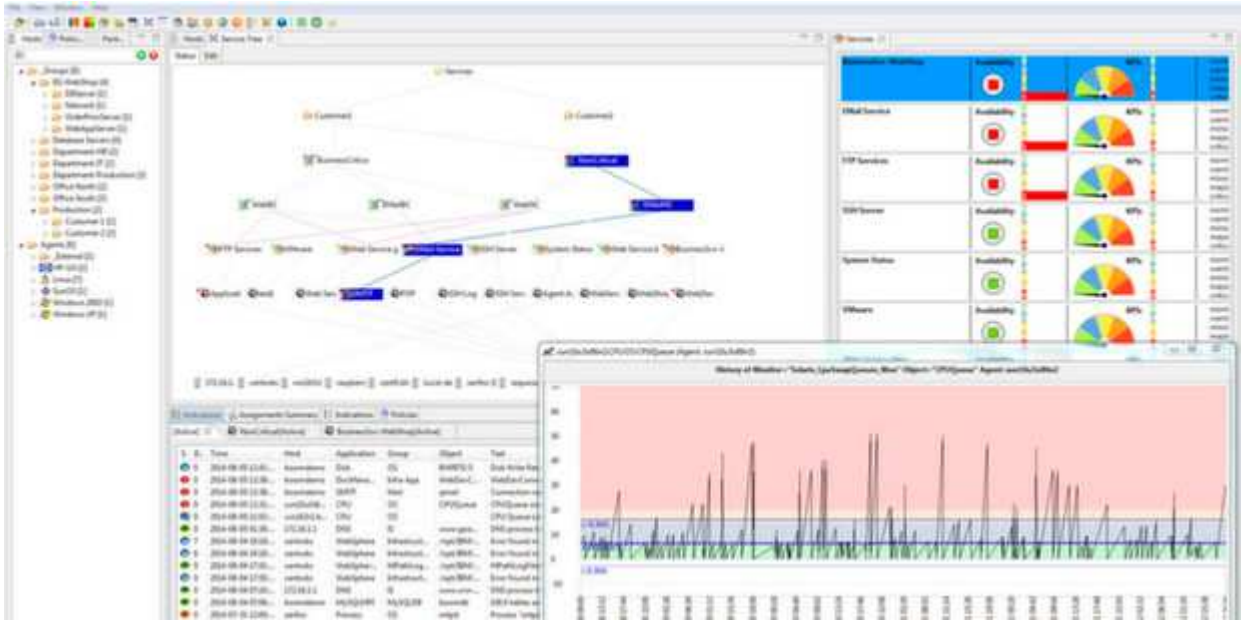
Beim Netzwerk-Monitoring muss der Zuschnitt stimmen

So sieht sie aus, die optimale Monitoring-Lösung!

12.08.14 | Autor / Redakteur: Joachim Hörnle / Andreas Donner



Eine IT-Monitoring-Lösung muss viele Aspekte vereinen und über eine offene Architektur verfügen; hier die Lösung MIDAS Boom (Bild: Blue Elephant Systems)

Unternehmen sind mehr denn je auf eine stets funktionierende IT angewiesen. Kommt es zu Verfügbarkeits- oder Performance-Einbußen, müssen die Ursachen schnellstens erkannt und beseitigt werden. Dies ist die Domäne des IT-Monitoring. Doch welche Monitoring-Tools sollte man einsetzen und welche Funktionen sollten diese Werkzeuge mitbringen?

Das Netzwerk-Monitoring muss nicht nur zur Funktionsverfügbarkeit von Netzwerkkomponenten, Systemen, Anwendungen bzw. in der Summe kompletter IT-Prozessketten und IT-Services beitragen. Das Tool-Set sollte auch aus dem Blickwinkel der Wirtschaftlichkeit und Rentabilität für das Unternehmen aufgehen.

