

Sonderdruck für MAGELLAN Netzwerke

NETZWERKMANAGEMENT

Administration mit Überblick

Netzwerkmanagement unterstützt den Administrator bei der Lokalisierung von auftretenden Fehlern im Netz und visualisiert auf Knopfdruck den Zustand des Netzwerks. Viele Systeme sind nach dem FCAPS-Modell aufgebaut, also nach Fault-, Configuration-, Accounting-, Performance- und Security-Management gegliedert, wobei nicht alle Lösungen alle fünf Bereiche abdecken und auch nicht abdecken müssen. Denn viele Unternehmen benötigen diesen Funktionsumfang nicht. Oft reichen sogar Freeware-Produkte oder die Elementmanager der Hersteller von aktiven Komponenten.

Im Grunde geht es dabei um die Verwaltung der aktiven Komponenten in LAN und WAN. Doch meist gehören zu den Aufgaben eines Netzwerkadministrators auch Softwareverteilung, System- sowie Service-Level-Management. Bei größeren Unternehmen sind die einzelnen Fachgebiete auf verschiedene Abteilungen verteilt. Die jeweils zuständigen Administratoren sorgen dann für die Überwachung ihrer Komponenten, konfigurieren sie und dokumentieren die jeweiligen Zustände per Report. Dies kann mit einer zentralen Managementlösung, einem Framework, erfolgen, auf das alle zugreifen. Es können jedoch auch für verschiedene Komponenten und Disziplinen unterschiedliche Werkzeuge zum Einsatz kommen, die die IT-Abteilung im besten Falle trotzdem zentral

verwaltet. Dieses Szenario nennt man Umbrella-Management.

ZUSTÄNDIGKEITEN Beim Netzwerkmanagement geht es vornehmlich um die Verwaltung und Pflege der Switches und Router im Netz. Damit ist auch klar, welche Abteilungen und Personen in entsprechende Projekte involviert sein müssen. Doch ist zum Beispiel ein Netzwerkmanagementsystem, das sowohl das LAN als auch das WAN umfasst, zum Scheitern verurteilt, wenn die Administratoren der Router und WAN-Systeme sich weigern, einen Zugriff auf ihre eigenen Systeme zu gewähren. Keine Abteilung lässt sich gern von einer anderen kontrollieren und gibt freiwillig Rechte und Überwachungsmöglichkeiten ihrer Komponenten ab. Um die

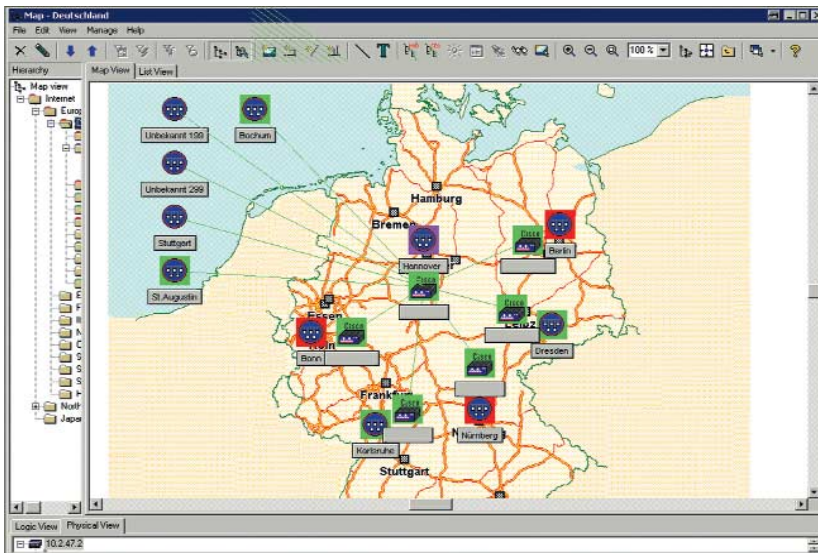
Implementierung eines neuen Managementsystems möglichst reibungslos durchzuführen, sollten folgende Fragen beantwortet werden:

- Wer muss in dieses Projekt involviert werden?
- Wer bestimmt, welches Produkt eingesetzt wird?
- Wer erhält welche Berechtigungen, mit dem Managementsystem zu arbeiten?

