

Warum System- und Netzwerk-Monitoring?

Eigentlich haben Sie die Frage nach dem Warum des System- und Netzwerk-Monitoring für sich selbst mit dem Kauf dieses Buches bereits beantwortet. Was ist Ihre Motivation, warum wollen Sie Ihre Systeme und Ihr Netzwerk überwachen?

- Ein urplötzlich eingetretener Ausfall eines kritischen Systems, der den Betrieb lahm gelegt hat?
- Vorausschauendes Handeln und Verbessern der Verfügbarkeiten der Systeme und des Netzwerks?
- Dokumentation der Verfügbarkeit Ihrer Systeme?

Vielfältige Motivationen können hinter der Entscheidung stehen, in den allermeisten Fällen wird aber vermutlich ein bereits eingetretenes konkretes Ereignis Auslöser für die Entscheidung sein - ein unerwarteter Ausfall einer Komponente der IT-Infrastruktur und damit verbunden die Frage:

Was kann ich tun, um so einen Ausfall zu verhindern oder zumindest schneller auf Ausfälle reagieren?

Kurzum, auch Netzwerk- und System-Monitoring ist keine Versicherung, die den Ausfall von Technik oder Software verhindert oder sehr viel unwahrscheinlicher macht - ein sinnvoll konfiguriertes Monitoring-System kann aber dazu beitragen, potenzielle sich abzeichnende Fehlerquellen bereits im Vorfeld wahrzunehmen oder im eingetretenen Fall eines Falles schneller reagieren zu können.

Ein altbekanntes Beispiel

Manfred Müller ist Systemadministrator der Metallschmiede, eines mittelständischen Betriebes, der uns in diesem Buch begleiten wird. Wie jeden Morgen startet Manfred seinen PC und meldet sich an der Domäne der Metallschmiede an. Zunächst startet er wie gewohnt seinen Webbrowser und seinen E-Mail-Client. Als er im Browser die Zugriffszahlen auf die Webseite der Metallschmiede vom Wochenende betrachtet und zeitgleich schaut, was sich nach dem Wochenende an E-Mails angesammelt hat, steht plötzlich der Juniorchef völlig aufgelöst im Büro - er hat keinen Zugriff auf die auf einem Server gespeicherten Daten, benötigt aber dringend Präsentationsunterlagen für einen Kunden, der gerade schon dabei ist, auf dem Firmenparkplatz sein Auto abzuschließen.

Mit Hochdruck schießen unserem Administrator zahlreiche Fragen durch den Kopf, darunter vielleicht auch die folgenden:

- Auf welchem System liegen die Daten des Juniorchefs?
- Sind nur die File-Services betroffen oder ist das System komplett ausgefallen?
- Gibt es Probleme mit weiteren Systemen oder gar dem Netzwerk?
- Ist Hardware defekt oder handelt es sich um ein Softwareproblem?
- Ist das Backup fehlerfrei abgelaufen?

Auf welchem System die Daten des Juniorchefs liegen, wird Ihnen auch ein Monitoring-System nicht verraten können (außer Sie bringen es ihm bei). Bei allen anderen der

genannten Fragen kann Ihnen ein Monitoring-System jedoch helfen - zwar nicht, indem es direkt den Fehler lokalisiert, aber indem es dazu beiträgt, den Fehler möglichst präzise einzugrenzen und dadurch schneller mit der eigentlichen Entstörung beginnen zu können.

Wie hilft System- und Netzwerk-Monitoring?

Nagios kann Ihnen helfen, Ihre Systemlandschaft im Auge zu behalten. Es macht das, was Sie niemals leisten können: Ständig den Überblick über den Zustand aller Systeme und Netzwerkkomponenten behalten. Und es hilft, zu dokumentieren. Was machen meine Systeme? Wie stark ausgelastet sind sie? Wie arbeiten meine Systeme im Normalbetrieb?

