

Speichernetze: Grundlagen und Einsatz*

Ulf Troppens · Rainer Erkens

27. März 2003

Zusammenfassung

Durchschnittlich verdoppelt sich in einem Unternehmen jedes Jahr die installierte Speicherkapazität. Das heißt: Wer heute 250GB Festplattenspeicher installiert hat, der wird in fünf Jahren ungefähr 8TB verwalten und sichern. Solche Datenmengen können nur noch mit Speichernetzen (Storage Area Networks, SANs) effizient verwaltet werden. Dieser Artikel bespricht grundlegende Techniken für Speichernetze wie Fibre Channel, Internet SCSI (iSCSI) und Network Attached Storage (NAS) und er beschreibt, wie diese Techniken helfen, IT-Systeme effizienter zu betreiben.

1 Motivation und Gliederung

Der Titel dieses Artikels ist eigentlich zu kurz gefasst, denn genau betrachtet geht es um die effiziente Datenhaltung. Dass das Thema „Datenhaltung“ heute sehr oft unter dem Blickwinkel der Speichernetze betrachtet wird, liegt vermutlich daran, dass Speichernetze erst seit kurzem verfügbar sind. Zudem ändern sie die IT-Architektur und den Betrieb von IT-Systemen nachhaltig. Speichernetze werden in der Großrechnerwelt schon seit langer Zeit erfolgreich eingesetzt. Im Open-Systems-Bereich (Unix/Linux, Windows, OS/400, Novell, MacOS) sind sie jedoch erst seit wenigen Jahren verfügbar, so dass hier viel Interesse und Lernbedarf besteht.

Dieser Artikel stellt zunächst die Grundidee von Speichernetzen vor und gibt einen Überblick über die dafür verfügbaren Techniken (Abschnitt 2). Dann besprechen wir mit Fibre Channel (Abschnitt 3), iSCSI und FCIP (Abschnitt 4) wichtige Übertragungstechniken für Speichernetze. Die Hochverfügbarkeit von

*Erscheint im Konferenzband zu GUUG FFG 2003 (<http://www.guug.de>).

Daten (Abschnitt 5) und die Beschleunigung der Datensicherung (Abschnitt 6) sind heute die zwei wichtigsten Gründe für die Einführung von Speichernetzen. Das Beispiel Datensicherung zeigt auch, wie Speichernetze helfen, große Datenmengen zu bewegen. Darauf gehen wir mit dem Network Attached Storage (NAS) auf eine weitere wichtige Neuentwicklung im Umfeld der Datenhaltung ein (Abschnitt 7). Abschließend reißen wir mit Bluefin und mit der Speichervirtualisierung zwei aktuelle Bereiche der Speicherverwaltung an (Abschnitt 8).

2 Die Grundidee von Speichernetzen

Die Grundidee von Speichernetzen ist es, die SCSI-Kabel zwischen Server und Speicher durch ein neues Netzwerk zu ersetzen, das zusätzlich zu dem bereits vorhandenem LAN installiert wird. Abschnitt 2.1 bespricht den damit verbundenen Übergang von der serverzentrierten zu der speicherzentrierten IT-Architektur. Abschnitt 2.2 stellt am Beispiel „Upgrade eines Anwendungsservers“ die Vorteile der speicherzentrierten IT-Architektur vor. Schließlich gibt Abschnitt 2.3 einen Überblick über die Techniken für die Realisierung von Speichernetzen.

2.1 Von der Serverzentrierung zur Speicherzentrierung

In herkömmlichen IT-Architekturen werden Speichergeräte in der Regel nur an einen einzelnen Server angeschlossen. Zur Erhöhung der Ausfallsicherheit werden Speichergeräte manchmal auch mit zwei Servern verbunden, wobei zu einem Zeitpunkt aber nur ein Server das Speichergerät wirklich nutzen kann. In beiden Fällen existiert Speicher nur in Abhängigkeit von dem Server, an dem er angeschlossen ist. Andere Server können nicht direkt auf die Daten zugreifen; sie müssen immer über den Server gehen, mit dem der Speicher verbunden ist. Fällt ein Server aus, so ist kein Zugriff auf die entsprechenden Daten möglich. Diese herkömmliche IT-Architektur wird deshalb auch als serverzentrierte IT-Architektur bezeichnet. Server und Speichergeräte werden hier in der Regel über SCSI-Kabel miteinander verbunden.

In serverzentrierten IT-Umgebungen ist der Speicher dem Rechner statisch zugeordnet, an dem er angeschlossen wird. Das heißt, wenn ein Rechner mehr Speicher benötigt, als an ihm angeschlossen

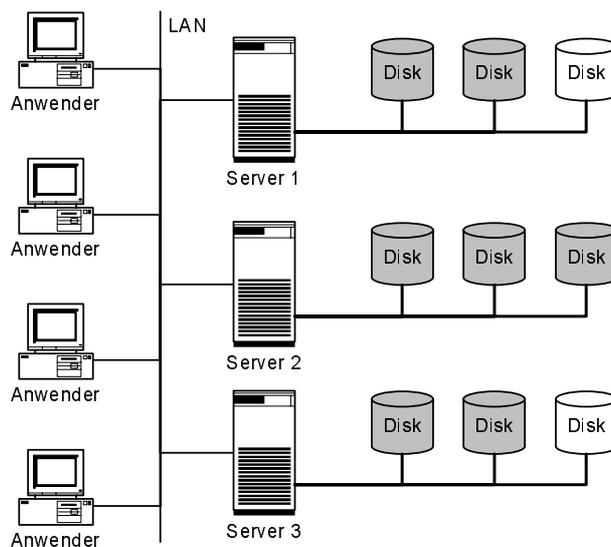


Abbildung 1: Die Speicherkapazität auf Server 2 ist erschöpft. Er kann nicht davon profitieren, dass an Server 1 und Server 3 noch Speicher frei ist.

ist, dann nützt es überhaupt nichts, dass an einem anderen Rechner noch freier Speicher vorhanden ist (Abbildung 1).

Speichernetze können die soeben geschilderten Probleme der serverzentrierten IT-Architektur lösen. Darüber hinaus bieten sie neue Möglichkeiten, Daten zu verwalten. Die Idee von Speichernetzen ist es, die SCSI-Kabel durch ein Netz zu ersetzen, das zusätzlich zu dem bereits existierenden LAN installiert und überwiegend für den Datenaustausch zwischen Rechnern und Speichergeräten genutzt wird (Abbildung 2).

