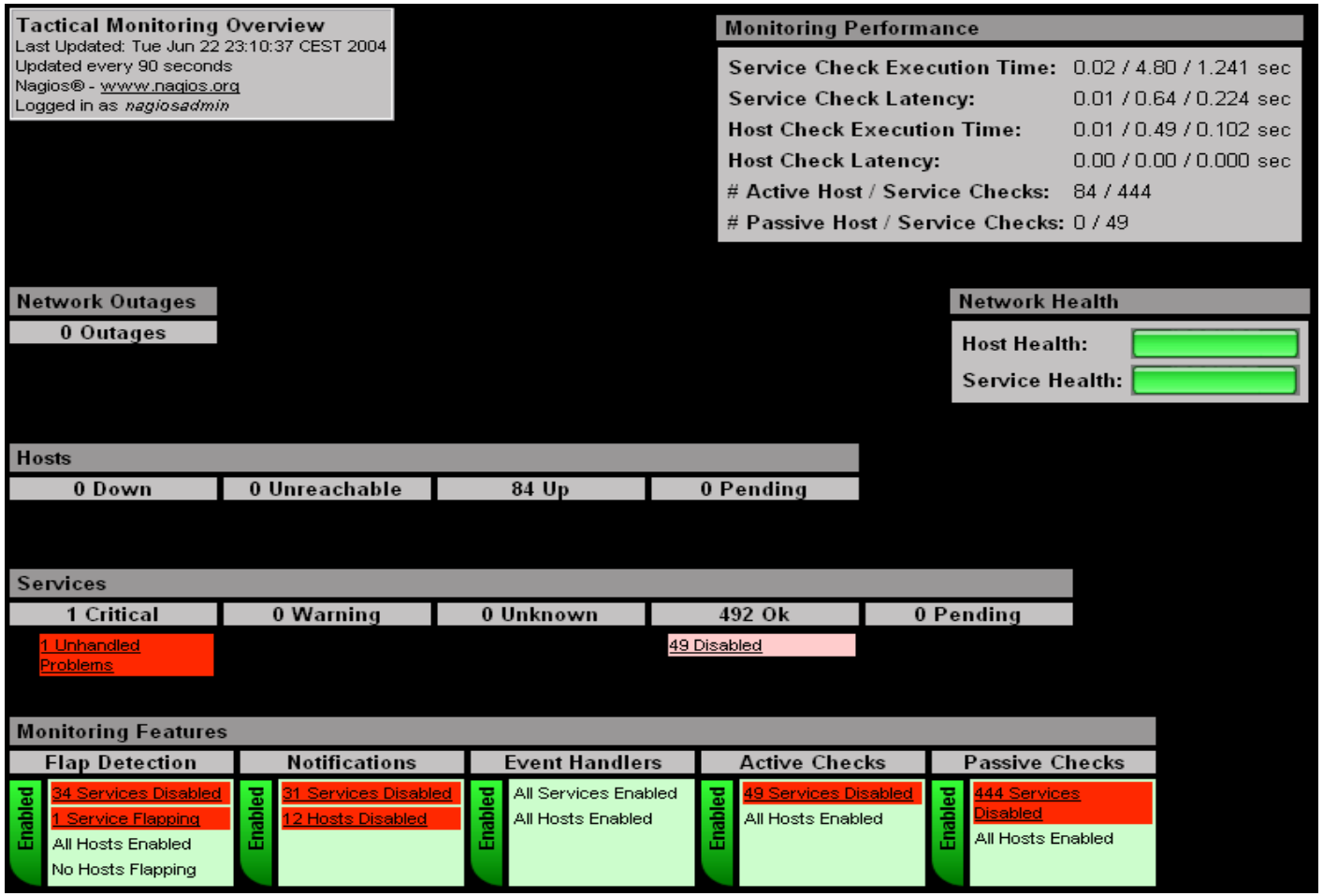
Weiteres

- Suchmaschine: www.nagiosexchange.org
- Eigene Scripte und Plugins (Shellscripts, Perl, VBScript, Java, Python, .NET, usw.)

