Überwachung im großen Stil: Nagios im Bundesverwaltungsamt

Alarmzentrale

Nicht allein der Kostenvorteil, sondern vor allem seine Flexibilität und Erweiterbarkeit bewogen das Bundesverwaltungsamt zum Einsatz des Open-Source-Monitoring-Favoriten Nagios. Heute überwacht er dort Tausende kritische Services. Julian Hein, Markus Kösters

© Paul-Georg Meister / pixelio.de

In den letzten Jahren hat Nagios in mehreren großen Firmen und Verwaltungen Einzug gehalten und die Anwender – darunter der Deutsche Bundestag, T-Systems oder das Bundesverwaltungsamt – berichten über ihre positiven Erfahrungen. Natürlich spielt dabei der Vorteil der Lizenzkosten-Freiheit eine Rolle, aber ein Argument hat sich als noch stärker erwiesen: die große Flexibilität und gute Erweiterbarkeit.

Noch fehlende Überwachungsmöglichkeiten lassen sich für Nagios schnell und einfach durch die Programmierung neuer Plugins ergänzen. Nicht einmal die Sprache gibt Nagios dafür vor. Das Repository listet Plugins in Perl, Bash-Skript, Python, Ruby, Java, VBScript, C, Delphi und sogar Dotnet.

Selbst die Kommunikation zwischen dem zentralen Überwachungsserver und den Clients lässt sich je nach Anforderung gestalten. Sei es durch verschiedene Kommunikationsprotokolle und Verschlüsselungsmechanismen oder sogar durch das Umkehren der Abfragerichtung. Kann Nagios einen besonders geschützten Server nicht direkt befragen, darf dieser seine Daten selbstständig an den Überwacher melden.

All dies ist mit einer Closed-Source-Lösung kaum umsetzbar. Hinzu kommt: Besonders in Deutschland hat Nagios eine große und aktive Anhängerschaft, die sich regelmäßig im Forum des Nagios-Portals austauscht oder auf der jährlichen Nagios-Konferenz [1] trifft. Zusätzlich hat vor allem die deutschsprachige Community eine große Zahl an Plugins, Erweiterungen und Integrationslösungen entwickelt und beteiligt sich rege an der Weiterentwicklung.

Size does matter

Ein oft zitiertes Vorurteil gegen OS-Programme jeder Spielart – auch gegenüber Nagios – ist, dass die quelloffene Software zwar für den kleinen oder mittleren Einsatzbereich geeignet, mit dem so genannten Enterprise-Segment aber überfordert sei. Für Nagios stimmt das Gegenteil. Hier verteilt ein interner Mechanismus die anfallenden Überwachungsaufträge bei Bedarf auf mehrere Checkserver, die dann ihre Ergebnisse an eine zentrale Instanz weitermelden. Dieses Distributed Monitoring genannte Feature erlaubt es, nahezu unbegrenzt große Netze zu überwachen.

Im Übrigen gilt das Gleiche wie bei jeder anderen Software: Je größer und komplexer das Umfeld und die Aufgabenstellung, desto mehr Planung ist notwendig – nicht nur mit Blick auf die Kapazität.

Nagios im Bundesverwaltungsamt

Das Bundesverwaltungsamt (BVA) begann 2004 mit der Sichtung verschiedener Überwachungswerkzeuge. Wegen der sehr unterschiedlichen Aufgaben dieser Behörde (siehe Kasten „Das Bundesverwaltungsamt“) und der sich daraus ergebenden Heterogenität der IT-Umgebung war allen Beteiligten von Anfang an klar, dass ein möglichst flexibles und offenes Überwachungssystem nötig ist. Außerdem sollten die verschiedenen Überwachungsanforderungen möglichst unabhängig umzusetzen sein und am Ende doch alle Daten in einer zentralen Sicht zusammenlaufen.