Im Gegensatz zur serverzentrierten IT-Architektur existiert Speicher in Speichernetzen völlig unabhängig von irgendwelchen Rechnern. Über das Speichernetz können mehrere Server direkt auf das gleiche Speichergerät zugreifen, ohne dass dabei zwangsläufig ein anderer Server involviert ist. Speichergeräte rücken damit in das Zentrum der IT-Architektur; Server hingegen werden zum Anhängsel an die Speichergeräte, die „gerade mal noch Daten verarbeiten dürfen“. IT-Architekturen mit Speichernetzen werden deshalb auch als speicherzentrierte IT-Architekturen bezeichnet.

Mit der Einführung eines Speichernetzes wird meistens auch der Speicher konsolidiert. Dabei werden die vielen kleinen, an die Rechner angehängten Festplatten durch wenige große Disksubsysteme-

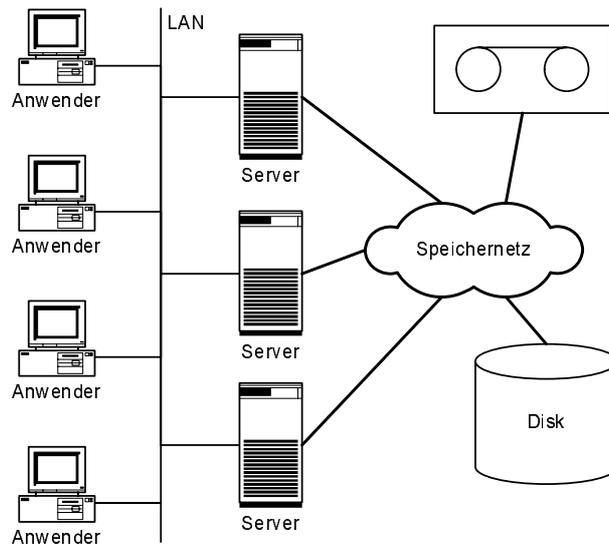


Abbildung 2: In der speicherzentrierten IT-Architektur werden die SCSI-Kabel durch ein Netz ersetzt. Speichergeräte existieren nun unabhängig von einem Server.

me ersetzt. Disksubsysteme haben heutzutage eine maximale Speicherkapazität von mehreren Zehn Terabyte. Über das Speichernetz können alle Rechner auf das Disksubsystem zugreifen und es so gemeinsam nutzen. Freie Speicherkapazität kann auf diese Weise dem Rechner flexibel zugewiesen werden, der sie gerade benötigt. Auf die gleiche Art und Weise können viele kleine Tape Libraries durch eine große ersetzt werden.

Man geht heute davon aus, dass etwa ein Drittel der in Frage kommenden Unternehmen bereits Speichernetze implementiert haben. Bis Ende 2004 sollen es zwei Drittel sein. Folglich sind für die professionelle Speicherverwaltung zumindest grundlegende Kenntnisse über Speichernetze unabdingbar.

2.2 Beispiel: Serverupgrade mit Speichernetzen

Im folgenden werden einige Vorteile der speicherzentrierten IT-Architektur anhand eines Beispiels verdeutlicht: In einer Produktionsumgebung ist ein Anwendungsserver nicht mehr leistungsfähig genug. Der altersschwache Rechner muss durch ein performanteres Gerät ersetzt werden. Während eine solche Maßnahme in einer herkömmlichen, serverzentrierten IT-Architektur sehr kompliziert sein kann, lässt sich dies mit einem Speichernetz elegant durchführen.

1. Vor dem Austausch ist der alte Rechner über das Speichernetz mit einem Speichergerät verbunden, welches er teilweise nutzt (Abbildung 3 zeigt die Schritte 1, 2 und 3).
2. Zunächst wird der neue Rechner mit der notwendigen Anwendungssoftware installiert. Der neue Rechner wird direkt an dem Ort aufgebaut, wo er letztendlich stehen soll. Mit Speichernetzen ist es nämlich im Gegensatz zu SCSI möglich, Rechner und Speicher mehrere Kilometer voneinander entfernt aufzustellen.
3. Als nächstes werden die Produktionsdaten zur Erzeugung von Testdaten innerhalb des Disksubsystems in wenigen Sekunden kopiert. Vergleichbar mit den Snapshots moderner Dateisysteme können Disksubsysteme in wenigen Sekunden selbst Terabyte-große Datenbestände (virtuell) kopieren (Instant Copy). Je nach Hersteller werden hierbei unterschiedliche Verfahren eingesetzt. Ein einfaches Verfahren wäre beispielsweise das Abtrennen eines Spiegels in einem RAID-1- oder einem RAID-10-Verbund.

Oft ist es erforderlich, zum Kopieren der Daten die Anwendungen herunterzufahren, damit die kopierten Daten konsi-

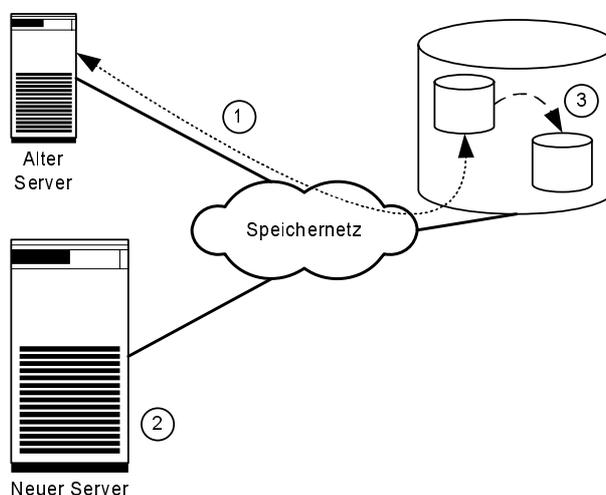


Abbildung 3: Ein Speichernetz verbindet den alten Server und das Speichergerät (1). Der neue Server wird aufgebaut und an das Speichernetz angeschlossen (2). Zur Erzeugung der Testdaten werden die Produktionsdaten innerhalb des Speichers kopiert. (3).

stent sind. Die Konsistenz ist Voraussetzung dafür, dass die Anwendung mit den Daten den Betrieb wieder aufnehmen kann. Einige Anwendungen sind auch in der Lage, im laufenden Betrieb einen konsistenten Zustand auf der Platte zu halten (Online Backup Mode von Datenbanksystemen).

4. Anschließend werden die kopierten Daten dem neuen Rechner zugewiesen und der neue Rechner intensiv getestet (Abbildung 4). Sollte das Speichersystem durch die Tests so stark belastet werden, dass die Performance für die eigentliche Anwendung nicht mehr ausreicht, so müssen die Daten erst mittels Remote Mirroring auf ein zweites Speichersystem übertragen werden. Moderne Disksubsysteme können solche Kopien mittels Remote Mirroring ohne Beteiligung eines Servers direkt von Disksubsystem zu Disksubsystem erstellen.