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

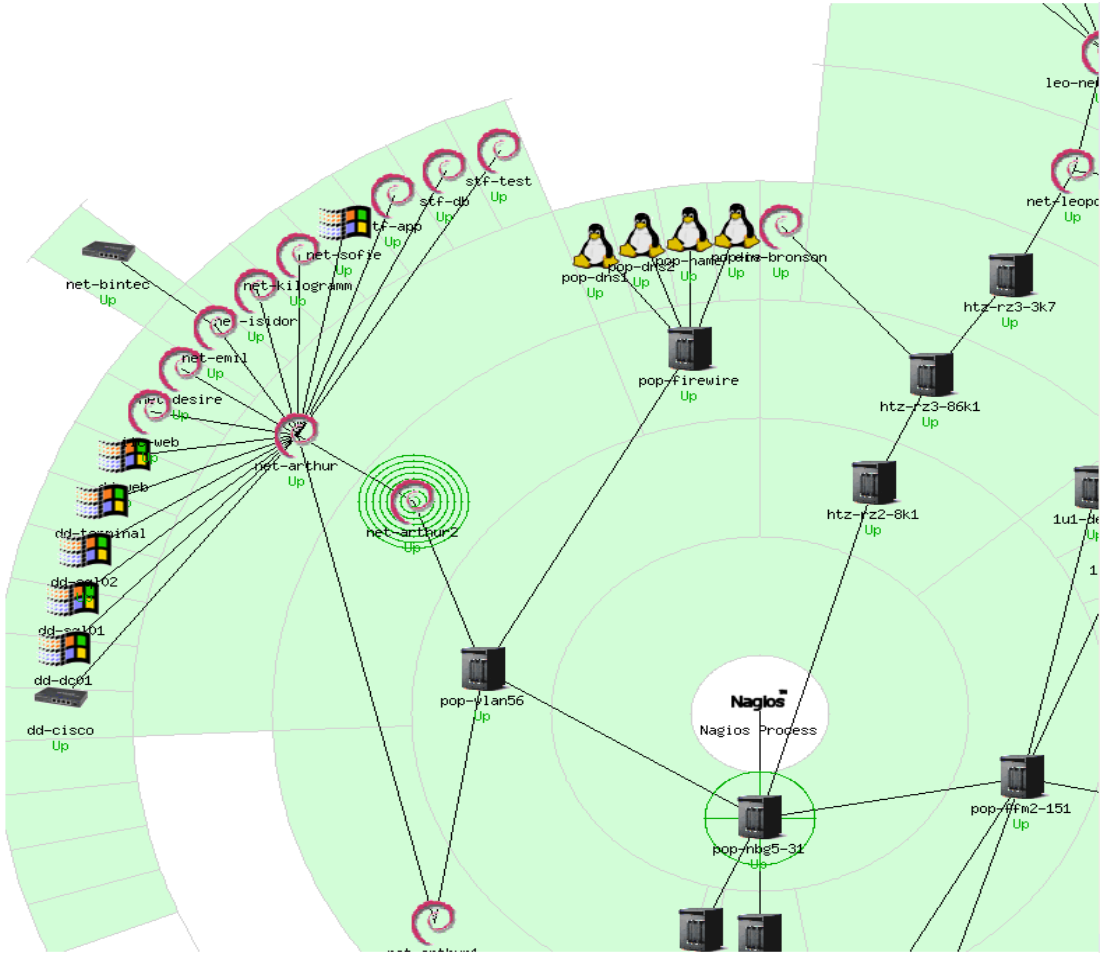
All Problems	All Types
0	17

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

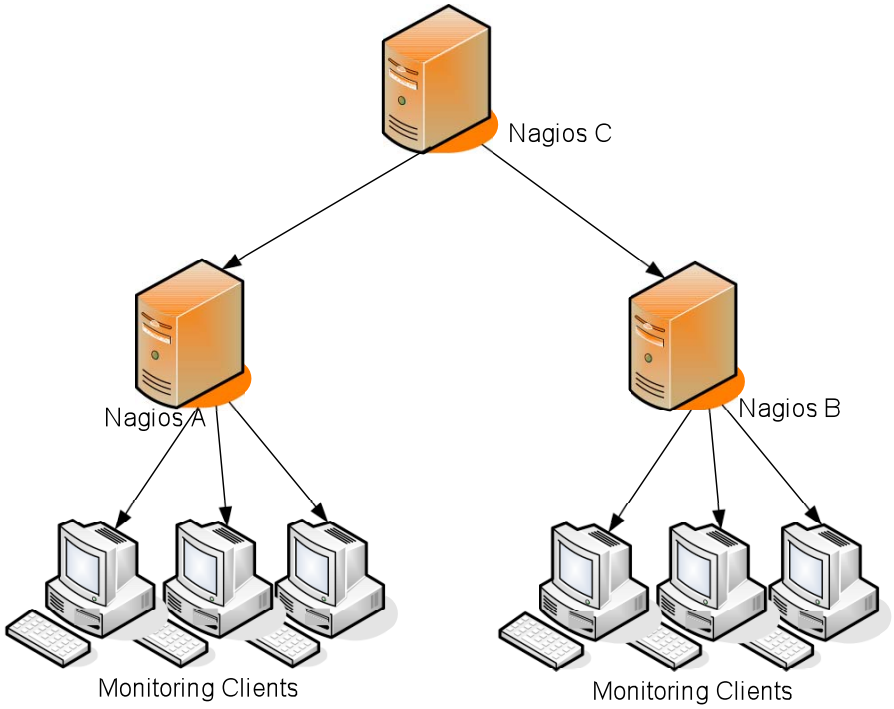
State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	17d 13h 32m 6s	99.996%	100.000%
	Scheduled	0d 0h 59m 30s	0.235%	0.235%
	Total	**17d 14h 31m 36s**	**99.996%**	**100.000%**
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**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 durch Asterisk Integration
- Eskalation der Benachrichtigung
- Umfangreiche Benachrichtigungseinstellungen
  - Personen & Gruppen
  - Zeitfenster & Intervalle
- Schnittstelle zu anderen Anwendungen
- Keine Benachrichtigungen bei Folgefehlern

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

Was spricht noch für Nagios?

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

Zusatzfunktionen für Nagios

NAGIOS ADDONS

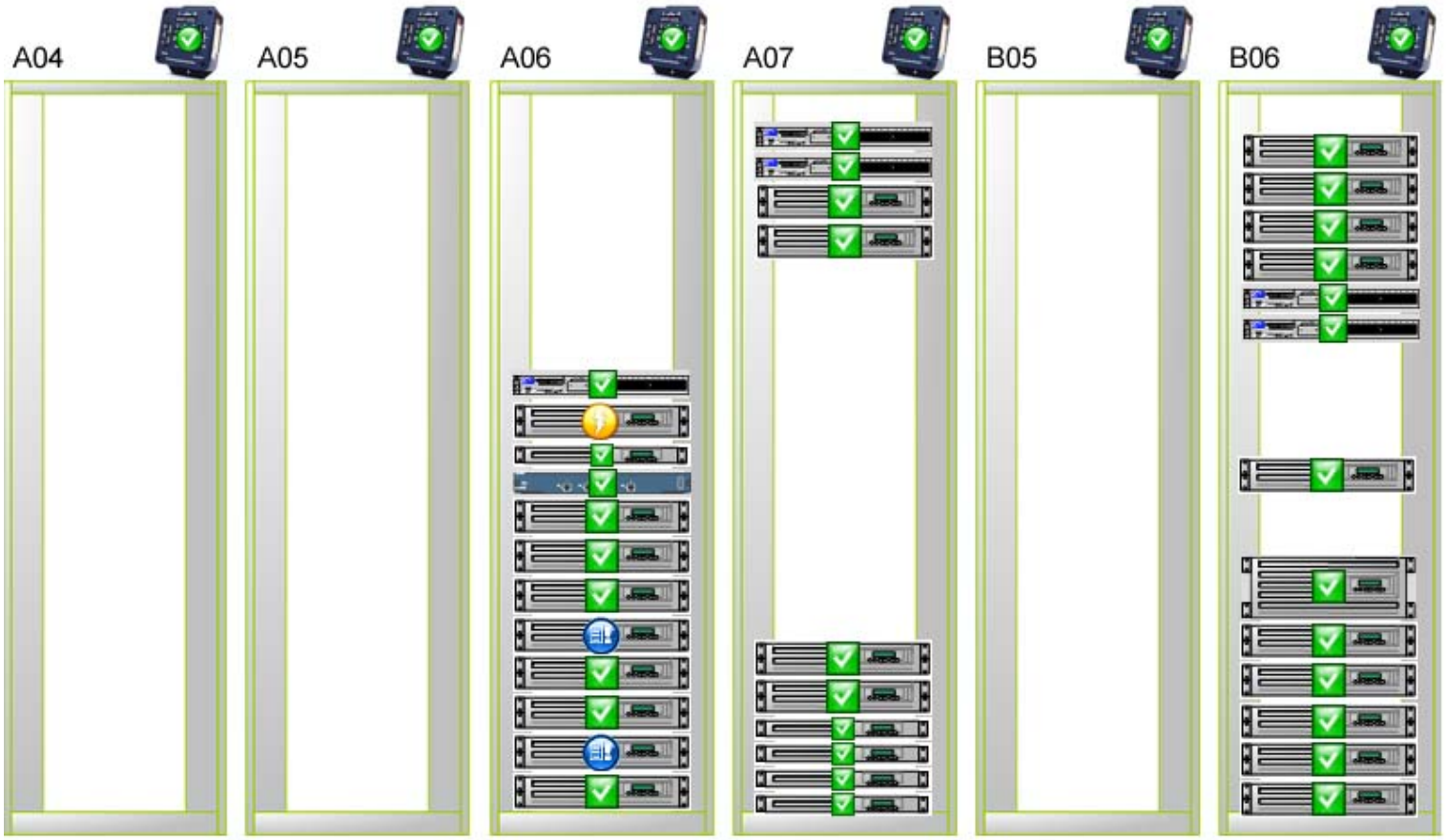
NDO (Nagios Data Out)

