

OpenSource Monitoring

...oder wie es sich günstig leichter
Leben lässt

ABOUT

		
Name	Christian Mies	
Alter	28 Jahre	
Beruf	Consultant / Projektleiter	
Kontakt	Christian.Mies@it-novum.com	
Hobbies	Triathlon	

AGENDA

- Was bedeutet Monitoring?
- Warum Open Source?
- Tools im Überblick
- Nagios als „De Fakto“ Standard
- Veredelung von Nagios
- Projekthürden bei Monitoringprojekten
- FAQ



OK, LOS GEHT'S...

WAS BEDEUTET MONITORING?

- **Verschiedene Ansichten des Monitoring**
 - Technische Sicht (Administratoren / Betrieb)
 - Organisatorische Sicht (Management / Planung)
 - Rechtliche Sicht (Datenschutz / ISO27000)

...TECHNISCH...

- Leichte Administration
- Flexibilität in Überwachungsmöglichkeiten
- Alarmierung
- Stabiler und skalierbarer Betrieb
- Minimieren der Routinearbeiten an Systemen

LEICHTE ADMINISTRATION

- Konzentration auf das Wesentliche
 - wenig Input → viel Output
- Gute Dokumentationen
 - Software und Addon sollten gut dokumentiert und leicht verständlich sein.
- Mit bewährtem Überwachung einrichten können
 - Jeder wie er / sie es am besten kann.

FLEXIBLE ÜBERWACHUNG

- Bordmittel nutzen
- Agentenbasiert und Agentenlos
- Standards integrieren
- Schnittstellen selbst definieren können.

ALARMIERUNG

- Visuelle Alarmierung
- Alarmierung via Audio
- Flexible Benachrichtigungswege, z.B.
 - E-Mail
 - Telefon
 - SMS
 - *Twitter, Jabber, etc... (?)*

STABILER BETRIEB

- Schnelle und einfache Installation
- Leichtes „Disaster Recovery“
- Modularer Betrieb
- Keine „lästigen“ Anrufe
 - „...Das System ist so langsam...“
- Wissen was wovon abhängt
- Weniger Systemausfälle

ROUTINE REDUZIEREN

- Kein tägliches Logfile lesen mehr...
- Nicht 30 Server jeden Morgen anpingen und mittags nicht wissen ob diese noch laufen...
- Kein manuelles Ausfüllen von Wartungsprotokollen ...

...ORGANISATORISCH...

- Planungssicherheit
- Kennzahlen
- Eskalationsmechanismen
- Reporting / Trends
- Integrationsmöglichkeiten
- IT - Servicemanagement
- Eye candy...

PLANUNGSSICHERHEIT

- Kapazitätsplanung
- Investitionssicherheit durch Kosteneinsparung
- Möglichkeit der Investitionsplanung

KENNZAHLEN

- Störungs-Anfälligkeit von Systemen
- Häufigkeit der Eskalation
- Kontrolle von Benachrichtigungen
- Auslastungen

REPORTING / TRENDS

- Historische Betrachtung von
 - Alarmierungen
 - Kapazitäten
- Trendanalyse für zukünftige Planungen
- Servicelevel Vereinbarungen überwachen / aufzeichnen

INTEGRATIONSMÖGLICHKEITEN

- Möglichst alle geschäftskritischen IT Bereiche sollen überwachbar sein
- Anbindung an Portale oder Reporting Tools
- Dritt – Tools (Assetcenter, Ticketsysteme, etc) sollten integrierbar sein

IT - SERVICEMANAGEMENT

- Service Level abbilden und überwachen können
- Geschäftsprozesse darstellen können

EYE CANDY

- Grafische Aufbereitung
 - Dashboards
- Leitstand Design
 - Leicht verständliche Ausgaben



...RECHTLICH...

- Historische Datenaufzeichnung
- Verfügbarkeitsmessungen
 - Beispiel: Verletzung von Verträgen
- Datenschutz

...MENSCHLICH...

