Bild: fotolia.com

IT-Management mit Augenmaß

Ob innerhalb des eigenen Unternehmens oder im Zusammenspiel mit externen Clouds: Das Geschäft steht und fällt mit der Betriebssicherheit der IT. Um die zu garantieren, ist ein umfassendes IT-Management gefordert, das vom Netzwerkkomponenten- und System- über das Anwendungs- bis hinauf zum Service-Management reicht. Doch „umfassend“ allein reicht nicht aus. Die Leistungsträger innerhalb der IT-Management-Architektur müssen ein gehöriges Maß an Intelligenz mitbringen, damit in jeder Einsatzkonstellation die IT immer verlässlich funktioniert. Schließlich muss die Gesamtlösung wirtschaftlich, das heißt hinsichtlich der Anschaffungs- und laufenden IT-Betriebskosten, vertretbar sein.

Die generelle Architektur eines leistungsfähigen und zwischen allen beteiligten Elementen wohl abgestimmten IT-Managements umfasst: Event-belieferte und -verarbeitende dezentrale Agenten, Monitoring-Stationen mit User-Interfaces, Operations-Management-Server und eine Konfigurations-Management-Datenbank. Mit Blick auf das Service-Management kristallisiert sich die Notwendigkeit eines Java-basierenden Operations-Managements heraus. Wichtige Stellschrauben, in diesem Fall für ein für das Unternehmen wirtschaftliches IT-Management, werden bereits mit einer ausgewiesenen Plattformunabhängigkeit gestellt. Anwender suchen sie bei IT-Management-Größen wie IBM, Microsoft oder HP vergeblich. Sie favorisieren jeweils für den IT-Management-Einsatz ihre eigenen Server-Plattformen und proprietären Technologien. Können hingegen die Operations-Management-Server und die Konfigurations-Management-Datenbank auf beliebige Plattformen platziert werden, beseitigt dies nicht nur die Herstellerabhängigkeit. Es stärkt auch den Investitionsschutz und es schont das Budget. Denn diese Leistungsträger können jetzt schon und auch künftig auf bereits vorhandenen Servern positioniert werden.

Dezentrale Agenten mit gehöriger Intelligenz

Dezentrale Agenten der neuen Generation sollten über autonome Monitoring-Fähigkeiten verfügen, damit sie gleich zwei Rollen übernehmen können: die klassische Überwachung sowie den Anstoß einer verteilten Verarbeitung von Events. Zur verteilten Verarbeitung sollten das Handling, die Bereitstellung und Ausführung von Monitoring-Funktionalitäten, First-Level-Korrelationen mit Event-Verdichtung, die Bewertung der Korrelationsergebnisse und bei Bedarf das Puffern von Daten gehören. Die Übernahme von Monitoring-Funktionalitäten beispielsweise, ist gefordert, wenn die zu überwachenden Netzwerkkomponenten, Systeme, Anwendungen oder Services lokal über keinen installierten Erfassungs-Agenten verfügen.

Leistungsfähige dezentrale Agenten sind mittlerweile in der Lage, hunderttausende an Events zu konsolidieren und auf diese Weise optimal für die Folgeschritte „First-Level-Korrelation“ und „Bewertung der Korrelationsergebnisse“ vorzubereiten. Wichtig für die zentralen Agenten ist auch das Angebot zusätzlicher Management-Plug-ins (MPIs). Sie werden als Ergänzung gebraucht, um darüber die Überwachungs- und Steuerungsfunktionalität für spezifische Anwendungen und Services zu erweitern. Im ein-

zelnen sollten zum Set an MPIs gehören:

- OS-MPIs,
- Internet-Services-MPIs für die Messung der Verfügbarkeit und Performance von Internet-Services (FTP, HTTP, LDAP, NTP, POP3, Radius, SFTP, SMTP, SSH) sowie
- weitere MPIs, so für Oracle, IBM-DB2, Microsoft-Exchange, Ganglia for Hadoop, Cluster/Service-Monitoring, SAP und Web-Application-Server wie Tomcat.