- Datenbank Schnittstelle für Nagios
- Basis vieler anderer AddOns
- Unterstützt mehrere Nagios Instanzen
- Schreibt alle internen Nagios Bewegungsdaten und Konfigs in die DB
- DB Unterstützung für
  - Nativ MySQL
  - Portierung auf Oracle
  - PostgeSQL geplant

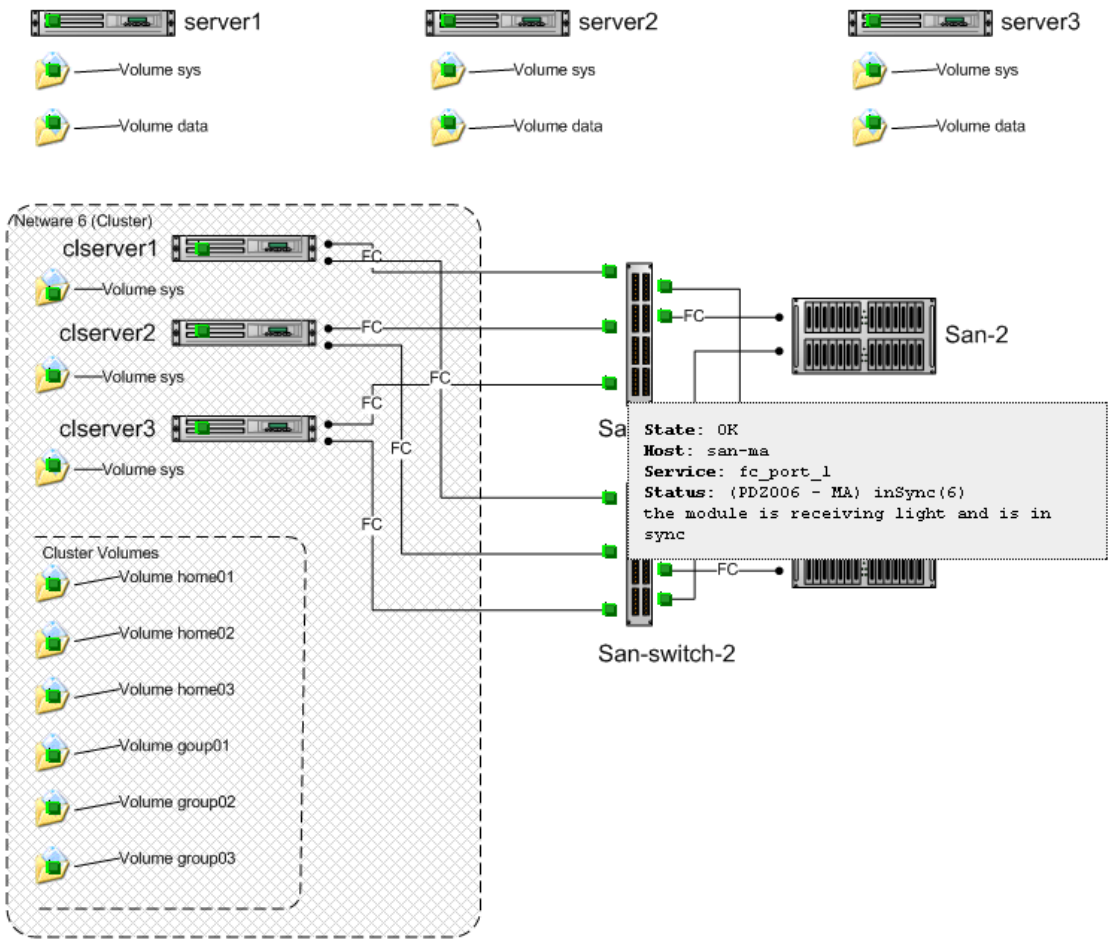
NagVis

- Visualisierung beliebiger Sachverhalte durch eigene Grafiken
- Anzeige von einzelnen Hosts oder Services
- Anzeige von Gruppen und hierarchischen Maps
- Direkte Verbindung mit Nagios Webinterface
- Konfiguration per Drag‘n‘Drop im Webinterface
- Automatische Generierung von Standardmaps

