Auf dem Silbertablett

Hohe Verfügbarkeit durch kontinuierliches Netz-Monitoring

Kai-Oliver Detken

Die IT-Infrastruktur ist für Anwender unsichtbar im Hintergrund verfügbar und macht meistens nur auf sich aufmerksam, wenn sie mal nicht funktioniert. Dabei sind die Anforderungen an die Verfügbarkeit heute selbst in kleineren Unternehmen so hoch, dass dieses Szenario eigentlich gar nicht erst auftreten dürfte. Zusätzlich müssen IT-Infrastrukturen technisch immer auf dem neuesten Stand gehalten werden, ohne dabei trotz vielfältiger Zeitprobleme die Dokumentation zu vernachlässigen. Die kontinuierliche Überwachung aller Netzkomponenten stellt daher ein wichtiges Kriterium dar, um eine möglichst hohe Verfügbarkeit erreichen zu können. Monitoring-Systeme sind dabei eine große Hilfe. Gleichzeitig schaffen sie eine höhere Anwenderzufriedenheit und helfen, den Dokumentationsgrad auf einem hohen Niveau zu halten.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Als Basisanforderung für ein effizientes Netzmanagement ist die einfache Verwaltbarkeit zu nennen. Folgende Unterteilungen, die auch nach ISO über das FCAPS-Modell (FCAPS – Fault, Configuration, Account, Performance, Security) definiert wurden, sind dabei zu berücksichtigen:

- Fault Management: Erkennen von Fehlern; Protokollieren, Melden und evtl. Beheben von Fehlerzuständen;
- Configuration Management: Inbetriebnahme und Konfiguration aller aktiven Komponenten innerhalb eines Netzes;
- Accounting Management: Sammeln und Auswerten von Accounting-Daten zur Rechnungsstellung oder Statistikerzeugung;
- Performance Management: Sammeln und Aufbereiten von Statistiken von aktiven Komponenten bez. Schwellwerte, Service Levels usw.;
- Security Management: Authentifizierung und Autorisierung von Benutzern, Verschlüsselung und Zugriffssicherheit;
- Planning Management: Analyse von Trends;
- Asset Management: Inventarisierung der Komponenten, aller Geräte und Einbeziehung des administrativen Personals.

Eine Monitoring-Lösung besteht aus einer Teilmenge dieses Modells, da die Überwachung und Eskalation von auftretenden Fehlern im Vordergrund steht und nicht die Konfiguration. Die Berücksichtigung aller ISO-Bereiche würde zwar ein optimales Netzmanagement beinhalten und die höchste Flexibilität und IT-Sicherheit ermöglichen. Dies kann aber ein einzelnes Tool nicht leisten.

Im Betrieb der meisten Netze – speziell bei Klein- und mittelständischen Unternehmen – wird oft auf ein reaktives Netzmanagement gesetzt. Dies bedeutet, dass der Anwender einen Fehler im Betrieb bemerkt und den Administrator über ihn informiert. Dieser hat dann die Aufgabe, aus der Fehlermeldung des Anwenders die Ursache zu ermitteln und danach umgehend das Problem zu beheben. Analog gilt dies für Überlastverhalten. Dabei sind Fehlerbeschreibungen von Anwendern meistens wenig hilfreich. Für den IT-Administrator ergeben sich damit mehrere Notwendigkeiten, um nicht erst dann reagieren zu müssen, wenn bereits ein Fehler aufgetreten ist. Er muss

- über den Zustand der betriebsrelevanten Dienste auf dem Laufenden sein;
- fundierte Aussagen über die Nutzung der Systeme machen können;
- die Trends in der Nutzung dokumentieren.

Dazu reicht normalerweise ein reines Monitoring-System aus. Entsprechende Netzmanagement- oder Monitoring-Lösungen haben viele Hersteller für ihre Systeme im Portfolio. Allerdings oft mit dem Nachteil, dass sie sich nur für die jeweilige Lösung einsetzen lassen. Interessanter sind daher Tools, die auch ein übergreifendes Monitoring ermöglichen und auf gemeinsame Standards setzen.

