Überwachen Sie schon oder konfigurieren Sie noch?

Peter Bekiesch, Herrmann & Lenz Solutions GmbH

Monitoring ist als Basis-Disziplin im Rechenzentrums- und Datenbank-Betrieb unerlässlich. Dabei tauchen vielen Fragen auf: „Wie setze ich nun ein adäquates und maßgeschneidertes Monitoring auf und wie betreibe ich es?", „Kaufe ich ein Produkt, baue ich etwas selbst oder soll ich mich doch in der Open-Source-Welt umschauen?", „Überwache ich meine gesamte IT oder nur Teile davon?" oder „Wie viel Zeit sollte ich für das Projekt veranschlagen?" Der Artikel liefert entsprechende Antworten nach dem Motto „Organisation ist nicht alles, aber ohne Organisation ist alles nichts."

Bevor man sich auf die Suche nach einem geeigneten Werkzeug macht, ob nun gekauft oder nicht, müssen zunächst einige Hausaufgaben gemacht werden. Ziel ist es, die Rahmenbedingungen und Anforderungen im Laufe des Projekts nicht ständig neu zu definieren, sondern bereits zu Beginn wichtige Eckdaten zu setzen und Entscheidungen zu treffen.

Was möchte ich überwachen?

Im ersten Schritt erstellt man eine Liste von Maschinen und Komponenten, die ins Monitoring fließen sollen. An dieser Stelle macht man sich schon vorab die Mühe und unterteilt diese Komponenten nach Produktiv-, Entwicklungs- und Testsystem. Die Einteilung kann selbstverständlich bei jedem abweichen. Es sollte unbedingt vermieden werden, bereits zu Beginn in einem Organisationschaos zu versinken. Klare Strukturen machen auch später das Leben viel einfacher.

Nachdem nun die Liste der Komponenten festgelegt wurde, stellt sich die Frage, was man möchte – oder besser, was man auf diesen Komponenten überwachen muss. Bereits frühere Artikel und einschlägige Literatur listen eine breite Palette von Messpunkten auf, deren Überwachung sinnvoll erscheint. Bei dem Großteil ist das auch der Fall. Niemand stellt in Frage, dass etwa Plattenplatz- und Hauptspeicher-Verbrauch oder die allgemeine Netzwerk-Erreichbarkeit zu den zwingend notwendigen Messpunkten gehören. Doch auch hier ist die Konzentration auf das Wesentliche wichtig. Weniger ist manchmal mehr.

Wer soll wann und wie benachrichtigt werden?

Neben dem Überwachen ist die zweite wichtigste Aufgabe des Monitorings, die Probleme zu melden. Hier kommen nun wieder Menschen ins Spiel. Man definiert sein Team, das später die Monitoring-Plattform bedienen und/oder betreiben soll. In diese Zusammenstellung muss unbedingt einfließen, ob im Schichtbetrieb gearbeitet wird oder eine Rufbereitschaft gewährleistet sein muss. Betreibt man seine Produktiv-Systeme 7x24? Muss im Notfall jemand geweckt werden? Reichen Benachrichtigungen per E-Mail aus oder sind hier andere Mittel notwendig?

Aus diesen Fragestellungen ergibt sich ein Benachrichtigungsprofil, das später in die Konfiguration einfließen wird. Es sollte auch nicht vergessen und unterschätzt werden, dass Rufbereitschaft oder nächtliche Benachrichtigungen des Monitorings (etwa per SMS oder Anruf) arbeitsrechtliche Themen berühren.

Welche Informationen soll das Monitoring zusätzlich liefern?

Dies ist eine sehr häufig unterschätzte Frage. Das Monitoring ist nicht einfach nur dazu da, einige Maschinen „anzupingen" oder mal den verfügbaren Plattenplatz zu prüfen. Ein Monitoring-System kann sehr viel tiefer gehende Informationen über die IT liefern. Der obligatorische SLA-Report sowie eine Statistik über die Verfügbarkeit der Komponenten gehören zu den ersten und wichtigsten Auswertungen.

Ein Monitoring sollte aber noch viel mehr liefern können, wenn es die notwendigen Voraussetzungen erfüllt. Dann ist der steigende Verbrauch des Plattenplatzes ebenso (grafisch) auswertbar wie die Auslastung eines Prozessors oder die Paket-Verlustrate auf dem Netzwerk. Klar sollte sein: Überall dort, wo Messpunkte überwacht werden, fallen Daten an. Diese Daten sollten gespeichert und auswertbar sein.