Nachdem ein erster Anforderungskatalog erarbeitet war, folgte eine intensive technische und finanzielle Evaluierung verschiedener Produkte, sowohl aus dem Open-Source- als auch aus dem kommerziellen Bereich. Gefordert waren Erweiterbarkeit, Flexibilität, Konfigurier-

Das Bundesverwaltungsamt

Das Bundesverwaltungsamt (BVA, [2]) ist in Deutschland der zentrale Dienstleister des Bundes. Die zum Innenministerium gehörende Behörde nimmt mehr als 100 verschiedene Aufgaben für mehrere Bundesministerien wahr. Dazu gehören beispielsweise die Bearbeitung der BAföG-Darlehn oder die Abwicklung von Visa-Angelegenheiten sowie die Unterstützung anderer Behörden und Institutionen bei der Verwaltungsmodernisierung.

Die Bundesverwaltung konsolidiert immer mehr IT-Dienstleistungen. Zu diesem Zweck entstand 2006 die Bundesstelle für Informationstechnik (BIT, [3]) als Dienstleistungszentrum des BVA. Fachlich untersteht sie dem Referat IT 2 im Bundesministerium des Innern, das auch die Aufgaben der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) wahrnimmt.

barkeit und Zukunftssicherheit, niedrige Kosten, vielfältige Überwachungsmöglichkeiten und Schnittstellen sowie gute Integrationsfähigkeiten.

In dieser Testphase stellte sich heraus, dass Nagios nicht alle Anforderungen des BVA out of the Box befriedigen konnte. Die kommerziellen Systeme boten in der Regel mehr Features. Ihnen mangelte es allerdings oft an den entscheidenden Stellen an Flexibilität. Dagegen ließen sich die fehlenden Funktionen bei Nagios leicht durch das Plugin-Konzept ausgleichen.

Da innerhalb des BVA ausreichend Know-how und Erfahrung mit der Skript-Programmierung vorhanden war, stellten neue Nagios-Plugins keine unüberwindbare Hürde dar, zumal sich die notwendigen Aufwände zuverlässig kalkulieren ließen. Vor allem waren sich die Projektgruppen sicher, auch zukünftig alle neuen Überwachungsanforderungen durch eigene Plugins abdecken zu können. Gegenüber dem Einsatz kommerzieller Produkte war Nagios damit erheblich preisgünstiger, und so ging es auch aus einer Wirtschaftlichkeitsbetrachtung als klarer Sieger hervor.

Umsetzung

Ab Anfang 2006 begann die Implementierung der gewählten Nagios-Lösung. Da sie hochverfügbar sein muss, laufen alle Nagios-Server in einem Heartbeat-Cluster. Jede Nagios-Instanz besteht aus einem aktiven Server, der die eigentliche Überwachung übernimmt, und einem zweiten Clusterknoten, der bei einem Ausfall einspringt.

Die Konfigurations- und Arbeitsdaten speichert die Installation in einem SAN, was zusätzliche Replikationsmechanismen unnötig macht. Die Last der aktiven Überwachungsanfragen teilen sich mehrere solcher Nagios-Instanzen, die jeweils einen Teilbereich des BVA-Netzwerks überwachen. Ihre Prüfungsergebnisse melden diese Server an einen zentralen Nagios-Master weiter, der die Ergebnisse auswertet, mit den hinterlegten Warnschwellen vergleicht und bei erkannten Fehlern entsprechende Meldungen verschickt.

Rechner am Handy

Da die BIT verschiedene hochverfügbare Anwendungen betreut, entschied man sich, das Bereitschaftsteam rund um die Uhr durch einen Telefonanruf über Nagios-Alarme zu informieren. Das ermöglicht ein Asterisk-Server, der im Fehlerfall einen Administrator auf dem Notfall-Handy anruft und ihm durch eine gesprochne Notiz informiert. Zusätzlich gibt es ein Sprachmenü, über das der Admin den Erhalt der Fehlermeldung bestätigen und damit die Eskalation an weitere Kollegen verhindern kann.

