Überwachung von Netzwerk und Peripherie

Die IT Mitteln sind zu einem unverzichtbaren Hilfsmittel geworden. Fällt zum Beispiel das E-Mail aus, ist die Aufregung oft sehr gross. Für den Administrator ist es dabei nicht einfach, immer den Überblick über den Zustand der vorhandenen Mittel zu behalten.

Um auf eine Störung frühzeitig reagieren zu können, werden Monitoring-Systeme eingesetzt. Sie überwachen per Netzwerk die Verfügbarkeit von Diensten und informieren den Administrator, wenn etwas nicht mehr im grünen Bereich läuft. So erfährt er schnell, wenn der Web-Server nicht mehr antwortet, ein Dienst abgestürzt oder eine Harddisk gefüllt ist. Da das Monitoring-System solche Dienste ständig prüft, können Fehler frühzeitig erkannt und geeignete Massnahmen getroffen werden.

Das Stichwort «Netzwerküberwachung» erzeugt bei Google eine Flut von über 59'000 Dokumenten. Dies beweist, dass das Thema sehr aktuell ist und in Zukunft vermutlich auch bleibt. In dieser Flut von Möglichkeiten den Überblick zu behalten ist nicht einfach. Dieser Beitrag kann ebenfalls nicht auf alle eingehen, sondern stellt lediglich einige davon vor.

Funktionsweise

Um eine sinnvolle Übersicht über das Netzwerk und die angeschlossenen Geräte zu bekommen, sollten die Monitoring-Programme mindestens folgende Funktionen haben:

- Statusüberwachung von Geräten (oft als reine Pings ausgeführt)
- Überwachung verschiedener Betriebssysteme (mindestens Windows, Unix und Linux)
- Überwachung von Protokollen (zum Beispiel HTTP, SMTP, usw.)
- Überwachung von Eventlogs
- Überwachung von Festplatten und deren Speicherbelegung
- Überwachung von Services und Prozessen
- Einfache Ansicht, die auf einen Blick den Zustand zeigt
- Verschiedenen Alarmierungsfunktionen (oft Net Send (Windowsnachrichten), E-Mail oder SMS)
- Loggingfunktionen (zur späteren Auswertung, zum Beispiel Verfügbarkeit eines Dienstes während einer bestimmten Zeit)

Zwei Programme, die diese Funktionen bieten und zudem kostenlos verfügbar sind, sind zum einen Nagios und zum anderen Big Brother. Auf beide soll in der Folge eingegangen werden.

ZUM AUTOR

Dipl.-Ing, FH, CISSP, Andreas Wisler
IT-Redaktor Maschinenbau
Geschäftsführer GO OUT
Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.goout.ch
info@goout.ch

Nagios

Als statusorientiertes Monitoring Programm hat sich in den letzten Jahren Nagios etabliert und wird auch in vielen Firmen eingesetzt. So überwacht Yahoo in den USA 100'000 Rechner mit Nagios. Die Kernfunktion, der Nagios-Prozess, kümmert sich dabei nur um den Aufruf der installierten Plug-ins. Diese liefern die Resultate zurück an Nagios, welches die Auswertung der Ergebnisse und die Benachrichtigung, die wiederum über Plug-ins geschieht, ausführt. Nagios läuft auf allen üblichen Unix-Varianten inklusive Linux. Es überwacht ebenfalls Windows-Systeme und Netzwerkkomponenten, die das Protokoll SNMP (Simple Network Management Protocol) sprechen. Bereits stehen dutzende von Plug-ins (Erweiterungen) zur Verfügung. Ebenso lassen sich diese Plug-ins einfach in beliebigen Programmiersprachen selbst entwickeln.

Nagios ruft ein Plug-in mit einer Reihe von konfigurierbaren Parametern, wie etwa dem zu prüfenden System auf und erhält den Status zurück: entweder «OK», «Warning», «Critical» oder «Unknown». Bei einem Statuswechsel durchläuft das Ereignis eine vordefinierte Filterkette. Erst wenn alle Filter eine Benachrichtigung erlauben, verschickt Nagios sie beispielsweise per E-Mail oder SMS an einzelne Kontaktpersonen oder Gruppen. Der gesamte Vorgang ist umfassend konfigurierbar; so können zum Beispiel verschiedene Kontaktgruppen zu unterschiedlichen Zeiten oder nacheinander benachrichtigt werden.

Mitte März ist die Version 3.0 erschienen. Die Statusübersicht wurde dabei nur marginal überarbeitet. Die vielen Änderungen sind unter der Haube zu finden. Erwähnenswert ist sicherlich die verbesserte Abfrage der zu überwachenden Geräte. Diese parallele Kontrolle erhöht die Geschwindigkeit und verhindert, dass eine blockierte Abfrage alle anderen Abfragen verzögert.