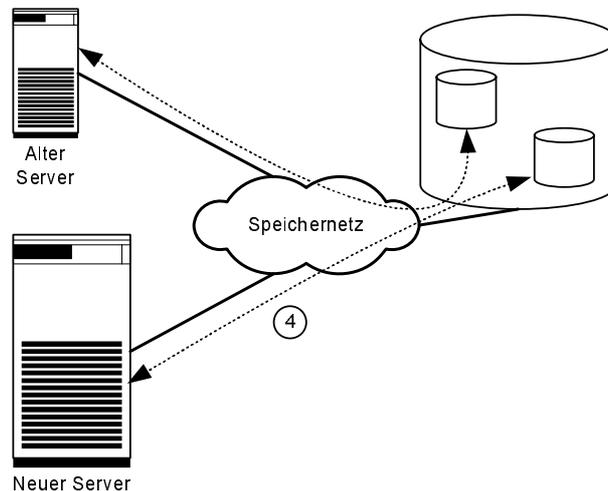


Abbildung 4: *Alter Server und neuer Server teilen sich das Speichersystem. Der neue Server wird parallel zum Anwendungsbetrieb mit den kopierten Produktionsdaten intensiv getestet (4).*

5. Nach erfolgreichem Test werden beide Rechner heruntergefahren und die Produktionsdaten dem neuen Server zugewiesen. Die Zuweisung der Produktionsdaten an den neuen Server dauert ebenfalls nur wenige Sekunden (Abbildung 3 zeigt die Schritte 5 und 6).
6. Schließlich wird der neue Server mit den Produktionsdaten wieder hochgefahren.

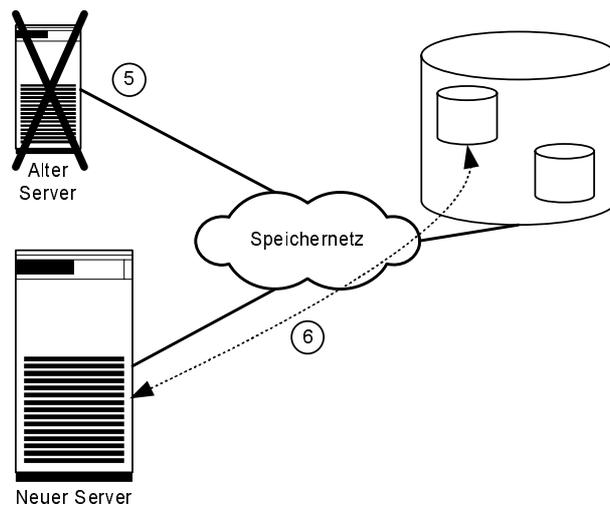


Abbildung 5: Schließlich wird der alte Server abgeschaltet (5) und der neue Server mit den Produktionsdaten hochgefahren (6).

2.3 Techniken für Speichernetze

Schaut man sich den I/O-Pfad von der Anwendung bis zur Festplatte an, so finden sich zwei Stellen, an denen man Speichernetze zwischenschalten kann (Abbildung 6). Wichtig ist die Unterscheidung zwischen dateibasierten Speichernetzen und blockbasierten Speichernetzen. Es bieten sich zahlreiche verschiedene Techniken für die Realisierung von Speichernetzen an (Abbildung 7).

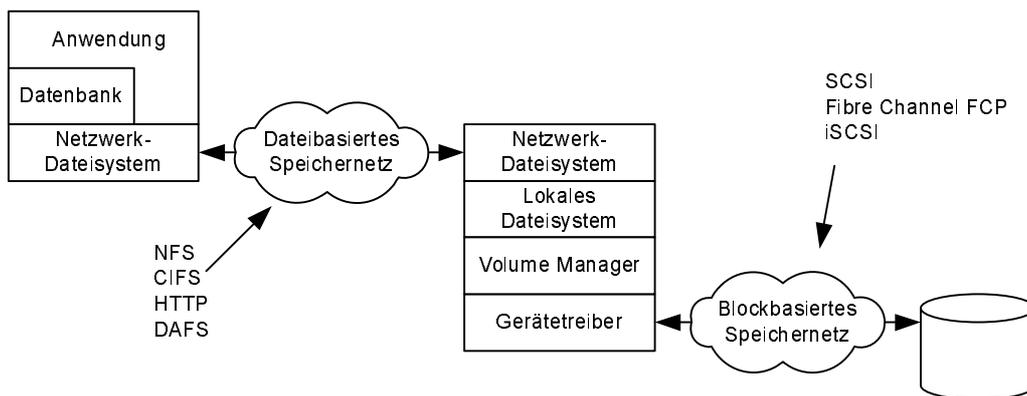


Abbildung 6: Speichernetze im I/O-Pfad

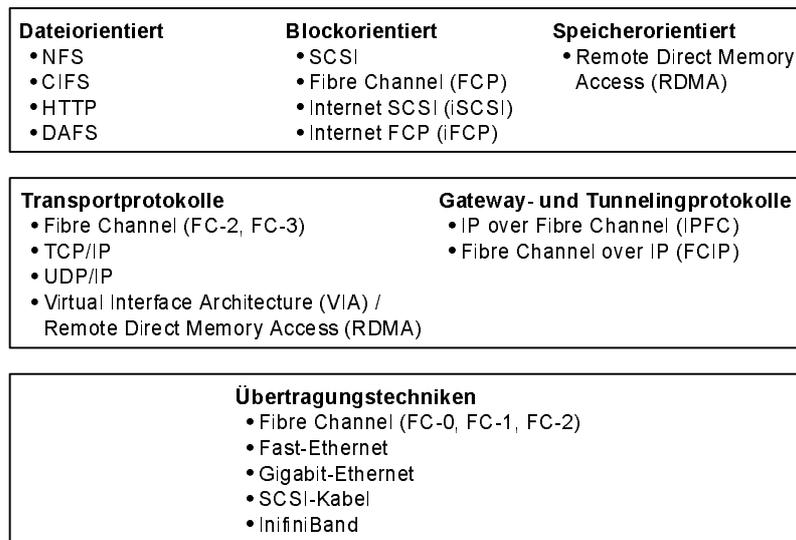


Abbildung 7: Das OSI-Referenzmodell stark vereinfachend kann man die Techniken für Speichernetze unterscheiden in Anwendungsprotokolle, Transportprotokolle und Übertragungstechniken.