Weiter gehört es zu den Aufgaben des Nagios-Master-Servers, Performancegraphen zu erstellen und Statusdaten in einer MySQL-Datenbank zu speichern. Der dafür notwendige Datenbankserver läuft ebenfalls im Heartbeat-Cluster mit Master-Slave-Replikation und dient als

zentrales Datawarehouse. Das ist zugleich die zentrale Datenquelle für unterschiedliche Reports.

Für Erweiterungen und Tests gibt es eine eigene Testumgebung in der sich Konfigurationsänderungen oder Erweiterungen vor der Implementierung ausführlich testen lassen. Insgesamt besteht die Monitoring-Architektur aktuell aus zwölf einzelnen Serverblades, die in sehr kurzen Zeitabständen mehr als 5000 verschiedene Überwachungen auf knapp 700 Devices übernehmen.

Überwachungen

Durch die vielen unterschiedlichen Aufgaben des BVA ergibt sich auch eine entsprechende Vielfalt der Hard- und Software. Das Plugin-Konzept von Nagios erlaubt es aber, auf den überwachten Clients nur die wirklich notwendigen Plugins zu installieren oder auszuführen. Der Overhead auf den Clients hält sich damit in einem vernünftigen Rahmen und bereits bestehende Remote-Installations- und Verwaltungssysteme lassen sich weiter nutzen.

Auf allen Servern überwacht Nagios die klassischen Betriebssystemparameter, also beispielsweise die Auslastung von CPU, Platten und Netzwerkschnittstellen sowie Zustand und Verfügbarkeit von Diensten, Prozessen und selbstverständlich des gesamten Systems. Neben Windows- und Linux-Systemen betrifft dies auch Sun-Rechner, die die BIT ebenfalls betreibt.

Wichtige Dienste wie Apache, Tomcat, Websphere, Fax- und Mailserver sowie alle Datenbanken kontrolliert das System mit anwendungsspezifischen Checks. Für die Komponenten des Netzwerks kommen meist SNMP-basierte Abfragen zum Einsatz, aus Sicherheitsgründen teilweise getunnelt. Router und Switches verwaltet das BVA mit Hilfe des HP Network Node Manager, der erkannte Probleme ebenfalls an Nagios weitermeldet. In der Windows-Welt überwacht Nagios zusätzlich auch das Active Directory, das viele andere Systemen innerhalb des BVA benötigen.

Die Überwachung der Hardware bewerkstelligen in Nagios integrierte herstellerspezifische Produkte. Diese Tools leiten ihre Fehlermeldungen einfach an Nagios weiter. Selbst die SAN-Systeme und deren Einzelkomponenten lassen sich durch SNMP-Abfragen komfortabel im Blick behalten.

Addons von der Stange

Viele der weitergehenden Anforderungen des Monitoring-Projekts bewerkstelligt nicht Nagios selbst, sondern eines der vielen Addons. Neben dem aktuellen Zustand von Servern und Ressourcen interessieren sich die Administratoren auch für den zeitlichen Verlauf bestimmter Parameter. Beispielsweise kommt es bei einer Festplatte nicht nur auf die aktuelle Belegung, sondern auch darauf an, wie sich der Füllstand über einen bestimmten Zeitraum entwickelt.

