7 Netzwerk-Datensicherung

Ziel des Kapitels

Netzwerk-Datensicherungssysteme können heterogene IT-Umgebungen mit mehreren Tausend Rechnern weitgehend automatisch sichern. In der klassischen Form bewegen Netzwerk-Datensicherungssysteme die zu sichernden Daten über das LAN, daher auch der Name »Netzwerk-Datensicherung«. Dieses Kapitel erklärt die Grundprinzipien der Netzwerk-Datensicherung und zeigt daran typische Performance-Engpässe für herkömmliche, serverzentrierte IT-Architekturen. Schließlich zeigt es, wie Speichernetze und intelligente Speichersysteme helfen, diese Performance-Engpässe zu überwinden.

Gliederung des Kapitels

Bevor auf technische Details eingegangen wird, werden zunächst einige Rahmenbedingungen besprochen, die bei der Datensicherung zu berücksichtigen sind (Kapitel 7.1). Dann werden die Dienste Datensicherung, Archivierung und hierarchische Speicherverwaltung erläutert (Kapitel 7.2) und gezeigt, welche Komponenten zu deren Implementierung notwendig sind (Kapitel 7.3 und 7.4). Es folgt eine Zusammenfassung der bis dahin besprochenen Maßnahmen, die Netzwerk-Datensicherungssysteme zur Performance-Steigerung bieten (Kapitel 7.5). Im Anschluss daran werden anhand der Netzwerk-Datensicherung weitere technische Grenzen serverzentrierter IT-Architekturen beschrieben (Kapitel 7.6), die über Kapitel 1.1 hinausgehen, und es wird begründet, dass diese Performance-Engpässe innerhalb der serverzentrierten IT-Architektur nur sehr eingeschränkt überwunden werden können (Kapitel 7.7). Dann wird gezeigt, wie mit einer speicherzentrierten IT-Architektur Daten wesentlich effizienter gesichert werden können (Kapitel 7.8). Darauf aufbauend wird die Sicherung von Fileservern (Kapitel 7.9) und Datenbanken (Kapitel 7.10) mit Speichernetzen und Netzwerk-Datensicherungssystemen diskutiert. Schließlich werden organisatorische Aspekte der Datensicherung behandelt (Kapitel 7.11).

7.1 Rahmenbedingungen der Datensicherung

Sicherungswerkzeuge der Betriebssysteme sind Insellösungen.

Datensicherung bereitet 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.

Wechselnde Rahmenbedingungen erschweren die Datensicherung zusätzlich. Hierfür sind vor allem drei Gründe zu nennen:

Rapides Wachstum der zu sichernden Datenmenge

1. Wie bereits in Kapitel 1 besprochen, verdoppelt sich die installierte Speicherkapazität je nach Unternehmen alle vier bis zwölf Monate. Dabei wächst der Datenbestand oft schneller als die allgemeine Infrastruktur (Personal, Netzkapazität). Trotzdem müssen die immer größeren Datenmengen gesichert werden.

Ständige Veränderung der zu sichernden Systeme und Anwendungen

2. In der heutigen Zeit müssen Geschäftsprozesse permanent an sich wandelnde Anforderungen angepasst werden. Mit der Veränderung der Geschäftsprozesse müssen auch die IT-Systeme angepasst werden, die diese unterstützen. Infolgedessen muss auch die tägliche Datensicherung kontinuierlich auf die sich ständig wandelnde IT-Infrastruktur abgestimmt werden.

Verkürzung des Zeitfensters für die Datensicherung

3. Durch Globalisierung, Internet und E-Business müssen immer mehr Daten rund um die Uhr verfügbar sein: Man kann es sich nicht mehr leisten, Anwendungen und Daten stundenlang für Benutzerzugriffe zu sperren, um die Daten in Ruhe zu sichern. Das Zeitfenster für die Datensicherung wird also immer kleiner.

Netzwerk-Datensicherung kann helfen, diese Probleme in den Griff zu bekommen.

7.2 Dienste der Netzwerk-Datensicherung

Dienste der Netzwerk-Datensicherung

Netzwerk-Datensicherungssysteme wie Computer Associates Arcserve, EMC Legato Networker, HP Omniback, IBM Tivoli Storage Manager oder Symantec Veritas NetBackup stellen unter anderem folgende drei Dienste zur Verfügung:

- Datensicherung (Backup)
- Archivierung
- Hierarchische Speicherverwaltung

Datensicherung (Backup)

Die Hauptaufgabe von Netzwerk-Datensicherungssystemen ist, regelmäßig Daten zu sichern (Backup). Dazu muss von allen Daten mindestens eine aktuelle Kopie gehalten werden, sodass sie nach einem Hardware- oder Anwendungsfehler (»Datei aus Versehen gelöscht oder

kaputt editiert«, »Fehler in der Datenbankprogrammierung«) wieder hergestellt werden können.

Archivierung

Aufgabe der Archivierung ist es, eine bestimmte Version der Daten einzufrieren, um später genau diese Version wiederherstellen zu können. Beispielsweise können nach Abschluss eines Projektes dessen Daten auf dem Backup-Server archiviert und danach von der lokalen Festplatte gelöscht werden. Dies spart lokalen Plattenplatz und beschleunigt Backup- und Restore-Prozesse, denn es müssen nur noch diejenigen Daten gesichert beziehungsweise wiederhergestellt werden, mit denen aktuell gearbeitet wird. Die Archivierung von Daten hat in den letzten Jahren so stark an Bedeutung gewonnen, dass wir sie im nächsten Kapitel gesondert (Kapitel 8) behandeln.

Hierarchische Speicherverwaltung (HSM)

Hierarchische Speicherverwaltung (Hierarchical Storage Management, HSM) schließlich gaukelt den Endanwendern quasi beliebig große Festplatten vor. HSM verlagert Dateien, auf die seit längerem nicht zugegriffen wurde, von der lokalen Festplatte auf den Backup-Server; im lokalen Dateisystem bleibt dann nur ein Eintrag im Directory stehen. Der Eintrag im Directory enthält Metainformationen wie Dateiname, Besitzer, Zugriffsrechte, Datum der letzten Änderung und so weiter. Im Dateisystem benötigen die Metadaten im Vergleich zu den eigentlichen Dateiinhalten kaum Platz, sodass durch die Verschiebung der Dateiinhalte von der lokalen Festplatte auf den Backup-Server wirklich Platz gewonnen wird.

Zugriff auf ausgelagerte Dateien

Greift nun ein Prozess auf den Inhalt einer solchen ausgelagerten Datei zu, blockiert HSM den zugreifenden Prozess, kopiert den Dateiinhalt vom Backup-Server zurück in das lokale Dateisystem und gibt erst dann den zugreifenden Prozess wieder frei. Für zugreifende Prozesse und somit auch für Endanwender ist dieser Vorgang bis auf die längere Zugriffszeit vollkommen verborgen. Ältere Dateien können so automatisch auf billigere Medien (Bänder) ausgelagert und gegebenenfalls zurückgeholt werden, ohne dass der Endanwender seine Verhaltensweisen ändern muss.

HSM vs. Datensicherung

Genau genommen sind HSM und Datensicherung beziehungsweise Datenarchivierung voneinander unabhängige Konzepte. Dennoch ist HSM Bestandteil vieler Netzwerk-Datensicherungsprodukte, wodurch die gleichen Komponenten (Medien, Software) sowohl für die Datensicherung als auch für HSM eingesetzt werden können. Beim Einsatz von HSM muss die eingesetzte Backup-Software zumindest HSM-fähig sein. Sie muss die Metadaten von verlagerten Dateien sowie die verlagerten Dateien selbst sichern, ohne die Dateiinhalte auf den Client zurückzuschaufeln. HSM-fähige Backup-Software kann Backup- und Restore-Prozesse verkürzen, weil von den ausgelagerten Dateien nur die Me-

tainformationen gesichert und wiederhergestellt werden müssen, aber nicht deren Dateiinhalte.

Realisierung als Client-Server-Anwendung

Ein Netzwerk-Datensicherungssystem realisiert die soeben vorgestellten Dienste Datensicherung, Archivierung und hierarchische Speicherverwaltung durch das Zusammenspiel von Backup-Server und einer Reihe von Backup-Clients (Abbildung 7.1). Der Server stellt zentrale Komponenten wie die Verwaltung der Backup-Medien bereit, die von allen Backup-Clients benötigt werden. Für unterschiedliche Betriebssysteme und Anwendungen kommen jeweils unterschiedliche Backup-Clients zum Einsatz. Diese sind auf die einzelnen Betriebssysteme beziehungsweise Anwendungen spezialisiert, um die Effizienz der Datensicherung beziehungsweise der Datenverlagerung zu erhöhen.