Architektur im Fokus

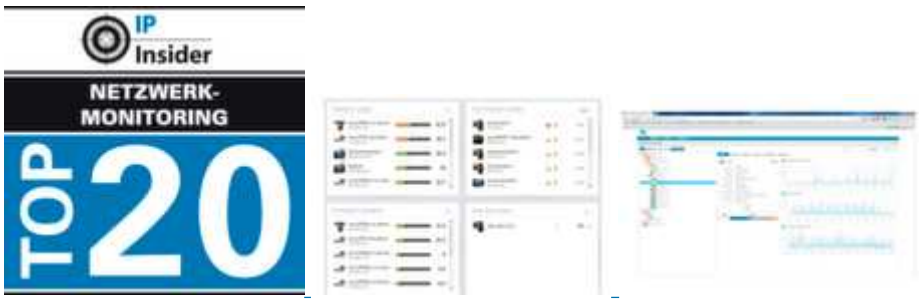
Bevor die Entscheider ihr Augenmerk auf die Einzelwerkzeuge und ihre Funktionen richten, sollten sie ihren Fokus auf die Architektur der Monitoring-Lösung legen. Zumal die Architektur nicht nur die Leistungsfähigkeit, sondern auch die Wirtschaftlichkeit der Monitoring-Lösung prägt. Für den Einsatz empfiehlt sich eine Architektur, die sich aus Operations-Management-Servern, intelligenten dezentralen Agenten, Monitoring-Stationen mit Benutzerschnittstellen und einer zentralen Konfigurations-Management-

Datenbank zusammensetzt.

Das Operations-Management sollte Java-basierend sein. Diese technologische Ausrichtung unterstützt die Herausbildung automatisierter IT-Prozessketten und darauf aufsetzend von IT-Services am besten. Außerdem sollte das Unternehmen bei der Monitoring-Lösung der Wahl auf eine plattformunabhängige Auslegung drängen. Nur unter dieser Voraussetzung kann das Unternehmen seine Operations-Management-Server sowie die Konfigurations-Management-Datenbank auf beliebigen Servern mit Betriebssystemen wie Windows, Linux, Solaris oder AIX platzieren, und somit kostensparend bereits vorhandene Server verwenden.

Plattformunabhängigkeit zahlt sich für das Unternehmen außerdem in einer geringeren Hersteller- und Produktabhängigkeit sowie in mehr Investitionsschutz aus. So ist das Unternehmen bei einer plattformunabhängigen Monitoring-Lösung auch künftig frei, was die Positionierung von Operations-Management-Servern und der Konfigurations-Management-Datenbank auf Rechnern mit unterschiedlichen Betriebssystemen betrifft.

TOP 20 MONITORING-TOOLS



Fotostrecke starten: Klicken Sie auf ein Bild (21 Bilder)

Operations-Management-Server: Entscheidend für Performance und Skalierbarkeit

Die Operations-Management-Server übernehmen nicht nur die Filterung und Weiterleitung von Events und steigern so die Performance. Über sie kann das Unternehmen auch seine Monitoring-Architektur beliebig skalieren und somit flexibel herausbilden. Je nachdem, wo die einzelnen Operations-Management-Server angesiedelt werden, kann die Monitoring-Architektur nach Bedarf organisiert und ausgerichtet werden.

Eine Zentralisierung der Monitoring-Lösung ist ebenso möglich wie die Delegation von Monitoring-Leistungen an interne Fachabteilungen oder die Ansiedelung der kompletten Monitoring-Funktionalitäten an einem beliebigen Ort innerhalb des Unternehmensradius in Form eines Expertenzentrums. Oder das Unternehmen positioniert Operations-Management-Server bei einem externen IT-Dienstleister, damit dieser Monitoring-Leistungen ganz, teilweise oder zeitweise übernehmen kann.

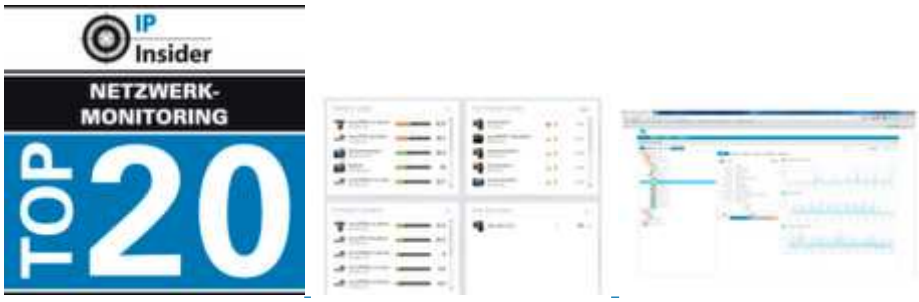
Der Operations-Management-Server ist außerdem entscheidend für die Qualität und Wirtschaftlichkeit der Monitoring-Leistungen, sofern der Hersteller darauf vorgefertigte Konfigurationen hinterlegt hat. Sie können ad hoc oder nur mit geringen Anpassungen eingesetzt werden. Besonders wichtig sind vorgefertigte Konfigurationen zur Überwachung von Systemressourcen, Syslogs, System- und Applikations-Logfiles, SNMP Management Information Bases (MIBs), SNMP Traps, für Windows-Management-Instrumentation-Monitoring (WMI) und für die Überwachung von Windows Event Logs bis hinauf von IT-Prozessen und IT-Services.