Herstellerlösungen

Nicht alle ISO-Bereiche des Netzmanagements sind für ein Unternehmen gleichermaßen relevant. So kann es z.B. bei einer heterogenen Netzumgebung Probleme bei einem einheitlichen Konfigurationsmanagement geben, da jeder Hersteller seine eigenen Tools hierzu anbietet. Es sollten aber Mindestanforderungen berücksichtigt werden können. Diese beziehen sich meist auf das Monitoring eines Netzes, um eine kontinuierliche Überwachung aller aktiven Komponenten unabhängig vom Hersteller ermöglichen zu können. Basis für dieses übergreifende Netzmonitoring ist zumeist das

Simple Network Management Protocol (SNMP), das in Serversystemen und Netzkomponenten gleichermaßen verwendet werden kann.
Durch Netz-Monitoring können Netze und Dienste überwacht und vorausschauend bzw. zeitnah im Fehlerfall

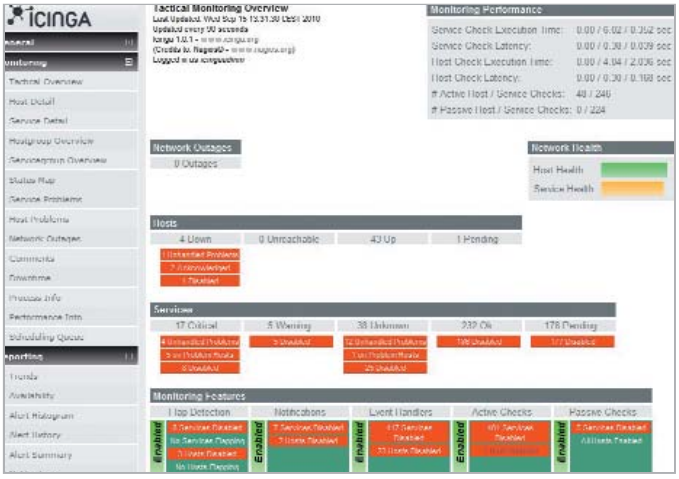

Bild 1: Spezielle Zustandsübersicht mit Hilfe von Icinga-Monitoring

Gegenmaßnahmen ergriffen werden, so dass Teilnehmer im Netz im besten Fall Fehler nicht bemerken. Hinzu kommt, dass ein solches Netz-Monitoring eine Übersicht über das gesamte Netz darstellt – das Netz wird visualisiert. Auch vereinen solche Lösungen gleich mehrere ISO-Bereiche in sich, wie z.B. das Fault- und das Performance-Management.
Als Monitoring-Lösungen stehen unterschiedliche Alternativen zur Verfügung. Hier einige Beispiele:

- Nagios/Icinga: quelloffene Lösung ohne Lizenzkosten, die kontinuierlich weiter entwickelt wird; weist besonders im Bereich Benachrichtigungen und Eskalationsstufen Stärken auf; unterstützt heterogene Netze;
- InterMapper: herstellerspezifische Lösung, die ursprünglich für große Internet Service Provider (ISP) entwickelt wurde; ihre Stärken liegen in der Benachrichtigung von Fehlern und interaktiven Netzübersicht; unterstützt heterogene Netze;
- HP OpenView: Softwareportfolio zum Managen und Überwachen von IT-Infrastrukturen großer Unternehmen; ermöglicht zusätzlich eine zentrale Verteilung von Software auf Clients und Servern; unterstützt heterogene Netze;
- HP Systems Insight Manager: stellt eine kontinuierliche Überwachung der Serversysteme bereit und warnt vor potenziellen Systemfehlern, die zu Ausfällen führen können; Konfigurationsmanagement für Serversysteme möglich; integrierte, automatische Geräteerkennung nicht nur für HP-Systeme; unterstützt heterogene Netze teilweise;
- Enterasys NetSight: Lösung zur Überwachung und Konfiguration von Netzkomponenten; weitere Bestandteile speziell für Enterasys-Komponenten: zentrale Kontrolle für sicherheitsrelevante Netzkomponenten, erweiterte Sicherheitsvorkehrungen, Secure-Networks-Policy-Lösungen; Stärken liegen im Konfigurationsmanagement und in der Unterstützung der IT-Sicherheit.