- Mehr Zeit für z.B. Familie, Sport, etc. 😊





1. HÜRDE GENOMMEN...

WARUM OPEN SOURCE SOFTWARE (OSS)

- Technisch
- Management
- Rechtlich

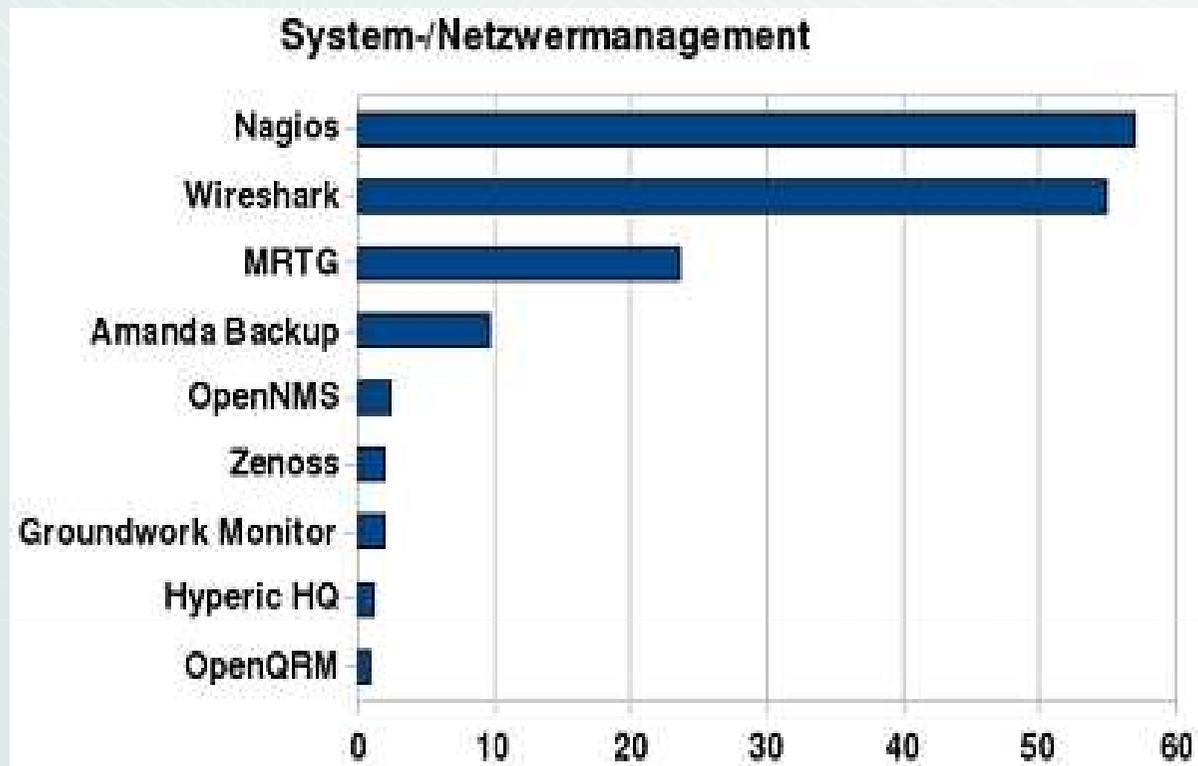


...TECHNISCH...

- Quellcode frei verfügbar
- z.T. Betriebssystem-unabhängig
- Vielfältige Literatur / Dokumentation
- Häufig direkte Kontakte zu Entwicklern möglich

...MANAGEMENT...

- Whitepaper für Open Source Monitoring
 - Google Hits “Whitepaper Open Source”: 31 Mio.
 - Google Hits “Whitepaper Open Source Monitoring”: 1,1 Mio.
- Pressestimmen / Bewertungen
 - Gartner (Linux Magazin 11/2009)
 - Computerzeitung → 
 - Handelsblatt → 
 - Computerwoche → 
 - Heise, C't, IX...
- Vor – und Nachteile



STUDIEN OPEN SOURCE MONITORING TOOLS

Quelle : <http://www.heise.de/open/artikel/Trendstudie-Open-Source-221696.html>

...RECHTLICH...

- IT-Grundschutz

- https://www.bsi.bund.de/cln_134/ContentBSI/grundschutz/kataloge/baust/b04/b04002.html

- ISO 27001

- CobIT

- IT Risk Management

VOR- UND NACHTEILE OSS

Vorteile

- Offene Standards
- Große Community
- Lizenzkostenfrei
- Herstellerunabhängig
- Flexibilität
- Erhöhte Sicherheit

Nachteile

- Professioneller Support ist häufig kostenpflichtig
- Wissenstransfer komplexer
- Ggf. lange Fehlerzyklen
- Teils schlecht Dokumentiert



WEITER GEHT'S..