weiter mit: Dezentrale Agenten: Auf die Intelligenz kommt es an

Dezentrale Agenten: Auf die Intelligenz kommt es an

Die dezentralen Agenten als Zulieferer und Empfänger der Operations-Management-Server sollten dazu in der Lage sein, nicht nur die empfangenen Events vorzuverarbeiten, sondern sie auch gezielt weiterzuverarbeiten. Dazu müssen diese Agenten mit Monitoring-Fähigkeiten aufwarten: autarker Anstoß einer verteilten Verarbeitung, First Level-Korrelationen mit Event-Verdichtung, selbsttätige Bewertung der Korrelationsergebnisse und zwischenzeitliches Puffern der Daten. Ganz wichtig: Diese integrierten Monitoring-Funktionen können auch für den Fall einspringen, dass die zu überwachenden Netzwerkkomponenten, Systeme und Anwendungen selbst über keinen Erfassungsagenten verfügen.

TOP 20 MONITORING-TOOLS



Fotostrecke starten: Klicken Sie auf ein Bild (21 Bilder)

Wichtig für ein professionelles Monitoring ist auch die Anzahl der Management-Plug-ins (MPIs), die die dezentralen Agenten beisteuern. Sie werden dazu gebraucht, um spezifische Anwendungen und Services in die Event-Verarbeitung, -Verdichtung und -Auswertung einzubeziehen. MPIs für die eingesetzten Betriebssysteme, zur Messung der Verfügbarkeit und Performance von Internet Services (FTP, HTTP, LDAP, NTP, POP3, Radius, SFTP, SMTP, SSH) sowie für Oracle, Microsoft Exchange, Ganglia for Hdoop, Cluster/Service-Monitoring, SAP und Web Application Server wie Tomcat sollten keinesfalls fehlen.

Passgenau dazu: Die Monitoring-Stationen

Zur Intelligenz der dezentralen Agenten und Operations-Management-Server muss die Ausrichtung der Monitoring-Stationen mit den Benutzerschnittstellen passen. Die Oberflächen müssen so beschaffen sein, dass das Bedienungspersonal zu keiner Zeit den Überblick über die problemträchtigen Events und die dazugehörigen Bewertungsergebnisse verliert, um von hier aus durch Umkonfigurationen schnell und gezielt eingreifen zu können.

Wesentlich erleichtert und beschleunigt werden die Umkonfigurationen, wenn die Monitoring-Stationen rollenbezogen arbeiten. Anhand von Rollen wird ausgewiesen, welcher Benutzer welche Zugriffsrechte auf welche Komponenten, Systeme, Anwendungen, Prozesse und Services hat und welche dezentralen Agenten entlang der Prozess- und Servicekette beteiligt sind.

So vorab informiert, kann das Bedienpersonal heilende Konfigurationen, sofern nicht vorkonfiguriert, bedarfsnah erstellen und die Konfigurationen schnell und gezielt den betroffenen IT-Elementen zuweisen.

Unverzichtbar für ein professionelles Monitoring an den Stationen sind darüber hinaus offene Application Programming Interfaces (APIs), um darüber die anwenderspezifischen Monitore zu integrieren. Solche APIs schützen nicht nur die Investitionen in bestehende Monitoring-Stationen. Sondern darüber können auch an diesen Monitoren Event-Texte frei erstellt und für den Einsatz in den dezentralen Agenten Schwellenwerte, Erfassungsintervalle, Kritikalitätsstufen, Inaktivitätszähler und Attribute flexibel festgelegt werden. Darüber hinaus sollten die Ausgaben der anwenderspezifischen Programme sowie bestehender Systemwerkzeuge reibungslos in die neue Monitoring-Lösung überführbar sein, ohne dass dafür zeit- und kostenaufwendig Skripts entwickelt werden müssen.

Konfigurations-Management-Datenbank: Schnelle Reaktion ist alles

Die Konfigurations-Management-Datenbank wird nicht nur als Hinterlegungsort für die Konfigurationen, einschließlich der vorgefertigten Konfigurationen, gebraucht. Von hier aus werden auch die Konfigurationen via Operations-Management-Server auf die dezentralen Agenten geladen.