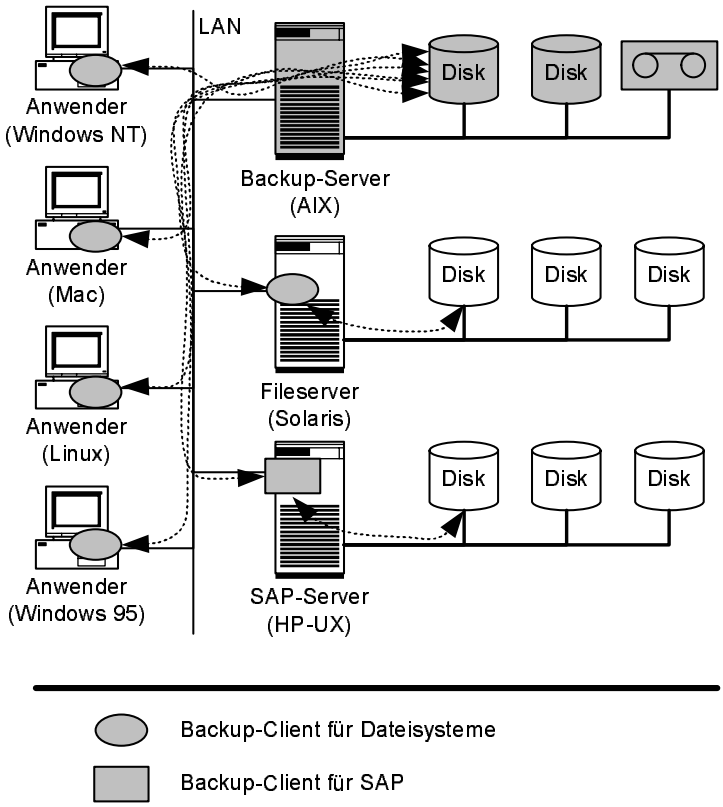

Abbildung 7.1
Netzwerk-Datensicherungssysteme können heterogene IT-Umgebungen automatisch über das LAN sichern. Auf allen zu sichernden Clients muss ein plattformspezifischer Backup-Client installiert werden.

Sprachgebrauch: »Backup-Server« und »Backup-Client«

Für Netzwerk-Datensicherungssysteme ist der Sprachgebrauch etwas nachlässig: Die Hauptaufgabe von Netzwerk-Datensicherungssystemen ist die Sicherung (Backup) von Daten. Server- und Clientinstanzen von Netzwerk-Datensicherungssystemen werden deshalb oft nur Backup-Server und Backup-Client genannt, unabhängig davon, was sie im Einzelnen leisten oder wofür sie gerade eingesetzt werden. Eine bestimmte Serverinstanz eines Netzwerk-Datensicherungssystems könnte

beispielsweise ausschließlich für HSM eingesetzt werden, sodass diese Instanz eigentlich HSM-Server genannt werden müsste – trotzdem wird diese Instanz meist als Backup-Server bezeichnet. Ein Client, der den Dienst Datensicherung (Backup) bereitstellt, unterstützt meistens auch die Dienste Archivierung und Wiederherstellung von Sicherungen und Archiven – trotzdem wird dieser Client in der Regel nur als Backup-Client bezeichnet. In diesem Buch folgen wir dem allgemeinen unsauberen Sprachgebrauch, weil Backup-Client einfach flüssiger zu lesen ist als Backup-Archivierungs-HSM-und-Wiederherstellungs-Client.

Weitere Vorgehensweise

Die beiden folgenden Abschnitte besprechen Details des Backup-Servers (Kapitel 7.3) und der Backup-Clients (Kapitel 7.4). Im Anschluss daran werden die Performance und der Einsatz von Netzwerk-Datensicherungssystemen betrachtet.

7.3 Serverkomponenten

Gliederung des Unterkapitels

Backup-Server bestehen aus einer ganzen Reihe von Komponenten. Im Folgenden stellen wir die wichtigsten Komponenten vor: Job Scheduler (Abschnitt 7.3.1), Error Handler (Abschnitt 7.3.2), Metadaten-Datenbank (Abschnitt 7.3.3) und Media Manager (Abschnitt 7.3.4).

7.3.1 Job Scheduler

Job Scheduler

Der Job Scheduler bestimmt, wann welche Daten gesichert werden. Er muss sorgfältig konfiguriert werden; die eigentlichen Datensicherungen laufen dann automatisch ab.

Automation durch Job Scheduler und Tape Library

Mit Hilfe von Job Scheduler und Tape Libraries können über Nacht viele Rechner gesichert werden, ohne dass ein Systemverwalter vor Ort Bänder wechseln muss. Kleine Tape Libraries haben ein Bandlaufwerk, ein Magazin mit Platz für etwa zehn Bänder und eine Wechselvorrichtung, die die verschiedenen Bänder automatisch zwischen Magazin und Bandlaufwerk hin- und herbewegen kann. Große Tape Libraries haben mehrere Dutzend Bandlaufwerke, Platz für mehrere Tausend Bänder und einen oder zwei Roboter zum Einlegen der Bänder.

7.3.2 Error Handler

Error Handler

Bei regelmäßiger automatischer Sicherung vieler Systeme wird es schwierig zu überwachen, ob alle automatisierten Sicherungen fehlerfrei durchgelaufen sind. Der Error Handler hilft, die Fehlermeldungen zu priorisieren, zu filtern und Berichte zu erstellen. So soll vermieden werden, dass Probleme bei der Datensicherung erst dann bemerkt werden, wenn ein Backup wieder eingespielt werden soll.

7.3.3 Metadaten-Datenbank

Metadaten-Datenbank

Die Metadaten-Datenbank und der Media Manager stellen zwei eher verborgene Komponenten dar. Die Metadaten-Datenbank ist das Gehirn eines Netzwerk-Datensicherungssystems. Sie enthält für jedes gesicherte Objekt etwa folgende Einträge: Name, Ursprungsrechner, Datum der letzten Änderung, Datum des letzten Backups, Name des Backup-Mediums usw. Beispielsweise erfolgt für jede zu sichernde Datei ein Eintrag in die Metadaten-Datenbank.

Incremental-Forever-Strategie zur Datensicherung

Der Aufwand für die Metadaten-Datenbank lohnt sich. Im Gegensatz zu von Betriebssystemen bereitgestellten Backup-Werkzeugen ermöglichen Netzwerk-Datensicherungssysteme die Umsetzung der Incremental-Forever-Strategie, bei der ein Dateisystem nur bei der ersten Sicherung vollständig gesichert wird. Bei anschließenden Sicherungen werden dann immer nur die Dateien gesichert, die seit der letzten vorhergehenden Sicherung geändert wurden. Auf dem Backup-Server kann dann durch Datenbankoperationen aus der ursprünglichen Vollsicherung und aus allen folgenden inkrementellen Teilsicherungen der aktuelle Zustand des Dateisystems berechnet werden, sodass keine weiteren Vollsicherungen mehr notwendig sind. Die Berechnungen in der Metadaten-Datenbank sind in der Regel schneller durchgeführt als eine neue Vollsicherung.

Point-in-Time Restore

Es ist sogar noch mehr möglich: Werden auf dem Backup-Server mehrere Versionen der Dateien gesichert, so kann beispielsweise ein ganzes Dateisystem oder ein Unterverzeichnis mit dem Stand von vor drei Tagen wiederhergestellt werden (Point-in-Time Restore) – die Metadaten-Datenbank macht es möglich.

7.3.4 Media Manager

Media Manager und Incremental-Forever-Strategie

Durch die Incremental-Forever-Strategie kann die Zeit für die Datensicherung im Vergleich zur Vollsicherung erheblich reduziert werden. Nachteil hierbei ist, dass die gesicherten Dateien im Laufe der Zeit über eine Vielzahl von Bändern verteilt sein können. Dies ist kritisch für die Wiederherstellung großer Dateisysteme, weil das Einlegen der Bänder (Tape Mounts) Zeit kostet. Hier kommt der Media Manager ins Spiel. Er kann dafür sorgen, dass auf einem Band nur Dateien eines einzigen Rechners liegen. Dies reduziert die Anzahl der Tape Mounts für Restore-Prozesse, sodass die Daten schneller wiederhergestellt werden können.

Tape Reclamation

Eine weitere wichtige Funktion des Media Managers ist die sogenannte Tape Reclamation. Infolge der Incremental-Forever-Strategie befinden sich auf den Sicherungsbändern immer mehr Daten, die nicht

mehr notwendig sind. Wird zum Beispiel eine Datei im Laufe der Zeit gelöscht oder sehr oft geändert, so können frühere Versionen der Datei auf den Sicherungsmedien gelöscht werden. Die so frei werdenden Lücken auf den Bändern können mit heutigen Techniken nicht direkt überschrieben werden. Bei der Tape Reclamation kopiert der Media Manager die verbleibenden, noch benötigten Dateien mehrerer Bänder, die nur noch zu einem gewissen Prozentsatz genutzt werden, auf ein gemeinsames neues Band. Die so freigeschaufelten Bänder werden dann wieder dem Vorrat ungenutzter Bänder hinzugefügt.

Streaming

Es gibt noch eine weitere technische Einschränkung beim Umgang mit Bändern. Heutige Bandlaufwerke können die Daten nur mit einer gewissen Geschwindigkeit auf die Bänder schreiben. Werden die Daten zu langsam an das Bandlaufwerk übertragen, so bricht dieses den Schreibvorgang ab, spult das Band ein Stück zurück und setzt dann den Schreibvorgang wieder fort. Das ständige Zurückspulen der Bänder kostet Performance und nutzt die Bänder unnötig ab, sodass sie schneller ausgemustert werden müssen. Besser ist es deshalb, die Daten schnell genug an das Bandlaufwerk zu senden, damit es die Daten in einem »Rutsch« auf das Band schreiben kann (Streaming).

LAN-Engpässe behindern Streaming

Das Problem dabei: Bei der Netzwerk-Datensicherung senden die Backup-Clients die zu sichernden Daten über das LAN an den Backup-Server, der die Daten an das Bandlaufwerk weiterleitet. Auf der Strecke vom Backup-Client über das LAN zum Backup-Server kommt es immer wieder zu Schwankungen der Übertragungsrate, wodurch das Streaming des Bandlaufwerks immer wieder unterbrochen wird. Es ist zwar möglich, für einzelne Clients durch zusätzliche Maßnahmen wie die Installation eines separaten LAN zwischen Backup-Client und Backup-Server Streaming zu erreichen (Kapitel 7.7). Diese Maßnahmen sind jedoch teuer und technisch nicht beliebig skalierbar, womit sie nicht für alle Clients wirtschaftlich realisierbar sind.

