



Aufgaben und Lösungen beim Systemmonitoring

(<http://www.zdnet.de/magazin/41557298/aufgaben-und-loesungen-beim-systemmonitoring.htm>)

von Steffen Rieger und Stephan Hucke, 25. Oktober 2011

Durch steigende Anforderungen der Geschäftsbereiche wird es für die IT immer wichtiger, ihre Systeme effizient im Blick zu behalten. Steffen Rieger und Stephan Hucke vom Dienstleister it-novum geben im Gastbeitrag für ZDNet einen Überblick über den Markt und die Technik dafür.

IT-Versorger müssen heute nicht nur in der Lage sein, IT-Komponenten bereitzustellen oder zu liefern. Immer wichtiger wird das kontinuierliche Arbeiten an Prozessen, effizientes Change- und Risiko-Management sowie die kosteneffiziente Gewährleistung von Service-Level-Agreements.

Der Alltag sieht aber meist anders aus: Er ist durch reaktives Handeln, fehlende Gesamtübersicht und umständliches Monitoring der Systemlandschaft durch einzelne Herstellertools oder auf manuelle Weise bestimmt. Das alles sind Zeitfresser, die den Kosten- und Handlungsdruck erhöhen.

Effizientes Systemmonitoring kann da Abhilfe schaffen, Aber was macht Systemmonitoring überhaupt aus? Welche Aufgaben fallen bei der Überwachung der IT-Landschaft an? Welche Lösungen hält der Markt derzeit dafür bereit? Welche Informationen können beim Monitoring geprüft werden? Und welches sind die gängigsten Verfahren zur Datengewinnung? Mit diesen Fragen beschäftigt sich der folgende Beitrag. Um sie zu beantworten, sind zunächst einige grundlegende Erläuterungen notwendig.

Das SNMP-Protokoll

Man kann zwar grundlegend viele verschiedene TCP/IP-Protokolle zur Übermittlung der Daten verwenden (zum Beispiel SSH zum Anstoßen eines lokalen Skriptes oder Telnet, das im Vergleich zu SSH aber keine Verschlüsselung nutzt). In der Praxis läuft es aber hauptsächlich auf das SNMP-Protokoll hinaus. Das Protokoll stellt die kleinste gemeinsame Einheit zur Überwachung und Steuerung jeglicher Hardware dar. Es interagiert mit dem Monitoring-Tool auf dem Session-Layer. Neben der Lese- und Schreibfähigkeit unterstützt es die Datenlieferung in SNMP v1 über TCP, SPX oder UDP.

Allerdings sind die Authentifizierungsmöglichkeiten gering. Schutz bieten lediglich die in "Lese-/Schreibzugriff" und "reiner Lesezugriff" aufgeteilten Communities mit ihren eigenen, in Klartext übertragenen Passwörtern. SNMP existiert bereits in Version 3. Neben allen v2-Funktionalitäten beherrscht die aktuellste Version 64-Bit Zähler, Benutzerkonten und Authentifizierung, zusätzlich die Verschlüsselung in DES und AES unter Nutzung von VACM.

Aktuellere Hardware unterstützt meist alle Varianten, in der Praxis wird innerhalb von LANs hinter der Firewall aber SNMP v1 bevorzugt. Gründe dafür sind Performance, Einfachheit und Kompatibilität. Bei SNMP v1 werden lediglich ein oder zwei "Community-Namen" konfiguriert. Nur bei besonderem Bedarf, etwa der ISO27001-Zertifizierung, ist es sinnvoll, SNMP v3 zu nutzen. V3 bietet zwar Abwärtskompatibilität, ist aber sehr komplex und verlangt viel Zeit für die Konfiguration.

Funktionen wie SNMP-WALK prüfen, welche Geräte, Objekte und Informationen sich abfragen lassen. Die anschließende Konfiguration von Parametern, Schwellwerten, Ausführungszeitplänen und das Hinterlegen von verantwortlichen Kontaktpersonen dient der Auswertung und der Benachrichtigung im Bedarfsfall. Die kann über Telefon, E-Mail, SMS oder Instant Messaging erfolgen.



Steffen Rieger ist Technischer Direktor beim Beratungsunternehmen it-novum und einer der beiden Autoren dieses Gastbeitrags für ZDNet (Bild: it-novum).