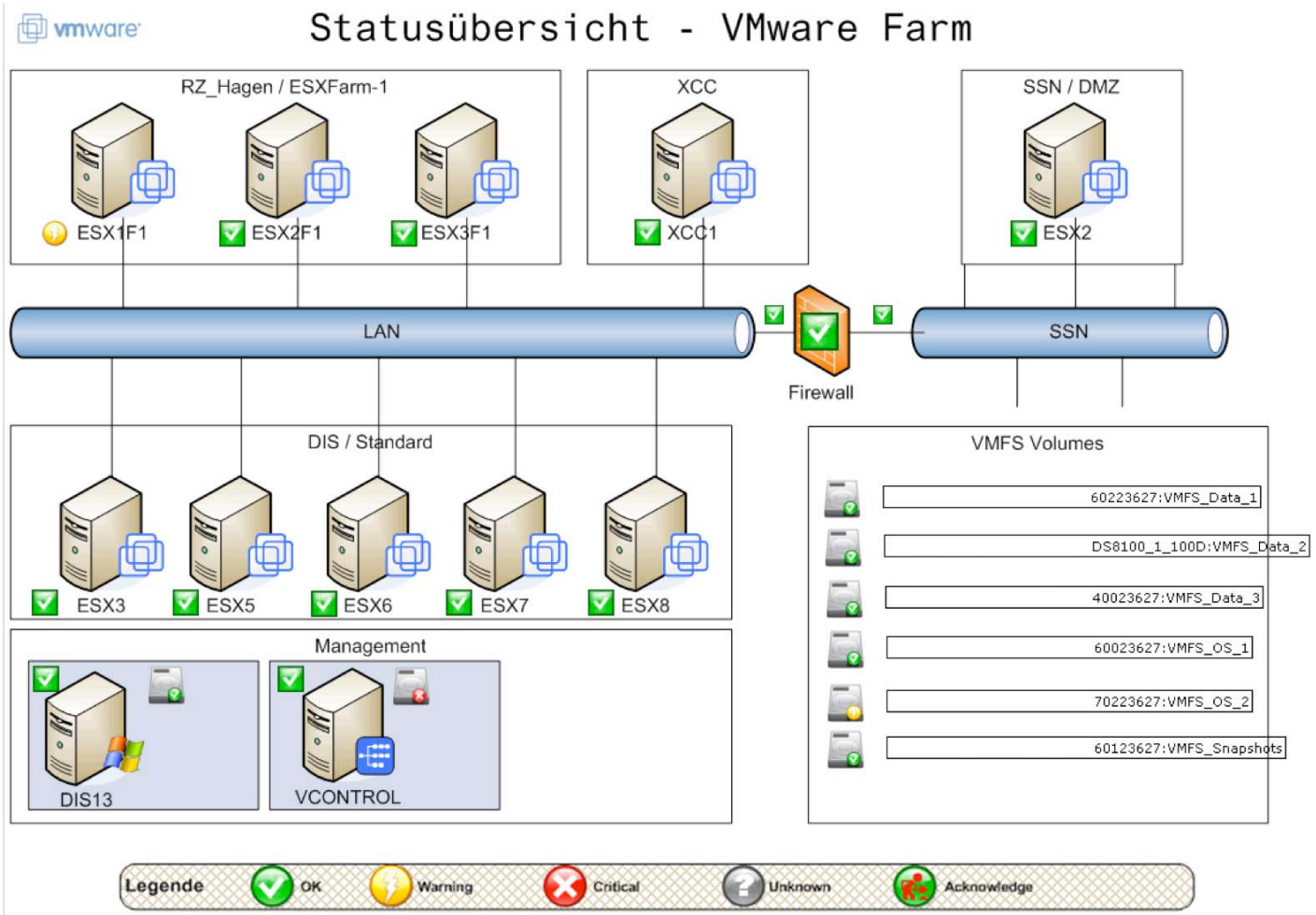
NagVis Rack Ansicht



NagVis SAN Ansicht

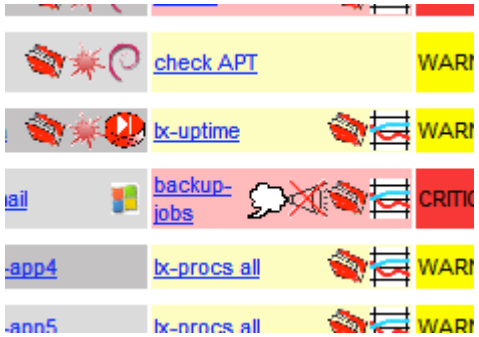


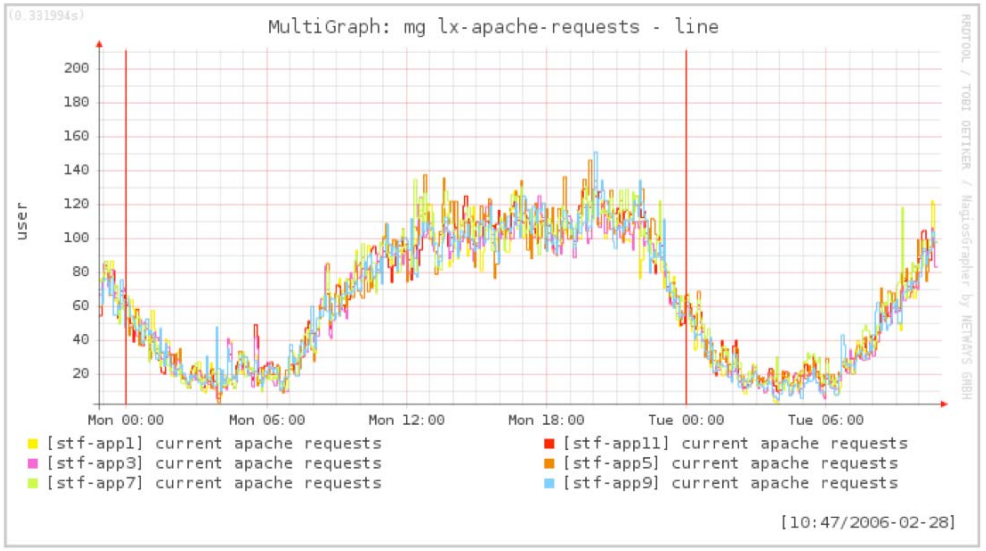
NagVis Netzwerkstruktur



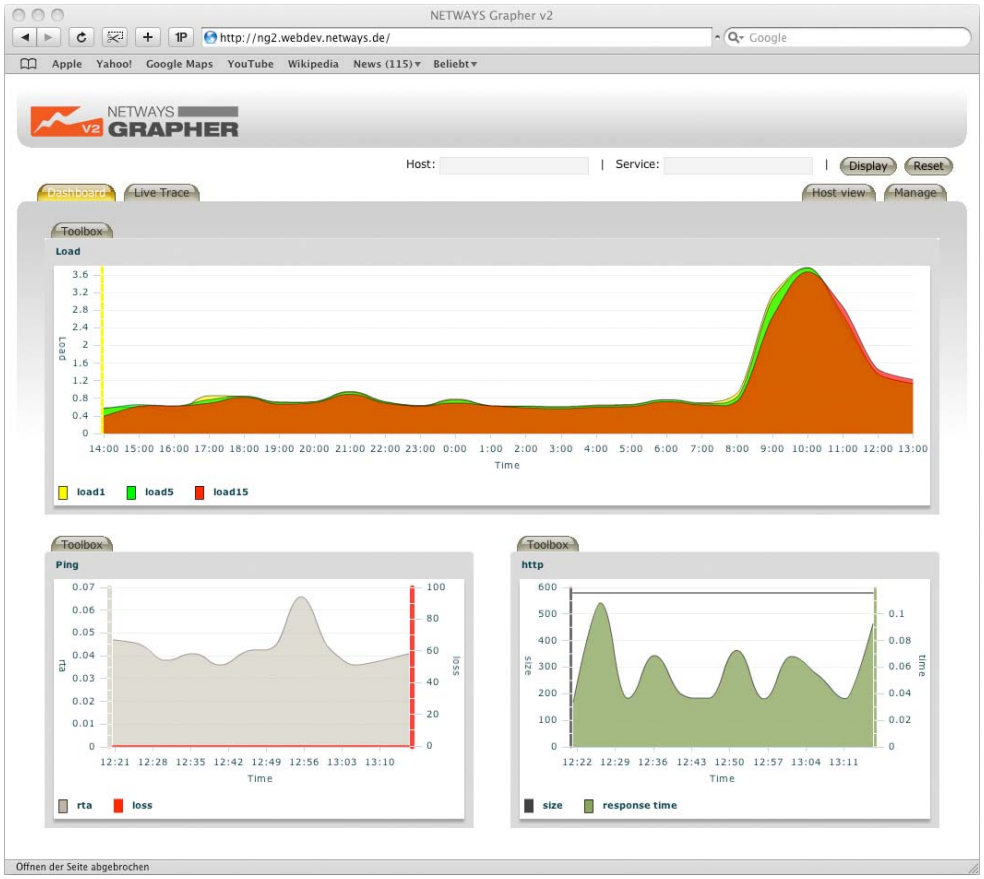
Charts: NagiosGrapher & PNP

- Anzeige quantitativer Messwerte
- Hoher Automatisierungsgrad
- Einfaches Handling im Webfrontend
- RRD Backend für Datenspeicherung