Ebenso muss die Projektleitung mit dem Team zu Beginn des Projekts genau festlegen, welche Anforderungen das System erfüllen soll. Nur wenn alle betroffenen Abteilungen zu Beginn des Projekts involviert werden, ist sichergestellt, dass es daran scheitert, dass einzelne Abteilungen ihre Mitarbeit oder den Zugriff auf ihre Systeme verweigern.

FUNKTIONSUMFANG Allen Systemen gemein ist die grafische Darstellung eines Netzwerks, bei denen die IT-Infrastruktur auf so genannten Maps abgebildet wird. Ebenso bieten viele Hersteller die Möglichkeit, wichtige Informationen über ein Webinterface abzurufen. Einige Lösungen arbeiten komplett webbasiert und somit plattformunabhängig.

Klassischerweise bilden die Systeme die IP-Netze ab und pro Map ein oder mehrere IP-Subnetze. Diese Darstellung berücksichtigt jedoch nicht die Abhängigkeiten auf Layer-2-Ebene des OSI-Modells. So kann etwa ein unbeantwortetes Ping auf einen Server häufig keinen Aufschluss darüber geben, warum der Server nicht erreichbar ist. Deswegen haben die Hersteller von Netzwerkmanagementsystemen ihre Software um Layer-2-Intelligenz erweitert. Diese Systeme erkennen, über welche Ports oder welche Schnittstelle die Router, Swit-



Das deutschlandweite Netz eines Unternehmens mit allen Router-Verbindungen, erstellt mit Realtech The Guard!
Quelle: Magellan

ches und Server miteinander verbunden sind. Durch das Polling einer Schnittstelle liefern diese Systeme Informationen darüber, ob ein Server nicht erreichbar ist, weil er ausgeschaltet ist oder ob die Links zum Backbone nicht verfügbar sind.

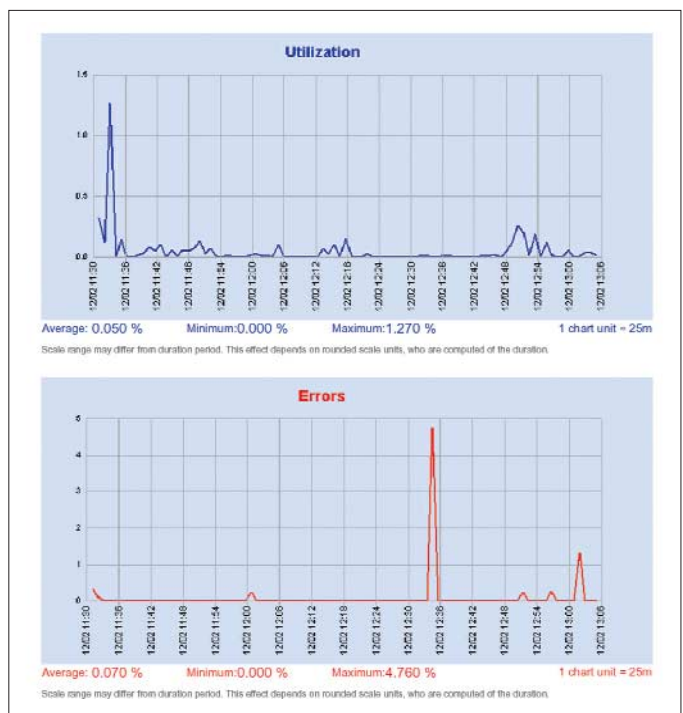
Viele Hersteller von Netzwerkmanagementlösungen verwenden das FCAPS-Modell (FCAPS: Fault, Configuration, Accounting, Performance und Security), um die verschiedenen Möglichkeiten ihrer Werkzeuge zu beschreiben. Dieses Modell erstellte die ITU (International Telecommunication Union) für das Provider- und Carrier-Umfeld, weshalb nicht alle dort beschriebenen Funktionen im LAN-Management benötigt werden. Meist decken die Systeme die Bausteine Fault-, Configuration- und Leistungsmanagement ab. Zudem überschneiden sich in der Praxis häufig die fünf Bausteine und können nicht klar getrennt werden. Einzelne Bausteine wie etwa das Accounting lassen sich auch über Insellösungen realisieren. Manchmal ist es sinnvoller, für Spezialaufgaben eine solche Insellösung zu verwenden. Denn Produkte, die versprechen, alles zu leisten und alles zu können, neigen in der Praxis dazu, sehr komplex und schwer beherrschbar zu sein.