Unterhalb des Volume Manager kommen blockorientierte Anwendungsprotokolle zum Einsatz. Je nach Technik findet man hier SCSI sowie SCSI-Ableger wie FCP, iFCP und iSCSI. Blockorientierte Speichernetze finden sich heute vor allem zwischen Rechnern und Speichersystemen. Aber auch innerhalb von großen Disksubsystemen werden immer mehr die SCSI-Kabel durch eine Netzwerk-Übertragungstechnik ersetzt. Im weiteren besprechen wir Fibre Channel (Abschnitt 3) und die Familie der IP-basierten Speicherprotokolle (iSCSI und FCIP, Abschnitt 4).

Oberhalb von Volume Manager und Dateisystem kommen dateiorientierte Anwendungsprotokolle zum Einsatz. Hier finden sich Anwendungsprotokolle wie NFS, CIFS, HTTP und FTP. Mit dem Network Attached Storage (NAS) werden wir die dateiorientierten Speichernetze später aufgreifen (Abschnitt 7).

3 Fibre Channel SAN

Der Fibre Channel ist heute *die* Technik für die Verwirklichung von Speichernetzen. Der Fibre-Channel-Protokollturm ist im Gegensatz zu TCP/IP und Ethernet aus einem Guss und gilt deshalb als be-

sonders effizient. Die wesentlichen Entwurfsziele von Fibre Channel sind

- die serielle Übertragung für hohe Geschwindigkeit und weite Entfernungen,
- die geringe Rate an Übertragungsfehlern,
- die geringe Verzögerung (Latenz) der übertragenen Daten,
- die Implementierung des Fibre-Channel-Protokolls in Hardware auf Hostbus-Adapterkarten zur Entlastung der Server-CPU's.

Der Fibre-Channel-Protokollturm untergliedert sich in fünf Schichten (Abbildung 8). Die unteren vier Schichten (FC-0 bis FC-3) definieren die grundlegenden Kommunikationstechniken, also die physikalische Ebene, die Übertragung und die Adressierung. Die obere Schicht (FC-4) definiert, wie Anwendungsprotokolle (Upper Layer Protocols, ULPs) auf das zugrundeliegende Fibre-Channel-Netz abgebildet werden. Der Einsatz der verschiedenen ULPs entscheidet beispielsweise, ob ein reales Fibre-Channel-Netz als IP-Netz, als Fibre Channel SAN (also als Speichernetz) oder für beides zugleich eingesetzt wird. Quasi neben dem Fibre-Channel-Protokollturm stehen die Link Services und die Fabric Services. Diese Dienste werden benötigt, um ein Fibre-Channel-Netz zu verwalten und zu betreiben.

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 nur die Anbindung von einem Speichergerät an einen Server und ist heute nur noch von geringer Bedeutung. Gegenüber SCSI bietet sie dennoch einige Vorteile, die für alle drei Topologien gelten: Fibre Channel erlaubt eine bidirektionale Übertragung von jeweils 200 MByte/s in jede Richtung. Hierbei können ohne weitere Geräte oder Signalverstärker (Repeater) Entfernungen von mehreren Kilometern überbrückt werden. Bis Ende diesen Jahres werden die ersten Geräte voraussichtlich 1 GByte/s unterstützen. Heute werden überwiegend dünne, bewegliche Glasfaserkabel eingesetzt, die sehr einfach handzuhaben sind. Zusätzlich ist gerade bei hohen Datenraten die serielle optische Übertragung weniger störanfällig als das parallele SCSI.

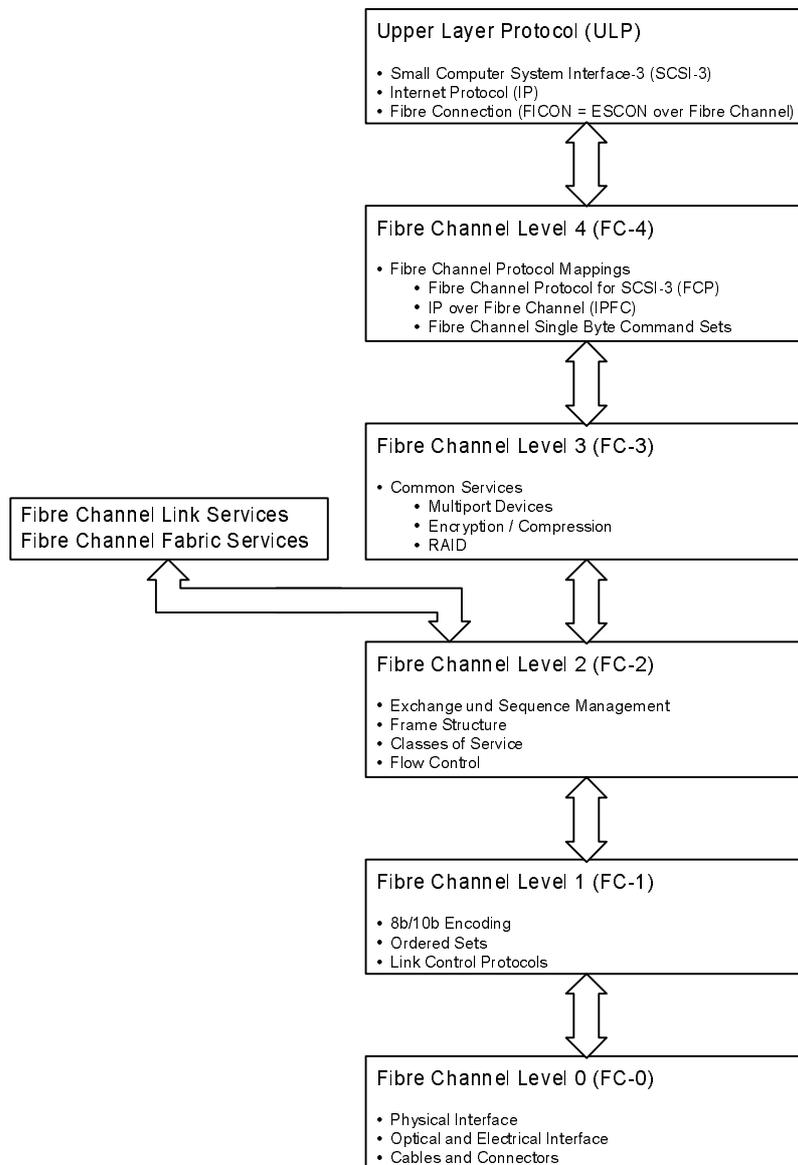


Abbildung 8: Der Fibre-Channel-Protokollturm gliedert sich in zwei Teile: Die unteren vier Schichten (FC-0 bis FC-3) realisieren die grundlegende Fibre-Channel-Übertragungstechnik. Die Link Services und die Fabric Services helfen, das Fibre-Channel-Netz zu verwalten und zu konfigurieren. Die obere Schicht (FC-4) definiert, wie die Anwendungsprotokolle (beispielsweise SCSI und IP) auf ein Fibre-Channel-Netz abgebildet werden.