Lösung: Speicherhierarchie im Backup-Server

Die Lösung: Der Media Manager verwaltet innerhalb des Backup-Servers eine Speicherhierarchie. Der Backup-Server muss dazu mit Festplatten und Tape Libraries ausgestattet sein. Für alle Clients, die die Daten nicht schnell genug für das Streaming liefern können, speichert der Media Manager die zu sichernden Daten zunächst auf Festplatte ab. Beim Schreiben auf Festplatte ist es egal, mit welcher Geschwindigkeit die Daten angeliefert werden. Wenn genügend zu sichernde Daten auf den Festplatten des Backup-Servers zwischengespeichert sind, verschiebt der Media Manager automatisch größere Datenmengen von den Festplatten des Backup-Servers auf dessen Bänder. Hierbei werden die Daten nur innerhalb des Backup-Servers umkopiert, sodass hier wieder das Streaming beim Beschreiben der Bänder gewährleistet ist.

Beispiel: Sicherung von Desktop-PCs

Diese Speicherhierarchie hilft zum Beispiel bei der Sicherung von Benutzer-PCs (Abbildung 7.2). Viele Anwender schalten ihre Rechner abends aus, sodass eine Sicherung über Nacht nicht gewährleistet werden kann. Deshalb werden Benutzer-PCs häufig über die Mittagszeit gesichert. Durch Incremental-Forever ist die täglich zu sichernde Datenmenge so gering, dass eine solche Sicherungsstrategie in der Regel vertretbar ist. Alle Benutzer-PCs werden dabei zunächst beispielsweise in dem Zeitfenster von 11.15 Uhr bis 13.45 Uhr auf die Festplatten des Backup-Servers gesichert. Der Media Manager im Backup-Server hat dann gut zwanzig Stunden Zeit, um die Daten von den Festplatten auf Bänder zu verschieben. Danach sind die Festplatten wieder frei, sodass in der nächsten Mittagspause die Benutzer-PCs wieder auf Festplatte gesichert werden können.

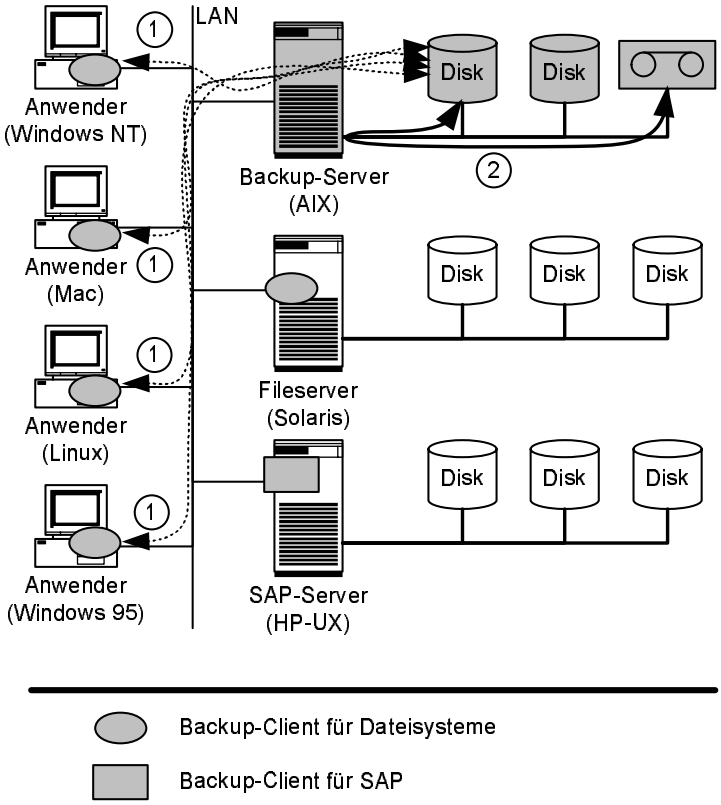

Abbildung 7.2
Die Speicherhierarchie im Backup-Server hilft, Anwender-PCs effizient zu sichern: Über die Mittagszeit werden alle PCs zunächst auf Festplatten des Backup-Servers gesichert (1). Der Media Manager hat nun bis zur nächsten Mittagspause Zeit, die Daten von den Festplatten auf Bänder umzukopieren (2).

Der Media Manager gewährleistet das Einlegen der richtigen Bänder.

Bei allen hier beschriebenen Operationen prüft der Media Manager, ob das jeweils richtige Band in das Laufwerk eingelegt wurde. Dazu schreibt der Media Manager auf jedes Band eine eindeutige Signatur, die er in der Metadaten-Datenbank vermerkt. Bei jedem Einlegen eines

Bands vergleicht der Media Manager die Signatur auf dem Band mit der Signatur in der Metadaten-Datenbank. So wird sichergestellt, dass keine Bänder unabsichtlich überschrieben und beim Restore auch die richtigen Daten zurückgeschrieben werden.

Der Media Manager überwacht das Altern der Bänder.

Weiter überwacht der Media Manager, wie oft ein Band benutzt wurde und wie alt es ist. Alte Bänder werden somit rechtzeitig ausgemustert. Gegebenenfalls kopiert er zuvor noch benötigte Daten auf ein neues Band. Außerdem müssen ältere Bandtypen ab und zu bewegt werden, damit sie länger halten; der Media Manager kann auch das Spulen länger nicht benutzter Bänder automatisieren.

Off-Site-Lager als Katastrophenschutz

Eine weitere wichtige Funktion des Media Managers ist die Verwaltung von Daten in einem sogenannten Off-Site-Lager. Dazu hält der Media Manager von allen zu sichernden Daten zwei Kopien. Die eine Kopie wird immer auf dem Backup-Server vorgehalten, damit im Bedarfsfall Daten schnell wieder hergestellt werden können. Bei einer größeren Katastrophe (Brand im Rechenzentrum) können allerdings die Kopien auf dem Backup-Server zerstört werden. Für solche Fälle hält der Media Manager eine zweite Kopie in einem Off-Site-Lager, das viele Kilometer entfernt sein kann. Der Media Manager unterstützt den Systemadministrator darin, die richtigen Bänder zwischen Backup-Server und Off-Site-Lager hin und her zu verlagern. Ja, er unterstützt sogar Tape Reclamation für Bänder, die sich gerade im Off-Site-Lager befinden, und er sorgt dafür, dass auch diese hin und wieder bewegt werden.

7.4 Backup-Clients

Basisclient für Dateisysteme

Für jede zu sichernde Plattform ist ein plattformspezifischer Client (Backup Agent) notwendig. Der Basisclient kann Dateien sichern und archivieren sowie die Dateien bei Bedarf wiederherstellen. Unter Plattform sind hier die verschiedenen Betriebssysteme und die von ihnen unterstützten Dateisysteme zu verstehen. Manche Basisclients bieten darüber hinaus HSM für ausgewählte Dateisysteme an.

Standard: Sicherung auf Dateiebene

Standardmäßig findet die Sicherung von Dateisystemen auf Dateiebene statt. Das heißt, jede geänderte Datei wird komplett neu an den Server übertragen und dort in die Metadaten-Datenbank eingetragen. Mit der Sicherung auf Volume-Ebene und der Sicherung auf Blockebene ist es möglich, die Granularität der zu sichernden Objekte zu ändern.

Alternative 1: Sicherung auf Volume-Ebene

Bei der Sicherung auf Volume-Ebene wird ein gesamtes Volume als ein einziges Objekt auf den Backup-Server gesichert. Man kann sich dies so vorstellen, dass die Ausgabe des Unix-Kommandos »dd« zum Backup-Server geschickt wird. Dies hat zwar den Nachteil, dass auch

freie Bereiche gesichert werden, auf denen gar keine Dateien abgelegt sind. Dafür sind auf dem Backup-Server nur sehr wenige Metadaten-Datenbank-Operationen notwendig und auf Clientseite muss nicht lange verglichen werden, welche Dateien sich seit der letzten Sicherung verändert haben. Dadurch können häufig Backups und Restores auf Volume-Ebene schneller durchgeführt werden als auf Dateiebene. Dies gilt insbesondere für die Wiederherstellung großer Dateisysteme mit vielen kleinen Dateien, da hierbei zeitgleich zur Wiederherstellung der Dateiinhalte zusätzlich das Dateisystem die Struktur des Dateisystems (Ordner und Verzeichnisse) neu anlegt.

Alternative 2: Sicherung auf Blockebene

Die Sicherung auf Blockebene optimiert die Sicherung für Außendienstmitarbeiter, die nur ab und zu mit ihrem Laptop über eine Wählleitung mit dem Firmennetz verbunden sind. Hier besteht der Performance-Engpass in der geringen Übertragungskapazität von Modem-, ISDN- oder VPN-Verbindungen. Wird von einer großen Datei auch nur ein Bit verändert, so muss die komplette Datei erneut durch die Wählleitung gezwängt werden. Für die Sicherung auf Blockebene hält sich der Backup-Client von jeder gesicherten Datei zusätzlich eine lokale Kopie. Wurde nun eine Datei verändert, so kann er feststellen, welche Teile der Datei verändert wurden. Der Backup-Client schickt dann nur die geänderten Dateifragmente (Blöcke) an den Backup-Server. Dieser kann dann die komplette Datei wieder rekonstruieren. Wie bei der Sicherung auf Dateiebene wird auch hier jede gesicherte Datei in die Metadaten-Datenbank eingetragen. Bei der Sicherung auf Blockebene wird also die Menge der zu übertragenden Daten reduziert zu Lasten des Speicherverbrauchs auf der lokalen Festplatte.

