

Grundlagen: System- und Netzwerk-Management

› In einer Client-/Serverumgebung helfen Management-Instrumente, Kosten zu sparen. Doch ohne entsprechendes Know-how scheitert man schnell an der Vielzahl der Standards.

› VON BERNHARD HALUSCHAK

Rechensysteme bilden die Basis in nahezu allen effizient geführten Unternehmen. Als technische Grundlage kommen dabei überwiegend Client-/Server-Topologien zum Einsatz.

In der Vergangenheit wurden diese Netzwerke vorwiegend dezentral administriert. Das verursachte in Unternehmen enormen Arbeitsaufwand und Kosten. Aus diesem Grund verlagerte man die Verwaltung der Rechner und Anwendungen an einen zentralen Standort. Aber erst ein ausgeklügeltes Netzwerk- und System-Management macht diese Verwaltungsform der Rechensysteme effektiv.

Sowohl das Netzwerk- als auch das System-Management befassen sich mit der Pflege und dem Überwachen (Monitoring) von Geräten und Anwendungen. Bei der Verwaltung der Systeme stehen die einzelnen Komponenten im Vordergrund. Als grundlegende Aufgaben fallen das Installieren und Aktualisieren von Software sowie das Überwachen und Steuern verschiedener System-Ressourcen an.

Das Netzwerk-Management betrachtet die einzelnen Geräte als eine voneinander abhängige Einheit. Ziel ist die störungsfreie Funktion des Netzwerkes bei optimaler Performance. Eine klare Trennung zwischen der Administration von Netzwerk und Systemen gibt es allerdings nicht. Änderungen im System-Management wirken sich in der Regel auch auf das Netzwerk-Management aus.

Unser Artikel bietet Ihnen einen Überblick über die wichtigsten Grundlagen der zentralen Verwaltung von Hardware, Software und Netzwerken.

› Wichtige Management-Standards

Die Vielzahl parallel existierender Standards macht das System- und Netzwerk-Management kompliziert. In der Netzwerk-Administration dominiert SNMP (Simple Network Management Protocol), sein Pendant bei der Geräteverwaltung heißt DMI (Desktop Management Interface).

SNMP

Seit mehr als einem Jahrzehnt bildet das 1988 entwickelte SNMP die Grundlage für die Verwaltung von TCP/IP-Umgebungen. Als Primärziel bei der Entwicklung des Protokolls fungierte die Unabhängigkeit von Betriebssystemen, Rechnerplattformen oder Geräten. Darüber hinaus sollte SNMP leicht erweiterbar sein und nur minimale System-Ressourcen belegen.

Eine SNMP-Umgebung besteht aus einer Management-Station und mindestens einer Netzwerkkomponente. Die Management-Station steuert und überwacht die Netzwerkkomponente, wie etwa einen Router, Drucker oder Host. Dort laufen so genannte Agenten-Prozeduren. Über SNMP tauscht die Manager-Station Daten mit den Agenten aus und erledigt deren Auswertung. Die Kommunikation zu den Agenten setzt eine Management-Information-Base (MIB) voraus. Diese gewährleistet, dass die

Manager-Station nur Informationen anfordert, die die Agenten-Prozeduren auch liefern können.

DMI

Die konsistente Verwaltung des gesamten Netzes via SNMP setzt voraus, dass alle enthaltenen Systeme und Komponenten dieses Protokoll auch unterstützen. Um dies für alle PC-Komponenten in einheitlicher Weise zu gewährleisten, entwickelte die Desktop Management Taskforce ab 1992 das DMI (Desktop Management Interface).

DMI kann über ein DMI-Komponenten-Interface herstellerspezifische Informationen aller Hard- und Software-Komponenten im PC abfragen. Dazu benötigt es allerdings die zur fraglichen Hardware gehörige Management-Information-Format-Datei (MIF), die im Lieferumfang des Geräts enthalten ist. Der Hersteller der Komponente definiert darin die verfügbaren Daten wie Produktname, Version oder Seriennummer. Diese Daten wertet der SNMP-Agent aus und leitet die Informationen an die Management-Konsole weiter.