Weitere Infos:
www.nagios.org
www.nagios-portal.de
www.nagiosexchange.org/

Big Brother

Eine Alternative zu Nagios, ist das für den nichtkommerziellen Betrieb ebenfalls kostenlos verfügbare Big Brother. Vor einigen Jahr wurde die Software von Quest übernommen. Die Freeware Version ist aber weiterhin im Internet herunterladbar.

Die Serverkonsole von Big Brother ist für Unix- und Windows-Systeme erhältlich. Im Gegensatz zu Nagios führt der Big Brother Dienst alle Überwachungen zentral aus. So können Systeme angepingt und Dienste aufgerufen werden. Erst wenn lokale Daten ausgewertet werden sollen (zum Beispiel Harddisk, Eventlogs usw.) kommen sogenannte Clients zum Einsatz. Diese werden direkt auf dem zu überwachenden System installiert. Verfügbar sind diese Clients für Novell, Mac OS, AS400, VAX OpenVMS VM/ESA und natürlich Unix und Windows (Windows Server 2008 muss von Hand installiert werden). Diese Vielfältigkeit garantiert eine lückenlose Überwachung. Sinnigerweise kommunizieren Clients und Server via den Port 1984 miteinander (Frei nach George Orwell).

Die Konfiguration erfolgt, eher untypisch für Windows-Ad-

Bild: Archiv

ministratoren, in Textdateien. Relativ einfach werden die zu kontrollierenden Systeme aufgelistet, wahlweise auch gruppiert, und die dazu gehörenden Services angegeben. Eine zweite Datei kümmert sich um die Alarmierung. Hier wird definiert, wer, wann und wie alarmiert werden soll. Einmal konfiguriert, genügt es, den Service zu starten.

Wie für Nagios auch, gibt es eine Vielzahl von Erweiterungen, die einfach hinzugefügt werden können. So ist es beispielsweise möglich, auch eine USV abzufragen und damit zu erkennen, wie lange die Restkapazität reicht oder ob die Lebensdauer der Batterie bald zu Ende geht.

Weitere Infos:
www.bb4.org
www.deadcat.net

Kommerzielle Produkte

Dass dieser Markt stark umkämpft ist, zeigen auch die vielen kostenpflichtigen Programme, die verfügbar sind. Zwei bekannte in dieser Gattung sind sicherlich WhatsUp von Ipswitch und HP Openview. An dieser Stelle sollen beide kurz vorgestellt werden.

Whats Up

WhatsUp Gold ist eine umfangreiche Lösung für Applikations- und Netzwerk-Monitoring und ist vollständig webbasierend. Im Gegensatz zu den vorgestellten kostenlosen Varianten, erfasst es die Netzwerkelemente automatisch und bindet diese ein. Zudem ist es möglich, Handlungsschemen zu definieren. Erst wenn mehrere Ereignisse zutreffen, wird entsprechend Alarm ausgelöst. Erweitert ist auch die Ausgabe der Daten. Dies hilft vor allem beim Berechnen von statistischen Werten.

Weitere Infos:
www.ipswitch.com
de.whatsupgold.com

HP OpenView

Das Portfolio von HP OpenView geht weit über eine reine Überwachung. OpenView deckt verschiedene Bereiche des IT-Managements ab und besteht aus einer Reihe integrierter Module. Für die Überwachung zuständig ist der Network Node Manager (NNM). Der NNM dient zur SNMP-Überwachung der IP-Ebene von Netzwerkkomponenten. Dies sind typischerweise Switches, Router und Firewalls. In der Advanced Edition sind weitergehende Kontrollen möglich. Verschiedene Plugins erweitern das Paket. Neben der grafischen Darstellung der Knoten gibt es einen Alarmbrowser, in dem Ereignisse angezeigt werden. Durch das Verknüpfen mit Skripten können ereignisabhängig Aktionen ausgelöst werden. Neben dem Überwachen der Erreichbarkeit der Netzwerkkomponenten werden typischerweise Bandbreitenkapazitäten, der Status von Interfaces, Leitungsfehler, Router-CPUs und Backups überwacht.

Weitere Infos:
www.hp.com

Der Vergleich zeigt, auch kostenlose Programme bieten eine Vielzahl von Möglichkeiten, ein Netzwerk komplett zu überwachen und entsprechend Alarme auszulösen. Dabei müssen sich diese nicht vor teuren, kommerziellen Programmen verstecken.

Stört es nicht, die Konfigurationen in Textdateien vorzunehmen und Abstriche an der grafischen Auswertung hinzunehmen, ist ein proaktiver Schutz durchwegs mit Freeware Programmen möglich.