



Ulf Troppens

Speicher im Netz

Professionelle Speicherverwaltung mit SAN und NAS

Exponentiell anwachsende Datenmassen erfordern immer ausgefeiltere Methoden der Speicherverwaltung. Moderne Speichertechniken wie Network Attached Storage (NAS) und Speichernetze (Storage Area Network, SAN), einst die Domäne großer Rechenzentren, dringen immer mehr auch in kleinere Netze vor.

Durchschnittlich verdoppelt sich in einem Unternehmen jedes Jahr die installierte Speicherkapazität: Wer heute mit 250 GByte Festplattenspeicher auskommt, wird in fünf Jahren um die 8 TByte verwalten und sichern. Solche Datenmengen benötigen eine professionelle Speicherverwaltung.

In traditionellen IT-Architekturen sind Speichergeräte (Fest-

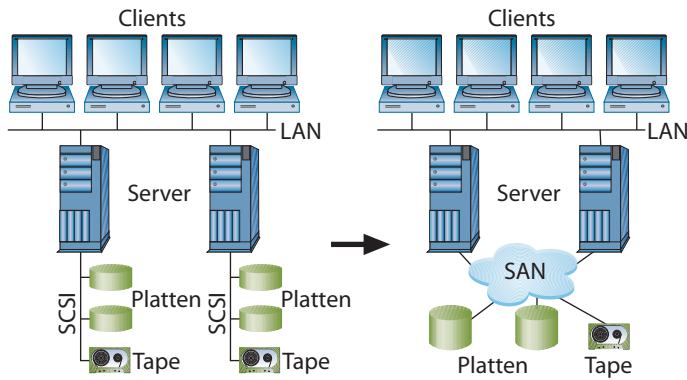
platten, Disksubsysteme oder Bänder) über SCSI-Kabel direkt an einen oder – zur Erhöhung der Ausfallsicherheit – zwei Server angeschlossen. Speicher existiert dabei immer nur in Abhängigkeit von dem Server, an den er angeschlossen ist: Andere Maschinen können nur indirekt über den vorgeschalteten Server auf die auf einem Speichergerät abgelegten Daten zugreifen.

Man spricht daher von einer serverzentrierten IT-Architektur.

Speichernetze (Storage Area Networks, SAN) entkoppeln Server und Speicher. Die Grundidee dahinter ist, die parallelen, lokalen SCSI-Kabel zwischen Server und Speicher zu entfernen und durch ein serielles Netzwerk zu ersetzen, das auch weitere Entfernungen überbrücken kann und zusätzlich zu dem bereits

vorhandenen LAN installiert wird. Dabei kommunizieren die Geräte weiterhin blockorientiert über das SCSI-Protokoll miteinander.

Mehrere Server können so direkt auf das gleiche Speichergerät zugreifen, ohne dabei den Umweg über einen anderen Server zu nehmen: Die Speichergeräte werden unabhängig von den Servern. Überspitzt gespro-



Ein Speichernetz macht Speichergeräte unabhängig von den Servern.

chen dürfen die Server als Anhängsel der Speichergeräte nur noch die darauf vorhandenen Daten bearbeiten und den Clients präsentieren. IT-Architekturen mit Speichernetzen bezeichnet man deshalb als speicherzentriert.

Auch Network Attached Storage (NAS) macht den Speicher unabhängig von den Servern, sodass ein Speichergerät mehreren Servern Speicherplatz zur Verfügung stellen kann. Der Unterschied zum SAN liegt vor allem im Zugriffsprotokoll: Die Geräte im Speichernetz präsentieren sich den Servern als blockorientierte SCSI-Geräte, während NAS-Filter als Dateiserver in Erscheinung treten, auf die dateiorientiert über Protokolle wie NFS, CIFS oder HTTP zugegriffen wird.

Im Rahmen der Einführung von Speichernetzen findet meist auch eine Speicherkonsolidierung statt. Dabei ersetzt man die vielen kleinen, an die jeweiligen Server angeschlossenen Festplatten, Disksubsysteme und Bandlaufwerke durch wenige große Speichergeräte, die von allen Servern über das Speichernetz gemeinsam genutzt werden. Entsprechende Disksubsysteme haben heute eine Kapazität zwischen einigen 100GByte und mehreren Dutzend TByte. Freie Speicherkapazität lässt sich flexibel den Servern zuweisen, die Speicherplatz benötigen. Gleichmaßen kann eine große Tape Library an die Stelle vieler kleiner treten. Zudem vereinfachen sich viele Verwaltungsaufgaben – der Textkasten „Speichernetze im Einsatz“ auf Seite 177 beschreibt ein Beispiel.

Fibre Channel

Traditionell kommt in Speichernetzen Fibre Channel als Low-Level-Protokoll zum Einsatz; neuere Ansätze sind die IP-basierten Protokolle iSCSI und FCIP, die die SCSI-Kommandos in IP-Pakete einpacken und über Ethernet verschicken. Disksubsysteme im Speichernetz, auf die blockorientiert zugegriffen wird, sind für die Software auf dem Server nicht von lokalen SCSI-Massenspeichern zu unterscheiden, auf denen das Serverbetriebssystem Dateisysteme anlegt und Volumes verwaltet. Anders als TCP/IP/Ethernet ist der Fibre-Channel-Protokollurm aus einem Guss und gilt deshalb als besonders effizient. Die wesentlichen Merkmale von Fibre Channel sind

- die serielle Übertragung für hohe Geschwindigkeit (200 MByte/s bidirektional) und weite Entfernungen (bis zu zehn Kilometern ohne weitere Geräte oder Repeater),
- die geringe Rate an Übertragungsfehlern,
- die geringe Latenz der übertragenen Daten,
- die Implementierung des Fibre-Channel-Protokolls in Hardware auf den Hostbusadaptern, um die Server-CPU's zu entlasten.