- Erstellung der Graphen in Echtzeit
- Umfangreiche Features
  - Berechnungen
  - Multigraphen
  - Datenkonsolidierung
  - Housekeeping





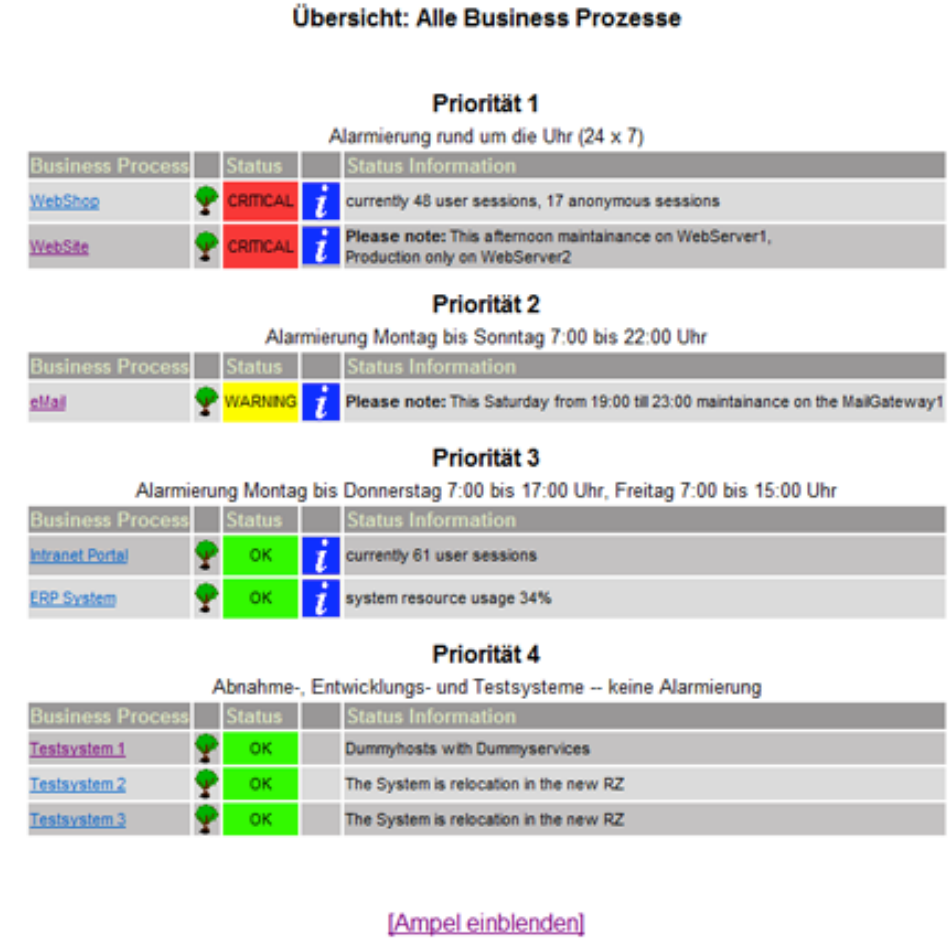
NETWAYS Grapher V2



- Flashbasierte Graphen in realtime
- Beliebige Datenquellen
- Eine zentrale Datenbank
- Browserkonfigurierbare Dashboards und Multigraphen
- Komplett anpassbares Datenmanagement
- Ajax Webinterface