Bedarfsgerechter Zuschnitt der Monitoring-Stationen

Auch die Monitoring-Stationen mit ihrem User-Interface sollten ein Höchstmaß an Intelligenz aufweisen, damit kein wichtiges Ereignis innerhalb der IT übersehen wird und bei Bedarf schnell durch Umkonfiguration reagiert werden kann. Eine rollenbasierende Ausrichtung der Monitoring-Stationen – Welcher Nutzer darf was einsehen und tun? – erleichtert die Erstellung und Verteilung von Konfigurationen erheblich. Außerdem schärft diese rollenbasierende Ausrichtung den Überblick über die Gesamtinstallation an dezentralen Agenten und Monitoring-Stationen mit den jeweils daran angeschlossenen Nutzern. Das liegt daran, dass Anwender mit gleichen Tätigkeitsanforderungen in einer Rolle zusammengefasst sind. Werden offene APIs (Application-Programming-Interfaces) für die Integration anwenderspezifischer Monitore unterstützt, können Event-Texte, Schwellenwerte, Erfassungsintervalle, Kritikalitätsstufen, Inaktivitätszähler und weitere wichtige Attribute beliebig konfiguriert werden.

Außerdem sollten die Entscheider darauf achten, dass auch die Ausgaben von Systemwerkzeugen wie Windows-Tasklist, Netstat, Unix-Top und -Sar sowie anwenderspezifische Programme für das Monitoring herangezogen werden können, ohne dass dafür Skripte entwickelt werden müssen. Das zahlt sich für das Unternehmen sowohl in punkto schnelle Inbetriebnahme und hohe Leistungsfähigkeit als auch in hohe Wirtschaftlichkeit der Monitoring-Lösung aus. Können bestehende Monitoring-Systeme einschließlich der verwendeten Regeln (Policies), Skripte und Programme eingebunden werden – sei es mit oder ohne Konvertierung –, verbessert dies zusätzlich die Leis-tungsfähigkeit (umfassende Überwachung und Steuerung) und Wirtschaftlichkeit der Monitoring-Gesamtlösung.

Operations-Management-Server mit dezentralen Agenten

Innerhalb der IT-Management-Lösungen, beispielsweise „MIDAS boom“ von Blue Elephant Systems, übernehmen Operations-Management-Server im Zusammenspiel mit den dezentralen Agenten die Filterung und intelligente Weiterleitung von Events. Diese Kombination eröffnet dem Unternehmen unterschiedliche Einsatzszenarien:

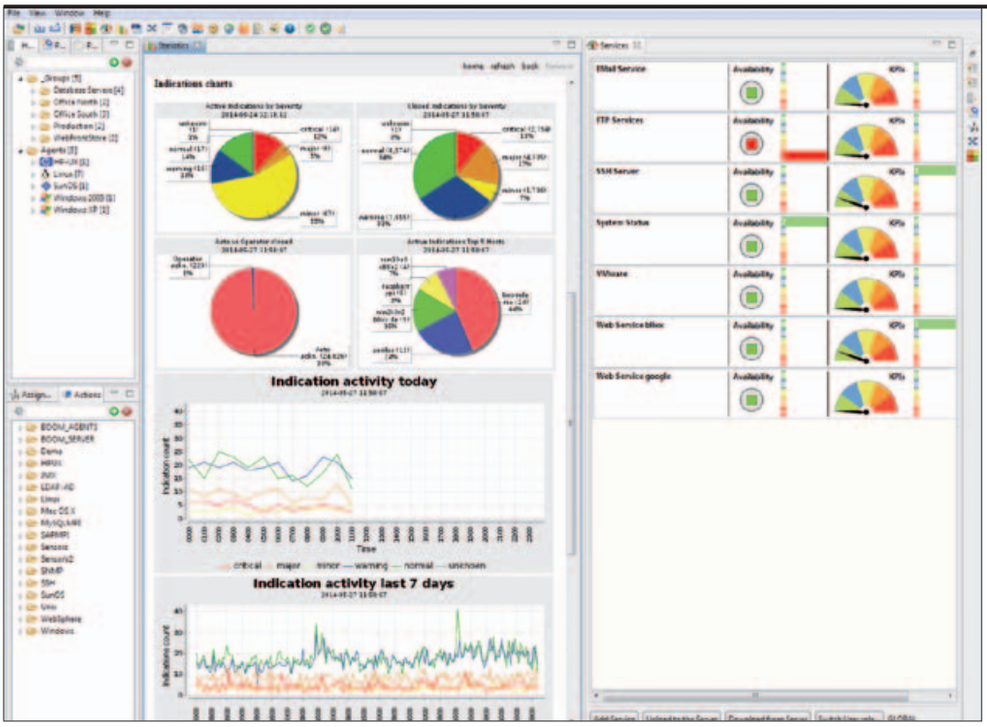
- zentralisiertes Management von verteilten Organisationen und Netzwerken,
- Herausbildung eines Expertisen-Zentrums, das innerhalb des Aktionsradius an einem beliebigen Ort angesiedelt sein kann,
- Einsatz von Abteilungs-Servern als Event-Weiterleitungsinstanzen sowie
- zeitweise Delegation von Management-Leistungen an externe IT-Dienstleister.