ÜBERSICHT DER TOOLS (AUSWAHL)

- Zenoss
- Cacti
- MRTG
- OpenNMS
- Nagios



ZENOSS

- Discovery / Assetmanagement
- Monitoring Software auf Linux Basis
- Clientless Monitoring
- Dashboard
- Kommerzielle + Community Variante verfügbar

VOR- & NACHTEILE

Nachteil

- Geringe Flexibilität für Überwachung
- Java Server notwendig
 - → Ressourcenintensiv
- Geringe Integration in 3. Tools

Vorteile

- Eye Candy
- Datenbankintegration

CACTI ODER MRTG

- Graphische Aufzeichnung von Daten
- Clientless Monitoring



VOR- & NACHTEILE

Nachteil

- Geringe Flexibilität für Überwachung
- Keine Benachrichtigung

Vorteile

- Eye Candy
- Historische Daten zum Vergleich
- Betriebssystem – Unabhängig
- Leichte Administration

OPENNMS

- Monitoringsoftware auf Linuxbasis
- Auto Discovery
- Clientless Monitoring
- Grafische Aufzeichnungen
- Verteiltes Monitoring
- Nur Communityversion

VOR- & NACHTEILE

Nachteil

- Geringe Flexibilität für Überwachung
- Java Server notwendig
 - → Ressourcenintensiv
- Geringe Integration in 3. Tools
- Komplex in der Administration

Vorteile

- Datenbankintegration
- Offene Schnittstellen

NAGIOS

- Monitoringsoftware auf Linuxbasis
- Clientless und Clientbased Monitoring
- Verteiltes Monitoring
- Komplexe Eskalations- + Benachrichtigungsmöglichkeiten

- Am Markt seit 1999 (Netsaint) / Nagios 2002
- Community Version und Enterprise Business

VOR- & NACHTEILE

Vorteile

- Offene Schnittstellen
- Eskalationsmanagement
- Performant
- Viele Addons
 - Historische Daten
 - Visualisierung
 - Business Impact
 - Discovery...
- Flexibilität

Nachteil

- „Langweilige“ Oberfläche in der Basis
- Komplex in der Administration



...WEITER...

NAGIOS ALS DE FAKTO STANDARD

- Flexibilität
- Tools
- Anwendungsbeispiele
 - Hardware / Infrastruktur
 - Betriebssysteme
 - Applikationen
 - Datenbanken

FLEXIBILITÄT...

- in der Administration
 - Web GUI, LDAP, Datenbank, Konsole...
- im Einsatz
 - Zentrale / dezentrale Überwachung
 - Anbindung an 3. Tools
 - Integration von 3. Tools
 - Benachrichtigung / Eskalation
- in der Planung
 - Nagios passt sich er Umgebung an nicht andersrum

TOOLS ...

• zur Integration in Nagios

- Grafische Aufzeichnung (PNP4Nagios, Ngraph, etc)
- Datenbank (Nagios NDO)
- Visualisierung (NagVis)
- Business Impact Analyse
 - Nagios BP
- Trapmonitoring
 - NagTrap
- Wiki (DokuWiki, T-Wiki, etc.)
- Assetcenter (iDoIT, RackIT, etc)

• in die Nagios integriert

- Ticketsysteme (OTRS, RT, etc.)
- Reporting Tools
- Kommerzielle Monitoring Tools
- Assetcenter (CMDBs)
- SAP
- Kennzahlensysteme

HARDWARE

- Server (HP, Dell, IBM, Fujitsu, etc.)
 - Statusüberwachung aktiv und passiv
 - ...
- WLAN /Switches / Router (HP, Cisco, Juniper, etc.)
 - u.a. Statusüberwachung
 - Service Level Überwachung (z.B. Verfügbarkeiten)
 - ...
- Drucker
- etc....

BETRIEBSSYSTEME

- Windows
 - Agentenlos und Agentenbasiert
 - Sehr komplexe Überwachung möglich
- Linux
 - Agentenlos und Agentenbasiert
 - Sehr komplexe Überwachung möglich
- Netware
 - Agentenlos und Agentenbasiert
 - Eingeschränkt aufgrund End of Life 2015
- Mac
 - Agentlos und Agentenbasiert
 - komplex

APPLIKATIONEN

- SAP
 - CCMS, RFC, etc.
- Java Application Server
- Webserver
- etc.



DATENBANKEN

- MSSQL
 - Agentenlos und Agentenbasiert
 - Komplex inkl. eigene Statements
- Oracle
 - Agentenlos und Agentenbasiert
 - Komplex inkl. eigene Statements
- MySQL
 - Agentenlos und Agentenbasiert
 - Komplex inkl. eigene Statements
- PostgreSQL
- DB2
- ...



LETZTE DISZIPLIN



VEREDLUNGEN VON NAGIOS

- Open ITCOCKPIT
- Groundwork
- Icinga
- uva...