Mit diesen Eigenschaften eignet sich Fibre Channel hervorragend für Speichernetze, obwohl das Protokoll ursprünglich mit dem Ziel entwickelt wurde, in LAN-Backbone-Netzen die Nachfolge von Fast-Ethernet und FDDI anzutreten. Heute fährt man Fibre Channel meist über dünne, bewegliche Glasfaserkabel, die einfach zu handhaben sind; aber

auch Kupferkabel ist als Medium möglich.

Der Fibre-Channel-Standard definiert drei Topologien: Point-to-point, Arbitrated Loop und Fabric, wobei die verschiedenen Topologien durch zum Teil unterschiedliche Protokolle beschrieben werden. Die Point-to-point-Topologie erlaubt es lediglich, ein Speichergerät an einen Server anzubinden und ist heute nur noch von geringer Bedeutung. Gegenüber SCSI bietet sie dennoch die grundlegenden Fibre-Channel-Vorteile der höheren Geschwindigkeit (bis Ende des Jahres dürften die ersten Geräte 1GByte/s unterstützen) und größeren Entfernungen zwischen Server und Speichergerät. Zudem ist gerade bei hohen Datenraten die serielle optische Übertragung über Glasfaser weniger störanfällig als das parallele SCSI.

Wichtiger sind Fabric und Arbitrated Loop, die sich trotz unterschiedlicher Protokolle miteinander kombinieren lassen. Arbitrated Loop definiert einen unidirektionalen Ring mit bis zu 126 Endgeräten (Server oder Speichergeräte), der über einen Fibre Channel Switch an ein Fabric angebunden werden kann. Das Arbitrated-Loop-Protokoll erlaubt zu einem Zeitpunkt immer nur den Datenaustausch zwischen zwei Geräten, sodass sich alle Geräte im Ring die Bandbreite von maximal 200MByte/s teilen müssen. Moderne, so genannte Switched Hubs ermöglichen jedoch auch zeitgleichen Datenverkehr trotz Arbitrated Loop, sodass hier ein höherer Gesamtdurchsatz erreichbar ist. Arbitrated Loops setzt man heute vor allem innerhalb von Disksubsystemen zur Anbindung von Festplatten sowie zum Anschluss mehrerer Bandlaufwerke an einen Switch-Port ein, da sich diese Topologie billiger als ein Fabric realisieren lässt.

Gewebe

Fabric ist in fast allen anderen Situationen die geeignete Wahl. Es ist sehr flexibel und verbindet theoretisch bis zu fünfzehneinhalb Millionen Endgeräte miteinander, wobei alle Geräte parallel miteinander Daten austauschen können. Typische Einstiegsconfigurationen bestehen aus einer Hand voll Servern, ein bis zwei Disksubsystemen, zwei Fibre

Channel Switches und gegebenenfalls einer Tape Library (siehe Kasten „Hochverfügbarkeit“ auf Seite 178).

Die Vernetzung der Geräte in einem Fabric erfolgt über Fibre Channel Switches, die je nach Größe zwischen acht und etwa 250 Ports haben, an die sich sowohl Endgeräte als auch weitere Switches anschließen lassen. Switches realisieren unter anderem das Routing sowie die Basisdienste Name Service und Zoning. Große Switches, die meist auch ausfallsicherer sind als die kleinen, bezeichnet man in Anlehnung an die Großrechnerwelt auch als Director.

Die Geräte in einem Fabric werden durch 16-stellige Hexadezimalzahlen, die so genannten World Wide Names (WWN), unterschieden. Sie dienen lediglich der Identifikation der Geräte, nicht zur Adressierung. Dafür erhalten alle Endgeräte bei der Anmeldung an ein Fabric eine sechsstellige Hexadezimalzahl zugewiesen, die so genannte Node ID. Der hierarchische Aufbau der Node IDs spiegelt die Netzwerkstruktur des Fabric wider. Dies hilft den Switches, die einzelnen Nachrichten sehr schnell zu routen.

Der Name Service gibt Auskunft über alle gerade an einem Fabric angeschlossenen Endgeräte. Endgeräte registrieren sich bei der Anmeldung beim Name Service und können dort auch nach anderen Endgeräten fragen. Kennt beispielsweise ein Server die WWN eines Speichergeräts, kann er dort die zur Adressierung der Fibre Channel Frames notwendige Node ID erfragen.

Zoning ermöglicht es, innerhalb des Fibre-Channel-Netzes Subnetze zu definieren. Mit Zoning können Server nur Speichergeräte sehen und darauf zugreifen, die in der gleichen Zone liegen. Zoning bietet also einen gewissen Schutz der Daten, weil ein Server nur noch die für ihn bestimmten Speichergeräte zu sehen bekommt. Dies vereinfacht auch die Verwaltung der Server, weil Betriebssystem und Verwaltungstools auf dem Server nur noch die relevanten Speichergeräte anzeigen.