Business Process View

- Zusammenfassung verschiedener Hosts oder Services
- Baumstruktur zur Abbildung von Geschaftsprozessen
- And/or Verknüpfungen
- Drilldown bis zum Service
- Testszenario durch Business Impact



Übersicht: Alle Business Prozesse

Priorität 1

Alarmierung rund um die Uhr (24 x 7)

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

Priorität 2

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

Business Process	Status	Status Information
eMail	WARNING	**Please note:** This Saturday from 19:00 till 23:00 maintainance 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
Intranet Portal	OK	currently 61 user sessions
ERP System	OK	system resource usage 34%

Priorität 4

Abnahme-, Entwicklungs- und Testsysteme -- keine Alarmierung

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

[Ampel einblenden]

Business Process View Ebenen

Status: Details für WebShop

	Host	Service	Status	Status Information
and*	Internet Connection		OK	
	Loadbalancer Cluster		OK	
	DNS Cluster		OK	
	WebShop Frontend Servers		CRITICAL	
	ERP System		OK	

* Die Anwendung ist für den Kunden ve

Status: Details für WebShop Frontend Servers

	Host	Service	Status	Status Information
or*	WebShop Frontend Servers Line1		CRITICAL	
	WebShop Frontend Servers Line2		CRITICAL	

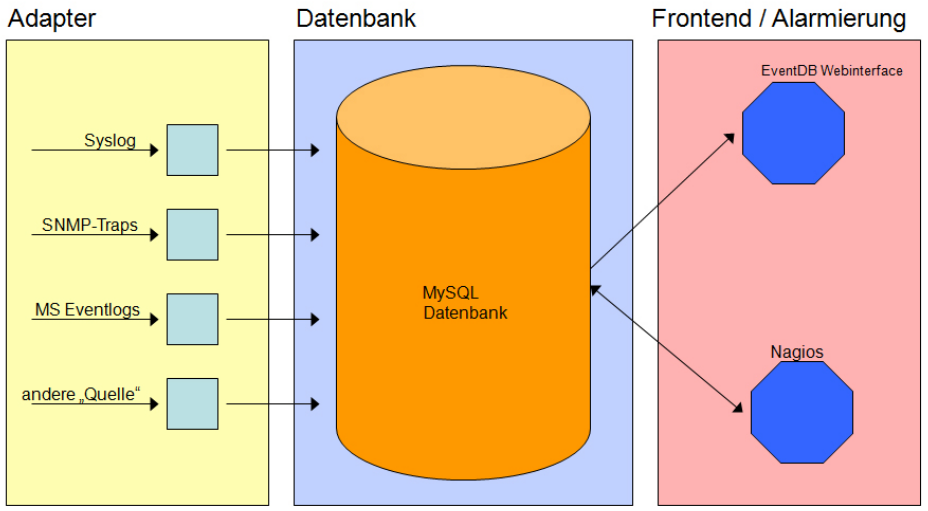
Status: Details für WebShop Frontend Servers Line2

	Host	Service	Status	Status Information
and*	nbp_webserver2	HTTPS	CRITICAL	HTTPS: CRITICAL, HTTPS/1.0 200 - 3000 bytes in 3000 seconds
	nbp_webserver2	HTTPD Slots	CRITICAL	HTTP: CRITICAL, HTTP OK HTTP/1.0 200 OK - 2000 bytes in 477.981 seconds
	nbp_appserver2	HTTP	OK	HTTP: OK, HTTP OK HTTP/1.0 200 OK - 0 bytes in 0 seconds

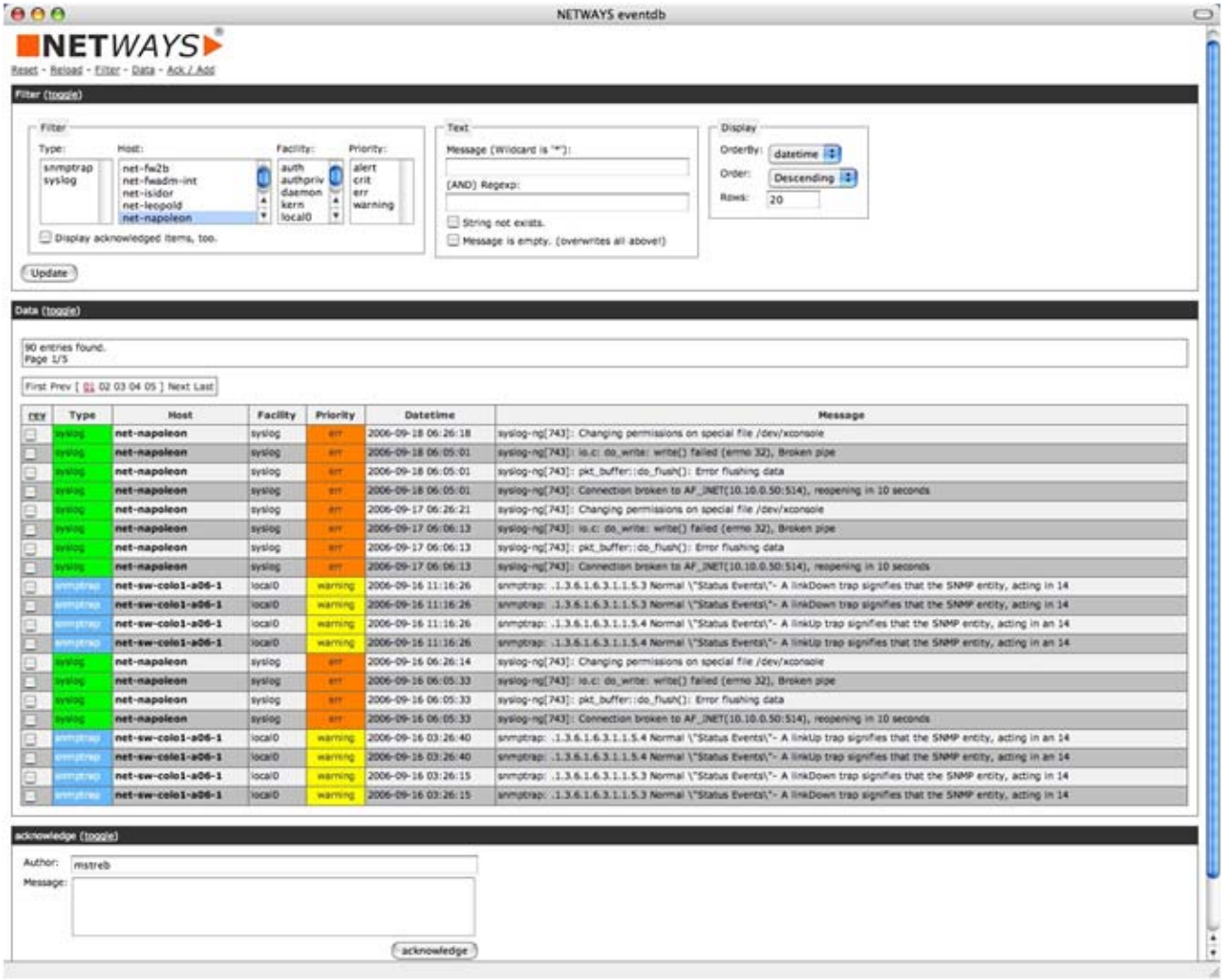
* Die Anwendung ist für den Kunden verfügbar, wenn keine der Komponenten im Status CRITICAL ist.