Eine wesentlich größere Bedeutung haben die Fabric und die Arbitrated Loop, die trotz unterschiedlicher Protokolle miteinander kombiniert werden können, so dass man auch eine gemischte Topologie betreiben kann. Die Arbitrated Loop definiert einen unidirektionalen Ring mit bis zu 126 Endgeräten (Server oder Speichergeräte). Ursprünglich konnten auf der Loop zu einem Zeitpunkt immer nur zwei Geräte miteinander Daten austauschen. Moderne, sogenannte Switched Hubs ermöglichen jedoch zeitgleichen Datenverkehr trotz Arbitrated Loop. Sie kann über einen Fibre Channel Switch an eine Fabric angebunden werden.

Die Arbitrated Loop wird heute vor allem innerhalb von Disksubsystemen zur Anbindung von Festplatten eingesetzt. Ein weiteres Einsatzgebiet ist der Anschluss von mehreren Fibre Channel Tape Drives an einen Switch-Port. Der Einsatz der Arbitrated Loop ist preisgünstiger als eine reine Fabric, so dass in beiden Fällen Kosten gesenkt werden können.

Schließlich definiert die Fabric ein Netzwerk, in dem alle Geräte gleichzeitig mit voller Bandbreite Daten austauschen können. Sie ist sehr flexibel und verbindet theoretisch bis zu 15 1/2 Millionen Endgeräte miteinander. Die Fabric ist in fast allen Situationen die zu bevorzugende Topologie.

Eine Fabric erfordert grundsätzlich einen oder mehrere miteinander verbundene Fibre-Channel-Switche als Schaltzentrale zwischen den Endgeräten. Fibre-Channel-Switche haben zwischen acht und etwa 250 Ports, an die sowohl Endgeräte als auch weitere Switche angeschlossen werden. Switche realisieren unter anderem das Routing sowie die Basisdienste Name Service und Zoning. Große Switche, die meist auch ausfallsicherer sind als die kleinen, bezeichnet man in Anlehnung an die Großrechnerwelt als Director.

4 IP Storage: iSCSI und FCIP

Fibre Channel ist heute eine etablierte Technik für Speichernetze und in fast allen Situationen die richtige Wahl. Dennoch zeichnet sich die Entwicklung ab, dass sich IP-basierte Speichernetze als Alternative zu Fibre Channel etablieren. Mit Internet SCSI (iSCSI) und Fibre Channel over IP (FCIP) stehen zwei Protokolle bereit, den blockorientierten Datenverkehr für Speichernetze über IP zu übertragen.

FCIP ist ein Tunneling-Protokoll, das zwei Fibre-Channel-Netze über eine IP-Strecke miteinander verbindet. Die Koppelung von

Speichernetzen über größere Distanzen ist wichtig für das automatische Kopieren von Bändern oder Festplatten zur Vorbeugung vor größeren Katastrophen. Bisher war hierzu hoher technischer Aufwand notwendig, da schwieriger zu handhabende WAN-Techniken wie DWDM oder SONET/SDH eingesetzt werden mussten.

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 Fibre Channel 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.

Im Zusammenhang mit iSCSI und FCIP hört man oft die Befürchtung, dass TCP/IP/Ethernet nicht leistungsfähig genug ist für die Realisierung von Speichernetzen. In Messungen über eine 10km-Gigabit-Ethernetstrecke wurden jedoch beim Schreiben auf ein Band ein Durchsatz von 30-40 MByte/s gemessen. Performance-Engpass war also das Bandlaufwerk und nicht das Netz. Es ist davon auszugehen, dass iSCSI und FCIP den meisten Performance-Anforderungen gerecht wird, zumal 10Gigabit-Ethernet vor der Tür steht. Lediglich für sehr hohe Performance-Anforderungen muss man sehen, ob iSCSI eine Alternative zu Fibre Channel ist, da der Protokoll-Overhead für iSCSI/TCP/IP/Ethernet deutlich größer ist als der für FCP/Fibre Channel.

5 Hochverfügbarkeit mit Speichernetzen

Die Anforderung der Hochverfügbarkeit ist heute einer der wichtigsten Gründe für die Einführung von Speichernetzen. Inzwischen sind Festplatten mit einer Kapazität von weit über 100GB erhältlich. Das heißt, mit einem RAID Controller (beispielsweise einem RAID-fähigen SCSI-Adapter) und einer handvoll Festplatten kann der Speicherbedarf sehr vieler Anwendungen befriedigt werden. Das Problem dabei: die Festplatten sind in einem Server eingebaut; bei Ausfall des Servers ist kein Zugriff auf die Daten möglich. Ist die Serverhardware defekt, so kann einige Zeit vergehen, bis die Festplatten samt RAID Controller in einem neuen Server eingebaut sind und die Anwendung wieder in Betrieb ist.

Abhilfe schafft hier ein Speichernetz. Hierbei werden wie besprochen die Festplatten aus dem Server ausgelagert und in einem

externen Disksubsystem untergebracht. Das Disksubsystem fasst seine internen physikalischen Festplatten mittels RAID zu virtuellen Festplatten zusammen und bietet so den gleichen Schutz vor Plattenfehlern wie ein im Server eingebauter RAID Controller. Darüber hinaus sind alle weiteren Komponenten heutiger Disksubsysteme redundant ausgelegt.

Mit einer sogenannten “Dual Fabric” (Abbildung 9) kann man die Ausfallsicherheit eines IT-Systems deutlich verbessern. Hierbei wird ein Server 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.

Schwachstelle der Dual Fabric sind also die Server. Bei Ausfall eines Servers können die entsprechenden Speicherbereiche per Softwarekonfiguration einem anderen Server zugewiesen werden. Wird dieser Vorgang manuell durchgeführt, so ist dies immer noch