Anwendungsprotokolle

Die bisher vorgestellten Mechanismen stellen lediglich die notwendige Infrastruktur für die

Kommunikation zwischen den Endgeräten bereit. Die Endgeräte müssen sich vor dem Datenaustausch jedoch noch auf ein gemeinsames Anwendungsprotokoll einigen. Der Name Service gibt daher auch Auskunft darüber, welche Anwendungsprotokolle ein Endgerät unterstützt.

Das so genannte Fibre Channel Protocol (FCP) ist für Speichernetze besonders wichtig. FCP bildet das SCSI-Protokoll auf das darunter liegende Fibre-Channel-Netz ab. Server und Speichergeräte tauschen dabei ihre Daten weiterhin über SCSI-Kommandos aus. Dieser Ansatz soll den Übergang von SCSI auf Fibre Channel erleichtern. Im Idealfall muss der Administrator nur einen Fibre-Channel-Hostbusadapter in den Server einbauen und einen neuen Gerätetreiber installieren. Das Betriebssystem erkennt über Fibre Channel angeschlossene Speichergeräte als SCSI-Devices, die es – wie jeden anderen SCSI-Massenspeicher – beispielsweise als Speicher für Dateisysteme und Datenbanken konfigurieren kann.

Zum Kabel hin haben SCSI und FCP dagegen wenig gemeinsam. SCSI benutzt parallele Kabel, mehrere Geräte hängen in einer Kette hintereinander. Für Fibre Channel muss die parallele Übertragung serialisiert werden, und ein Fabric bietet gewichtete Punkt-zu-Punkt-Verbindungen zwischen den einzelnen Geräten. Entsprechend erfordern Arbitrierung und Suchen nach Geräten am SCSI-Bus ganz andere Mechanismen als die vergleichbaren

Operationen in einem Fibre-Channel-Netz.

Ein weiteres Anwendungsprotokoll ist die Fibre Connection (FICON). Sie bildet das aus der Großrechnerwelt bekannte ESCON-Protokoll auf ein Fibre-Channel-Netz ab. Dadurch ist es möglich, die Speichernetze für Großrechner und offene Systeme (Unix, Windows, iSeries, Novell und so weiter) in einem physikalischen Netz zu integrieren. Dadurch können sich beide Welten gemeinsame Speicherressourcen teilen. Mit IP over Fibre Channel (IPFC) schließlich ist es möglich, IP-Datenverkehr über eine Fibre-Channel-Verbindung abzuwickeln. Zusammen erlauben es die drei genannten Protokolle, sämtlichen Datenverkehr über Fibre Channel zu übertragen, wobei IPFC in der Praxis nur von geringer Bedeutung ist.

Alternative: iSCSI und FCIP

Fibre Channel ist heute eine etablierte Technik für Speichernetze und daher im Normalfall die richtige Wahl. Dennoch zeichnet sich zunehmend eine Tendenz ab, sämtlichen Datenverkehr über IP und Ethernet abzuwickeln. So ist das Telefonieren über IP inzwischen zumindest innerhalb von Bürogebäuden bereits etabliert. Eine durchgängig IP-basierte Netzwerkinfrastruktur für Telefon, herkömmlichen LAN-Datenverkehr und Speicherdatenverkehr bietet Kostenvorteile gegenüber mehreren parallel betriebenen Netzwerktechniken. Mit Internet SCSI (iSCSI) und Fibre Channel over IP (FCIP, nicht zu verwechseln mit IP over Fibre Channel, IPFC) existieren zwei Protokolle, um den Datenverkehr für Speichernetze über IP zu übertragen.

FCIP ist ein Tunneling-Protokoll, das zwei Fibre Channel Switches über eine IP-Strecke miteinander verbindet. Die Kopplung von Speichernetzen über größere Distanzen ist wichtig für das Duplizieren

von Daten über große Entfernungen, um größeren Katastrophen vorzubeugen. Bisher war hierzu hoher technischer Aufwand notwendig, da man schwieriger zu handhabende WAN-Techniken wie DWDM oder SONET/SDH einsetzen musste. Zahlreiche Hersteller haben jedoch inzwischen FCIP-fähige Netzwerkgeräte auf den Markt gebracht oder arbeiten an FCIP-Lösungen, sodass sich FCIP wohl noch in diesem Jahr als wichtige Alternative etablieren dürfte. Zurzeit wird das Protokoll unter dem Dach der IETF standardisiert. Es ist damit zu rechnen, dass der FCIP-Standard in den nächsten Monaten ratifiziert wird.

Während FCIP eine sinnvolle Ergänzung zu Fibre Channel ist, zielt iSCSI darauf ab, Fibre Channel als Netzwerktechnik für Speichernetze abzulösen. iSCSI hat vergleichbare Aufgaben wie das Fibre Channel Protocol FCP, nämlich das SCSI-Protokoll auf ein serielles Netz abzubilden. Allerdings bildet iSCSI den SCSI-Datenverkehr auf TCP/IP und nicht auf Fibre Channel ab. Selbstverständlich muss iSCSI ebenfalls Dienste wie Routing, Name Service und Zoning bereitstellen.