EventDB

- Zentrale Schnittstelle für ereignisbezogene Meldungen
  - Logfiles von Servern und Anwendungen
  - E-Mail Benachrichtigungen
  - SNMP Traps
- Verbesserte Analyse
- Einfache Integration in Nagios
  - Typ des Events
  - Anzahl Meldungen
  - Zeitraum
  - Freitextsuche
  - Wiederherstellungsmeldung

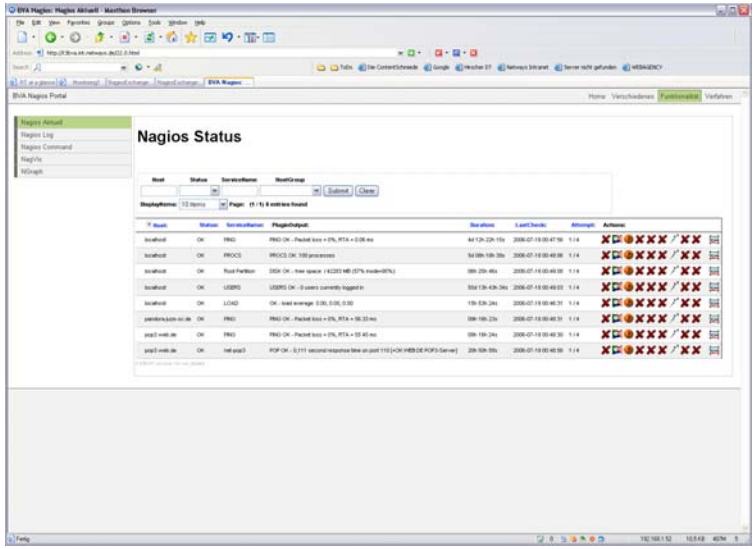


EventDB Webfrontend



NETWAYS Portal für Nagios

- Alternatives Webinterface für Nagios mit erweiterten Funktionen
  - Design komplett durch Templates steuerbar
  - Benutzerverwaltung mit Anbindung an LDAP, ADS oder NDS
  - Freie Konfiguration aller Ansichten
  - Datenanzeige als Listen, Grafiken, Tachometer, Eventkonsole
- Datenquellen
  - Nagios & AddOns
  - Tickets
  - Wiki-Inhalte
  - SQL Datenbanken
  - Anwendungen durch Proxy



Integration mit anderen Systemen (Beispiele)

NAGIOS INTEGRATION

Wiki

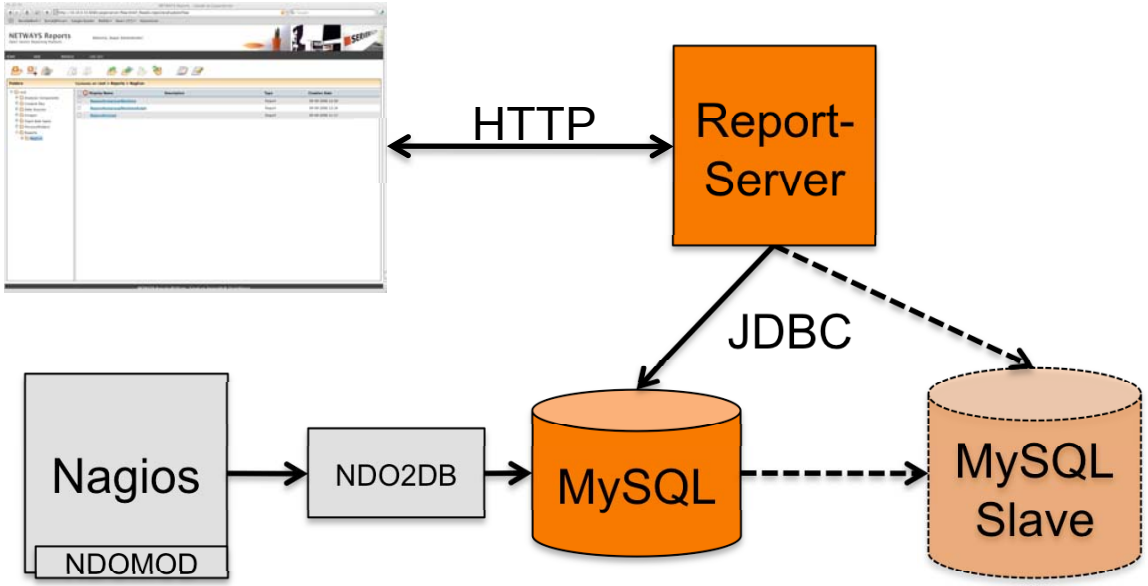
- Ablage von Dokumentation
- Einfache Integration in Nagios Frontend
- Schnell und unkompliziert durch Webzugriff
- Einfache Dokumentationssyntax
- Verfolgung von Änderungen und Diffs
- Ablage von Binärdateien