Zudem birgt diese Kombination aus Operations-Management-Server und dezentralen Agenten für das Unternehmen den Vorteil in sich, dass die IT-Management-Gesamtlösung gut skalierbar ist, somit Performance-Verlusten im IT-Betrieb durch Lastverteilung wirkungsvoll entgegengewirkt werden kann. Wichtig ist überdies , dass der Operations-Management-Server auf so viel wie möglich vorgefertigte Konfigurationen zurückgreift, die im Bedarfsfall schnell zugewiesen werden können. Beispiele dafür sind vorgefertigte Konfigurationen:

- zur Überwachung von System und Applikations-Logfiles,
- zur Überwachung von Diensten und Prozessen,
- zur Überwachung der Systemressourcen (CPU und Speicherauslastung, freier Plattenplatz, Disk und Netzwerkauslastung),
- zur Überwachung von Windows-Event-Logs, einschließlich Parsing,
- zum WMI- (Windows-Management-Instrumentation-)Monitoring, einschließlich Remote-WMI-Monitorings mittels Unix- und Windows-Agenten,
- zum Syslog-Monitoring, einschließlich Parsing,
- zur Überwachung von SNMP-MIBs (Management-Information-Bases) sowie
- zur Überwachung von SNMP-Traps, einschließlich Parsing.

Die Problemanalyse und -behebung wird beschleunigt, wenn über den Operations-Management-Server Automatismen, vorkonfigurierte Einstellungen, die manuell initiiert werden, sowie vorkonfigurierte manuelle Aktionen ausgelöst werden können. Letzteres erlaubt, im Rahmen des IT-Managements Konfigurationen, Regeln und Aktionen auszurollen und bei Bedarf gezielt zu modifizieren, um auf diese Weise die interne Sicherheitsstrategie besser umzusetzen sowie menschliche Fehlbedienungen auf ein Minimum zu reduzieren. Mittels

Quelle: Blue Elephant Systems



Event-Anzeigen nach Kritikalität, Zustand (aktiv oder geschlossen) und wichtigen Orten der Entstehung. Auch rückwirkende Zeitbetrachtungen – im Verlauf des Tages, innerhalb der letzten sieben Tage – sind möglich, um Problemtrends frühzeitig zu erkennen.

automatischer Aktionen können zusätzliche Diagnoseinformationen direkt bei der Erkennung eines Problems gesammelt und Korrekturen durchgeführt werden.

Der Event-Verarbeitungsmodus des Operations-Management-Servers sollte flexibel einstellbar sein, um das Handling der Events nach Bedarf einrichten zu können. Im Slave-Modus werden die Events mit ihrer Abarbeitung automatisch archiviert. Im Mirror-Modus werden nach ihrer Spiegelung auf dem Quell-Server die Events kontrolliert weitergeleitet. Dabei werden Aktionen wie das Schließen von Tickets automatisch zwischen Quell- und Ziel-Server synchronisiert. Im Master-Modus erfolgt die Weiterleitung der Events als FYI (For-Your-Information/Interest)-Botschaften. In diesem Modus können Kontrollaktionen ausschließlich auf dem Quell-Server ausgeführt beziehungsweise durch ihn initiiert werden, beispielsweise die Erzeugung von Backups und die Einrichtung weiterer Kontroll-Server. Auch Aktivitäten wie E-Mails zum Schließen von Tickets können bei diesem eingestellten Modus nur vom oder mit Erlaubnis des Quell-Servers erledigt werden.