Der Schwerpunkt von *Nagios* bzw. *Icinga* ist das übergreifende System-/Netzmonitoring. Aktiv wird nicht in bestehende Prozesse eingegriffen. Nagios ist eine modular aufgebaute Softwarelösung, bestehend aus einem Nagios-Kern und Plugins, die die Überwachung von Hosts und deren Diensten durchführen. Neben zahlreichen mitgelieferten und frei verfügbaren Plugins lassen sich diese auch selbst entwickeln und einbinden. Bei Nagios kann exakt eingestellt werden, zu welchem Zeitpunkt ein Fehler oder eine Schwellwertüberschreitung vorliegt und ob man eine Mitteilung darüber per SMS, E-Mail und/oder Telefon erhalten möchte. Unabhängig vom Hersteller kann Nagios alle Netzkomponenten und Serversysteme erfassen und überwachen (*Bild 1*). Dies kann sich auch auf Anwendungen wie zum Beispiel Datenbanken herunterbrechen lassen.
Das sehr detaillierte Eskalationsmanagement in mehreren Stufen ist ein Vorteil von Nagios. So muss nicht bei jedem Zwischenfall alarmiert werden, sondern nur, wenn kritische Systeme betroffen sind. Dabei wird zwischen Hosts und Services oder auch zwischen unterschiedlichen Zeiten (Geschäftszeiten, Feierabend, Feiertage) und Mitarbeitern (IT-Administrator, Abteilungsleiter usw.) unterschieden. Eine Dienste- und Topologieübersicht ist ebenfalls über eine Weboberfläche erreichbar. Neben den typischen Netzdiensten wie SMTP, POP3, http, SNMP, NNTP, Ping usw. können Serversysteme genauer untersucht werden. Aktive Netzsysteme wie Router und Switche kann man ebenso mit einbeziehen wie Temperatur- und Feuchtigkeitssensoren. Neben den mannigfaltigen Monitoring-Lösungen bietet Nagios bzw. Icinga den großen Vorteil der Lizenzfreiheit (GPL-Lizenz). Icinga ist ein Fork von Nagios, der von einer deutschen Community entwickelt wird. Die Kompatibilität zu Nagios ist aber gewährleistet. Man kann beide Varianten problemlos einsetzen.
Der *InterMapper* ist ein Echtzeit-Netz-Monitoring der Firma Dartware, das eine Überwachung von Windows- und Linux-Diensten sowie allen SNMP-unterstützenden Geräten ermöglicht. Mit einem Subnetz-Scan kann in kurzer Zeit das Netz nach allen verfügbaren Geräten durchsucht werden. Die gefundenen Geräte werden anschließend auf einer Karte angezeigt und können dort so platziert werden, wie sie auch in Wirklichkeit im Raum oder Gebäude aufzufinden sind. Die erstellten Karten können jederzeit exportiert oder importiert werden, so dass eine Echtzeitdokumentation des Netzes und seiner Serversysteme möglich ist.
Durch das Setzen der sog. Probes kann jedes Gerät auf der Karte nach vielen verschiedenen Parametern überwacht werden. Der InterMapper liefert dafür standardmäßig fast hundert Probes mit, wobei diese auch selbst erstellt werden können. Die Client-Server-Software verfügt über eine intuitiv zu bedienende grafische Benutzeroberfläche, die über einen Geräteausfall sofort grafisch und akustisch unterrichtet. Weiterhin können Benachrichtigungen per E-Mail, SMS, Command-Line-Skripte, Syslog-Meldungen usw. erfolgen.

InterMapper bietet das Importieren von Kundendaten im CVS- oder XML- und das Exportieren im CVS-Format. Die Software ist lauffähig auf allen Java unterstützenden Betriebssystemen. Er ist keine freie Softwarelösung. Die Lizenzkosten werden nach der Anzahl der Geräte gestaffelt.

Der Konfigurations- und Überwachungsmanager *HP OpenView* von Hewlett-Packard ist zur Überwachung von großen IT-Infrastrukturen und zur Softwareverteilung gleichermaßen geeignet. Für die Netzüberwachung stellt SNMP die zentrale Komponente dar. Es können Firewalls, Switche, Router usw. mit Hilfe dieses Protokolls in das Monitoring eingebunden werden. Weitere Smart-Plugins (SPI) für die Überwachung von Routing-Protokollen, HSRP, Multicasting usw. können integriert werden. Die Gesamttopologie wird grafisch dargestellt, ein Alarm-Browser stellt die einzelnen Events und SNMP-Traps dar. Durch das Verknüpfen mit Skripten können ereignisabhängig Aktionen ausgelöst werden. Neben dem Überwachen der Erreichbarkeit der Netzkomponenten werden auch Bandbreitenkapazitäten, der Status von Interfaces, Leitungsfehler, Router-CPUs und Backups überwacht. Weiterhin werden Leistungsdaten gesammelt und grafisch aufbereitet.

Für das Applikations- und Systemmanagement findet eine zentrale Steuerung über den Managementserver statt, die z.B. das Verteilen von Monitorskripten mit Meldungen über den System- und Applikationsstatus an die Agenten auf den einzelnen Systemen beinhaltet. Über eine grafische Benutzeroberfläche können Administratoren diese Meldungen ansehen und ggf. hinterlegte Aktionen starten. Eine Lizensierung findet nach Anzahl der angeschlossenen Knoten statt.