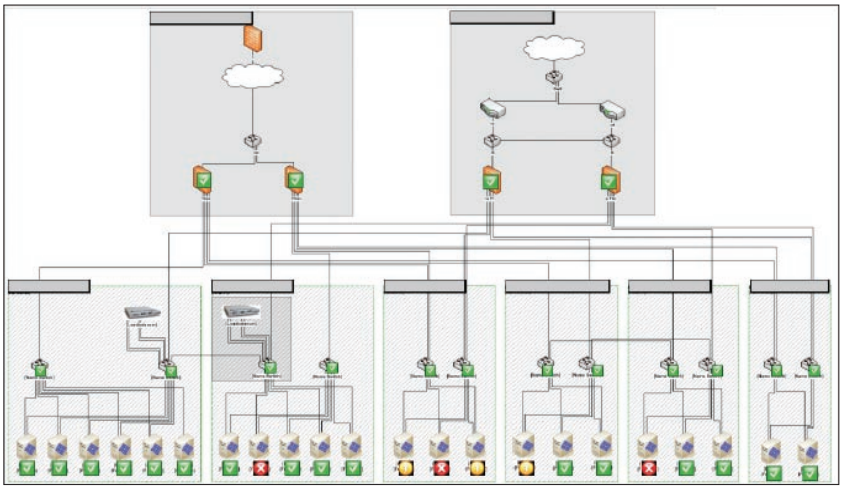
Solche Daten fragt Nagios mit jedem Überwachungslauf ab, speichert sie und gibt sie später über die Perfdata-Schnittstelle an andere Anwendungen weiter. Die BIT setzt an dieser Stelle den Nagios Grapher [5] ein, der sich vor allem durch einen hohen Automatisierungsgrad auszeichnet. So erkennt er neu in Nagios aufgenommene Hosts und Services selbstständig und beginnt vollautomatisch mit der Datensammlung. Der Aufruf der Grafiken erfolgt einfach aus dem Nagios-Webinterface heraus, das dafür keine weiteren Änderungen oder Patches braucht.

Nagvis [6] – ein weiteres Addon – zeigt Netzwerkpläne, in die sich eine Anzeige des aktuellen Status integrieren lässt (Abbildungen 1 und 2). Bestimmte Bereiche innerhalb der Zeichnung ändern dabei, sobald Nagios ein Problem festgestellt hat, ihre Farbe nach dem Ampelschema. So lassen sich auch hochkomplexe Zusammenhänge, Prozesse oder ganze Netzwerke inklusive ihres aktuellen Zustands in einer Grafik überschaubar darstellen.

Das Monitoring Information Portal

Ein wichtiges Ziel des Monitoring-Projekts war es auch, den zuständigen Mitarbeitern des BVA aussagekräftige Informationen über den aktuellen Zustand ihrer Fachverfahren oder IT-Ressourcen zu geben. Da sich das Nagios-Webinterface mit seiner Listendarstellung aber eher an Administratoren richtet und Kenntnisse der Implementierung voraussetzt, sollten die Nagios-Daten zusammen mit anderen Informationen in einem zentralen Monitoring Information Portal (MIP) zusammenlaufen. Dieses Portal (Abbildung 3, [7]) entstand auf der Grundlage des ebenfalls quelloffenen CMS Typo3.

Das Content Management System bringt



◀ **Abbildung 1: In schematischen Darstellungen der Netzwerk-Infrastruktur kann Nagvis Statusinformationen einblenden, die dadurch intuitiv der jeweiligen Hardware zuzuordnen sind.**

▶ **Abbildung 2: Physische Komponenten kann Nagvis nicht nur schematisch, sondern auch direkt abbilden und Nagios-Statusinformationen einblenden. Im Bild ein Rack mit Status-Ampeln.**