Die Historie, der Blick in die Vergangenheit, ist für die Gegenwart und die Zukunft ein kostbarer Schatz an nützlichen Informationen. Diese intelligent ausgewertet und im besten Fall miteinander korreliert, ergeben Hinweise auf Schwachstellen und möglicherweise anstehende Probleme. Das Ziel eines Monitorings sollte es nicht nur sein, aktuelle Probleme zu erkennen, sondern auch, neue zu verhindern, bevor sie entstehen.

Ein Monitoring-System kaufen oder Open Source einsetzen?

Die letzte Frage in diesem Kontext befasst sich nun mit dem Werkzeug selbst. Es sollen hier nicht die Vor- und Nachteile kommerzieller Werkzeuge oder der auf dem Open-Source-Markt verfügbaren Werkzeuge aufgezählt werden. Man sollte vielmehr das Thema aus mehreren Blickwinkeln betrachten. Es gibt viele gute Gründe für kommerzielle Software, für Open Source und natürlich auch für selbst erstell-

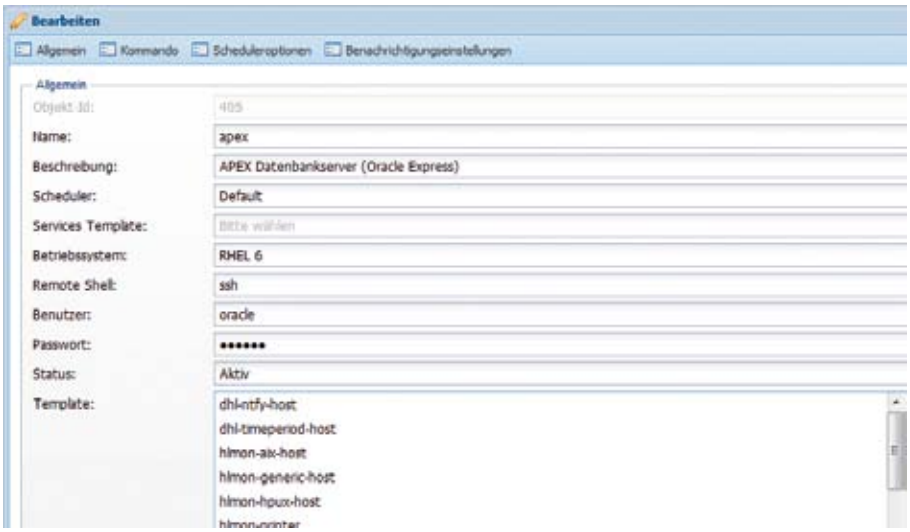

Abbildung 1: Das Aufsetzen des Systems

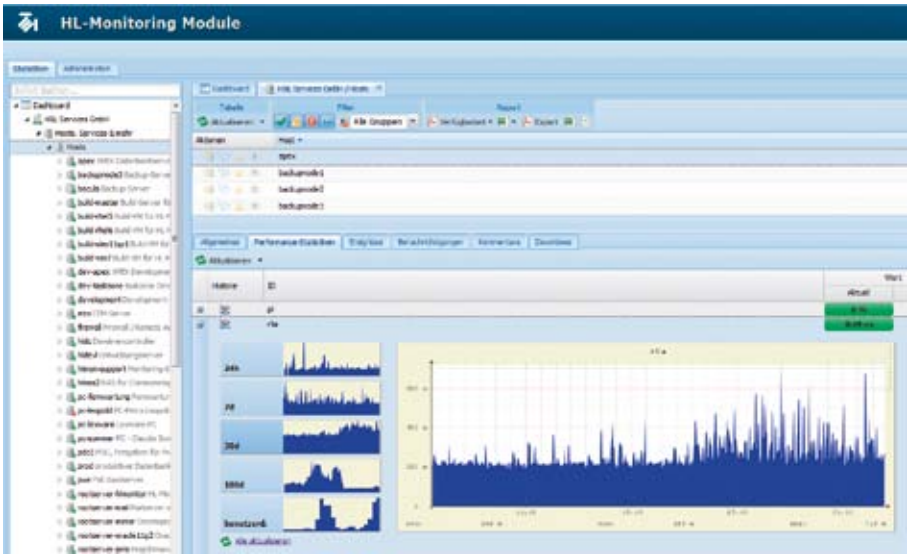

Abbildung 2: Die Messpunkte

te Komponenten. Muss man sich für die eine oder die andere Seite entscheiden? Nein! Der Autor verfährt nach dem Prinzip: „Von allem das Richtige".