Da es derzeit noch kaum iSCSI-fähige Speichergeräte gibt, verbindet iSCSI in erster Linie Server mit SANs auf Fibre-Channel-Basis. So genannte iSCSI-Fibre-Channel-Gateways sorgen für die Umsetzung zwischen FCP/Fibre Channel und iSCSI/TCP/IP/Ethernet. Auf dem Server wird dazu ein iSCSI-Gerätetreiber installiert; den SCSI-Datenverkehr zum Speichergerät wickelt der Server dann via iSCSI über eine herkömmliche LAN-Netzwerkkarte ab. Es ist allerdings davon auszugehen, dass in den nächsten ein bis zwei Jahren auch große Tape Libraries und Disksubsysteme mit iSCSI-Ports ausgestattet sein werden, sodass es dann möglich ist, reine iSCSI-Speichernetze zu realisieren.

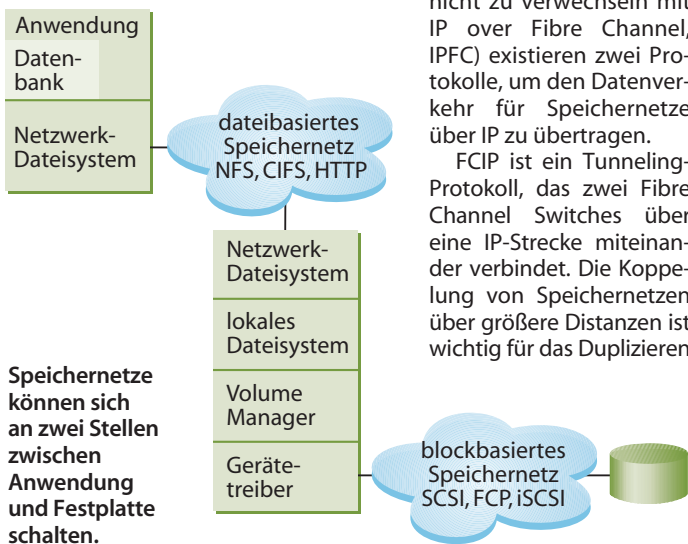
Im Zusammenhang mit iSCSI und FCIP hört man oft die Befürchtung, dass TCP/IP und Ethernet nicht leistungsfähig genug für die Realisierung von Speichernetzen seien. In Messungen über eine Gigabit-Ethernet-Strecke von zehn Kilometern Länge hat sich jedoch beim Schreiben auf ein Band ein Durchsatz von 30 bis 40MByte/s ergeben – Performance-Engpass war das Band-

laufwerk, nicht das Netz. Man kann daher davon ausgehen, dass iSCSI und FCIP den meisten Performance-Anforderungen gerecht werden, zumal 10-Gigabit-Ethernet vor der Tür steht. Die einzige Unbekannte ist im größeren Overhead des iSCSI/TCP/IP/Ethernet-Protokollturms zu sehen, der dem Einsatz für sehr hohe Performance-Anforderungen im Weg stehen könnte. Hier muss man auf Erfahrungen und Messungen in realen Produktionsumgebungen warten, um zu sehen, ob iSCSI auch für höchste Performance-Anforderungen geeignet ist.

Network Attached Storage (NAS)

Network Attached Storage (NAS) ist die andere wichtige Entwicklung, die sich in den letzten Jahren in der professionellen Speicherverwaltung etabliert hat. NAS-Server sind vorkonfigurierte Fileserver. Sie bestehen aus einem oder mehreren internen Servern, vorkonfigurierter Plattenkapazität und einem für das Filesharing optimierten Betriebssystem. Hierbei handelt es sich je nach Hersteller entweder um eine Eigenentwicklung oder um eine für das Filesharing optimierte Windows- oder Unix-Version.

NAS-Fileserver haben gegenüber einem selbst konfigurierten Fileserver zwei Vorteile: Zum einen können sie durch die Optimierung auf das Filesharing aus vergleichbarer Hardware mehr herausholen als ein universelles Betriebssystem. Zum anderen hat der Hersteller das System bereits für das Filesharing vorkonfiguriert, sodass der Administrationsaufwand für NAS-Server geringer ausfällt. Beispielsweise konfigurieren die Hersteller bei NAS-Servern mit Windows 2000 die notwendigen Einstellungen für das heterogene Filesharing zwischen Unix, Windows, Novell und MacOS vor. Zudem ist oft zusätzliche Software zum Anlegen von Snapshots von NTFS-Filesystemen, zur Replikation der Dateien auf einen zweiten NAS-Server zwecks Erhöhung der Ausfallsicherheit oder zum Suchen nach Viren vorinstalliert. Auch wenn die Vorkonfiguration der NAS-Server eine Menge Administrationsaufwand spart – bei Fehlersituationen sind nach wie vor tiefer gehende Kennt-



nisse des dem NAS-Fileler zugrunde liegenden Betriebssystems erforderlich.

NAS-Server gliedern sich in drei große Bereiche: kleinere NAS-Fileler als klassische Abteilungsserver, große NAS-Server beispielsweise als Webserver für Internet-Portale und schließlich die so genannten NAS-Gateways, manchmal auch als NAS-Heads bezeichnet. Letztere verfügen über keine internen Festplatten, sondern werden an ein schon vorhandenes SAN angeschlossen und speichern ihre Daten dort auf einem Disksubsystem. Dazu bringen sie bereits die notwendige Hardware, etwa einen Fibre-Channel-Hostbusadapter, und entsprechende Treiber mit. NAS-Gateways sind vor allem dann interessant, wenn bereits ein lokales Speichernetz als „Backend“ für einen Fileserver vorhanden ist.