Anwendungsspezifische Clients

Neben den Standard-Clients für Dateisysteme stellen die meisten Netzwerk-Datensicherungssysteme spezielle Clients für verschiedene Anwendungen bereit. Beispielsweise gibt es spezielle Clients für IBM Lotus Domino oder Microsoft Exchange, die es ermöglichen, einzelne Dokumente zu sichern und wiederherzustellen. Später wird die Sicherung von Dateisystemen und NAS-Servern (Kapitel 7.9) und von Datenbanken (Kapitel 7.10) noch genauer diskutiert.

7.5 Performance-Gewinne durch Netzwerk-Datensicherung

Netzwerk-Datensicherungssysteme steigern die Effizienz der Datensicherung.

Die zugrunde liegenden Hardwarekomponenten bestimmen den maximalen Durchsatz von Netzwerk-Datensicherungssystemen. Die Softwarekomponenten bestimmen, wie effizient die vorhandene Hardware tatsächlich genutzt wird. An verschiedenen Stellen dieses Kapitels wurde

bereits besprochen, wie Netzwerk-Datensicherungssysteme helfen können, die bestehende Infrastruktur besser auszunutzen:

- *Performance-Steigerung durch Archivierung von Daten*
  Das Löschen bereits archivierter Daten von Festplatten kann die tägliche Datensicherung beschleunigen, weil weniger Daten zu sichern sind. Aus dem gleichen Grund können Dateisysteme schneller wiederhergestellt werden.

  Weniger lokale Daten durch Archivierung

- *Performance-Steigerung durch hierarchische Speicherverwaltung (HSM)*
  Durch die Verlagerung von Dateiinhalten auf den HSM-Server können Dateisysteme schneller wiederhergestellt werden. Für ausgelagerte Dateien können die Directory-Einträge vergleichsweise schnell wiederhergestellt werden; der Hauptteil der Daten, nämlich die Dateiinhalte, brauchen nicht vom HSM-Server zurückgeholt zu werden.

  Weniger lokale Daten durch HSM

- *Performance-Steigerung durch die Incremental-Forever-Strategie*
  Nach der ersten Sicherung werden nur noch die Daten gesichert, die seit der letzten vorherigen Sicherung geändert wurden. Auf dem Backup-Server wird mit Hilfe der Metadaten-Datenbank aus der ersten Sicherung und aus allen folgenden inkrementellen Sicherungen der letzte Zustand der Daten berechnet, sodass keine weiteren Vollsicherungen mehr notwendig sind. Das Zeitfenster für die Datensicherung kann so erheblich verkleinert werden.

  Incremental-Forever-Strategie

- *Performance-Steigerung durch Reduzierung der Tape Mounts*
  Der Media Manager kann dafür sorgen, dass zusammengehörige Daten nur über wenige Bänder verteilt werden. Für die Wiederherstellung von Daten kann so die Anzahl der zeitaufwendigen Bänderwechsel verringert werden.

  Reduzierung der Tape Mounts

- *Performance-Steigerung durch Streaming*
  Zum effizienten Beschreiben von Bändern ist es notwendig, dass die Daten schnell genug an das Bandlaufwerk übermittelt werden. Ist dies nicht gewährleistet, so kann der Backup-Server die Daten erst auf Festplatte zwischenspeichern und dann in einem Rutsch an das Bandlaufwerk senden.

  Schnelleres Beschreiben der Bänder durch Streaming

- *Performance-Steigerung durch Backup auf Volume-Ebene oder auf Blockebene*
  Standardmäßig werden Dateisysteme auf Dateiebene gesichert. Große Dateisysteme mit vielen Hunderttausend Dateien können manchmal schneller gesichert werden, wenn sie auf Volume-Ebene gesichert werden. Laptops können schneller gesichert werden, wenn nur diejenigen Blöcke, die verändert wurden, über das Modem an den Backup-Server übermittelt werden.

  Performance-Steigerung durch Backup auf Volume-Ebene und Backup auf Blockebene

7.6 Performance-Engpässe der Netzwerk-Datensicherung

Gliederung des Unterkapitels

Irgendwann sind aber die technischen Grenzen für die Performance-Steigerung der Datensicherung erreicht. Bei den technischen Grenzen sind anwendungsspezifische Grenzen (Abschnitt 7.6.1) und solche zu unterscheiden, die durch die serverzentrierte IT-Architektur bedingt sind (Abschnitt 7.6.2).

7.6.1 Anwendungsspezifische Performance-Engpässe

Definition: Anwendungsspezifischer Performance-Engpass

Unter anwendungsspezifischen Performance-Engpässen sind all die Engpässe zu verstehen, die auf die Anwendung »Netzwerk-Datensicherung« zurückzuführen sind. Für andere Anwendungen spielen diese Performance-Engpässe keine Rolle.

Performance-Engpass: Metadaten-Datenbank

Der Hauptkandidat für anwendungsspezifische Performance-Engpässe ist die Metadaten-Datenbank. Sie muss eine ganze Menge leisten. Fast jede Aktion im Netzwerk-Datensicherungssystem zieht eine oder mehrere Operationen auf der Metadaten-Datenbank nach sich. Werden beispielsweise von einer Datei mehrere Versionen gesichert, so erfolgt für jede Version ein eigener Eintrag in die Metadaten-Datenbank. Die Sicherung eines Dateisystems mit mehreren Hunderttausend Dateien kann so eine ganze Reihe von Datenbankoperationen nach sich ziehen.

Performance-Engpass: Interne Busse

Einen weiteren Kandidaten für anwendungsspezifische Performance-Engpässe birgt die Speicherhierarchie in sich: Beim Umkopieren der Daten von Festplatte auf Band muss der Media Manager die Daten von der Festplatte über den I/O-Bus und den internen Bus in den Hauptspeicher laden, nur um sie von dort über internen Bus und I/O-Bus zum Bandlaufwerk weiterzuleiten. Das heißt, während des Umkopierens der Daten von Festplatte auf Band können die Busse verstopfen. Gleiches gilt für die Tape Reclamation.

7.6.2 Performance-Engpässe aufgrund der serverzentrierten IT-Architektur

Performance-Engpässe in serverzentrierten IT-Architekturen

Neben diesen beiden anwendungsspezifischen Performance-Engpässen zeigen sich in der Netzwerk-Datensicherung einige Probleme, die typisch sind für eine serverzentrierte IT-Architektur. Zur Erinnerung sei noch einmal erwähnt, dass in einer serverzentrierten IT-Architektur Speichergeräte nur in Abhängigkeit von Servern existieren. Der Zugriff auf Speichergeräte erfolgt immer über die Rechner, an denen die Speichergeräte angeschlossen sind. Die im Folgenden beschriebenen Perfor-

mance-Engpässe gelten für alle Anwendungen, die in einer serverzentrierten IT-Architektur betrieben werden.

Problem 1: Verstopfung der internen Busse

Angenommen, ein Backup-Client möchte Daten zum Backup-Server sichern (Abbildung 7.3). Der Backup-Client lädt die zu sichernden Daten von der Festplatte über den SCSI-Bus, den PCI-Bus und den Systembus in den Hauptspeicher des Anwendungsservers, nur um sie von dort erneut über den Systembus und den PCI-Bus an die Netzwerkkarte weiterzuleiten. Auf dem Backup-Server müssen die Daten erneut zweimal durch die Busse geschleust werden. Bei der Datensicherung werden in der Regel größere Datenmengen am Stück gesichert. Während der Sicherung können also die Busse der beteiligten Rechner zum Engpass werden, insbesondere wenn der Anwendungsserver zusätzlich die I/O-Last der Anwendung zu tragen hat oder der Backup-Server mehrere zeitgleiche Sicherungen unterstützen soll.

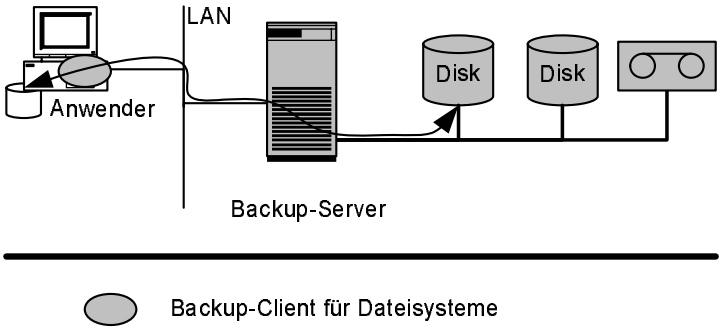

Abbildung 7.3
Bei der Netzwerk-Datensicherung müssen alle zu sichernden Daten durch beide Rechner geschleust werden. Mögliche Performance-Engpässe sind: interne Busse, CPU und das LAN.

Problem 2: Hohe CPU-Last durch das TCP/IP-Protokoll

Die Netzwerkkarte überträgt die Daten über TCP/IP und Ethernet zum Backup-Server. Bisher war der Datenaustausch via TCP/IP mit einer hohen CPU-Last verbunden. Allerdings kann die CPU-Belastung durch TCP/IP-Datenverkehr mit dem zunehmenden Einsatz von TCP/IP Offload Engines (TOE) vernachlässigt werden (vgl. Abschnitt 3.5.2, »TCP/IP und Ethernet als I/O-Technik«).

7.7 Eingeschränkte Möglichkeiten zur Performance-Steigerung

Die Netzwerk-Datensicherung ist ressourcenintensiv.