Nagios/Icinga ist wohl das bekannteste Open-Source-Monitoring-Werkzeug auf dem Markt. Es hat inzwischen einen Status erreicht, der es beinahe zum Standard macht. Die simple Struktur von Hosts und Services ist leicht verständlich und einfach umzusetzen. Um das riesige Nagios/Icinga-Universum scharen sich inzwischen unzählige Plug-in-Hersteller, die Komponenten für Nagios/Icinga anbieten, um mit deren Hilfe nicht nur IT-Komponenten zu überwachen.

Was insgesamt in dieser Betrachtung fehlt, sind unter anderem folgende Fragen: „Wie viele Ressourcen benötigt man, um das Monitoring aufzusetzen und zu betreiben?", „Wie viel Aufwand muss man in die Konfiguration stecken?", Welche Plug-ins setzt man am besten ein?", Funktionieren die frei verfügbaren Plug-ins fehlerfrei?", „Wie viele Ressourcen sind notwendig, um das System auf einem aktuellen Stand zu halten?", „Was unternimmt man, wenn das Monitoring-System selbst ein Problem hat?" oder „Wer hilft einem?"

Die Grundannahme wäre jetzt, dass ein kommerzielles Produkt nun auf alle diese Fragen eine passende Antwort bietet. Dem ist aber meistens nicht so. Auch hier finden sich häufig versteckte Zeitfresser und Kosten. „End-to-End-Monitoring", in der Praxis, „Eierlegende Wollmilchsau" genannt, hört sich gut an und ist sicherlich ein sehr anspruchsvolles und interessantes Unterfangen. Braucht man das wirklich oder kann man sich gegebenenfalls dorthin entwickeln? Ein umfangreiches Rechte-System – wer darf was im Monitoring sehen, welche Maschine, welchen Messpunkt, welchen Report – braucht man das wirklich? Reicht nicht eine einfache Unterscheidung nach Schreib- und Lese-Rechten und bei Bedarf auch die Aufteilung in unterschiedliche Mandanten aus? Nicht selten befasst man sich allein mit diesem Thema mehrere Wochen, ehe auch nur eine Maschine überwacht wird. Der Autor verfolgt die Philosophie „Transparenz für alle". Warum soll der Datenbank-Administrator nicht wissen und sehen, dass es auf dem Server oder der Netzwerkleitung Störungen gibt? So ließe sich häufig die Standardaussage von Anwendern, „Die Datenbank läuft nicht", schon frühzeitig entkräften.

Dies sollte als Fragenkatalog am Anfang reichen, um die wichtigsten Eckpunkte zu definieren. Man sollte nur nicht dem Zwang verfallen, die 100-prozentige Lösung liefern zu wollen. Das schafft man nämlich nicht, denn dafür benötigt man unverhältnismäßig viele Ressourcen und zieht somit das Projekt unnötig in die Länge. Mit einer entsprechend akribisch erstellten Checkliste ausgestattet ist man gut gerüstet, um ein erfolgversprechendes Monitoring-Projekt zu starten.

Das Beispiel eines Hybrids unter den Monitoring-Systemen

„HL-Monitoring Module" wurde mit dem Ziel geschaffen, schnell und vor allem einfach eine Monitoring-Umgebung aufzusetzen. Selbstverständlich wird nicht an Funktionalität gespart. Lästiges Nach-Installieren von Komponenten oder Plug-ins gehört der Vergangenheit an. Der Kern erlaubt eine vollständige Server- und Netzwerk-Überwachung, zudem ist hier eine umfassende Oracle-, SQL-Server- und VMware-Überwachung in einem Werkzeug vereint. Hiermit lassen sich mehrere Ebenen auf einfache Art und Weise überwachen und die gewonnenen Messdaten sind sofort grafisch auswertbar.

Die Lösung ist kompatibel zu Nagios-/Icinga-Plug-ins, die nahtlos in-

Abbildung 4: Überwachung und Analyse

tegriert werden können. Auch eigenentwickelte Routinen lassen sich auf einfache Art einbinden. Somit müssen mühsam erstellte Programme nicht in den Papierkorb wandern.