Der *HP Systems Inside Manager* (SIM) beinhaltet Hardware-Fehler-, Konfigurations- und Asset-Management für Serverkomponenten. Das Hardware-Fehlermanagement überwacht z.B. Festplattenausfälle, die so konfiguriert werden können, dass eine automatische Benachrichtigung erfolgt oder ein Skript gestartet wird. Auch lassen sich Diagnosedaten an ein HP-OpenView-System schicken. Bei Ausfall des Betriebssystems kann der Inside Manager direkt auf die ILO-Schnittstelle zugreifen, damit der Fehler remote analysiert werden kann. Innerhalb des Konfigurationsmanagements können Fehler isoliert und Änderungen an der Hard- oder Softwarekonfiguration vorgenommen, Konfigurations-Snapshots verglichen und nicht autorisierte Softwareaktualisierungen erkannt werden. Die Softwarebereitstellung kann zentral gepflegt und ausgerollt werden. Das Asset-Management erkennt automatisch Geräte und andere an das Netz angeschlossene Systeme. Zusätzlich werden relevante Daten zu jedem Gerät erfasst und in benutzerdefinierbaren Berichten zusammengefasst. So erhält man einen besseren Gesamtüberblick über die Komponenten und deren Auslastung.

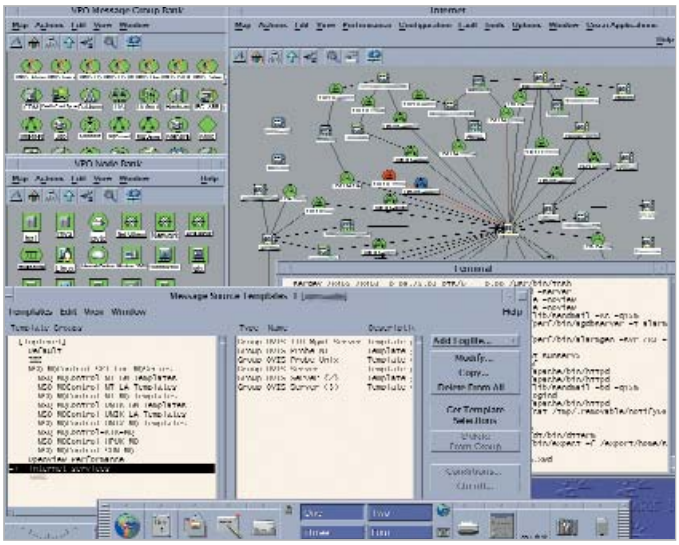

Bild 2: Network Map von HP OpenView

Das System *NetSight* (wurde jüngst in NMS – Network Management System – umbenannt) kann als Konfigurations-Tool für aktive Komponenten von Enterasys eingesetzt werden. Es ist dabei auch in der Lage, das LAN grafisch aufzubereiten. Hierbei werden dann auch netzweite Informationen wie z.B. Spanning Tree, VLANs, Multicast, Geräte und Teilnehmer mit einbezogen. Ebenfalls werden die Policys pro Port über den Policy-Manager überwacht, falls weitere Sicherheitsmaßnahmen wie 802.1x mit eingesetzt werden sollten. Dazu gehören auch die Einbindung von Gästezugängen, Verbreitung regulärer Mandanten und Festlegung von Benutzerrollen. So dürften Administratoren z.B. SNMP, ICMP (Ping) und TFTP nutzen, während normale Mitarbeiter auf Datenbank-, ERP- und Mailsysteme nur Zugriff haben. Client- und Serversysteme können nach DNS-Namen, MAC- oder IP-Adresse gesucht werden. Ein integrierter Inventory-Manager kann zentrale Updates auf Enterasys-Komponenten vornehmen. Bez. der Zugriffssicherheit ist ein ACL-Manager enthalten, der es ermöglicht, Access-Control-Listen zu erstellen und an die Enterasys-Router auszurollen. Es müssten Lizenzkosten pro Knoten und Funktion eingeplant werden.

Fazit

Im Netzmanagementbereich können verschiedene Lösungen eingesetzt bzw. miteinander kombiniert werden. Um für ein Unternehmen die effektivste Lösung auswählen zu können, bedarf es allerdings vorab einer detaillierten Anforderungsanalyse, die auch die vorhandenen aktiven Komponenten (Switche, Router, Server usw.) mit einbeziehen sollte. Daraus resultierend kann eine Abschätzung erfolgen, welches Netzmanagement ausreichend bzw. welche Funktionalität umsetzbar ist.

Aufgrund oft vorhandener heterogener Netzinfrastrukturen bietet sich aber in den meisten Fälle die Kombination mehrerer Netzmanagement- oder Monitoring-Lösungen an. Diese sollten so eingesetzt werden, dass sie sich gegenseitig ergänzen und möglichst keine doppelten Überwachungen ausführen. Nur so erhält der IT-Administrator einen zeitnahen Überblick über alle seine aktiven Komponenten und kann bei Problemen rechtzeitig Maßnahmen ergreifen. Übergreifende Standards sollten unterstützt werden. *(bk)*