Zentrale Event- und Performance-Datenbank

In einer zentralen Datenbank werden die Events, Anmerkungen und der zugehörige Bearbeitungsstatus (offen, zugewiesen, geschlossen) gespeichert. Die Auswertung dieser Information ermöglicht es, Bereiche mit hohem Arbeitsaufwand zu identifizieren und das Monitoring nach Bedarf zu optimieren. In diesem zentralen Repository werden auch die erfassten Performance-Werte hinterlegt. Sie sollten als Performance-Graphe darstellbar sein. Über diese grafische Darstellung tritt die Performance einzelner Netzwerkkomponenten, Systeme, Anwendungen und Services, ebenso wie ihre Beziehungen untereinander, an den Monitoren plastisch vor Augen. Ebenso erlaubt die Langzeitauswertung der Performance-Werte die Erkennung von Trends und bildet so die Grundlage für Kapazitätsplanungen.

Konfigurations-Datenbank: schnell erkennen und eingreifen

Die Konfigurations-Management-Datenbank ist nicht nur wichtig als Hinterlegungsort für vorgefertigte Konfigurationen, auf die die Operations-Management-Server zurückgreifen. In der Konfigurations-Management-Datenbank sollten System-Rollen (Assignment-Groups) hinterlegt sein. Über sie kann festgelegt werden, wie beispielweise ein Linux-System mit Apache und Oracle-Datenbank oder ein Windows-Exchange-Server überwacht werden soll. Die vorgefertigten Konfigurationen und System-Rollen, vom Hersteller hinterlegt in diesem Repository, sind die wesentlichen Garanten für eine schnelle Problemerkennung und schnelle Eingriffe, um innerhalb der IT auftretenden Problemen gezielt entgegenzusteuern. Mit der Zahl der vorgefertigten Konfigurationen, die ad hoc eingesetzt werden können, steigt zudem die Wirtschaftlichkeit des IT-Management-Einsatzes. Zum Ausliefe-

rungsumfang von „MIDAS boom“, beispielsweise, gehören mehr als 500 solcher Konfigurationen allein für eine eingehende Überwachung von Netzwerkkomponenten, Systemen, Anwendungen und Services.

Eröffnet das IT-Managementsystem der Wahl zusätzlich Konfigurationen per API oder Command-Line, können System-Rollen (Assignment-Groups) auch integriert in übergeordneten Prozessen konfiguriert werden. Sobald innerhalb der Konfigurations-Datenbank ein System angelegt oder die Anwendung auf einem System geändert wird, wird automatisch durch das kombinierte Konfigurations-/Workflow-System die passende System-Rolle zugewiesen. Das System stellt automatisch sicher, dass die dezentralen Agenten immer mit dem richtigen, vollständigen und aktuellen Satz von Regeln, Skripten und Programmen arbeiten. Wenn das Monitoring-System dies nicht gewährleistet, ist seine Funktionsfähigkeit nicht sichergestellt. Sie müsste in diesem Fall mit hohem manuellen Aufwand hergestellt werden.

Auf die Wirtschaftlichkeit achten

Der Einsatz einer professionellen IT-Management-Lösung scheitert oftmals daran, dass die Preise oder Lizenzen dafür gerade von den großen Herstellern viel zu teuer ausgelegt werden. Das verleitet viele Unternehmen zum Sparen am falschen Ende, dem IT-Management, und damit an der IT-Betriebssicherheit. Zu komplexe Architekturen, dazu die Plattformabhängigkeit, treiben die Kosten für die IT-Management-Systeme der großen Hersteller, damit auch die IT-Betriebkosten der Unternehmen, zusätzlich in die Höhe.

Umgekehrt führen eine moderatere Vertriebspolitik, eine weniger komplexe IT-Management-Architektur und ein plattformunabhängiger Einsatz zu deutlich niedrigeren Anschaffungs- und IT-Betriebskosten. Auch darauf sollte das Unternehmen genau achten, bevor es die Entscheidung für das eine oder andere IT-Management-System trifft. Einsparungen bei den Anschaffungskosten von bis zu 80 Prozent sind möglich.

Wie bereits gesagt: Die Gesamtlösung muss für das Unternehmen wirtschaftlich, das heißt hinsichtlich der Anschaffungs- und laufenden IT-Betriebskosten, vertretbar sein, schon allein um mit Blick auf das eigene Budget bei der IT-Betriebssicherheit keine Kompromisse machen zu müssen.

Joachim Hörnle,
Geschäftsführer von Blue Elephant Systems