FAULT-MANAGEMENT Das Fault-Management ist grundlegender Bestandteil aller Systeme. Es übernimmt die Aufgaben Alarm-Handling, Trouble-Detection, Trouble-Correction, Test und Acceptance sowie Network-Recovery. Dabei geht es darum,

die Zeit zwischen dem Auftreten eines Fehlers und der Wiederherstellung der Betriebsfähigkeit zu minimieren. Über das Polling von SNMP-Variablen in den Agenten der Netzwerkkomponenten und durch den Empfang der SNMP-Meldungen (Traps) erkennt das System Fehler und analysiert sie. Ein Fehler kann die Nichtverfügbarkeit eines Systems sein oder die Überschreitung eines Schwellwerts, wenn die Last auf einem Link zu einem Server oder zwischen zwei Switches eine kritische Grenze überschreitet. Über die Root-Cause-Analyse ermittelt das System die Fehlerursache, etwa den fehlenden Link zum Backbone. Die Ursache eines Fehlers korreliert das System mit den verschiedenen Fehler- und Zustandsmeldungen, löst einen Alarm aus, und das Configuration-Management behebt im besten Fall den Fehler wieder – beispielsweise führt es Neustarts von Systemen durch oder ruft externe Programme zur Fehlerbehebung auf.

Grundlegend ist allerdings, dass die Alarmmeldungen abhängig von Uhrzeit und Wochentag per E-Mail, SMS oder Pager einen zuständigen Mitarbeiter direkt und sofort erreichen. Viel zu häufig stehen Netzwerkmanagementsysteme in Rechenzentren und melden Alarmer, die erst zur Kenntnis genommen werden, wenn Benutzer oder Kunden anrufen und sich über die Nichtverfügbarkeit beschweren. Auch falsch konfigurierte Systeme werden nicht mehr beachtet, wenn sie ständig Alarmer auslösen, die dann aber die IT-Infrastruktur nicht beeinträchtigen. Ein so arbeitendes System führt häufig dazu, dass das Personal das Netzwerkmanagementsystem nicht mehr beachtet, weil es keine Hilfe darstellt. Viele Systeme bieten daher zusätzlich die Möglichkeit, automatisch in einem Helpdesk einen Call oder ein Trouble-Ticket zu eröffnen. Gerade dies ist für Unternehmen interessant, die ihre IT ITIL-konform gestalten möchten. ITIL steht für IT-Infrastructure Library. Darin sind zwölf Kernprozesse des IT-Service-Managements definiert. Der Grundgedanke dahinter ist, dass gut funktionierende Managementprozesse zu einem guten Service führen.

CONFIGURATION-MANAGEMENT Das Configuration-Management überwacht,



Anzeige von Auslastung und aufgetretenen Fehlern bei The Guard! von Realtech
Quelle: Magellan

kontrolliert und verändert Komponenten. Dazu bedient es sich aller Funktionen, die im Zusammenhang mit den Konfigurationsdaten stehen. Dazu zählen das Sammeln, Darstellen, Kontrollieren und Aktualisieren von Konfigurationsparametern. Das Configuration-Management muss durch ein Auto-Discovery in der Lage sein, alle Komponenten eines Netzwerks zu entdecken, sie zu erkennen und sie zu klassifizieren. Das Auto-Discovery muss neben den Adressinformationen eines Netzwerknotens (IP-Adresse und MAC-Adresse) auch noch tiefer gehende Informationen eines Knotens auslesen. Für eine LAN- und WAN-Topologie reicht es nicht aus, wenn aus einem Router oder Layer-3-Switch die gerouteten IP-Netze ausgelesen werden, denn auch alle weiteren Topologieinformationen sind interessant und notwendig. Dazu gehört zum Beispiel die Bridge-MIB oder die Forwarding-Database. Durch diese Informationen kann eine genaue Topologie eines Netzwerks dargestellt werden, etwa wie Switches und Router physikalisch miteinander verbunden sind. In der Praxis können somit sehr einfach Redundanzmechanismen überwacht werden. Der Ausfall eines Servers kann somit bis auf den betreffenden Switchport zurückverfolgt werden. Mit dieser Topologie und Visualisierung ist auch eine gute Dokumentationsmöglichkeit verbunden, sofern eine Exportfunktion, zum Beispiel nach Visio, vorgesehen ist. Des Weiteren muss über das Configuration-Management die Möglichkeit gegeben sein, Schwellwerte auf die unterschiedlichsten Parameter zu setzen, etwa auf Netzlast oder Broadcasts. Das Konfigurieren der Komponenten selbst lässt sich häufig einfacher und besser über Elementmanager der jeweiligen Komponentenhersteller realisieren.