› SNMP-Topologie

Zu den Hauptaufgaben eines Netzwerk-Managements auf der Basis von SNMP zählen das Überwachen und Steuern der Netzwerk-Funktionen sowie die vorbeugende Diagnose und Problemanalyse. Die Umsetzung der Daten - das Sammeln und Auswerten von Informationen einzelner Netzwerkknoten - so genannter Nodes - erweist sich in der Praxis als komplex.

So gilt es beispielsweise, zwischen drei verschiedenen Arten von Knoten (Nodes) zu unterscheiden:

- › Gemanagte Nodes: Netzwerkknoten, die ständig Informationen zum Status des Netzwerks sammeln und senden.
- › Management Nodes: Netzwerkknoten, die Informationen von einem gemanagten Node anfordern.
- › Ungemanagte Nodes: Hierzu zählen alle Komponenten, die Netzwerk-Management nicht unterstützen oder nicht über ein kompatibles Protokoll verfügen.

Jeder gemanagte Knoten muss einen SNMP-Agenten zur Verfügung stellen. Dieser ermittelt Informationen und überträgt sie auf Anforderung an den Management Node. Der Datenaustausch beginnt stets mit einem Request des Management Node an den Agenten des Empfängers. Der prüft die Berechtigung der Anfrage, ermittelt die angeforderten Informationen und schickt sie an die Administrations-Konsole.

Als Management Node kommt in der Regel eine Workstation mit installierter Netzwerk-Management-Software zum Einsatz. Das System sammelt in definierten Zeitabständen die Daten der gemanagten Nodes ein. Da dieses System ebenfalls überwacht werden muss, kann aber auch hier durchaus ein lokaler SNMP-Agent laufen.

› Netzwerk-Management

Eine zentral installierte, herstellerübergreifende Netzwerk-Management-Software wie HP OpenView sammelt alle einlaufenden SNMP-Daten in einer Datenbank. Diese Angaben bereitet das Überwachungssystem grafisch auf, so dass der Netzwerkadministrator einen guten Überblick über den Zustand seines Netzwerks erhält. Zudem wertet die Netzwerk-Software alle relevanten Informationen aus, wie Auslastung, Betriebsstatus oder Performance, um bei Überschreitung definierter Schwellwerte den Administrator zu alarmieren.

Die folgende Übersicht fasst alle wichtigen Funktionen des Netzwerk-Managements zusammen:

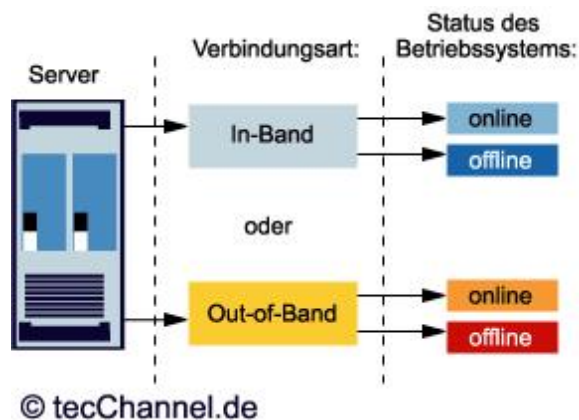
- › Konfigurationsverwaltung: Beinhaltet die Bereitstellung und Steuerung von Netzwerk-Komponenten. Hilft zudem bei der Regelung der Planung, Erweiterung,

Änderung und Wartung der Netzwerkkonfiguration und der Konfigurationsdaten.

- › Fehlermanagement: Hilft, drohende Engpässe eines Netzwerks rechtzeitig festzustellen. Netzwerkprobleme können somit im Vorfeld durch entsprechende Lösungsvorschläge verhindert werden.
- › Performance-Management: Erfasst und überwacht alle Performance-relevanten Vorgänge im Netzwerk. Dient zur Kontrolle und Steigerung der Netzwerk-Effizienz.
- › User-Administration: Vereinfacht die Einrichtung und Pflege von Benutzerkonten. Regelt die Verteilung der Netzwerk-Ressourcen.