Extra Service Notes

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
- Ticketsysteme
  - Open Source: Request Tracker & OTRS
  - Kommerziell: OmniTracker, HP ServiceDesk,
  - Weitere einfach implementierbar über CLI des Ticketsystems

Advanced Reporting

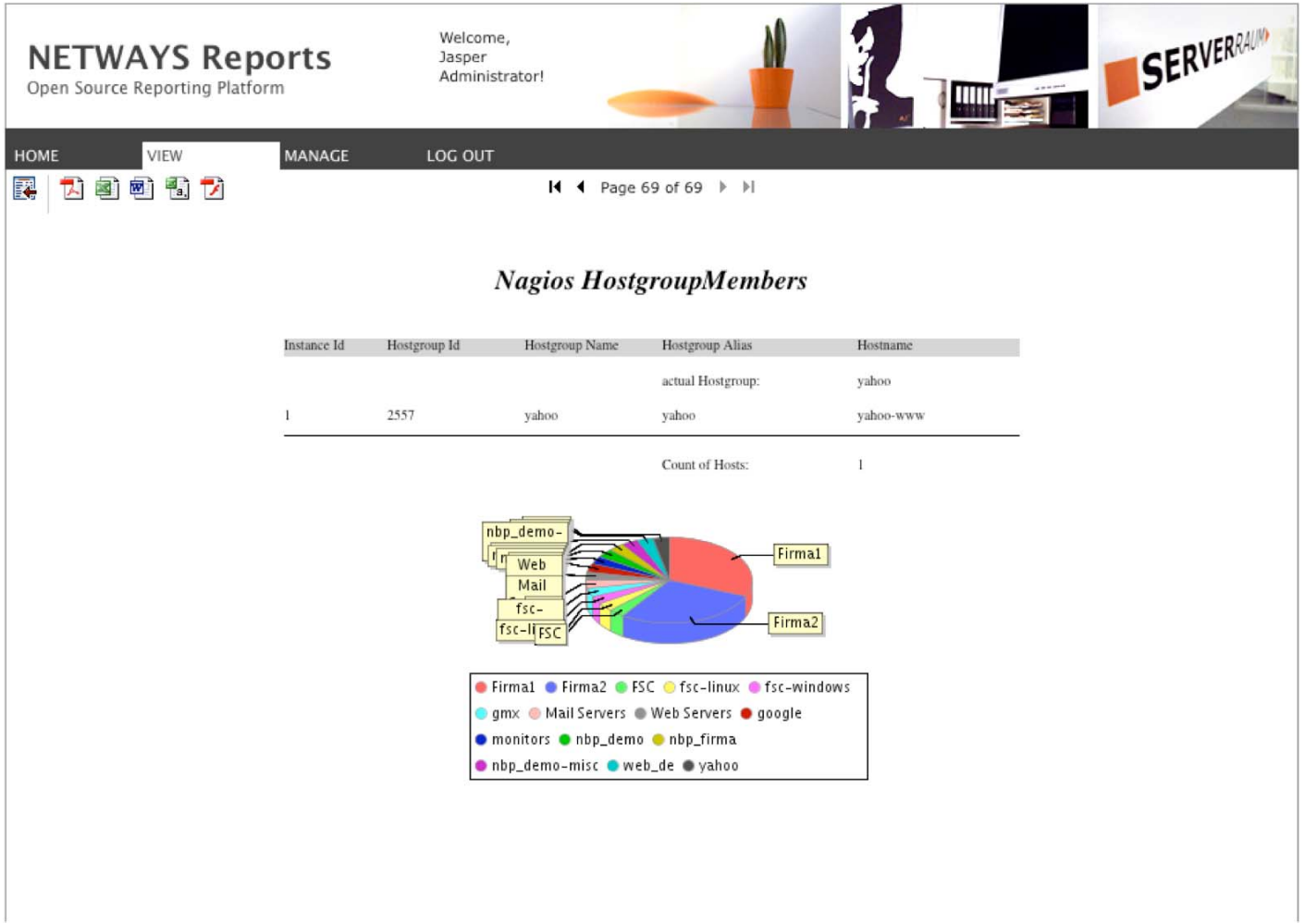


- Bereitstellung der Daten durch NDO AddOn
- Speicherung der Daten in einer dedizierten Reporting DB
- Generierung von Reports durch externen Reporting Server
  - Kommerzielle Versionen: Crystal Reports, Business Objects, usw.
  - Open Source: Pentaho, Jasper, BIRT

Features Jasper Reporting

- Report Erstellung
  - Erstellung der Reports im Jasper Client
  - Realtime Development mit Voransicht
  - WYSIWYG Layout
  - Unterstützung gängiger Eingangsformate
  - Diagrammtypen: Balken, Linien, Pie
  - Gruppierung, Parametrisierung, Subreports
- Verteilung via Webserver oder eMail
  - Ausgabeformate: PDF, HTML, Excel, Word, Flash
  - Automatische Generierung und Versand
- Integration durch Java API und Webservice

Screenshot


NETWAYS Reports
Open Source Reporting Platform
Welcome,
Jasper
Administrator!
HOME
VIEW
MANAGE
LOG OUT
Page 69 of 69
Nagios HostgroupMembers
Instance Id
Hostgroup Id
Hostgroup Name
Hostgroup Alias
Hostname
actual Hostgroup:
yahoo
1
2557
yahoo
yahoo
yahoo-www
Count of Hosts:
1
nbp_demo-
Web
Mail
fsc-
FSC
Firma1
Firma2
Firma1 Firma2 FSC fsc-linux fsc-windows
gmx Mail Servers Web Servers google
monitors nbp_demo nbp_firma
nbp_demo-misc web_de yahoo

Fazit

- Nagios bietet sehr viel out-of-the-box
- Gute Erweiterbarkeit durch AddOns
- Framework für alle möglichen Überwachungsanforderungen
- Nagios ist stabil, getestet und weit verbreitet
- Sehr viel Erfahrung und Support im Markt vorhanden

Nagios ist eine ausgereifte Monitoring Lösung für Netzwerke aller Größenordnungen

Fragen & Antworten

NETWAYS GmbH
Deutschherrnstrasse 15-19
90429 Nürnberg

Tel.: +49 911 92885-0
Fax: +49 911 92885-77

info@netways.de

http://www.netways.de
http://blog.netways.de