Datensicherung ist eine ressourcenintensive Anwendung, die Speichergeräte, CPU, Hauptspeicher, Netzkapazität, interne Busse und I/O-Busse stark beansprucht. Der enorme Ressourcenbedarf für die Datensicherung wird bei der Planung von IT-Systemen nicht immer ausreichend berücksichtigt. Oft ist dann zu hören: »Das Backup ist an dem langsamen Netz schuld« oder »Das langsame Netz ist daran schuld, dass

das Restore so lange braucht«. Die Wahrheit: Das Netz ist für Endanwender-Datenverkehr und Backup-Datenverkehr nicht ausreichend dimensioniert. Häufig ist die Datensicherung diejenige Anwendung, die die meiste Netzkapazität benötigt. Deshalb ist es oft sinnvoll, die Datensicherung als die primäre Anwendung anzusehen, für welche die IT-Infrastruktur im Allgemeinen und das Netz im Besonderen dimensioniert werden.

Gliederung des Unterkapitels

In jeder IT-Umgebung können die meisten Rechner mit einem Netzwerk-Datensicherungssystem ausreichend gesichert werden. In fast jeder IT-Umgebung gibt es aber, meist nur einige wenige, Rechner, für die zusätzliche Maßnahmen erforderlich sind, um sie schnell genug sichern oder gegebenenfalls wiederherstellen zu können. In der serverzentrierten IT-Architektur gibt es drei Lösungsansätze, solche Datenmonster zu bändigen: Die Installation eines separaten LAN für die Netzwerk-Datensicherung zwischen Backup-Client und Backup-Server (Abschnitt 7.7.1), die Installation mehrerer Backup-Server (Abschnitt 7.7.2) und die Installation von Backup-Client und Backup-Server auf dem gleichen physikalischen Rechner (Abschnitt 7.7.3).

7.7.1 Separates LAN für die Netzwerk-Datensicherung

Ansatz 1: Zusätzliches LAN für die Datensicherung

Die einfachste Maßnahme zur Performance-Steigerung für die Sicherung von schwergewichtigen Backup-Clients besteht darin, zusätzlich zu dem bereits installierten LAN ein weiteres LAN zwischen Backup-Client und Backup-Server zu installieren und dieses ausschließlich für die Datensicherung zu benutzen (Abbildung 7.4). Hierbei kann sich auch eine teure, aber leistungsfähige Übertragungstechnik wie Gigabit-Ethernet oder 10-Gigabit-Ethernet rechnen.

Belastung der Busse

Der Ansatz, neben dem bereits existierenden LAN ein weiteres Netz für die Datensicherung zu installieren, ist vergleichbar mit der Grundidee von Speichernetzen. Im Gegensatz zu Speichernetzen werden hier aber nur Rechner miteinander verbunden; ein direkter Zugriff auf alle Speichergeräte ist nicht möglich. Alle Daten werden also weiterhin über TCP/IP und durch Anwendungsserver und Backup-Server geschleust, sodass interne Busse und I/O-Busse weiterhin verstopft werden.

Nicht skalierbar

Einzelne Backup-Clients können also von der Installation eines separaten LAN für die Netzwerk-Datensicherung profitieren. Dieser Ansatz ist aber nicht beliebig skalierbar. Aufgrund der starken Beanspruchung des Backup-Servers kann dieser neben der Sicherung eines einzelnen schwergewichtigen Clients keine weiteren Rechner sichern.

Dennoch für viele Umgebungen ausreichend

Trotz der Limitierungen ist die Installation eines separaten Backup LAN in vielen Umgebungen ausreichend. Mit Fast-Ethernet kann man immerhin einen Durchsatz von über 10 MByte/s erreichen. Noch at-

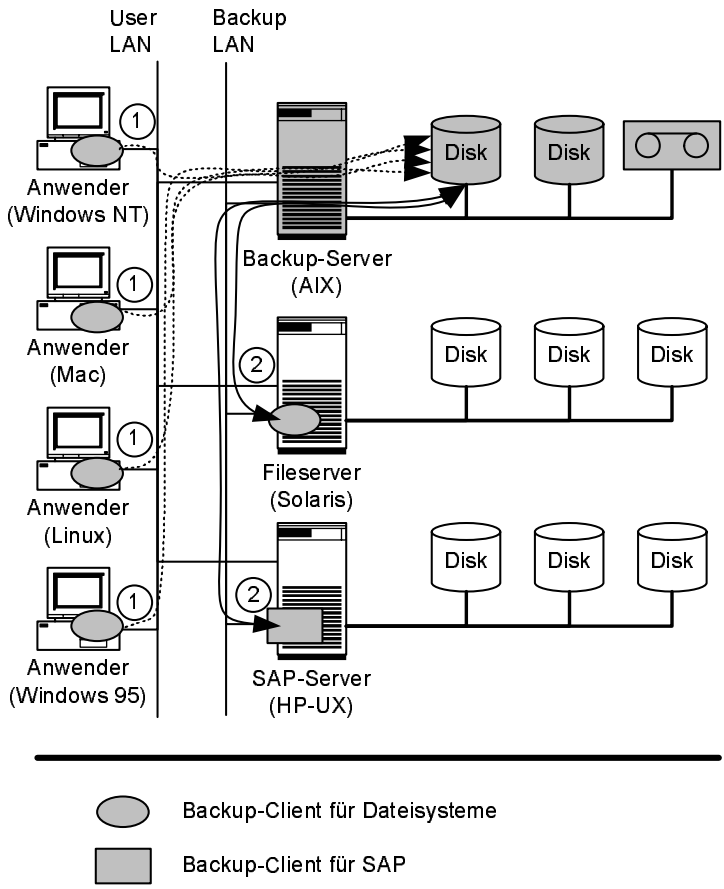

Abbildung 7.4
Ansatz 1: Ein zweites LAN kann den Durchsatz der Netzwerk-Datensicherung erhöhen. Normale Clients sichern nach wie vor über das User LAN (1). Nur die schwergewichtigen Clients sichern über das zweite LAN (2).

traktiver wird die LAN-Technik durch Gigabit-Ethernet, 10-Gigabit-Ethernet und die oben erwähnten TCP/IP Offload Engines, die die Server-CPU bezüglich des TCP/IP-Datenverkehrs erheblich entlasten.

7.7.2 Mehrere Backup-Server

Ansatz 2: Installation mehrerer Backup-Server

Mit der Installation mehrerer Backup-Server wird die Last des Backup-Servers auf mehr Hardware verteilt. Beispielsweise wäre es möglich, jedem schwergewichtigen Backup-Client einen speziellen Backup-Server zuzuordnen, der ausschließlich für die Sicherung dieses Clients installiert wird (Abbildung 7.5). Darüber hinaus wird ein weiterer Backup-Server zur Sicherung aller anderen Backup-Clients benötigt. Dieser Ansatz ist sinnvoll bei Performance-Engpässen der Metadaten-Datenbank oder in Kombination mit der ersten Maßnahme, der Installation eines separaten LAN zwischen schwergewichtigem Backup-Client und Backup-Server.

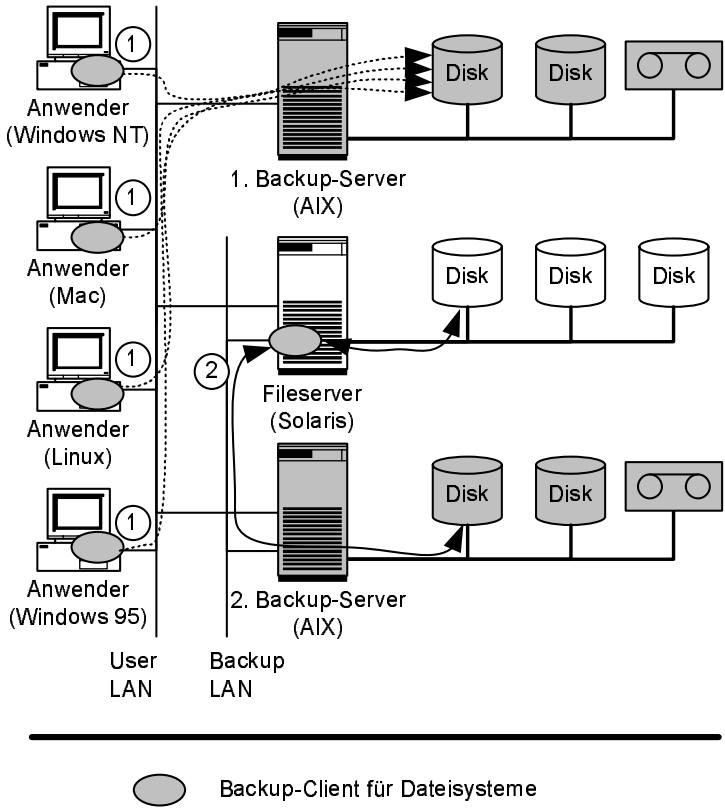

Abbildung 7.5
Ansatz 2: Für schwergewichtige Backup-Clients wird ein dedizierter Backup-Server installiert. Normale Clients sichern weiterhin auf den ersten Backup-Server(1). Der schwergewichtige Client sichert über das separate LAN auf seinen eigenen Backup-Server (2).

Belastung von CPU und Bussen auf dem Anwendungsrechner

Mit der Installation mehrerer Backup-Server und eines separaten LAN für die Datensicherung kann die Leistungsfähigkeit der Backup-Infrastruktur erheblich gesteigert werden. Auf Seiten der schwergewichtigen Backup-Clients bleibt aber das Problem bestehen, dass alle zu sichernden Daten von der Festplatte über die Busse in den Hauptspeicher und von dort erneut durch die Busse zur Netzwerkkarte geschleust werden müssen. Das heißt, auf der Seite des Anwendungsservers verursacht die Datensicherung nach wie vor eine starke Beanspruchung von CPU und Bussen. Der Ressourcenbedarf für die Datensicherung könnte im Konflikt stehen mit dem Ressourcenbedarf für die eigentliche Anwendung.