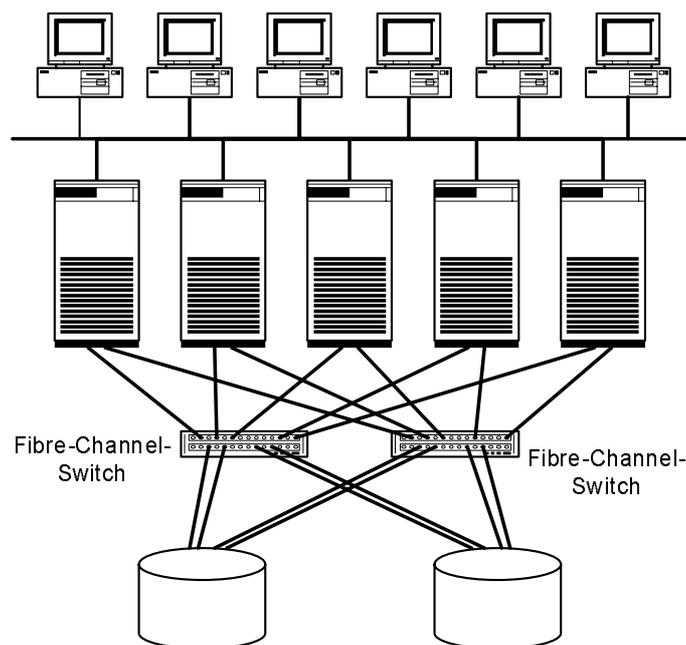


Abbildung 9: Die “Dual Fabric” ist eine typische Einstiegskonfiguration in ein Fibre Channel SAN. Bei ihr sind alle Komponenten des I/O-Pfades (Fibre-Channel-Hostbus-Adapter, Switches und Kabel) redundant ausgelegt, so dass bei Ausfall einer Komponente im Speichernetz der Server weiterhin auf die Daten zugreifen kann.

schneller, als der Umbau interner Festplatten. Die Übernahme der Festplatten durch einen zweiten Server kann mit entsprechender Clustersoftware automatisiert werden, so dass die Reaktionszeit hierfür noch kürzer ist.

6 Netzwerkdatensicherung

Neben der Hochverfügbarkeit und der Speicherkonsolidierung sind Anforderungen an die Datensicherung ein weiterer Grund für den Einsatz von Speichernetzen. Der Vorgang der Datensicherung beziehungsweise der Datenwiederherstellung kann mit Hilfe von Disksubsystemen und von Speichernetzen deutlich beschleunigt werden.

Generell bereitet die Datensicherung Systemverwaltern immer wieder Kopfzerbrechen. Es müssen immer mehr Daten in immer kürzerer Zeit gesichert werden. Moderne Betriebssysteme bringen zwar eigene Werkzeuge zur Datensicherung mit. Jedoch stellen diese Werkzeuge nur Insellösungen dar, die bei steigender Anzahl und Heterogenität der zu sichernden Systeme völlig unzureichend sind. Es fehlt beispielsweise die Möglichkeit, zentral zu überwachen, ob alle Datensicherungen über Nacht erfolgreich durchgelaufen sind, oder es mangelt an einer übergeordneten Verwaltung der Sicherungsmedien.

Abhilfe schaffen hier sogenannte Netzwerkdatensicherungssysteme, die selbst heterogene Umgebungen weitgehend automatisch sichern können. Dabei handelt es sich um Client-Server-Anwendungen, wobei ein Backup-Server die Sicherungsmedien zentral verwaltet. Auf den zu sichernden Rechnern wird plattformspezifische Client-Software installiert, die die Daten über das LAN zum Backup-Server sichert (Abbildung 10).

Abbildung 10 veranschaulicht auch gleich die Engpässe der Netzwerkdatensicherung: Sie belastet das Benutzer-LAN und alle zu sichernden Daten müssen durch die Busse des Sicherungservers geschleust werden. Dennoch ist die Sicherung über LAN für die meisten Rechner völlig ausreichend. Allerdings findet sich in fast jeder IT-Umgebung mindestens ein schwergewichtiger Server (Datenbankserver, Fileserver), für den eine Sicherung über LAN nicht mehr praktikabel ist.

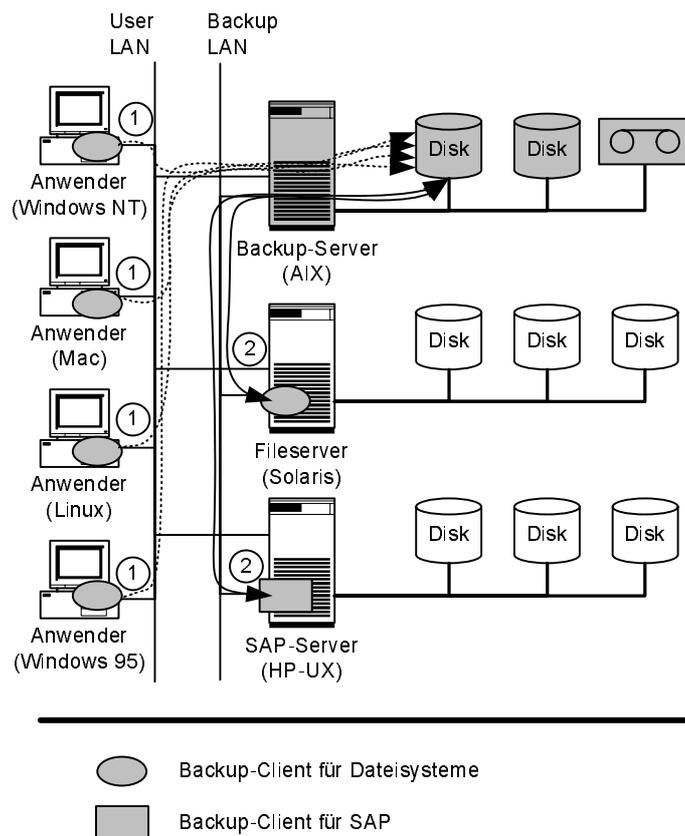


Abbildung 10: Netzwerkdatensicherungssysteme sichern alle Daten auf einen zentralen Backupserver. Normale Clients werden nach wie vor über das Benutzer-LAN gesichert (1). Schwergewichtige Clients werden über ein zweites LAN gesichert, um das Benutzer-LAN zu entlasten (2).

Eine Verbesserung bringt hier die Datensicherung über Speichernetze (Abbildung 11). Technisch ideal ist das sogenannte Server-free Backup, bei dem unter Steuerung des Netzwerkdatensicherungssystems die Daten direkt von dem Disksubsystem über das Speichernetz auf das Sicherungsmedium kopiert werden. Dies entlastet das Benutzer-LAN sowie die Busse von beiden Servern, also dem Backupserver und dem Anwendungsserver. Server-Free Backup ist heute noch vergleichsweise aufwändig zu realisieren, so dass es in Produktionsumgebungen derzeit kaum eingesetzt wird.