Fälschlicherweise werden NAS und SAN immer wieder als sich widersprechende Konzepte dargestellt. Tatsächlich handelt es sich jedoch um zwei Techniken, die unterschiedliche Anforderungen adressieren und sich hervorragend miteinander kombinieren lassen. Speichernetze verbinden Server und Speichergeräte auf Blockebene, der Datenaustausch erfolgt über das SCSI-Protokoll. NAS-Server dagegen arbeiten auf Dateiebene – sie stellen ihren Nutzern die Daten mit Protokollen wie NFS, CIFS und HTTP bereit. NAS-Server können von einem Speichernetz profitieren, indem sie ihre Plattenkapazität über das Speichernetz beziehen (NAS-Gateway) oder zur Datensicherung im Speichernetz vorhandene Bandlaufwerke benutzen.

Netzwerkdatensicherung

Spricht man über das professionelle Speichern von Daten, stellt sich natürlich gleich die Frage nach der Datensicherung. Zwar bringen moderne Betriebssysteme eigene Backup-Werkzeuge mit, aber die stellen nur Inselösungen dar, die bei steigender Anzahl der zu sichernden Systeme völlig unzureichend sind. Da fehlt es dann an der zentralen Überwachung, ob alle Backups über Nacht sauber durchgelaufen sind, oder es mangelt an einer übergeordneten Verwaltung der Sicherungsmedien.

Abhilfe schaffen hier Netzwerkdatensicherungssysteme wie HP Omniback, IBM Tivoli Storage Manager (TSM), Legato Networker oder Veritas NetBackup. Sie sind in der Lage, heterogene IT-Umgebungen mit mehreren tausend Rechnern weitgehend automatisch zu sichern. Der Umstieg von reinen

Betriebssystemmitteln zu einem solchen zentralen Sicherungssystem kann sich jedoch auch schon für kleinere Installationen mit einer zweistelligen Zahl von Rechnern lohnen.

Netzwerk-Backup-Systeme sind Client-Server-Anwendungen, bei denen ein Datensicherungsserver alle Sicherungsmedien ver-

waltet und alle Sicherungsvorgänge zentral überwacht. Auf den übrigen Rechnern läuft ein Backup-Client, der die zu sichernden Daten zum Backup-Server überträgt. Neben den Standard-Clients, die die Dateisysteme unter allen möglichen Betriebssystemen sichern, gibt es spezielle Clients, die die Si-

Speichernetze im Einsatz

Ein Beispiel soll die Vorteile von Speichernetzen verdeutlichen. In einer Produktionsumgebung ist ein altersschwacher Server durch ein leistungsfähigeres Gerät zu ersetzen, wobei der neue Server mit dem alten Datenbestand weiterarbeiten soll. Während sich ein solcher Austausch in einer serverzentrierten IT-Architektur mit SCSI-Kabeln und internen Festplatten sehr schwierig gestalten kann, ist das mit einem Speichernetz vergleichsweise einfach durchzuführen.

Vor dem Austausch ist lediglich der alte Server über das Speichernetz an das Speichergerät angeschlossen. Zunächst installiert man den neuen Server mit der notwendigen Anwendungssoftware und schließt ihn an das Speichernetz an, sodass er auf das gleiche Disksubsystem zugreifen kann. Dabei wird der neue Server direkt an dem Ort aufgebaut, wo er letztendlich stehen soll – Speichernetze können nämlich, anders als SCSI-Kabel, problemlos Entfernungen von mehreren Kilometern überbrücken.

Innerhalb des Disksubsystems lassen sich die Produktions-

daten zwecks Erzeugung von Testdaten innerhalb von wenigen Sekunden kopieren. „Instant Copy“ bezeichnet diese Fähigkeit moderner Disksubsysteme, vergleichbar mit den Snapshots moderner Dateisysteme, selbst terabytegroße Datenbestände (virtuell) zu kopieren. Je nach Hersteller kommen hierbei unterschiedliche Verfahren zum Einsatz, beispielsweise das Abtrennen eines Mirrors in einem RAID-1- oder einem RAID-10-Verbund.

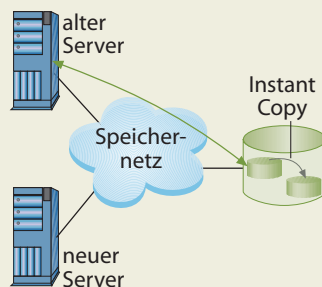
Datenkonsistenz

Entscheidend beim Kopieren mittels Instant Copy ist die Konsistenz der Daten in der so erstellten Kopie, da die Anwendung nach einem Neustart den Betrieb nur mit konsistenten Daten wieder aufnehmen kann. Schlimmstenfalls ist dazu vor dem Anlegen der Kopie die Anwendung herunterzufahren, damit sie im Hauptspeicher gepufferte Daten auf Festplatte schreibt. Viele Anwendungen können aber auch im laufenden Betrieb einen konsistenten Zustand auf Festplatte halten, etwa Datenbanken, die ein On-

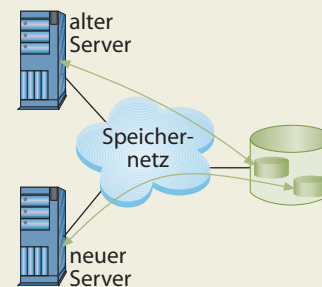
line-Backup im laufenden Betrieb erlauben.