Das Entsenden von aktiven SNMP-Checks durch das Monitoring-Tool liefert Statusdaten in fest konfigurierten Intervallen und validiert sie nach einer fixen Anzahl an Prüfungen von Soft-State zu Hard-State-Zuständen. Diese sogenannten SNMP-GETS fragen Daten im Auftrag der Anwendung aktiv ab.

Eine moderne Überwachungslösung sollte jedoch zusätzlich den Empfang von passiven SNMP-TRAPS unterstützen. Bei diesem Verfahren werden die Gerätekomponenten so konfiguriert, dass sie bei zeitkritischem Status selbständig Ereignisse über einen aktiven Agenten übermitteln. Die Kommunikationsmöglichkeiten zwischen SNMP und Hardware ergeben sich durch die hardwareseitig integrierten und in der Monitoring-Anwendung migrierten MIBs (**Management-Information-Base**^[1], das heißt: Beschreibungsdateien) der Hersteller. Sie können auch durch die menschlich lesbaren Object Identifier (OIDs) manuell eingepflegt werden. OIDs sind meist in umfangreichen Listen im Internet zu finden.

Die Sensorik

Rechenzentren und Serverräume unterliegen besonderen Sicherheitsvorschriften. Schon ein Kabelbrand im Serverschrank kann katastrophale Folgen für ein Unternehmen haben. Für entsprechende Hardware oder potenzialfreie Schaltungen, zum Beispiel an Zugangstüren, können Zustände über einen Agenten mittels des SNMP-Protokolls abgeholt, ausgewertet, validiert und an die hinterlegte Kontaktperson oder -gruppe gesendet werden. Um Auskunft über klimatische und räumliche Gegebenheiten, seismographische Aktivitäten, Statusinformationen von der USV oder sogar kompletten Produktionsanlagen zu bekommen, gibt es unterschiedliche Module, zum Beispiel für Rauch, Gas, Wasser, Erschütterung oder Bewegung.

Linux-/Unixbasierte Systeme überwachen

Durch den Einsatz von SSH- oder tooleigener Daemons lassen sich lokal installierte Skripte (zum Beispiel Shell und Perl) mit ihren Commands ausführen, um Antworten zu erhalten. Der Log-in kann per Public-Key-Methodik erfolgen. Auch Syslog-Events sind über aktive Checks direkt abfragbar.

Eine andere Methode ist der Einsatz eines lokalen Agenten. Dieser wird vom Monitoring-Server aktiv aufgefordert, sämtliche ungefilterte Informationen zu liefern. Für Linux/Unix-Umgebungen bietet sich NET-SNMP (bereits in v5.x.x) mit eigenem Daemon an. Dieser enthält eine Vielzahl nützlicher Kommandozeilen-Tools, Agenten und Bibliotheken, welche die Grundlage für die SNMP-Implementierung im Open-Source-Bereich darstellen.

Windowsbasierende Systeme mit Agenten überwachen (clientbased)

Die Daten des Windows-Eventlog müssen auf eine andere Art als die der Unix-Syslog abgefragt werden. Hier besteht keine direkte Transfermöglichkeit der Plug-ins. Grundsätzlich bieten windowsbasierende Systeme mehrerer Möglichkeiten zur Abfrage an, zum Beispiel durch NSClient++, OpMon-Agent, NC_Net. Dazu kommen die herstellerspezifischen Möglichkeiten des jeweiligen Tools. Wichtig ist, dass der entsprechende Agent auf dem Windows-System aktiv ist.

WMI – Checks ohne Agenten (clientless)

Windowsbasierende Workstations und Server bringen bereits die **WMI**^[2]-Schnittstelle mit, so dass auf eine direkte lokale Installation auf dem Client-PC verzichtet werden kann. Die Schnittstelle besitzt Lese- und Schreibfähigkeit und kann auf fast alle Einstellungen des Systems zugreifen – sowohl auf Betriebs- als auch Anwendungsebene. Zur Überwachung werden daher häufig Perfmon-Werte, Ereignisseprotokolle, Inventardaten oder Dienste und Prozesse ausgewertet. Es handelt sich dabei um eine Query-Language, die eine Anmeldung am System erfordert und für die Administration und Fernwartung besonders hilfreich ist.