Dagegen findet sich LAN-free Backup oft in Produktionsumgebungen. Hierbei sichert der Backup-Client auf dem Anwendungs-

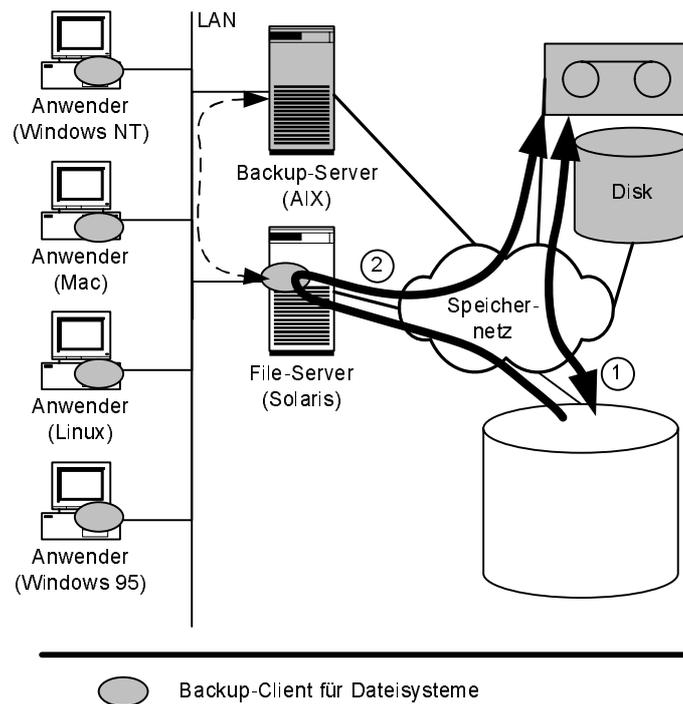


Abbildung 11: Die Datensicherung über Speichernetze entlastet das Benutzer-LAN. Server-free Backup sichert die Daten direkt von der Ursprungsfestplatte auf das Sicherungsmedium, so dass es zusätzlich die Busse von Anwendungsserver und Backupserver entlastet (1). LAN-free Backup entlastet nur die Busse des Backup-Servers (2); dafür ist es einfacher zu realisieren als Server-Free Backup.

server die Daten über das Speichernetz direkt auf die Sicherungsmedien, wobei der Backupserver die Sicherungsmedien nach wie zentral verwaltet. Man kann LAN-free Backup heute durchaus als Standardtechnik für die Sicherung großer Datenmengen bezeichnen. Die Busse des Anwendungsrechners werden zwar weiterhin stark beansprucht. Dafür werden das Benutzer-LAN und die Busse des Backup-Servers entlastet, so dass dieser mehrere Sicherungen parallel betreiben kann.

Trotz der Vorteile von LAN-Free Backup und Server-Free Backup, kann die Sicherung großer Datenmengen einige Stunden dauern. Dies ist für Anwendungen, die Rund um die Uhr verfügbar sein müssen, nicht mehr akzeptabel. Mit Hilfe von Instant Copies kann die Unterbrechung des Anwendungsbetriebs selbst bei sehr großen Datenbeständen auf wenige Minuten reduziert werden (Abbildung 12).

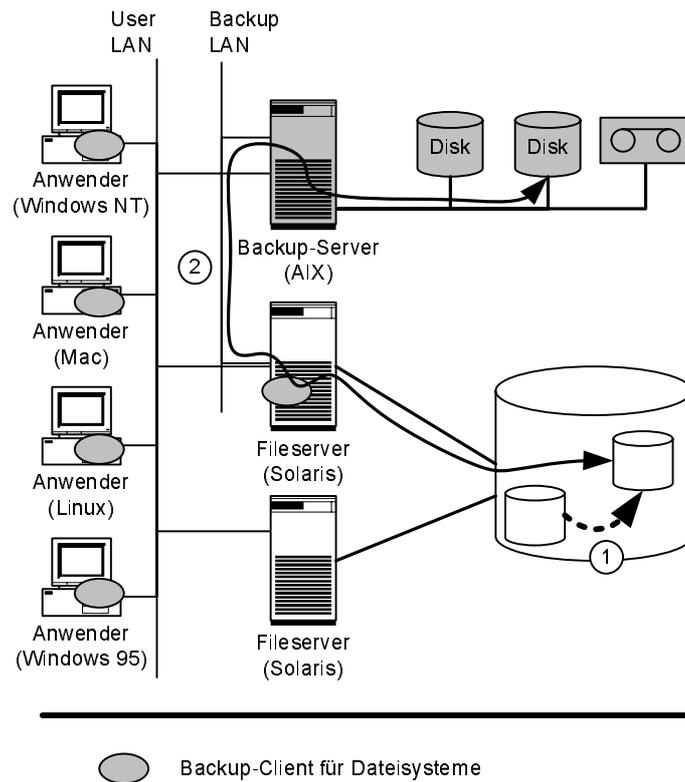


Abbildung 12: Die Anwendung wird für kurze Zeit so betrieben, dass sich auf den Festplatten ein konsistenter Datenzustand befindet, der mittels Instant Copy innerhalb von wenigen Sekunden (virtuell) kopiert wird (1). Danach kann die Anwendung sofort wieder auf Normalbetrieb umschalten; die Daten werden parallel zum Anwendungsbetrieb von der Instant Copy gesichert (2).

Hierbei wird dem Anwendungsserver ein zweiter Server zur Seite gestellt, der ausschließlich der Datensicherung dient. Beide Server sind direkt über SCSI oder über ein Speichernetz mit dem Disksubsystem verbunden, wobei ein Speichernetz hierbei nicht unbedingt notwendig ist. Für die Datensicherung wird zunächst die Instant Copy wie im Beispiel „Serverupgrade mit Speichernetzen“ beschrieben erzeugt: (1.) Anwendung herunterfahren, (2.) Instant Copy erzeugen und (3.) Anwendung neu starten. Danach wird von dem zweiten Rechner aus auf die Instant Copy zugegriffen und die Daten werden von dort aus parallel zum Anwendungsbetrieb gesichert. Wird die Instant Copy im Disksubsystem aufgehoben, so können im Fehlerfalle die Daten mit dieser Kopie in wenigen Sekunden wiederhergestellt werden.

7 Network Attached Storage (NAS)

Die bisher besprochenen Techniken und Anwendungsbeispiele sind den blockorientierten Speichernetzen zuzuordnen. Im Gegensatz dazu kommen wir mit dem Network Attached Storage (NAS) nun zu einer dateiorientierten Technik. NAS-Server sind vorkonfigurierte Fileserver, die vom Hersteller speziell für das Filesharing optimiert werden. 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 ein neuentwickeltes Betriebssystem oder um ein Windows oder ein Unix, das speziell für das Filesharing getuned wurde.

