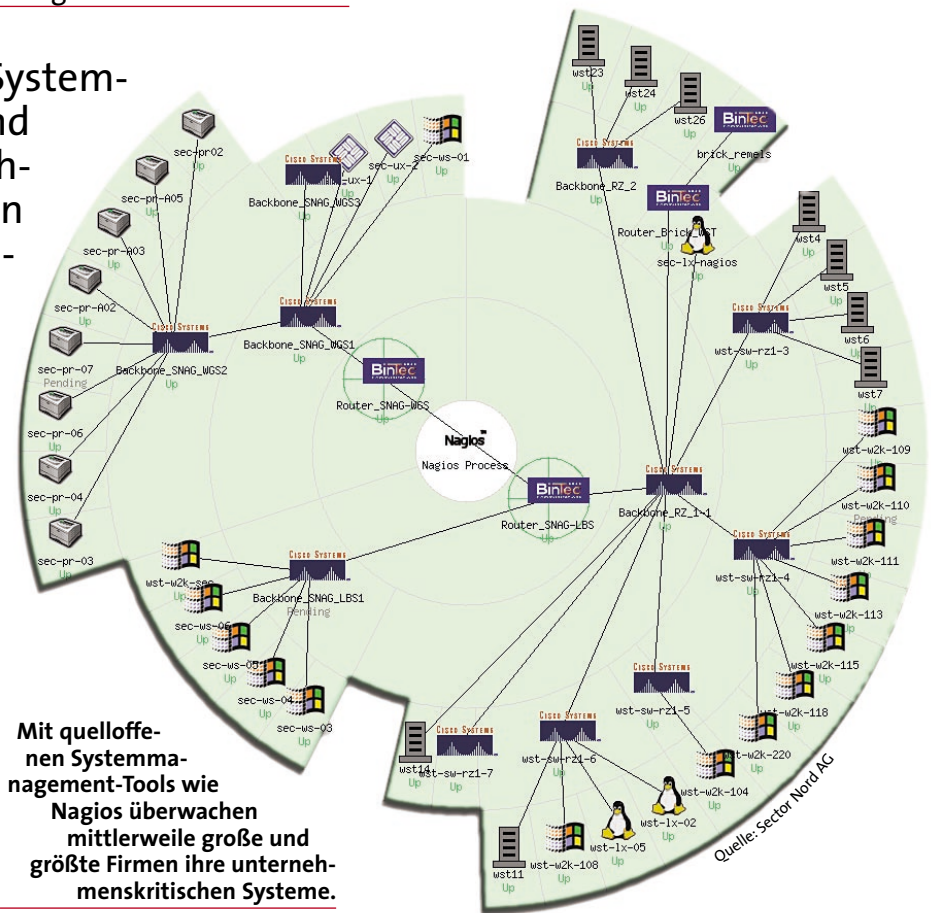


# SYSTEMMANAGEMENT MIT OPEN-SOURCE-TOOLS

VON JÜRGEN HÖFLING | [juergen.hoefling@informationweek.de](mailto:juergen.hoefling@informationweek.de)

Quelloffene Netzwerk- und Systemmanagement-Werkzeuge sind dem Bastlerstadium entwachsen. Mittlerweile überwachen in Deutschland Flugzeugbauer, Kältetechniker und Banken ihre unternehmenskritischen Systeme mit Open-Source-Tools.

**F**ehler in den Informations- und Kommunikations-Systemen können ganz unterschiedliche geschäftliche Relevanz haben. Der Ausfall eines Controllers innerhalb eines vernetzten Druckerpools mag ein Unternehmen, bei dem alles online abgewickelt wird und das Drucken nur ein gelegentliches Zusatzinstrument ist, »mit links« abtun, einem Output-Management-Dienstleister hingegen



Mit quelloffenen Systemmanagement-Tools wie Nagios überwachen mittlerweile große und größte Firmen ihre unternehmenskritischen Systeme.



»Die Nagios-Installation machte sich praktisch unmittelbar bezahlt«

DR. JÜRGEN OVERFELD, CIO Linde Kältetechnik

würde dadurch die gesamte Geschäftsgrundlage entzogen.

Angesichts einer immer komplexer werden ITK-Infrastruktur ist freilich nicht nur die geschäftspolitische Bewertung von Havarien ein Problem, sondern schon das permanente Überwachen sämtlicher potenzieller Fehlerquellen. »Bei uns werden alle fünf Minuten

Hunderte von möglichen Fehlerquellen abgefragt«, sagt Dr. Jürgen Overfeld, CIO der Linde Kältetechnik GmbH & Co KG. Overfelds Team muss über 2000 mögliche Problempunkte auf 200 Servern und Netzwerkgeräten im Griff haben. Eine solche Aufgabe lässt sich laut Overfeld nur mit automatischen Hilfsmitteln in Form von Systemmanagement-Werkzeugen erledigen.