Nagios kann aber nicht nur aktuelle Zustände prüfen und bei Abweichungen vom Soll Benachrichtigungen versenden, richtig eingesetzt kann Nagios Ihnen helfen bereits vorbeugend vor dem Auftreten zahlreicher Standardprobleme einzugreifen. Vollgelaufene Festplatten? Nagios und sinnvoll eingesetzte Erweiterungen helfen Trends zu erkennen, wie sich die Belegung von Speicherplatz auf welchem System und auf welcher Partition entwickelt.

Wie hilft Ihnen dieses Buch?

Um ehrlich zu sein: Indem es anders ist.

Nagios ist ein etabliertes, über Jahre hinweg entwickeltes System zum Netzwerk- und System-Monitoring. Zahlreiche verschiedensprachige Bücher wurden bereits veröffentlicht, und dennoch versucht dieses Buch, anders zu sein. Ziel ist nicht, Nagios bestmöglich und umfassend zu dokumentieren, sondern den Einstieg in Nagios einfach zu gestalten und Sie bei der Implementierung eines ersten kleinen Nagios-Systems zu begleiten.

Manfred Müller, der Systemadministrator der zuvor bereits erwähnten Metallschmiede, wird auf diesem Weg unser Begleiter sein. Anhand der beispielhaften Systemlandschaft der Metallschmiede, eines mittelständischen Unternehmens, werden wir gemeinsam ein Nagios-System konfigurieren. Hauptaugenmerk ist nicht die umfassende Dokumentation aller verfügbaren Prüfwerkzeuge oder Erweiterungen, sondern die praktische Relevanz der wichtigsten Prüfwerkzeuge - in Nagios-Terminologie: Plugins und Erweiterungen, und ihre wichtigsten Optionen.

Als mächtiges Werkzeug steht Ihnen auf der dem Buch beiliegenden CD ein fertig konfiguriertes und direkt einsetzbares Nagios-System zur Verfügung. Sie können das System entweder direkt von der CD auf echter Hardware starten oder auch in der - auch in einer kostenfreien Version vorliegenden - Virtualisierungslösung Virtualbox nutzen. Damit entfällt ein lästiges Sichern der erzielten Zwischenergebnisse - und Sie können nach Zeit und Belieben Ihr virtuelles Nagios-System immer wieder „aufwecken“.

Wie ist dieses Buch aufgebaut?

Dieses Buch ist, wie Sie vermutlich bereits festgestellt haben, in drei Teile gegliedert, die aufeinander aufbauen.

In Teil 1 lernen Sie Nagios kennen.

- **Kapitel 1** (da sind wir gerade) bestärkt Sie darin, dass Netzwerk- und System-Monitoring wichtig ist, und bringt Ihnen Aufbau und Idee dieses Buches näher.

- **Kapitel 2** beschreibt die Nutzung der diesem Buch beiliegenden CD.

- **Kapitel 3** hilft Ihnen, Nagios kennenzulernen. Was sind die Features und Vorteile? An welchen Stellen hat Nagios Macken, wo sollte ich entsprechend vorsichtig sein? Wie funktioniert Nagios eigentlich? Wie kann ich mit dem Webinterface arbeiten, welche Möglichkeiten bietet es? Und zu guter Letzt schauen wir uns anhand der beiliegenden Beispielkonfiguration eine simple Umsetzung eines Nagios-Systems an, die als Ideengeber und Anregung dient.

In Teil 2 beginnen Sie analog zur Metallschmiede ein Nagios-System zu konfigurieren.

- In **Kapitel 4** steigen wir in die Konfiguration des Nagios-Systems ein und erledigen alles, was zu Beginn konfiguriert werden will. Wie bauen wir unsere Konfiguration so auf, dass wir uns auch in vier Wochen noch schnell zurecht finden? Welche Hosts wollen wir überwachen?

- In **Kapitel 5** richten wir die Überwachung von Netzwerkdiensten wie Webservern, Mail-Systemen und Netzwerkkomponenten ein. Sind Dienste erreichbar? Liegen die Antwortzeiten innerhalb eines vorgegebenen Toleranzbereiches?