Nun erhält der neue Server für intensive Tests Zugriff auf die kopierten Daten. Sollten die Tests das Disksubsystem so stark belasten, dass die Performance der eigentlichen Anwendung darunter leidet, muss man die Testdaten zunächst auf ein zweites Disksubsystem kopieren. Moderne Disksubsysteme können solche Kopien mittels Remote Mirroring ohne Beteiligung eines Servers direkt von Speichergerät zu Speichergerät erstellen.

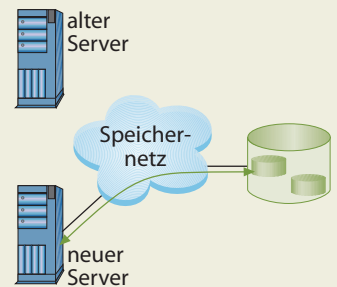
Nach erfolgreichem Test muss man beide Server herunterfahren, um die Produktionsdaten dem neuen Server zuzuweisen. Die Zuweisung selbst dauert – wie auch das Kopieren mittels Instant Copy – nur wenige Sekunden, da hierzu lediglich einige Konfigurationsänderungen in der Software notwendig sind. Insbesondere muss man an der physikalischen Verkabelung zwischen Servern und Speichergeräten nichts ändern. Schließlich wird der neue Server mit den Produktionsdaten wieder hochgefahren.



Alter und neuer Server sind an das Speichernetz angeschlossen, die Produktionsdaten des alten Servers werden innerhalb des Disksubsystems (virtuell) kopiert.



Der neue Server wird parallel zum Anwendungsbetrieb mit den kopierten Produktionsdaten getestet.



Schließlich wird der alte Server abgeschaltet und der neue Server mit den Produktionsdaten gestartet.

Anwendungsprotokolle

dateiorientiert: **blockorientiert:**

- NFS
- CIFS
- HTTP
- SCSi
- Fibre Channel (FCP)
- Internet SCSi (iSCSi)
- Internet FCP (IFCP)

Transportprotokolle:

- Fibre Channel (FC-2, FC-3)
- TCP/IP
- UDP/IP

Gateway- und Tunnelingprotokolle:

- IP over Fibre Channel (IPFC)
- Fibre Channel over IP (FCIP)

Übertragungstechniken:

- Fibre Channel (FC-0, FC-1, FC-2)
- Fast-Ethernet
- Gigabit-Ethernet
- SCSi-Kabel
- InfiniBand

Die Techniken in Speichernetzen lassen sich einteilen in Anwendungsprotokolle, Transportprotokolle und Übertragungstechniken.

Daten auf die Festplatte schreibt. Instant Copy erzeugt dann in wenigen Sekunden eine (virtuelle) Kopie. Anschließend startet die Anwendung wieder, während die im Disksubsystem kopierten Daten parallel zum Anwendungsbetrieb auf Band gesichert werden. Bei entsprechender Unterstützung der Software (Stichwort „Online Backup Mode“ von Datenbanken) kann die Anwendung sogar unterbrechungsfrei durchlaufen, während die Instant Copy angelegt wird.

nur mit einzelnen Komponenten umgehen können.

Hinter dem Schlagwort Storage Resource Management (SRM) verbergen sich die vermissten integrierten Verwaltungswerkzeuge. Sie unterstützen heute vor allem das Reporting und die Überwachung (Monitoring): Welcher Server belegt wie viel Platz auf welchen Speichersystemen? Wie weit sind die darauf angelegten Dateisysteme gefüllt? Wie ist der Status der einzelnen Komponenten? Zur Konfiguration kann ein zentrales Verwaltungssystem jedoch bestenfalls die proprietären Element-Manager der einzelnen Komponenten aufrufen. Zwei Ansätze versprechen eine Verbesserung: Standardisierung und Virtualisierung.

Die Standardisierung der Konfigurationsschnittstellen ist Voraussetzung dafür, dass die Hersteller von SRM-Systemen die Komponenten verschiedener Anbieter verwalten können – ohne einheitliche Schnittstellen ist der Entwicklungs- und Testaufwand viel zu hoch. Als Standard in der Speicherverwaltung existierte bislang nur das Simple Network Management Protocol (SNMP), das mit Get-,

Speicherverwaltung

Je nach Größe eines IT-Systems erfordert die Verwaltung der Speicherressourcen und des Speichernetzes erheblichen Aufwand. Dies liegt vor allem daran, dass umfassende Verwaltungssysteme noch fehlen, die eine zentrale Konfiguration und Überwachung aller Komponenten integrieren. Stattdessen kommen Speichersysteme, Hostbusadapter, SAN Switches, Volume Manager, Datenbanken, Dateisysteme, NAS-Server und so weiter mit proprietären Verwaltungswerkzeugen, so genannten Element-Managern, daher, die

cherung wichtiger Anwendungen wie Datenbanken oder Mailserver auch im laufenden Betrieb übernehmen.

Die Datensicherung im Netz ist eine sehr ressourcenintensive Anwendung, denn sie muss große Datenmengen in möglichst kurzer Zeit zu den Backup-Medien bewegen. Sie belastet CPU, Hauptspeicher, Busse, Speichergeräte und die Netze der beteiligten Systeme in hohem Maße. Es ist keineswegs ungewöhnlich, dass das Netzwerk-Backup mehr Systemressourcen benötigt als die eigentlichen Anwendungen.