Solche Werkzeuge sollten indes nicht nur Problemmelder, sondern bis zu einem gewissen Grad auch Problemlöser sein. Zu einer effizienten Problemlösung trägt schon bei, wenn die von jedem Überwachungspunkt produzierten Datenmassen miteinander korreliert und nach bestimmten Vorgaben ver-

dichtet werden können, so dass schlussendlich aussagekräftige Beziehungen zwischen Ereignissen und Service-Prozessen zustande kommen.

Systemmanagement ist ein intelligent organisiertes Wechselspiel von leistungsfähigen Automatismen und menschlicher Expertise. Dies wird auch so bleiben, trotz allen Marketing-Getrommels um »selbstheilende« oder »autonome« Systeme. Im Gegenteil: die ständige funktionale Anreicherung der Systeme erzeugt erhöhte Anforderungen an Benutzer und Administratoren, welche die vom System produzierten Daten interpretieren und hinsichtlich ihrer Relevanz einordnen müssen. Das ist wohl der Hauptgrund dafür, dass in

Foto: Linde Kältetechnik

vielen Unternehmen die teuren und mit vielen Funktionen befrachteten Systemmanagement-Werkzeuge wie Tivoli, CA Unicenter oder HP OpenView oft bei weitem nicht ausgereizt werden.

## QUELLOFFENES NAGIOS-TOOL BEI LINDE KÄLTETECHNIK

Schlanke Systemmanagement-Werkzeuge haben deshalb in vielen Fällen nicht nur die geringeren Einstandskosten für sich, sondern vor allem auch die geringeren Folgekosten.

Besonders günstig ist der »Systemmanagement-Einstand« bei Werkzeugen aus dem Open-Source-Bereich. Wer sich hier für das »nackte« quelloffene Programmpaket entscheidet, zahlt für Lizenzen erst einmal gar nichts. »Natürlich ist aber ein bestimmter Aufwand für Schulungen, Plug-in-Programme und Anpassungs-Software anzusetzen«, meint Julian Hein, Managing Director beim Nürnberger Systemintegrator Netways GmbH, einem Spezialisten für das quelloffene Management-Werkzeug Nagios. Heins Unternehmen hat viel Erfahrung mit der Implementierung von Nagios in ausgedehnten Netzwerklanschaften. Netways hat nicht nur die oben erwähnte Installation bei Linde Kältetechnik begleitet, sondern im Frühjahr auch ein großes Projekt bei T-Systems in Kiel aufgesetzt, bei dem es um die Überwachung von rund 3700 Servern, Routern und Switches ging.



Foto: Sector Nord AG

**»Der Kunde kann nach ein bis zwei Tagen Schulung das ganze System selbstständig konfigurieren«**

**STEFAN SCHÄFER**,  
Vorstand bei  
Sector Nord AG

Übrigens wurde dabei eines der oben genannten großen Systemmanagement-Werkzeuge abgelöst.

Der Mehrwert, den Netways in Sachen Nagios liefert, besteht vor allem in Schulung. Das in mehrtägigen Workshops vermittelte Wissen bleibt allerdings nicht graue Theorie, sondern hat die tatsächliche Implementierung des

quelloffenen und unter GNU-Lizenz stehenden Systempaketes Nagios zum Ziel. »In einem ersten Workshop bei Linde Kältetechnik wurden 130 Server und Netzwerkgeräte in die Überwachung aufgenommen. In einem weiteren Workshop soll dieser Überwachungspool auf rund 200 Geräte erweitert werden«, beschreibt Julian Hein die Vorgehensweise. Und Martin Keusch, Domino/Linux-Administrator und Projektleiter für die Nagios-Einführung bei Linde Kältetechnik ergänzt: »Neben der allgemeinen Verfügbarkeit werden auch noch die bereitgestellten Dienste der Systeme



Foto: Netways GmbH

**»Wir haben gerade ein Nagios-Projekt bei T-Systems zur Überwachung von 3700 Geräten aufgesetzt«**

**JULIAN HEIN**,  
Managing Director bei  
Netways GmbH

überwacht werden. Damit kontrolliert der Nagios-Server insgesamt über 2000 potenzielle Fehlerquellen auf ihre korrekte Funktionsweise«. CIO Jürgen Overfeld ist schon jetzt sehr angetan von der Leistungsbilanz: »Durch den vollständigen Wegfall der Lizenzkosten und die kurze Implementierungszeit macht sich die Nagios-Installation praktisch unmittelbar bezahlt«.