Zu den besonderen Stärken zählt unter anderem die simple Administration, mit der neue Überwachungspunkte binnen Minuten eingebunden werden können. Dazu ein Beispiel: Um fünfundzwanzig Server und fünfundzwanzig Oracle-Datenbanken in die Überwachung aufzunehmen, ist ein Zeitbedarf von etwa zwei Stunden zu veranschlagen. Lästiges Schreiben von Konfigurationsdateien gehört der Vergangenheit an (siehe Abbildung 1).

Im vollständig webbasierten Cockpit können alle Mess-Ergebnisse direkt begutachtet und ausgewertet werden. Die Archivierung der erfassten Messdaten erfolgt automatisch. Hierbei sind keinerlei zusätzliche Installationen oder Aktionen seitens des Administrators notwendig. Neue Messpunkte werden automatisch gespeichert und ausgewertet (siehe Abbildung 2). Selbstverständlich umfasst die grafische Auswertung auch Daten, die im Oracle- oder SQL-Server-Umfeld gewonnen wurden. Die Korrelation der Daten ist ein einfaches, sehr mächtiges Mittel, um Schwachstellen oder Trends zu erkennen (siehe Abbildung 3).

Die Anzahl der virtualisierten Systeme auf Basis von VMware steigt stetig. Das Programm wird diesem Umstand gerecht und bietet eine umfassende Überwachung komplexer VMware-Umgebungen an. Die nahtlose Integration in die bestehende Monitoring-Landschaft schafft ungeahnte Möglichkeiten der Überwachung und Analyse (siehe Abbildung 4).

Fazit

Gleich zu Beginn sollte man wichtige Eckpunkte und Rahmenbedingungen festlegen, an denen man sich im Projektverlauf orientieren kann. Man sollte erst gar nicht versuchen, die „Eierlegende Wollmilchsau“ zu erschaffen, das haben schon viele versucht und sind gescheitert. Besser ist es, früh zu starten und früh in die Phase zu gelangen, in der schon wichtige Komponenten überwacht werden. Es müssen nicht gleich alle Komponenten sein, weniger ist mehr. Man kann später immer noch kontinuierlich aufstocken und somit das System besser kennenlernen.

Am besten schaltet man die Benachrichtigungen nacheinander ein, um nicht gleich zu Beginn mit einer E-Mail- oder SMS-Flut konfrontiert zu werden. Jedes System durchläuft eine Kalibrierungsphase, in der die Schwellwerte an die Realität angepasst, überflüssige Messpunkte entfernt und die Benachrichtigungsprofile den realen Gegebenheiten angeglichen werden. Monitoring ist ein Langzeitvorhaben, ein lebendes Projekt, ein System, das ständig verfeinert und optimiert wird.

Peter Bekiesch
peter.bekiesch@hl-services.de

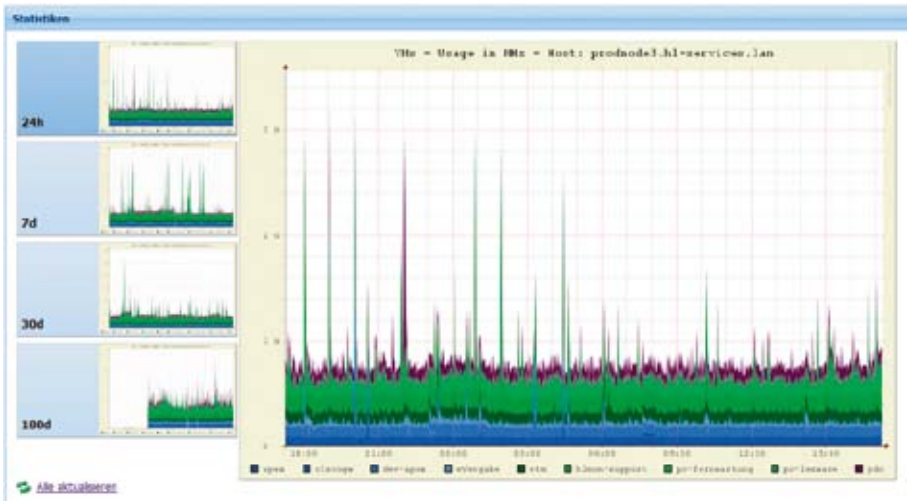

Abbildung 3: Die Korrelation der Daten