In serverzentrierten IT-Architekturen ohne eigenes Speichernetz erfolgt die Datensicherung über das LAN, was für Arbeitsplatzrechner und kleinere Fileserver oder Datenbanken auch problemlos funktioniert. Beim Sichern großer Datenmengen hingegen wird das LAN zum Engpass. Mit einem Speichernetz ist es möglich, die Daten direkt vom Anwendungsserver (so genanntes „LAN-free Backup“) oder dem Disksubsystem („Server-free Backup“) übers Speichernetz auf eine zentrale Tape Library zu sichern. Die Daten werden dabei auch nicht mehr durch den Backup-Server geschleust, sodass der mehr Rechner parallel sichern kann.

Mit entsprechend ausgelegten Disksubsystemen lässt sich das Zeitfenster für die Daten-

sicherung auf wenige Minuten oder gar Sekunden reduzieren, sodass die Anwendung rund um die Uhr läuft und trotzdem ein konsistenter Datenbestand gesichert wird. Hierzu fährt der Administrator die Anwendung kurz herunter, damit sie alle im Hauptspeicher gepufferten

Hochverfügbarkeit mit Speichernetzen

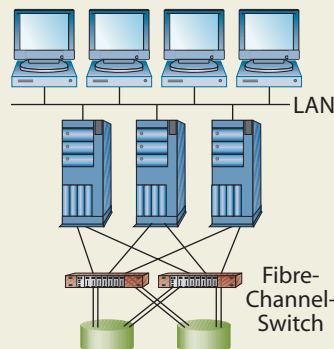
Die Forderung nach Hochverfügbarkeit ist heute einer der wichtigsten Gründe für die Einführung von Speichernetzen. Bei Festplattenkapazitäten jenseits von 100GByte kann schon ein interner RAID-Controller mit einer Hand voll in den Server eingebauten Festplatten den Speicherbedarf der meisten Anwendungen befriedigen. Das Problem dabei: Bei einem Ausfall des Servers ist auch kein Zugriff auf die Daten möglich. Ist die Serverhardware defekt, so kann einige Zeit vergehen, bis die Festplatten samt RAID-Controller in einen neuen Server eingebaut und die Anwendungen wieder gestartet sind.

Ein Speichernetz, bei dem die Festplatten aus dem Server ausgelagert und in einem externen Disksubsystem untergebracht werden, schafft hier Abhilfe. Das Disksubsystem fasst seine physikalischen Festplatten mittels

RAID zu virtuellen Festplatten zusammen und bietet so den gleichen Schutz vor Plattenfehlern wie ein im Server eingebauter RAID-Controller. In modernen Disksubsystemen sind darüber hinaus alle weiteren Komponenten redundant ausgelegt.

Bleibt das Speichernetz selbst als „single point of failure“. Hier kann man ein so genanntes „Dual Fabric“ einsetzen: Der Server wird über zwei getrennte

I/O-Pfade mit dem Speicher verbunden. Durch die Redundanz der Disksubsysteme und die Redundanz des I/O-Pfades zu den Disksubsystemen sind die Daten und der Zugriff vom Server auf die Daten gut geschützt. Mittels Clustersoftware kann man sich zusätzlich vor einem Serverausfall schützen. Ist für eine Anwendung hohe Verfügbarkeit unverzichtbar, so kommt man um den Einsatz eines Dual Fabric kaum herum.



Bei einem „Dual Fabric“ sind Fibre-Channel-Adapter, Switches und Kabel redundant ausgelegt, sodass der Datenzugriff auch bei Ausfall einer Komponente im I/O-Pfad gewährleistet ist.

Set- und Trap-Operationen lediglich ein rudimentäres Management erlaubt.

Deutliche Besserung ist durch Bluefin zu erwarten. Bluefin ergänzt die WBEM-Architektur (Web Based Enterprise Management) um Elemente für das Speichermanagement. Das „Web“ in WBEM steht dabei für die eingesetzten Techniken: XML als Format zur Kodierung von Informationen, HTTP als Transportprotokoll. Kernstück von WBEM ist ein objektorientiertes Datenmodell (das Common Information Modell, CIM), das Bluefin um Klassen für die in der Speicherverwaltung vorkommenden Komponenten erweitert. Zusätzlich definiert Bluefin Dienste, die das Auffinden von Ressourcen erleichtern und den synchronisierten Zugriff auf Ressourcen gewährleisten sollen.

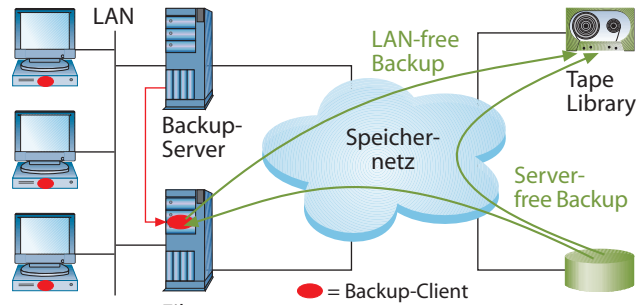
Bluefin ist noch ein sehr junger Standard, dessen Weiterentwicklung seit August 2002 in den Händen der Storage Networking Industry Association (SNIA) liegt [1]. Nach Meinung der SNIA sind etwa 70 Prozent der benötigten Funktionen für die Verwaltung eines Speichernetzes bereits verabschiedet. Der aktuelle Standard beschreibt vor allem die Komponenten eines Fibre Channel SAN; Techniken wie NAS und iSCSI fehlen bislang. Einige Speichersysteme unterstützen bereits zumindest Teile von Bluefin. Es ist davon auszugehen, dass weitere Speichersysteme und die ersten Speicherverwaltungssysteme in Kürze folgen werden.