Zu dieser günstigen Amortisationsrate tragen nicht zuletzt die speziellen Eingabemasken bei, die im Rahmen des Workshops von dem Netways-Berater zusammen mit den Administratoren von Linde Kältetechnik entwickelt worden sind. Damit ließ sich nach Aussage von Martin Keusch ein Vielfaches der normalen Konfigurationsarbeit einsparen, vor allem aber werde der Zeitaufwand für eventuelle spätere Änderungen deutlich reduziert.

Benutzerseitige Kommunikationsstrukturen wie spezifische Eingabemasken und »ein geschultes Auge« für die wirklich kritischen Punkte, die überwacht werden müssen, sind wesentlich für die Einsatztauglichkeit von quelloffener Software im professionellen Umfeld.

Hersteller kommerzieller Systemmanagement-Produkte betonen mit Recht

diesen Aspekt: »Da IT-Administratoren häufig das Wissen fehlt, was sie wie zu überwachen haben, sollte der Hersteller entsprechendes Wissen mitliefern«, sagt zum Beispiel Sven Kniest, Product Line Manager Systems Management Solutions EMEA bei NetIQ. Kniest hebt besonders auf die Performance-Überwachung ab, die mittlerweile genauso wichtig sei wie die Verfügbarkeitsmessung, indes ganz spezielle Anforderungen stelle: »Nur wenn der Hersteller bei der Auswahl der Parameter und Grenzwerte, die bei den verschiedenen Servern und Applikationen gemessen werden sollen, mit vorgefertigten Überwachungsfunktionen Hilfestellung leistet und dafür auch entsprechende Automatismen bereitstellt, lassen sich häufige Fehlalarme vermeiden«, sagt der NetIQ-Manager.

Systemintegratoren im Bereich quelloffener Software haben dies natürlich erkannt. Die Workshops von Netways verbinden deshalb die Nagios-Schulung explizit mit der Sensibilisierung für die entscheidenden Systeme beziehungsweise Parameter, die überwacht werden müssen. Mit dieser Sensibilisierung gehen in aller Regel Anpassungs- und Ergänzungsprogrammierungen einher, beispielsweise in Form von Datensammel-Programmen (Plug-Ins, Agenten) für bestimmte Anwendungen und Systeme. Derartige Anpassungen und Ergänzungen sind natürlich kein Spezifikum quelloffener Systeme, sondern auch bei kommerziellen Systemen gang und gäbe.

## »PAKETIERTES NAGIOS« BEI AIRBUS UND OLB

Die große Hemmschwelle für viele Anwender, quelloffene Software einzusetzen, liegt vermutlich in der Angst, trotz kompetenter Hilfe später mit dem Systemmanagement-Projekt »an die Wand zu fahren«, weil die Kapazitäten fehlen, die von der Open-Source-Community ständig weiterentwickelten Tools vernünftig zu integrieren. Systemintegratoren wie die niedersächsische Sector Nord AG haben deshalb aus Nagios, eigenentwickelten Agenten und zertifizierter Hardware von Fujitsu-Siemens sowie dem Betriebssystem SUSE SLES8 ein Komplettpaket gebildet, das sie unter dem Namen SNAG-



View verkaufen. Trotzdem sind die Kosten »für eine SNAG-View-Komplettlösung im Regelfall günstiger als allein die Wartungskosten für die klassischen Lösungen wie beispielsweise CA-Unicenter oder Tivoli«, sagt Jürgen Wodniok, Netzwerk- und Systemadministrator bei der Oldenburgischen Landesbank. Die OLB überwacht derzeit mit SNAG-View über 200 Standorte mit mehr als 500 Netzwerkknoten.

Durch die von Sector Nord entwickelten Datenbank-Agenten wird Nagios in Gestalt von SNAG-View auch zu einem leistungsfähigen Datenbank-Monitoring-Werkzeug. Am Standort Bremen von Airbus Deutschland überwacht SNAG-View sowohl die Datenbanken als auch die Applikationen unter OpenVMS. »Das OpenVMS-Cluster mit sechs Alpha-Servern ist verantwortlich für ein Produktionslogistik- und Telefonmanagementsystem, die Hochregallagersteuerung, das fahrerlose Transportsystem sowie für ein Erprobungs- und Qualitätsdatensicherungs-System«, berichtet Peter Biewald, Grup-

## »OPEN SOURCE« KOSTET KOMPLETT WENIGER ALS ALLEIN DIE WARTUNG REIN KOMMERZIELLER TOOLS

penleiter Systemintegration und DB-Administration im Werk Bremen von Airbus Deutschland.