Voraussetzung ist ein Windows-Server, auf dem alle WMI-Skripte installiert sind. Er stellt das Kommunikationsprotokoll für die Übermittlung der Daten zwischen WMI-Proxy und Monitoring-Tool bereit. Das Protokoll sorgt dafür, dass die Parameter an die lokalen Plug-ins übergeben werden.

Bei der Frage nach clientless oder clientbased Monitoring ist ein grundlegendes Problem, dass die binäre Implementierung von Client-Software ein Eingriff in das bestehende System darstellt und Probleme hervorrufen kann. Deshalb werden häufig clientless Standardmethoden verwendet.

Applikationen über CCMS überwachen (clientless)

CCMS^[3] (Computer Center Management System) ist ein SAP-eigenes Monitoringwerkzeug, das der zentralen Überwachung der SAP-Netweaver-Komponenten dient. Dadurch lässt sich das Verhalten von SAP-Systemen bewerten und ihre größtmögliche Verfügbarkeit sicherstellen. Der SAP-Alert-Monitor als Monitorsammlung empfängt Daten unter anderem von Agenten der Satellitensysteme, die Auskunft über Performance- oder Zustandsdaten abliefern.



AUTOR

Steffen Rieger ...

... ist Technischer Direktor bei der **it-novum GmbH**^[4], einem Beratungsunternehmen mit Schwerpunkt auf SAP, Open Source und IT-Service-Management in den Bereichen Applikationen und Infrastruktur. Stephan Hucke ist Consultant Systemmanagement bei dem Dienstleister.

Dazu gehören zum Beispiel Speicher-/CPU-Auslastung, Disk I/Os, Datenbanken, Antwortzeiten, Ausgabesteuerung oder Security- und Systemlogs. SAP liefert dazu verschiedene sinnvolle Templates, die manuell ergänzt werden können. Auf der Monitoring-Seite ist ein Client installiert, der mit aktiven Plug-ins die CCMS-Daten über eine der RFC-Schnittstellen abfragt. Voraussetzungen für den Remotezugriff sind die Installation der SAP-Bibliotheken auf Windows und Linux/Unix. Je nach Tool können auch SLA-Reportings, Business-Process-Monitoring und Trendanalysen zur Funktionalität gehören.

Systemnahe Applikationen

J2EE-, Web-, Domain-Name-, Mail-, Fileserver, Proxies und entsprechende Queues lassen sich problemlos über die netzwerkfähigen Protokolle SMTP, HTTP, DNS, DIG, POP3, IMAP oder FTP abfragen (mit oder ohne Verschlüsselung). Nicht jedes Protokoll besitzt passende Plug-ins. Individuelle bestehende Plug-ins nutzen die Protokolle, um zu prüfen, ob der TCP oder UDP-Port offen ist und dort ein Dienst existiert. Für eine Überwachung in die Tiefe finden spezifische Agenten Verwendung. Die Antworten wertet das Monitoring-Tool aus.

Cloud

Auch ESX-, KVM-, Citrix- oder XEN-Farms können im Bereich der Auslastung einzelner Komponenten überwacht werden. Ebenso sind der Traffic, eingeloggte User, Lizenzen oder laufenden Sessions kontrollierbar. Abfragen werden über die vom Hersteller gelieferten APIs abgewickelt, so dass keine zusätzliche systemseitige Installation nötig ist. Der Monitoring-Markt bietet viele Lösungen. Während sich in großen Unternehmen HP OpenView oder IBM Tivoli finden, greift der Mittelstand gerne auf What's Up Gold von Ipswitch oder Orion von SolarWinds zurück.

Das unixbasierte HP OpenView ist besonders auf große IT-Landschaften ausgelegt und stellt eigentlich eine Suite dar, die um unzählige Einzelwerkzeuge erweitert werden kann. In Überwachungsszenarios findet der HP Network Node Manager Verwendung. Er spielt seine Stärken bei HP-Komponenten aus und bietet viele Automatisierungsmöglichkeiten sowie eine einfache Konfiguration.

Die Kehrseite: Durch die umfangreichen Funktionalitäten und Wertedarstellungen wird es schnell komplex, weshalb langwierige Einarbeitungen und Schulung Programme sind. Zu den sehr hohen Lizenzkosten addieren sich Support und Folgekosten dazu, zum Beispiel Subscription oder Zusatzmodule. Gleiches gilt für IBM Tivoli. Bei entsprechender Unternehmensgröße befindet man sich kostenmäßig daher schnell im sechsstelligen Bereich. Die ausgeprägte Funktionalität führt also zu einer starken Abhängigkeit zum Hersteller.