Speichervirtualisierung

Das Ziel der Virtualisierung ist es, die Kosten für das Speichermanagement zu reduzieren,

indem der Zugriff auf die gespeicherten Daten und deren Verwaltung vereinfacht wird. Bisher fehlt eine zentrale Sicht auf die Daten: Server können zwar mehrere Speichergeräte einbinden, „sehen“ jedoch nicht den Ressourcenverbrauch anderer Server. gleichermaßen kann ein Speichergerät mehrere Server bedienen, jedoch fehlt ihm ein Überblick über die Speichernutzung auf anderen Speichergeräten. Speichervirtualisierung verwaltet die Speicherressourcen über Server- und Speichergerätegrenzen hinweg, sodass der Administrator einen zentralen Überblick gewinnt und den Speicher leichter verwalten kann. Idealerweise soll das in heterogenen Umgebungen mit Servern und Speichergeräten verschiedener Hersteller funktionieren.

Mit dem Einsatz von Speichervirtualisierung kann ein Systemverwalter schnell feststellen, welcher Server auf welchem Speichergerät wie viel Platz belegt oder auf welchem Speichergerät noch freier Speicher vorhanden ist. Man unterscheidet zwischen Speichervirtualisierung auf Blockebene und auf Dateiebene. Im ersten Fall kann man sich die Virtualisierung als Volume Manager fürs Speichernetz, im zweiten Fall als Dateisystem über das ganze Speichernetz vorstellen. In beiden Fällen ist zusätzliche Hardware nötig, die einen Teil der Aufgaben von Volume Manager oder Dateisystem auf diese neue Virtualisierungsinstanz verlagert. Allerdings ist die Speichervirtualisierung eine relativ neue Technik, sodass viele Anwender noch abwarten. Mit einem größeren Einsatz von Virtualisierung ist ab 2004 zu rechnen.



Die Netzwerkdatensicherung hilft, das Backup zu automatisieren.

Fazit

Speichernetze, NAS-Server und intelligente Disksubsysteme sind heute wichtige Bausteine der professionellen Datenverwaltung. Der Einsatz von NAS-Servern wird auch für kleinere Netze heute kaum noch in Frage gestellt. Dagegen gelten Storage Area Networks (SANs) zu Unrecht häufig als eine Technik für große Rechenzentren, obwohl sie auch für viele Mittelständler und Behörden nicht mehr wegzudenken sind – insbesondere wenn es um die Hochverfügbarkeit von Daten und Anwendungen und um die effiziente Datensicherung geht.

Der Einsatz von Speichernetzen ändert die IT-Architektur nachhaltig: Sie ersetzen die SCSI-Kabel zwischen Servern und Speichergeräten durch ein neues Netz; Speicher existiert unabhängig von einem Server. Wichtigste Technik zur Realisierung von Speichernetzen ist heute der Fibre Channel. In naher Zukunft dürfte der Einsatz von IP-basierten Speichernetzen jedoch deutlich zunehmen.

Unabhängig von der zugrunde liegenden Übertragungstechnik bieten Speichernetze Vorteile hinsichtlich der Verfügbarkeit und flexiblen Zuweisung freier Speicherkapazitäten an die einzelnen Server und Anwendungen. Im Zusammenspiel mit Disksubsystemen bieten Speichernetze zudem viele Möglichkeiten, die Datensicherung zu beschleunigen.

Während die Hardware von Speichernetzen heute schon sehr gut funktioniert, fehlt es noch an der Software, die die Möglichkeiten von Speichernetzen effektiv ausnutzt. Hier sind insbesondere die Integration von

Funktionen wie Instant Copy und Remote Mirroring in Anwendungen wie Datenbanken und Datensicherungssysteme, die automatisierte Zuweisung freier Ressourcen durch Speichervirtualisierung sowie die zentrale Verwaltung von Speichernetzen zu nennen. (odi)

Ulf Troppens ist Mitarbeiter des TotalStorage Interoperability Center der IBM in Mainz und Co-Autor des Buches [2].

Literatur

- [1] Storage Networking Industry Association: www.snia.org
- [2] Ulf Troppens, Rainer Erkens: Speichernetze – Grundlagen und Einsatz von Fibre Channel SAN, NAS, iSCSI und InfiniBand, dpunkt-Verlag, 2003.
- [3] Links zu weiterführenden Themen: www.speichernetze.com/ links

Vergleich von SAN und NAS			
	SAN		NAS
	Fibre Channel	iSCSI	
verbindet	Server und Speichergerät	Server und Speichergerät	Client oder Anwendungs-server und NAS-Server
über	eigenes Speichernetz	eigenes Speichernetz	LAN
überträgt	Datenblöcke	Datenblöcke	Dateien
Netz	Fibre Channel	TCP/IP	TCP/IP
Protokoll	FCP	iSCSI	NFS, CIFS, HTTP
integriertes Dateisystem	nein	nein	ja
Eignung für Datenbanken	ja	bedingt	eher nein
Produktionsreife	ja	bedingt	ja

SAN und NAS adressieren unterschiedliche Einsatzfelder.