› Remote-Server-Management

Eine wesentliche Funktion jedes Server-Management-Systems ist der Zugriff auf den Server aus der Ferne. Man unterscheidet hier zwischen In-Band- und Out-of-Band-Verbindungen. Die Out-of-Band-Kommunikation erfolgt über das Netzwerk-Interface der Maschine. Dagegen benutzt eine In-Band-Verbindung die USB-Schnittstelle, den seriellen Port oder ein Modem zur Datenübermittlung. Entscheidend für die Funktionalität ist, dass die Kommunikation nicht nur lokal, sondern auch remote möglich sein muss.



Kontakt: Dem Administrator stehen mehrere unterschiedliche Kommunikationskanäle zur Verfügung, um einen per remote überwachten Server zu erreichen.

In der Regel werden auf der Serverseite Controller-Karten eingesetzt, die sich über ein eigenes unabhängiges Stromnetz mit Energie versorgen. Diese Lösungen verfügen über ein eigenes Betriebssystem und integrierte SNMP-Agenten sowie über ein User- und Alarm-Management. Mit Hilfe dieser Funktionen ist eine Systemanalyse bei einem Betriebssystemausfall oder aufgetretenen Hardware-Fehler möglich. Ein Neustart via remote kann ebenfalls eigenständig erfolgen.

So erstellt zum Beispiel die Zusatz-Hardware bei einem Serverabsturz einen Statusbericht. Anhand dieser Informationen kann der Administrator die Ursache der Fehlfunktion im Remote-Modus analysieren und gegebenenfalls beheben.

Umfangreiche Schutzmechanismen verhindern den Missbrauch des Remote-Zugangs durch Unbefugte. Dazu zählen Passwortschutz und Protokollierung des Remote-Datenverkehrs sowie eine automatische Verschlüsselung der Daten bei der Übertragung. Der Modemzugriff kann aus Sicherheitsgründen auch per Call-Back erfolgen.

› Inventory-Management

Das Inventory-Management dient der Bestandserfassung aller im Unternehmensnetzwerk verfügbaren Komponenten. Dazu fragt die Management-Software in regelmäßigen Zeitabständen die Konfigurationsdaten aller Geräte im Netz ab. Sie umfassen je nach verwendeter Management-Software mehr oder weniger detaillierte Informationen über das Mainboard (Bezeichnung, Hersteller, Seriennummer), BIOS-Version, Prozessor, Speicherausbau, Steckkarten oder Laufwerke sowie die Hard- und Software-seitige

-Installation. Es beinhaltet die automatische Verteilung und Installation der Applikation beziehungsweise deren Updates. Ein optimales Software-Management-System sollte folgende wichtige Eigenschaften haben:

- › Alle Installationen erfolgen von einer zentralen Stelle und werden von dieser protokolliert.
- › Die Verteilung der Software ist individuell für verschiedene Zielsysteme konfigurierbar.
- › Der Verteilungsprozess verursacht keine Performance-Engpässe im Netzwerk oder auf den Zielsystemen.
- › Eine Lizenzverwaltung der installierten Software ist im Management-System implementiert.

› Performance-Management und Monitoring

Das System-Performance-Management arbeitet eng mit dem Hardware- und Software-Monitoring zusammen. Denn zur Analyse der entsprechenden System-Performance ist eine Überwachung (Monitoring) und Meldung bei Grenzwertverletzungen dieser Komponenten erforderlich.

Zu den grundlegenden Funktionen eines Performance-Managements gehören die Überwachung der Auslastung der Netzwerk-Verbindungen zu den Servern, die Kontrolle der Basisprozesse auf den Servern und die Erfassung der verfügbaren Massenspeicherkapazität. Zusätzlich sollte man die CPU-Auslastung und das Antwortzeitverhalten von Applikationen für eine optimale Performance-Analyse berücksichtigen.

Welche Performance-Optimierungen und Überwachungsfunktionen die meisten Vorteile bringen, hängt in erster Linie von der Größe und Komplexität sowie von den festgelegten Vorgaben für die Verfügbarkeit des Client-/Server-Systems ab. Darüber hinaus müssen wirtschaftliche Aspekte für die Realisierung der verschiedenen Funktionen berücksichtigt werden.