Firmen mit weniger üppigem Budget bedienen sich daher gerne kleinerer Überwachungsalternativen. Das windowsbasierte What's Up Gold oder Orion sind bereits für wesentlich niedrigere Lizenzkosten zu haben. Erweiterungen und Monitoringaufwand (zum Beispiel die Anzahl zu überwachender Geräte) werden extra abgerechnet, ebenso wie der kostenpflichtige Support.

Vor diesem Hintergrund stellt Open Source eine interessante Option zu teuren und häufig überdimensionierten kommerziellen Lösungen dar. Da können die ehrliche Beantwortung der Frage nach dem "Was brauche ich eigentlich?" helfen, Kosten zu sparen und gleichzeitig effizienter und flexibler zu werden.

Neben quelloffenen Tools wie CACTI, openNMS oder MRTG sticht das linuxbasierte Framework **Nagios**^[5] hervor. Gründe sind die sehr starke Community, die lange Entwicklungshistorie und eine große Funktionsvielfalt, die zu der hohen Marktakzeptanz und breiten Etablierung auch im Enterprise-Umfeld beigetragen haben.

Nagios deckt Anforderungen an halb- oder vollautomatisches Discovery mit Filterregeln, Eventkorrelation oder Visualisierung der Systemlandschaft genauso ab wie den Wunsch nach Business-Reportings, Geschäftsprozessmonitoring, Eskalationsmanagement, Recovery, etc. Die Integration von Drittsystemen wie einer CMDB oder eines Ticketsystems ist durch die offenen Schnittstellen jederzeit möglich.

Eine auf Nagios basierende Variante ist das relativ neue Projekt **open-IT-Cockpit**^[6]. Der Fokus liegt hier auf der einfachen Überwachung komplexer IT-Landschaften: Das Tool bietet plattformabhängige Visualisierung durch eine eigene intuitive Websoftware, einfache Installer und eine grafische Oberfläche. Dadurch kompensiert es die komplizierte Konfiguration und Installation von Nagios über Kommandozeilen.

Fazit

Ob Closed oder Open Source: Die Lösungen unterscheiden sich neben dem Lizenz- und Supportmodell maßgeblich im Funktionsumfang, der Visualisierung (zum Beispiel Graphenerstellung, zusammenstellbare Infrastruktur-/Monitoringübersicht) und der Umsetzung einer einfachen Konfiguration - entscheidende Voraussetzungen für Bedienbarkeit und Leistung. Die eigenen Anforderungen sollte man daher genau mit den der favorisierten Lösung abgleichen, denn langfristig kann die Kostenschere stark auseinanderklaffen.

Gute Monitoring-Lösungen überwachen zentral und einheitlich. Sie helfen, die täglichen Routinearbeiten am System zu automatisieren - und damit letztendlich zu verringern. Die IT bleibt dabei individuell skalierbar und zeigt rechtzeitig bedenkliche Entwicklungen. Eine solche Überwachung führt langfristig zu einer wertschöpfenden IT, die Stabilität, Qualität, Effizienz und Transparenz schafft. Neben einer einfachen Konfiguration sollte eine moderne Lösung die Möglichkeit bieten, auch komplexe Prozesse, Dienste oder SLAs übersichtlich zu visualisieren. Das schafft nicht nur bei der Führungsebene Vertrauen und Zufriedenheit, sondern auch bei internen und externen Kunden.

URLs in diesem Artikel:

[1] = http://de.wikipedia.org/wiki/Simple_Network_Management_Protocol#Management_Information_Base

[2] = http://de.wikipedia.org/wiki/Windows_Management_Instrumentation

[3] = http://help.sap.com/saphelp_nw70/helpdata/en/c4/3a5dba505211d189550000e829fbbd/content.htm

[4] = <http://www.it-novum.de>

[5] = <http://www.zdnet.de/magazin/41501912/nagios-das-schweizer-messer-der-netzwerkueberwachung.htm>

[6] = <http://www.open-itcockpit.com>

Copyright (c) 2011 CBS Interactive GmbH. Alle Rechte vorbehalten.