

# Den Fehler finden, bevor der Anwender ihn bemerkt

MARTIN KLAPDOR\*

Mangelhafte Antwortzeiten geschäftskritischer Applikationen informiert schnell zu finden ist oft ein Problem. Dies scheitert oft an der fehlenden Integration zwischen Endanwender-Monitoring und herkömmlichen Messmethoden. Ein Lösungsweg besteht im Einsatz eines so genannten Distributed Agent Controller.

➔  
Bevor Endanwender unter schlechten Antwortzeiten leiden, sollte man durch Monitoring Abhilfe schaffen.



© Fujitsu Siemens Computers

**WIEN** – Das System- und Netzwerkmanagement orientiert sich zunehmend an nichttechnischen Kriterien. Entscheidend ist letztlich, ob Anwendungen sicher und schnell genug bereitgestellt werden, um geschäftskritische Prozesse am Laufen zu halten. Anstatt von System- und Netzwerkmanagement ist folglich immer mehr von Begriffen wie Business Service Management die Rede. Die technische weicht der Kundenperspektive, aus Gerätemanagement wird Servicemanagement. Endanwender-Monitoring (EAM) ist eine Konsequenz aus dieser Sicht der Dinge.

Anstatt das interne Frühwarnsystem nur auf den Leistungsdaten der Komponenten, Leitungen und Systeme aufzubauen, gehen Unternehmen dazu über, Leistung aus Benutzersperspektive zu messen. Dabei werden Roboter beziehungsweise Transaktionsgeneratoren auf geschäftskritische Dienste angesetzt, für die vertraglich vereinbarte Service Level Agreements (SLA) gelten. In definierten Intervallen führen beispielsweise mehrere PC diese Transaktionen real durch, messen Antwortzeit und Verfügbarkeit, vergleichen diese mit dem SLA und melden Verstöße an eine zentrale Konsole.

Die Vorteile dieses Verfahrens: Die Informationen über SLA-Verstöße sind zentral verfügbar, objektiv nachweisbar und unter standardisierten Bedingungen zustande gekommen. Außerdem bekommt der Administrator Erkenntnisse unter anderem darüber, ob Probleme nur punktuell oder über ganze Geschäftseinheiten oder Niederlassungen hinweg auftreten. Werkzeuge von Herstellern wie Auditec, Segue oder Mercury messen die virtuellen Erfahrungen von Endanwendern in Echtzeit. Im Idealfall können damit Probleme behoben werden, bevor reale Anwender

unter schlechten Antwortzeiten leiden. Das ist aber nur möglich, wenn auch die Fehlerursache möglichst schnell herausgefunden und behoben wird. Hier beginnen aber die Probleme: der Administrator steht vor der Herausforderung, ein Resultat zu haben, dessen Ursache er nicht kennt. Zwar hat jedes größere Unternehmen zusätzlich eine Reihe von Messgeräten und Agenten im Einsatz – aber die eigentliche Schwierigkeit besteht darin, den Zusammenhang zwischen Endanwendermessung und den Messwerten der Netzwerke, Komponenten und Anwendungen herzustellen. Performance-Probleme sind oftmals nicht auf isolierte Ursachen wie zum Beispiel zu geringe Bandbreite zurückzuführen. Vielmehr sind es häufig komplexe Problemkonstellationen, die aus der Interaktion zwischen Netzwerk, Netzkomponenten, den verschiedenen Anwendungsschichten und der Programmlogik resultieren. Es gilt also, eine ganzheitliche Sicht auf die IT-Infrastruktur zum Zeitpunkt des Endanwenderalarms zu bekommen.

Bei maschinell durchgeführtem EAM ist das aber wegen der Unvorhersehbarkeit eines Alarms extrem schwierig. Vor allem bei Störungen, die nicht dauernd und regelmäßig, sondern nur sporadisch auftreten, ist es fast unmöglich, die wahre Wurzel des Übels ausfindig zu machen – denn um dies zu erreichen, müssten alle Netzwerk-, Komponenten- und Systemmesswerte für genau den Zeitpunkt derjenigen Transaktion vorhanden sein, die den Alarm verursacht hat. Häufig werden zum Beispiel Link-Auslastungen in Intervallen von fünf bis 60 Minuten ausgewertet – bei einer Transaktions-

dauer von einer Minute oder kürzer ist die Wahrscheinlichkeit groß, dass der Zeitpunkt des Alarms nicht in der Statistik auftaucht.

Eine automatische Synchronisation der verschiedenen Messungen ist ihrerseits mit mehreren Problemen verbunden. Das Unternehmen müsste dazu Werkzeuge von nur einem einzigen Hersteller einsetzen und spezielle Software einsetzen, um die Daten in einer Oberfläche zusammenzuführen. Aber auch, wenn eine Synchronisation von Endanwender-, Netzwerk- und Systemmessungen gelingt, scheitert das Verfahren häufig an der unterschiedlichen Messgranularität. Das heißt: die Messwerte sind zwar synchron, beleuchten aber verschiedene Ebenen und Perspektiven, so dass eine integrierte Sicht auf die Transaktion unmöglich wird. Das kann zu dem Effekt führen, dass das CPU-, Router- und Netzwerk-Monitoring keine Probleme anzeigen, während das EAM Alarm schlägt.

## TRANSAKTIONSBEZOGENE PAKETAUFZEICHNUNG

Eine mögliche Lösung des Problems besteht im Einsatz eines so genannten Distributed Agent Controller (DAC), einer Software, die die »Spur« einer definierten Transaktion über mehrere Tiers hinweg verfolgt und archiviert. Die Agenten werden auf allen beteiligten Tiers/Servern installiert und vom DAC gleichzeitig gestartet und wieder beendet. Aufgezeichnet werden dabei Netzwerk-Traces, die einzelne diskrete Pakete enthalten und dadurch Aussagen über Ende-zu-Ende-Verhalten von Transaktionen ermöglichen. Die Synchronisation der Paketaufzeichnung mit der Endanwender-

messung ist dabei denkbar einfach, da der DAC über eine Kommandozeilensteuerung direkt von den verwendeten aktiven Endanwendermonitoren gestartet werden kann. Zur Einrichtung dieses Automatismus müssen in das Skript des Transaktionsgenerators nur wenige Zeilen eingebaut werden. Beginnt der Transaktionsgenerator eine Messung, startet er automatisch den DAC, welcher sofort alle Agenten aktiviert. Damit ist das eine Teilproblem gelöst: Der Administrator hat eine Paketaufzeichnung von exakt derjenigen Transaktion, die den Alarm ausgelöst hat. Für die Problemanalyse liegt eine synchrone und durchgängige Informationsbasis mit konsistenter Granularität vor. Zur Problemanalyse werden die Traces anschließend in ein so genanntes Application Characterization Environment (ACE) importiert. Dieses Werkzeug kann mithilfe einer Vielzahl von Analyse- und Visualisierungstechniken den »Charakter« einer Transaktion darstellen, so dass der Administrator auf die Fehlerursachen schließen kann. Basis hierfür ist zum einen die Möglichkeit, die aufgezeichneten Traces zu synchronisieren und somit das exakte Laufzeitverhalten einer Transaktion darzustellen. Zum anderen ist das Analysetool in der Lage, die Kommunikationsprotokolle zu decodieren. Das heißt: nicht nur die von einem Paket jeweils adressierten Ports können bei der Analyse berücksichtigt werden, sondern auch die dabei durchgeführten Operationen auf Applikationsebene. Sogar der Inhalt einzelner SQL-Statements lässt sich auf diese Weise eruieren. [.]

\* Der Autor ist Senior Applications Engineer bei Opnet Technologies.