Erfordert viele kleine Tape Libraries

Ein weiteres Problem besteht in der Realisierung der Speicherhierarchie innerhalb der einzelnen Backup-Server. Denn nun benötigt jeder Backup-Server seine eigene Tape Library. Viele kleine Tape Libraries sind teurer und unflexibler als eine große Tape Library. Deshalb möchte man eigentlich lieber eine große Tape Library kaufen, die von allen Servern genutzt wird. In einer serverzentrierten IT-Architektur ist es aber nur sehr eingeschränkt möglich, mehrere Rechner an die gleiche Tape Library anzuschließen.

7.7.3 Backup-Server und Anwendungsserver auf dem gleichen physikalischen Rechner

Ansatz 3: Anwendungsserver, Backup-Server und Backup-Client auf einem Rechner

Die dritte Möglichkeit zur Performance-Steigerung besteht darin, Backup-Server und Anwendungsserver auf dem gleichen physikalischen Rechner zu installieren (Abbildung 7.6). Infolgedessen muss auch der Backup-Client auf diesem Rechner laufen. Backup-Server und Backup-Client kommunizieren hierbei statt über LAN über Shared Memory (Unix) beziehungsweise Named Pipe oder TCP/IP Loopback (Windows). Shared Memory hat im Vergleich zu den Bussen eine unendliche Bandbreite, sodass die Kommunikation zwischen Backup-Server und Backup-Client nicht mehr die limitierende Größe ist.

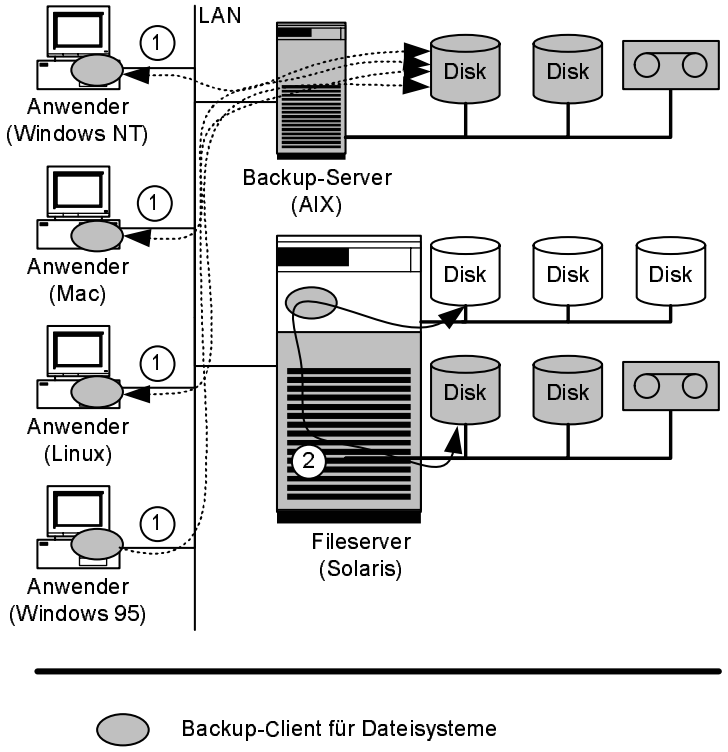

Abbildung 7.6
Ansatz 3: Anwendungsserver, Backup-Server und Backup-Client werden alle auf einem Rechner installiert. Normale Clients werden weiter auf den ersten Backup-Server gesichert (1). Nur der schwergewichtige Client wird innerhalb des gleichen Rechners gesichert (2).

Belastung der Busse

Die Verstopfung der internen Busse bleibt aber bestehen: Nun lädt der Backup-Client die zu sichernden Daten von den Festplatten über die Busse in den Hauptspeicher. Der Backup-Server übernimmt die Daten aus dem Hauptspeicher und schreibt sie erneut über die Busse auf das Sicherungsmedium. Die Daten werden also auch hier zweimal durch den internen Bus gejagt. Tape Reclamation und eventuelle Kopieraktionen innerhalb der Speicherhierarchie des Backup-Servers könnten die Busse zusätzlich belasten.

Reduzierung der CPU-Last ungewiss

Die Änderung der CPU-Auslastung kann ohne weitere Informationen nicht genauer bestimmt werden. Durch die Shared-Memory-Kommunikation (beziehungsweise Named Pipe oder TCP/IP Loopback) entfällt der CPU-intensive Betrieb der Netzwerkkarte. Dafür muss nun ein Rechner die Last der Anwendung, des Backup-Servers und des Backup-Clients tragen. Dieser Rechner muss übrigens für alle drei Anwendungen ausreichend Hauptspeicher besitzen.

Mangelnde Entkopplung von Produktionsdaten und Sicherheitskopien

Problematisch bei diesem Ansatz ist die Kopplung von Produktionsdaten und Sicherheitskopien. Zwar können beide mit WAN-Techniken wie Dark Fiber, DWDM oder FCIP ausreichend räumlich voneinander entfernt werden. Dennoch kann beispielsweise ein Administrationsfehler oder ein Virusbefall auf dem Rechner zu dem gleichzeitigen Verlust von Produktionsdaten und Sicherheitskopien führen. Deshalb sollte man die Backup-Medien täglich aus der Tape Library in ein Off-Site-Lager schaffen. Allerdings widerspricht dies dem Anspruch der Netzwerk-Datensicherung, die Datensicherung weitgehend zu automatisieren.

7.8 Datensicherung mit Speichernetzen

Gliederung des Unterkapitels

Speichernetze bieten neue Möglichkeiten, die soeben geschilderten Performance-Engpässe der Netzwerk-Datensicherung zu umgehen. Sie verbinden Server und Speichergeräte, sodass Produktionsdaten bei der Datensicherung direkt von der Ursprungsfestplatte auf die Backup-Medien kopiert werden können, ohne sie durch einen Server zu schleusen (Server-free Backup, Abschnitt 7.8.1). LAN-free Backup (Abschnitt 7.8.2) und LAN-free Backup mit Shared-Disk-Dateisystemen (Abschnitt 7.8.3) sind zwei weitere Alternativen, die Datensicherung mittels Speichernetzen zu beschleunigen. Weitere Möglichkeiten zur Beschleunigung von Datensicherung und Datenwiederherstellung ergeben sich aus dem Einsatz von Instant Copies (Abschnitt 7.8.4) und Remote Mirroring (Abschnitt 7.8.5). Mit der Einführung von Speichernetzen ergibt sich außerdem der Nebeneffekt, dass mehrere Backup-Server eine Tape Library gemeinsam nutzen können (Abschnitt 7.8.6).

7.8.1 Server-free Backup

Server-free Backup: von Festplatte direkt auf das Sicherungsmedium

Das ultimative Ziel der Datensicherung über ein Speichernetz ist das sogenannte Server-free Backup (Abbildung 7.7). Bei der Datensicherung stellt der Backup-Client zunächst fest, welche Daten gesichert werden müssen, und schickt dann nur die entsprechenden Metadaten (Dateiname, Zugriffsrechte usw.) über das LAN an den Backup-Server.

Die Dateiinhalte, die den Hauptteil der zu übertragenden Datenmenge ausmachen, werden dann von der Ursprungsfestplatte über das Speichernetz direkt auf das Sicherungsmedium (Festplatte, Band, Optical) geschrieben, ohne dass ein Server dazwischengeschaltet ist. Dabei koordiniert das Netzwerk-Datensicherungssystem die Kommunikation zwischen Ursprungsfestplatte und Sicherungsmedium. Ein kürzerer Transportweg für die Sicherung von Daten ist mit heutigen Techniken nicht möglich.

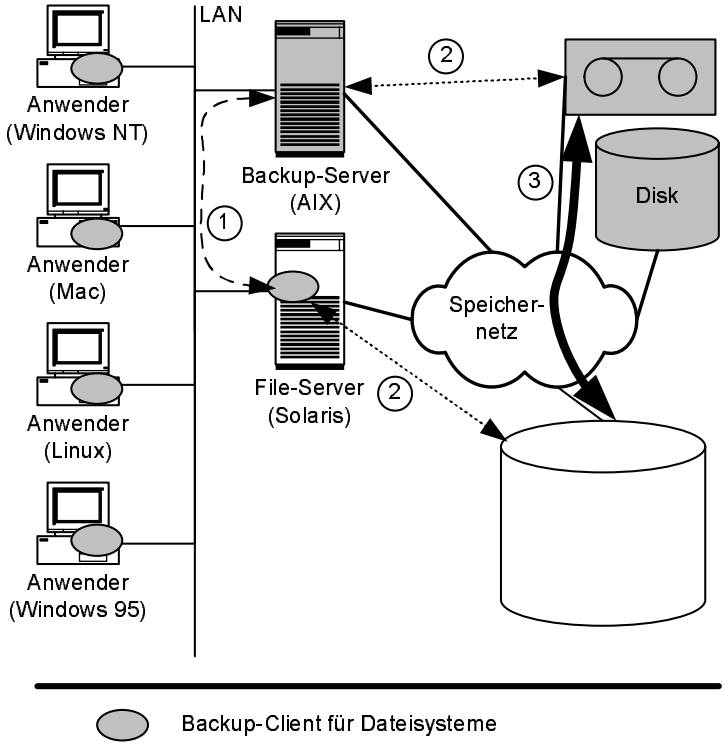

Abbildung 7.7
Beim Server-free Backup tauschen Backup-Server und Backup-Client leichtgewichtige Metadaten über das LAN aus (1). Nachdem geklärt ist, welche Datenblöcke zu sichern sind, konfiguriert das Netzwerk-Datensicherungssystem die Speichergeräte für die Datenübertragung über das Speichernetz (2). Die schwergewichtigen Dateiinhalte werden dann über das Speichernetz direkt von der Ursprungsfestplatte auf das Backup-Medium kopiert (3).