Sind in dieser Datenbank Systemrollen, so genannte Assignment Groups, hinterlegbar, trägt dies zusätzlich zu schnellen, gezielten und wirtschaftlichen Reaktionen bei Störungen innerhalb der IT sowie auf Prozess- und Serviceebene bei. Mittels einer Assignment Group kann die Überwachungsform für bestimmte Systemkonstellationen festgelegt werden. Außerdem trägt die Kombination aus Systemrolle und dazugehörigen Konfigurationen dazu bei, dass via Monitoring-Konsole potenzielle Probleme schneller erkannt und Umkonfigurationen ad hoc und gezielt durchgeführt werden können.

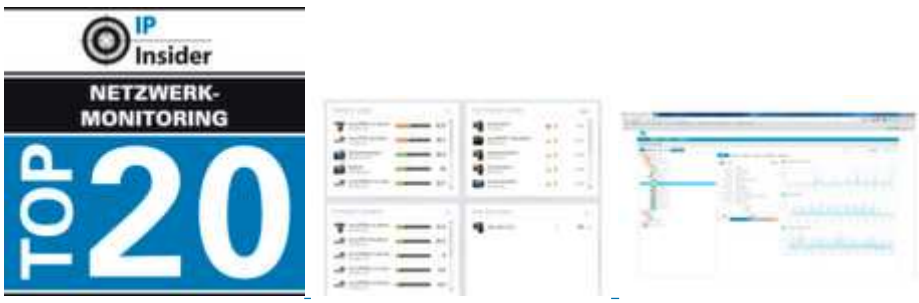
Leistungsfähige Monitoring-Lösungen halten für schnelle und wirtschaftliche

Reaktionen im Problemfall hunderte vorgefertigter Konfigurationen vor. Innerhalb der Konfigurations-Management-Datenbank von MIDAS boom von Blue Elephant Systems sind dies bspw. mehr als 500 für unterschiedliche Netzwerkkomponenten, Systeme und Anwendungen sowie für IT-Prozesse und IT-Services.

Offene APIs und Command Lines machen es möglich, dass auch Konfigurationen für IT-Prozesse und IT-Services in Systemrollen einbezogen werden können. Mit der Neuanlage einer Netzwerkkomponente, eines Systems, einer Anwendung, eines IT-Prozesses oder eines IT-Services oder der Neuzuordnung einer Anwendung, eines Prozess- oder Serviceabschnitts werden anhand der Systemrolle alle zusammengehörigen Konfigurationen zusammengefasst und die Einzelkonfigurationen über ein integriertes Workflow-System an die zuständigen dezentralen Agenten übertragen.

Auf diese Weise wird sichergestellt, dass die dezentralen Agenten, zuständig für die jeweiligen IT-Elemente, Prozess- oder Serviceabschnitte, stets mit den richtigen, aktuellen und vollständigen Regeln, Skripten und Programmen arbeiten.

TOP 20 MONITORING-TOOLS



Fotostrecke starten: Klicken Sie auf ein Bild (21 Bilder)

Lizenzierung

Wesentlichen Einfluss speziell auf die Wirtschaftlichkeit des Monitoring-Einsatzes hat auch die Preis- und Lizenzpolitik des Herstellers. Insbesondere die großen Hersteller von Monitoring-Lösungen tendieren dazu, neben einer strikten Plattformabhängigkeit und Herstellerbindung, ihre Offerten viel zu teuer auszulegen. Mit diesen hohen Einstiegskosten rückt für Anwender dieser Monitoring-Toolsets eine Amortisierung in weite Ferne, sofern diese Schwelle für sie überhaupt erreicht ist.

Zusätzlicher Push fürs Monitoring durch SDN und OpenFlow

Durch Software-Defined Networking und Protokolle wie OpenFlow wird Monitoring für Unternehmen noch wichtiger. Beide Trends verstärken nicht nur die Dynamik innerhalb der IT, sondern sie generieren darin auch zusätzliche Single Points of Failures. Demzufolge sollten auch die Controller und Forwarder unbedingt ins Monitoring einbezogen werden, um ständig ihre Verfügbarkeit und korrekte Funktionsweise

automatisiert zu überwachen und ihre Events bei Bedarf einer Analyse zu unterziehen.


Joachim Hörnle (Bild: Blue Elephant Systems)

Fazit

„Drum prüfe, wer sich ewig bindet“, ob er bei alternativen und kleineren Herstellern nicht eine bessere, herstelleroffenere und in der Anschaffung deutlich günstigere Monitoring-Lösung findet. Je nach Wahl des Herstellers sind Einsparungen allein bei den Anschaffungskosten von bis zu 80 Prozent durchaus möglich.

Über den Autor

Joachim Hörnle ist Geschäftsführer von Blue Elephant Systems.