### IMMER GRÖßERES FUNKTIONSSPEKTRUM

Nach Darstellung von Stefan Schäfer, Vorstandchef bei der Sector Nord AG, ist der Kunde mit dem vorinstallierten SNAG-View-Paket nach ein bis zwei Tagen Schulung in der Lage, das ganze System selbstständig zu konfigurieren. Für weiter gehende Wünsche wie SNMP- oder Traffic-Agenten haben die Niedersachsen Web-Frontends entwickelt, welche die Einstellungen um »einiges erleichtern«. Somit müsse

für die Pflege nicht extra ein Administrator abgestellt werden.

Traffic-Agenten bilden eine der Keimzellen der quelloffenen Systemmanagement-Software. Beispiele sind die von Tobias Oetiker von der ETH Zürich entwickelten Programmpakete »Multi Router Traffic Grapher« (MRTG), das Datenhaltungswerkzeug »Round Robin Database Tool« (RRDtool) und das Überwachungstool »SmokePing« zum Erfassen von Latenzzeiten und Paketverlusten. Zu diesen Freak-Tools sind mittlerweile viele andere quelloffene Management-Programme hinzugekommen (siehe Kasten), nicht zuletzt aber auch eine Menge Plug-Ins für Datenbanken, ERP-Systeme und viele andere Applikationen. Dadurch sind quelloffene Systemmanagement-Lösungen entstanden, die weit mehr können als nur »auf den Netzwerkverkehr horchen und dann Kurvendigramme zeichnen«. Und die Community entwickelt ständig weiter. Nagios beispielsweise gibt es inzwischen in der Development-Version 2.0, die »wesentliche Verbesserungen gegenüber der offiziellen Version enthält und die von einigen unserer Kunden schon produktiv eingesetzt wird, weil sie absolut stabil läuft«, sagt Julian Hein von Netways.

### AUSGEREIFTE SOFTWARE

Systemmanagement auf Basis quelloffener Software ist längst nicht mehr auf Administrations-Cracks oder Bastler beschränkt. Aber natürlich muss entsprechende technische Expertise erworben und ein Systemmanagement-Pflichtenheft aufgebaut werden, aus dem ersichtlich ist, welche Punkte überwacht und welche Parameter gemeldet werden sollen. Das freilich ist eine Aufgabe, die bei jedem Systemmanagement-Tool zu leisten ist. Auch Tivoli oder Unicenter können nicht von der Direktionssekretärin bedient werden. ■

## QUELLOFFENE MANAGEMENT-WERKZEUGE

Netzwerk- und Systemmanagement ist ein weites Feld. Es reicht vom einfachen, auf dem Simple Network Management Protocol (SNMP) aufbauenden Überwachungstool bis zum Service-Management-Framework, und vom herstellereigenen Spezialwerkzeug bis zum Universal-Monitor für heterogene Systeme. Die folgende Liste ist weder vollständig noch sind die aufgeführten Tools in ihrem Funktionsumfang gleichwertig. Gleiches gilt aber auch für die kommerziellen Tools. Auch dort gibt es leichtgewichtige Systeme wie »WhatsUp« von Ipswitch oder funktionsmächtige Systeme wie Tivoli oder Unicenter.

Name	Funktion	Web-Adresse
Big Brother	Netz- und System-Überwachungswerkzeug	<a href="http://www.quest.com">http://www.quest.com</a>
Big Sister	Netz- und System-Überwachungswerkzeug	<a href="http://bigsister.graeff.com">http://bigsister.graeff.com</a>
MRTG	Traffic-Überwachung	<a href="http://ee-staff.ethz.ch">http://ee-staff.ethz.ch</a>
Nagios	Netz- und Systemüberwachung	<a href="http://www.nagios.org">http://www.nagios.org</a>
Penemo	Netzwerk- und Systemüberwachung	<a href="http://sourceforge.net">http://sourceforge.net</a>
PIKT	Netz- und System-Überwachungswerkzeug	<a href="http://pikt.org">http://pikt.org</a>
RRDTool	Datenhaltung für Traffic-Kontrolle	<a href="http://ee-staff.ethz.ch">http://ee-staff.ethz.ch</a>
Sentinix	Netz- und Systemüberwachung, Security	<a href="http://www.sentinix.org">http://www.sentinix.org</a>
Snort	Intrusion Detection	<a href="http://www.snort.org">http://www.snort.org</a>