Performance-Analyse

Die Performance von Server-free Backup wird vor allem von der Leistungsfähigkeit der zugrunde liegenden Speichersysteme und der Verbindung im Speichernetz bestimmt. Die Verlagerung des Transportweges für den Hauptteil der Daten vom LAN in das Speichernetz, ohne dass dabei noch ein Server an der Übertragung selbst beteiligt ist, bewirkt, dass sowohl auf dem Backup-Client als auch auf dem Backup-Server die internen Busse, die I/O-Busse und die CPU entlastet werden. Der Koordinationsaufwand für den Datenverkehr zwischen Ursprungsfestplatte und Sicherungsmedium verbraucht deutlich weniger Server-Ressourcen als der Datenverkehr selbst.

3rd-Party SCSI Copy Command

Für Server-free Backup müssen die Datenblöcke innerhalb des SCSI-Protokolls zwischen zwei SCSI-Geräten kopiert werden. Dazu wurde das SCSI-Protokoll um das sogenannte 3rd-Party SCSI Copy Command erweitert. Dieses kann auch mit den leicht unterschiedlichen SCSI-Protokollen für Festplatten und Bändern umgehen. Das 3rd-Party SCSI Copy lässt sich an verschiedenen Stellen realisieren: in einem SAN-Switch, in einer speziellen im Speichernetz angeschlossenen Box, die ausschließlich für die Protokollkonvertierung zuständig ist, oder in einem der beiden beteiligten Speichersysteme selbst.

Schwierigkeiten bei der Implementierung von Server-free Backup

Ein Hauptproblem der Implementierung von Server-free Backup besteht darin, dass die SCSI-Blöcke auf dem Weg von der Ursprungsfestplatte zum Sicherungsmedium konvertiert werden müssen. Beispielsweise werden auf Ursprungs- und Sicherungsmedium in der Regel unterschiedliche Blöcke adressiert. Oder beim Restore einer gelöschten Datei in einem Dateisystem muss diese in einem anderen Bereich wiederhergestellt werden, wenn der frei gewordene Platz inzwischen mit anderen Dateien belegt ist oder seit der letzten Sicherung das Dateisystem defragmentiert wurde. Die Realisierung der Kopierfunktion innerhalb des SCSI-Protokolls muss also Kenntnis über die Datenstruktur von Dateisystemen und Datenbanken haben und wissen, wie diese ihre Daten auf SCSI-Ebene speichern.

Produktionsreife fraglich

Nach unserem Kenntnisstand hat Server-free Backup es bestenfalls von den Labors der Hersteller in deren Democenter geschafft. Vor allem in den Jahren 2002 und 2003 betrieben einige Hersteller hier aggressives Marketing, indem sie behaupten, dass ihre Datensicherungsprodukte Server-free Backup unterstützen. Nach unseren Erfahrungen wird Server-free Backup auch im Jahr 2007 so gut wie überhaupt nicht in Produktionsumgebungen eingesetzt, obwohl es nun seit einiger Zeit verfügbar ist. Unserer Meinung nach ist dies ein Beleg dafür, dass Server-free Backup bei dem heutigen Stand der Technik noch immer sehr schwierig zu implementieren, zu konfigurieren und zu betreiben ist.

7.8.2 LAN-free Backup

LAN-free Backup: Umgehung des Backup-Servers

LAN-free Backup umgeht die Notwendigkeit des 3rd-Party SCSI Copy Command, indem es vergleichbare Funktionen innerhalb des Backup-Clients realisiert (Abbildung 7.8). Metadaten werden wie bei Server-free Backup über das LAN geschickt. Dateiinhalte gehen aber nicht mehr über den Backup-Server. Für die Sicherung lädt der Backup-Client die Daten von der Festplatte über die entsprechenden Busse in den Hauptspeicher und schreibt sie von dort über die Busse und das Speichernetz direkt auf das Sicherungsmedium. Dazu muss der Backup-Client über das Speichernetz auf die Sicherungsmedien des Backup-Servers

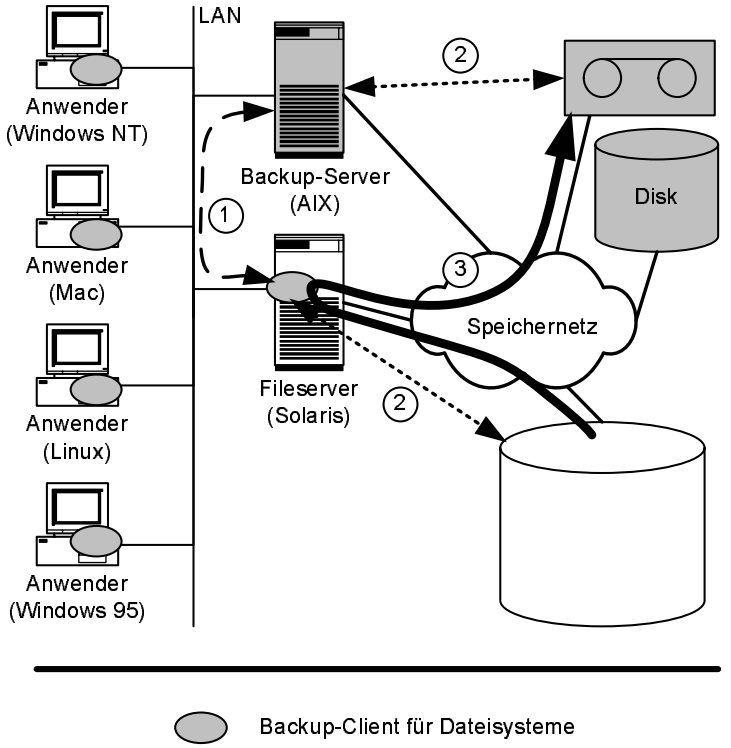

Abbildung 7.8
Auch beim LAN-free Backup tauschen Backup-Server und Backup-Client leichtgewichtige Metadaten über das LAN aus (1). Der Backup-Server bereitet seine Speichergeräte für die Datenübertragung über das Speichernetz vor und übergibt dann die Kontrolle über die Speichergeräte an den Backup-Client (2). Dieser kopiert dann die schwergewichtigen Dateiinhalte über das Speichernetz direkt auf das Backup-Medium (3).

zugreifen können. Außerdem müssen Backup-Server und Backup-Client den Zugriff auf gemeinsame Geräte synchronisieren. Dies ist leichter zu realisieren als Server-free Backup, weil nun die Daten oberhalb der SCSI-Ebene in höhreren Schichten des Betriebssystems kopiert werden.

Performance-Analyse

Wie beim Server-free Backup wird auch beim LAN-free Backup die CPU von Backup-Server und Backup-Client entlastet, indem der Datenverkehr vom LAN in das Speichernetz verschoben wird. Dagegen werden beim LAN-free Backup nur noch die Busse des Backup-Servers, aber nicht mehr die des Backup-Clients entlastet. Dies kann sich auf andere Anwendungen (Datenbanken, File- und Webserver) auswirken, die zeitgleich zu der Datensicherung auf dem Backup-Client laufen.

Produktionsreif, Support-Matrix beachten

LAN-free Backup wird seit vielen Jahren zuverlässig und stabil in Produktionsumgebungen eingesetzt. Allerdings unterstützen die Hersteller von Netzwerk-Datensicherungssystemen Backup über LAN für mehr Anwendungen (Datenbanken, Dateisysteme, Mailsysteme) als für LAN-free Backup, wobei nicht jede Anwendung auf jedem Betriebssystem unterstützt wird. Beim Einsatz von LAN-free Backup muss also unbedingt auf die Support-Matrix (siehe Abschnitt 3.4.6, »Interoperabilität von Fibre Channel SAN«) der Hersteller geachtet werden. Es ist davon auszugehen, dass im Laufe der nächsten Jahre die Anzahl der unterstützten Anwendungen und Betriebssysteme weiter zunimmt.

7.8.3 LAN-free Backup mit Shared-Disk-Dateisystemen

LAN-free Backup mit Shared-Disk-Dateisystemen

Wer bereits heute ein Dateisystem sichern will, für das LAN-free Backup noch nicht unterstützt wird, kann sich unter Umständen mit Shared-Disk-Dateisystemen helfen (Abbildung 7.9). Shared-Disk-Dateisysteme werden auf mehreren Rechnern installiert. Der Zugriff auf die Daten wird über das LAN synchronisiert. Die einzelnen Dateizugriffe erfolgen dagegen direkt über das Speichernetz (Kapitel 4.3). Für die Datensicherung wird das Shared-Disk-Dateisystem auf dem Fileserver und dem Backup-Server installiert. Voraussetzung hierfür ist, dass ein Shared-Disk-Dateisystem verfügbar ist, das die Betriebssysteme von Backup-Client und Backup-Server unterstützt. Der Backup-Client wird dann auf dem gleichen Rechner gestartet, auf dem auch der Backup-Server läuft, sodass Backup-Client und Backup-Server die Daten über Shared-Memory (Unix) beziehungsweise Named Pipe oder TCP/IP Loopback (Windows) austauschen können.