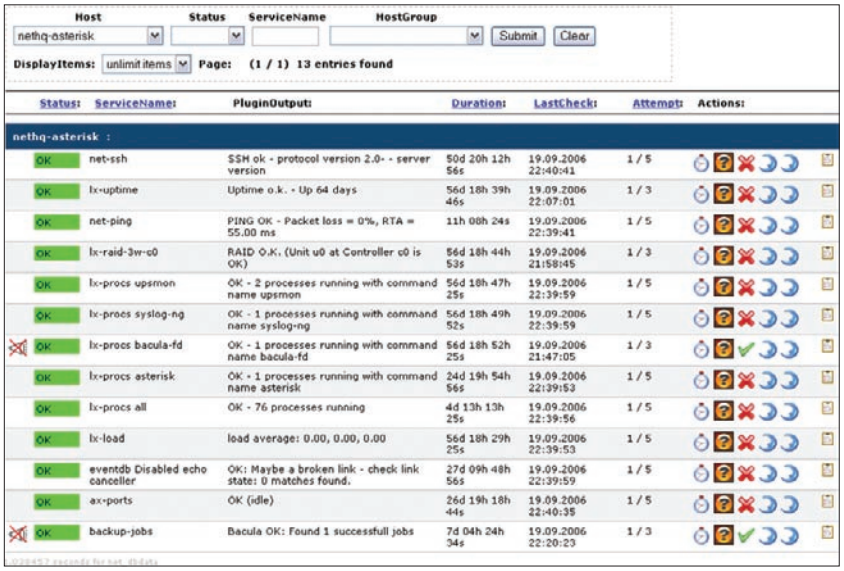


Abbildung 3: Das auf der Grundlage von Typo3 entwickelte Nagios-Portal bietet eine benutzerfreundliche Statusübersicht, etwa für die Anwender von Fachverfahren in der Behörde.

eine Fülle an Features mit, beispielsweise Authentifizierung gegen Active Directory, Benutzerverwaltung, das Typo3-Templatesystem und weitere Funktionen, die das Portal nutzt. Es verfügt darüber hinaus über eine Schnittstelle (API), mit dem sich der Funktionsumfang ganz ohne Änderung des Quellcode erweitern lässt.

Die Hauptextension stellt Daten und Informationen aus der Nagios-NDO-Datenbank und anderen Datenquellen dar. Mit Hilfe dieses Systems stehen den Mitarbeitern des Amtes im MIP zu den verschiedenen Fachverfahren neben den aktuellen und historischen Zuständen aus Nagios zusätzlich auch die Performance-Charts, die Netzwerkpläne als Nagvis-Karten, offene und geschlossene Tickets und viele andere Informationen zentral zur Verfügung.

Fazit und weiterer Ausbau

Inzwischen ist das Nagios-Monitoring zum unverzichtbaren Bestandteil der IT-Infrastruktur des BVA geworden. Für seine Betreuung entstand ein eigenes Team innerhalb der Bundesstelle, das für Betrieb und den Ausbau verantwortlich ist und die Fachabteilungen unterstützt. Alle Beteiligten werten die Implementierung als vollen Erfolg.

Die nächste größere Entwicklungsstufe besteht im Update auf die gerade erschienene Nagios-Version 3. Aktuell laufen die ersten Tests mit der Version 3.0rc1. Das Update hat das Ziel, dank der besseren Performance von Nagios 3.0 mit dem bestehenden Hardware-Ausbau künftig noch mehr gleichzeitige Überwachungen durchführen zu können. *(jcb)* ■

Infos

[1] Nagios-Konferenz: [http://www.nagioskonferenz.de]

[2] BVA: [http://www.bva.bund.de]

[3] BIT: [http://www.bit.bund.de]

[4] Nagiosexchange: [http://www.nagiosexchange.org]

[5] Nagios Grapher: [http://www.nagiosgrapher.de]

[6] Nagvis: [http://www.nagvis.org]

[7] Nagios Portal: [http://sourceforge.net/projects/nagiosportal/]

Die Autoren

Julian Hein ist Gründer und geschäftsführender Gesellschafter der Netways GmbH, die sich seit mehr als zehn Jahren mit der Implementierung und dem Betrieb von großen und komplexen Netzwerken aller Hersteller beschäftigt. Der Hauptfokus dabei ist die Nutzung von Linux und Open-Source-Tools.

Markus Kösters ist als Systemadministrator bei der Bundesstelle für Informationstechnik (BIT) tätig. Er verfügt über umfangreiche Erfahrungen mit Unix- und Open-Source. Er leitete das Teilprojekt Incident Management, welches unter anderem die Einführung eines umfassenden System-Monitorings beinhaltet.