- **Kapitel 6** befasst sich mit Dingen, die sich über das Netzwerk eigentlich schlecht überwachen lassen - etwa der Belegung lokalen Speicherplatzes. Hier hilft uns die Erweiterung NRPE (keine Sorge, dieses Kürzel wird Ihnen bald sehr vertraut sein) auf Linux- oder UNIX-Systemen bzw. ihr Pendant NSClient++ auf Windows-Systemen.

- **Kapitel 7** befasst sich mit passiver Überwachung. Systeme melden selbst, ob Prüfungen erfolgreich verlaufen oder Fehler aufgetreten sind. Auch die Verarbeitung von SNMP-Traps, etwa von Routern oder Switches, reißen wir kurz an.

- In **Kapitel 8** setzen wir ein Benachrichtigungskonzept um. Die schönsten Prüfungen von Hosts und Services nützen uns erst dann etwas, wenn Fehlerzustände auch schnell wahrgenommen werden können.

- **Kapitel 9** beschreibt die Festinstallation eines Nagios-Systems. Während Sie bisher das dem Buch beiliegende Rundum-sorglos-Paket nutzen konnten, werden in diesem Kapitel die für die gängigen Distributionen nötigen Schritte zur Inbetriebnahme des eigenen Nagios-Servers beschrieben.

In Teil 3 stellen wir Anreize dar, sich intensiver mit Nagios zu beschäftigen.

- In **Kapitel 10** werden Erweiterungen beschrieben, die Schwächen von Nagios abstellen

können und eine Abfallverwertung bereits anfallender Daten ermöglichen. Aus Daten wie etwa über die Speicherplatzbelegung können mit PNP z. B. Graphen erzeugt werden, die das Ablesen von Trends und das Erkennen von Normalzuständen bei Systemen ermöglichen. NagVis hingegen erlaubt Ihnen, eine Übersicht über die von Ihnen überwachten Systeme nach eigenen Vorstellungen und Anforderungen umzusetzen.

- **Kapitel 11** ist unsere Plugin-Schmiede. Anhand simpler Beispiele in gängigen Programmiersprachen wie Perl und PHP bekommen Sie einen ersten Eindruck davon, wie leicht Ihr Nagios-Monitoring-System um weitere Prüfmöglichkeiten erweiterbar ist.

Einfach mal „Danke!“ sagen

Lobhudeleien sind Bestandteil eines jeden Buches, und immer läuft man als Autor Gefahr, wichtige Menschen zu vergessen, ja zu übergehen. Dennoch sind diese Zeilen - verfasst am Ende der Arbeiten an diesem Buch - auch ein Teil innerlicher Genugtuung und dürfen nicht fehlen.

Ich möchte diese Zeilen nicht nur als „Dank“, sondern zugleich auch als Entschuldigung nutzen - in der langen Zeit, die dieses Buch gebraucht hat, sind zahlreiche andere, mir eigentlich sehr wichtige, Projekte deutlich zu kurz gekommen. Insbesondere meine Mitarbeit im Entwicklergremium Council der Gentoo-Distribution musste hinter diesem Buch zurückstehen.

Danken möchte ich insbesondere meinem Lektor Volker Bombien, der die Ausdauer hatte, dieses Projekt von der ersten vagen Idee über zahlreiche Diskussionen, Rückschläge und verschobene Termine bis hin zum fertigen Buch zu begleiten. Als Geber von Ideen und Anregungen und als Korrektor hat auch Tobias Klausmann, der als Fachlektor tätig war, einen erheblichen Anteil an diesem Buch. Nicht zuletzt gilt mein Dank auch Michael Gisbers, mit dem ich rund um den LinuxTag nicht nur das ein oder andere leckere Steak verzehren durfte, sondern der auch mit Ideengeber für dieses Buch war.

Ein besonderer Dank gilt ebenfalls allen, die an Nagios selbst sowie an zahlreichen Projekten rund um Nagios mitarbeiten und diese vorantreiben und ständig besser machen.

Widmen möchte ich dieses Buch meinen Großeltern, die - allesamt - wohl sehr stolz auf mich gewesen wären.

Oberhausen, im Mai 2009

Tobias Scherbaum