OPEN ITCOCKPIT

- Veredlung von Nagios seit 2006
 - Wissen seit „netsaint“
- Datenbankbindung
- PHP Oberfläche
 - Bidirektionale Konfiguration (Konsole und GUI)
- Basis beinhaltet bereits viele 3. Tools
- Umfassendes SLA-Monitoring, BPM, Eventkorrelation, integriertes Assetcenter als Modul verfügbar, E2E, Trendanalyse, etc.
- IT-Novum als Lösungs- und Supportanbieter mit eigenem Entwicklerteam
- www.itcockpit.de

ICINGA

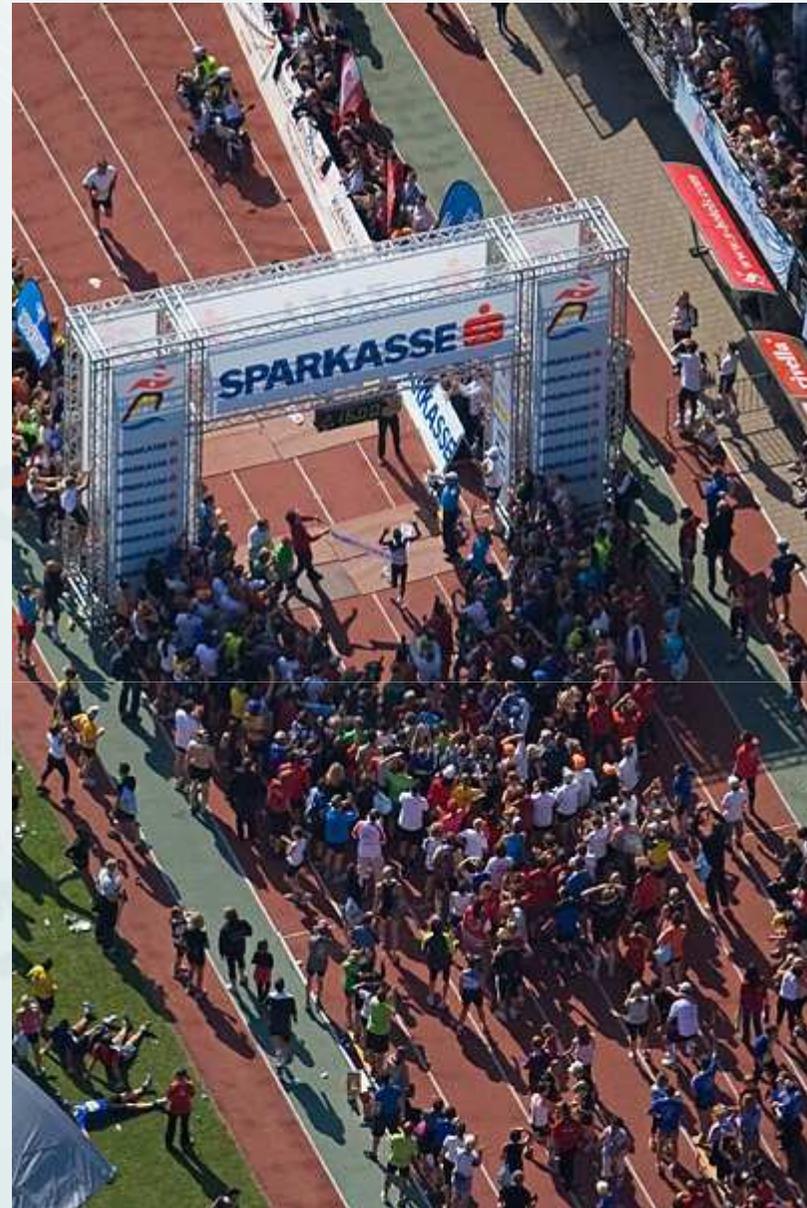
- Nagios Fork im Sommer 2009
 - PHP Oberfläche
 - Datenbankbindung
 - Konfigurationsoberfläche
- Community gestützt
- URL: www.icinga.org

GROUNDWORKS

- Oberflächenveredlung seit 2005
- PHP Oberfläche
- Datenbankbindung
- Eigene Module bereits integriert
- URL:

<http://www.groundworkopensource.com/community/>

2 DINGE NOCH...



PLANUNG VON OS MONITORING EINSÄTZEN

- Ziele
 - **KLARE** und **MESSBARE** Anforderungen festlegen
 - Qualitätskriterien für Lösung festlegen
- Personal
 - Alle betroffenen Bereiche und Mitarbeiter in die Planung einbeziehen
 - Mitarbeiter sensibilisieren
 - Beratung von Beginn an einplanen
- Dokumentation
 - Dokumentationsumfang festlegen
- Umsetzung
 - Evaluierung mit einplanen



FRAGEN?



VIELEN DANK!