› Integration unterschiedlicher Management-Systeme

In einer heterogenen Netzwerk-Topologie arbeiten nicht nur Server eines Herstellers, sondern unterschiedliche Systeme müssen miteinander kommunizieren und verwaltet werden. Sie erzeugen durch Management-Agenten und -Systeme verschiedener Hersteller eine Vielzahl von proprietären Datensätzen. Für ein zentrales System-Management (Single Point of Administration) stellt das auf Grund des damit verbundenen Analyse-Aufwands ein nahezu unlösbares Problem dar.

Daher bieten viele Hersteller so genannte Integrationsmodule für ein bereits vorhandenes standardisiertes Management-Framework an. Zu den wichtigsten Verwaltungsplattformen zählen derzeit **HP OpenView** (<http://www.openview.hp.com/>) , **IBM Tivoli** (<http://www.tivoli.com/>) und **CA Unicenter** (<http://ca.com/>) . Durch Integrationsmodule für diese Schaltzentralen können Funktionen wie Netzwerk- und Software-Management herstellerübergreifend genutzt werden.

Die Nutzung von Modulen zur Anpassung an ein zentrales Management-System bringt auch Nachteile. Der Administrator muss je nach vorhandener Systemumgebung verschiedene herstellereigene Integrationsmodule installieren und pflegen. Darüber hinaus können oft besondere Zusatz-Features des Herstellers nicht genutzt werden, da sie nicht in das vorhandene Management-System integrierbar sind.

› Fazit

Ein zentrales Netzwerk- und System-Management beinhaltet eine Vielzahl von Funktionen, die den Administrator bei der Verwaltung seines Systems entlasten. Zusätzlich spart es Kosten, die durch dezentrale zeitintensive Technikereinsätze zur Wartung und Verwaltung entstehen würden.

Voraussetzung dafür ist ein einheitliches Management-System, das auf standardisierte Protokolle und Schnittstellen zugreifen kann. Müssen in ein bereits bestehendes System Fremdanlagen integriert werden, sind Integrationsmodule für die Weiterleitung der gesammelten Management-Daten wichtig.

In diesem Artikel haben wir die wichtigsten Grundlagen eines Netzwerk- und System-Managements angesprochen. In weiteren Beiträgen planen wir einzelne Punkte herauszugreifen und unter die Lupe zu nehmen sowie um Bereiche wie Security-Management, Intelligent-Platform-Management-Interface (IPMI) und Windows-Management-Instrumentation (WMI, besser bekannt als WBEM) zu erweitern. Zusätzlich sollen Management-Systeme von [Dell](http://www.euro.dell.com/countries/de/deu/gen/default.htm) (<http://www.euro.dell.com/countries/de/deu/gen/default.htm>) , [Fujitsu-Siemens](http://www.fujitsu-siemens.de/index.html) (<http://www.fujitsu-siemens.de/index.html>) , [HP](http://www.hp.com/country/de/ger/welcome.html) (<http://www.hp.com/country/de/ger/welcome.html>) , [IBM](http://www.ibm.com/de/) (<http://www.ibm.com/de/>) und [Intel](http://www.intel.com/deutsch/) (<http://www.intel.com/deutsch/>) ihre Funktionalität und Praxistauglichkeit unter Beweis stellen. (hal)

› Weitere Themen zu diesem Artikel:

[Netzwerk-Utilities für Windows](http://www.tecchannel.de/betriebssysteme/215/index.html) (<http://www.tecchannel.de/betriebssysteme/215/index.html>)

[Test: Remote Control Software](http://www.tecchannel.de/software/445/index.html) (<http://www.tecchannel.de/software/445/index.html>)

[Test: Funknetze nach IEEE 802.11](http://www.tecchannel.de/hardware/620/index.html) (<http://www.tecchannel.de/hardware/620/index.html>)

Copyright © 2001
IDG Interactive GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Interactive GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in tecChannel unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von tecChannel aus gelinkt wird, übernimmt die IDG Interactive GmbH keine Verantwortung.