ACCOUNTING Die Abrechnung über die Verwendung der Netzwerkdienste und die Zuordnung zu Verursachern, Personen und Gruppen ist Sache des Accounting-Managements. Diese Aufgabe ist relativ komplex und mit den meisten Netzwerkmanagementsystemen nur aufwändig und kostenintensiv zu realisieren. Ein klassisches SNMP-Management kann diese Aufgabe häufig nicht meistern. Hierzu bedarf es anderer Datenkollektoren. Jedoch spielt das Zuordnen von Kosten für eine wachsende Zahl von Unternehmen eine tragende Rolle

und sollte deshalb im Rahmen eines Netzwerkmanagements stets bedacht werden.

PERFORMANCE-MANAGEMENT Das Performance-Management liefert im Idealfall sämtliche relevante Daten der Kommunikationsprozesse eines Unternehmens. Die Sammlung dieser Daten kann über SNMP/RMON, also über Polling und Traps aus den einzelnen Komponenten oder über externe Datenquellen erfolgen. Das

sich mit der Zugangsbeschränkung und Nutzerrechten eines Netzwerks beschäftigt. Darunter fallen zum Beispiel Identifizierung, Authentifizierung und Autorisierung. Hierfür gibt es Speziallösungen.

FAZIT Nicht immer sind alle Bausteine des FCAPS-Modells nötig. In kleinen und homogenen Netzwerken reicht für das Netzwerkmanagement häufig der Elementmanager des Herstellers der aktiven Kompo-



Verfügbarkeitsreport für einen Switch, erstellt mit dem Netzwerkmanager von Realtech The Guard!
Quelle: Magellan

Leistungsmanagement zeigt Echtzeitstatistiken von Switch- oder Router-Ports an und sollte dazu in der Lage sein, Reports über diese Statistiken zu generieren. Ebenso muss dieses Werkzeug die Antwortzeiten der Komponenten messen können und zum Beispiel auch die Auslastung einer Switch- oder Router-CPU mit einbeziehen. Die Reports erlauben es dem Netzwerkadministrator, Aussagen über die Leistungsfähigkeit seines Netzwerks für die Zukunft zu treffen. Ein gutes Performance-Tool ist daher die Grundlage für Baselineing und Trending, um Aussagen über die normale Netzwerkleistungsfähigkeit und Aussagen über die zukünftige Entwicklung des Datenaufkommens zu treffen. Im besten Falle vermeiden Leistungsanalysen Engpässe und erhöhen somit die Verfügbarkeit eines Netzwerks.

SECURITY-MANAGEMENT Das Sicherheitsmanagement spielt für das Netzwerkmanagement nur eine geringe Rolle, da es

nenten aus – etwa Ironview von Foundry, Cisco Works oder Epicenter von Extreme. Ein Netzwerkmanagementsystem muss nicht zwangsläufig teuer sein. Wenn es richtig eingesetzt wird, sind die Kosten durch verkürzte Ausfallzeiten sehr schnell wieder erwirtschaftet. Auch bei kleinen Netzwerken lohnt sich ein solches System, wobei der Administrator dafür nicht zwangsläufig komplexe Frameworks wie Tivoli oder HP Openview einsetzen muss. Hier bietet sich eine entsprechende Free-ware-Lösung (Nagios) oder zum Beispiel Whats Up Gold von Ipswitch an.

(Oliver Thewes/db)

Der Autor ist Consultant bei Magellan Netzwerke in Köln.

Weitere Informationen:

www.ital.co.uk
www.itu.int