NAS-Server haben gegenüber selbstkonfigurierten Fileservern zwei Vorteile: Durch die Optimierung für das Filesharing können sie aus vergleichbarer Hardware mehr herausholen als ein universelles Betriebssystem. Außerdem werden vom Hersteller bereits wichtige Einstellungen für das Filesharing vorgenommen, so dass der Administrationsaufwand für NAS-Server geringer ist als für herkömmliche selbstkonfigurierte Fileserver. Beispielsweise konfigurieren die Hersteller für auf Windows 2000 basierenden NAS-Servern die notwendigen Einstellungen für das heterogene Filesharing zwischen Unix, Windows, Novell und MacOS vor. Weiterhin ist oft zusätzliche Software vorinstalliert, wie Virens Scanner, Software für Snapshots von NTFS-Dateisystemen oder Software für die Spiegelung von Dateien auf einen zweiten NAS-Server (Replikation) zur Erhöhung der Ausfallsicherheit. Die Vorkonfigurierung der NAS-Server spart jede Menge Administrationsaufwand — für die Behandlung von Fehlersituation sind jedoch weiterhin tiefere Kenntnisse des einem NAS-Server zugrundeliegendem Betriebssystems erforderlich.

Die Produktkategorie der NAS-Server gliedert sich in drei große Bereiche: kleinere NAS-Server als klassische Fileserver für Abteilungen oder Projekte, große NAS-Server als Webserver für Internetportale und schließlich die sogenannten NAS Gateways, manchmal auch als NAS Heads bezeichnet. NAS Gateways verfügen über keine internen Platten, stattdessen speichern sie ihre Daten auf einem im Speichernetz vorhandenem Disksubsystem. Dafür sind sie mit der notwendigen Hardware (beispielsweise Fibre-Channel-Hostbus-Adapter) und Software (Fibre Channel oder künftig iSCSI Device Driver) ausgestattet. NAS Gateways sind vor allem dann vorteilhaft, wenn ein lokales Speichernetz bereits vorhanden ist.

Fälschlicher Weise werden auch heute noch NAS und SAN (also

Fileserver und Speichernetze) manchmal als sich widersprechende Konzepte dargestellt. Bei NAS und Speichernetzen handelt es sich jedoch um zwei Techniken, die unterschiedliche Anforderungen adressieren und sich hervorragend miteinander kombinieren lassen. Speichernetze (Fibre Channel SANs und iSCSI SANs) verbinden Server und Speichergeräte auf Blockebene. Der Datenaustausch erfolgt mit dem 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 vorhandenen Bandlaufwerke benutzen.

8 Verwaltung von Speichernetzen: Bluefin und Virtualisierung

Je nach Größe eines IT-Systems erfordert die Verwaltung der Speicherressourcen und des Speichernetzes erheblichen Aufwand. Beispielsweise ist es heute schwierig, folgende Fragen schnell zu beantworten: Welcher Server belegt wieviel Platz auf welchen Speichersystemen? Wie weit sind die darauf angelegten Dateisysteme gefüllt? Wie ist der Status der einzelnen Komponenten?

Wünschenswert wäre ein zentrales Verwaltungssystem, das die Überwachung, das Reporting und die Konfiguration aller Speicherressourcen ermöglicht. Stattdessen werden Speichersysteme, Hostbus-Adapter, SAN Switches, Volume Manager, Datenbanken, Dateisysteme, NAS-Server und so weiter mit proprietären Verwaltungswerkzeugen, sogenannten Element-Managern ausgeliefert, die nur die Verwaltung einzelner Komponenten erlauben.

Ein Ansatz zur Entwicklung solcher Verwaltungssysteme ist die Standardisierung der entsprechenden Schnittstellen zu den einzelnen Komponenten. Dies ist Voraussetzung dafür, dass die Hersteller von Verwaltungssystemen den Entwicklungs- und Testaufwand für die Integration von Komponenten verschiedener Hersteller bewältigen können. Die Praxis hat gezeigt, dass das Simple Network Management Protocol (SNMP) für diese Zwecke nicht ausreichend ist. Besserung ist mit der Storage Management Interface Specification (SMIS), besser bekannt unter Bluefin, in Sicht. Bluefin spezifiziert hierzu die entsprechenden Schnittstellen und Hilfsdienste.

Ein anderer Ansatz ist die Speichervirtualisierung. Sie soll die

Kosten für die Speicherverwaltung reduzieren, indem es den Zugriff auf die gespeicherten Daten sowie deren Verwaltung vereinfacht. Man unterscheidet zwischen Virtualisierung auf Blockebene und Virtualisierung auf Dateiebene. Je nachdem kann man sich die Virtualisierung als Volume Manager oder als Dateisystem im Speichernetz vorstellen, die als zusätzliche Schicht zwischen den Servern und den Speichergeräten eingefügt wird. Speichervirtualisierung vereinfacht die Speicherverwaltung indem es die Speicherressourcen über Server- und Speichergerätegrenzen hinweg verwaltet und somit eine zentrale Sicht auf die Speicherressourcen ermöglicht.

9 Zusammenfassung

Der Einsatz von Speichernetzen ändert die IT-Architektur nachhaltig: Sie ersetzen die SCSI-Kabel zwischen Servern und Speichergeräten durch ein neues Netz; Speicher existiert nun unabhängig von einem Server. Es gibt viele Techniken für die Realisierung von Speichernetzen. Am wichtigsten ist heute der Fibre Channel. In naher Zukunft wird der Einsatz von IP-basierten Speichernetzen vermutlich stark zunehmen. Unabhängig von der zugrundeliegenden Übertragungstechnik bieten Speichernetze Vorteile bezüglich der Hochverfügbarkeit und der flexiblen Zuweisung freier Speicherkapazität an die einzelnen Server. Im Zusammenspiel mit Disksubsystemen bieten Speichernetze viele Möglichkeiten, die Datensicherung zu beschleunigen. Während die Hardware von Speichernetzen heute schon sehr gut funktioniert, wird mehr Software benötigt, die neuen Möglichkeiten von Speichernetzen noch mehr auszunutzen. Hier sind insbesondere die Integration von Funktionen wie Instant Copy und Remote Mirroring in Anwendungen wie Datenbanken und Datensicherungssysteme, die automatisierte Zuweisung freier Ressourcen (Virtualisierung) sowie die zentrale Verwaltung von Speichernetzen zu nennen.

- [1] Ulf Troppens und Rainer Erkens: Speichernetze – Grundlagen und Einsatz von Fibre Channel SAN, NAS, iSCSI und InfiniBand, dpunkt.Verlag, 2003.
- [2] www.speichernetze.com/links.html: Zahlreiche Verweise zu weiterführenden Themen.

Ulf Troppens und Rainer Erkens sind Mitarbeiter im IBM Total-Storage Interoperability Center in Mainz und Autoren des Buches „Speichernetze – Grundlagen und Einsatz von Fibre Channel SAN, NAS, iSCSI und InfiniBand“.