Performance-Analyse

Bei LAN-free Backup mit Hilfe eines Shared-Disk-Dateisystems muss die Performance des Backup-Servers kritisch überprüft werden.

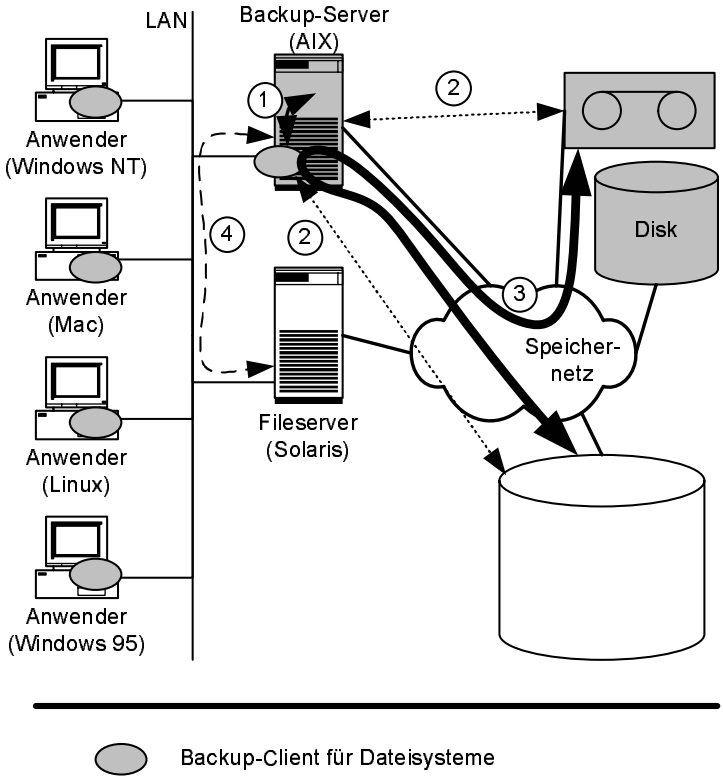

Abbildung 7.9
Für das Backup mit Shared-Disk-Dateisystemen laufen Backup-Server und Backup-Client auf dem gleichen Rechner (1). Produktionsdaten und Backup-Medien sind auf dem Backup-Server im Zugriff (2), sodass über das Speichernetz gesichert wird (3). Das Shared-Disk-Dateisystem benötigt ein LAN für die leichtgewichtige Synchronisation paralleler Datenzugriffe (4).

Es müssen noch immer alle Daten durch die Busse des Backup-Servers geschleust werden. Zusätzlich läuft auf dieser Maschine der Backup-Client und das Shared-Disk-Dateisystem. Innerhalb des Netzwerk-Datensicherungssystems ist kein LAN-Datenverkehr mehr notwendig; allerdings benötigt nun das Shared-Disk-Dateisystem LAN-Datenverkehr für die Synchronisation zeitgleicher Datenzugriffe. Der Datenverkehr für die Synchronisation des Shared-Disk-Dateisystems ist aber vergleichsweise gering. Letztendlich muss man für jeden Einzelfall messen, ob die Datensicherung mit einem Shared-Disk-Dateisystem die Performance steigert.

Produktionsreif

Die Performance von LAN-free Backup mit Hilfe eines Shared-Disk-Dateisystems ist zwar nicht so gut wie die Performance von reinem LAN-free Backup. Sie kann aber deutlich besser sein als bei der Sicherung über das LAN. Deshalb hat sich dieser Ansatz in Produktionsumgebungen bewährt, sodass darin eine interessante Übergangslösung bis zu der Verfügbarkeit von LAN-free (oder gar Server-free) Backup zu sehen ist. Des Weiteren ist davon auszugehen, dass diese Form der Datensicherung mit dem zunehmenden Einsatz von Shared-Disk-Dateisystemen an Bedeutung gewinnen wird.

7.8.4 Datensicherung mit Instant Copies

Datensicherung mit Instant Copies

Neben Server-free Backup und LAN-free Backup bieten die Kopierdienste von Disksubsystemen und Dateisystemen einen weiteren Ansatz, die Datensicherung zu beschleunigen. Instant Copies können selbst Terabyte-große Datenbestände in wenigen Sekunden virtuell kopieren, also den aktuellen Zustand der Produktionsdaten einfrieren und über einen zweiten Zugriffspfad verfügbar machen. Die Produktionsdaten können nach wie vor über den ersten Zugriffspfad gelesen und verändert werden, sodass der Betrieb der eigentlichen Anwendung fortgesetzt werden kann, während zeitgleich der eingefrorene Zustand der Daten über den zweiten Zugriffspfad gesichert wird.

Instant Copies auf drei Ebenen

Instant Copies lassen sich auf drei verschiedenen Ebenen realisieren:

(1.) im Disksubsystem

1. *Instant Copy auf Blockebene*
   (Disksubsystem oder blockbasierte Virtualisierung)
   Die Instant Copy im Disksubsystem wurde ausführlich in Abschnitt 2.7.1 besprochen: Intelligente Disksubsysteme können alle Daten einer Festplatte innerhalb weniger Sekunden virtuell auf eine zweite Festplatte kopieren. Der eingefrorene Datenzustand kann über die zweite Festplatte abgerufen und gesichert werden.

(2.) im Dateisystem

2. *Instant Copy auf Dateiebene*
   (Dateisystem, NAS-Server oder dateibasierte Virtualisierung)
   Viele Dateisysteme bieten ebenfalls die Möglichkeit, Instant Copies zu erstellen. Instant Copies auf Dateisystemebene werden im Allgemeinen als Snapshots bezeichnet (Abschnitt 4.1.3). Im Gegensatz zu Instant Copies im Disksubsystem kann hier über einen speziellen Verzeichnispfad auf den Snapshot zugegriffen werden.

(3.) in der Anwendung

3. *Instant Copy in der Anwendung*
   Schließlich bieten inbesondere Datenbanken die Möglichkeit, intern den Datenbestand für die Datensicherung einzufrieren, während die Anwender weiterhin auf sie zugreifen (hot backup, online backup).

Vergleich der drei Ansätze

Instant Copies im Dateisystem und in der Anwendung haben den Vorteil, dass sie mit jeder Hardware realisierbar sind. Instant Copies in der Anwendung können die interne Datenstruktur der Anwendung ausnutzen und so effizienter arbeiten als Dateisysteme. Andererseits benötigen Anwendungen diese Funktionen nicht, wenn das zugrunde liegende Dateisystem sie bereits zur Verfügung stellt. Beide Ansätze verbrauchen Systemressourcen auf dem Anwendungsserver, die man manchmal lieber der eigentlichen Anwendung zur Verfügung stellen will. Dies ist der Vorteil von Instant Copies in externen Geräten wie Disksubsystemen, NAS-Servern oder einer im Speichernetz platzierten Virtualisierungsinstanz. Sie erfordern zwar spezielle Hardware, dafür werden Aufgaben von dem Anwendungsserver auf das externe Gerät verlagert, sodass der Anwendungsserver entlastet ist. Dies kann unter Umständen die Lizenzkosten für die Anwendungssoftware senken, wenn diese auf Basis der eingesetzten Prozessorleistung berechnet wird.

Konsistenz der gesicherten Daten

Die Sicherung mit Instant Copy muss mit den zu sichernden Anwendungen synchronisiert werden. Datenbanken und Dateisysteme puffern Schreibzugriffe im Hauptspeicher, um deren Performance zu erhöhen. Dadurch sind die Daten auf der Festplatte nicht immer in konsistentem Zustand. Die Datenkonsistenz bildet die Voraussetzung dafür, dass die Anwendung mit diesem Datenbestand neu starten und den Betrieb fortsetzen kann. Für die Datensicherung ist deshalb darauf zu achten, dass zuerst eine Instant Copy mit konsistenten Daten erzeugt wird. Die Vorgehensweise sieht also etwa so aus:

1. die Anwendung herunterfahren,
2. die Instant Copy durchführen,
3. die Anwendung wieder hochfahren und
4. die Daten von der Instant Copy sichern.

Trotz des Herunterfahrens und Neustarts der Anwendung ist das Produktionssystem sehr schnell wieder in Betrieb.

Steuerung durch Anwendung

Datensicherung mit Instant Copies wird noch attraktiver, wenn die Instant Copy von der Anwendung selbst gesteuert wird: In diesem Fall muss die Anwendung dafür sorgen, dass die Daten im Speicher konsistent sind, und dann den Kopiervorgang anstoßen. Die Anwendung kann anschließend den Betrieb nach wenigen Sekunden fortsetzen. Es ist nicht mehr erforderlich, die Anwendung anzuhalten und neu zu starten.

Schnelle Datenwiederherstellung mit Instant Copies

Instant Copies ermöglichen es also, unternehmenskritische Anwendungen mit nur sehr geringen Unterbrechungen stündlich zu sichern. Dies beschleunigt auch die Wiederherstellung von Daten nach Anwendungsfehlern (»Versehentliches Löschen eines Table Space«). Statt die Daten zeitaufwendig von Bändern einzuspielen, kann einfach auf eine eingefrorene Kopie zurückgesetzt werden, die noch im Speichersystem vorhanden ist.

Application Server-free Backup

Mit Hilfe von Instant Copies im Disksubsystem kann man das sogenannte Application Server-free Backup realisieren. Hierbei wird dem Anwendungsserver ein zweiter Server zur Seite gestellt, der ausschließlich zur Datensicherung dient (Abbildung 7.10). Beide Server sind di-

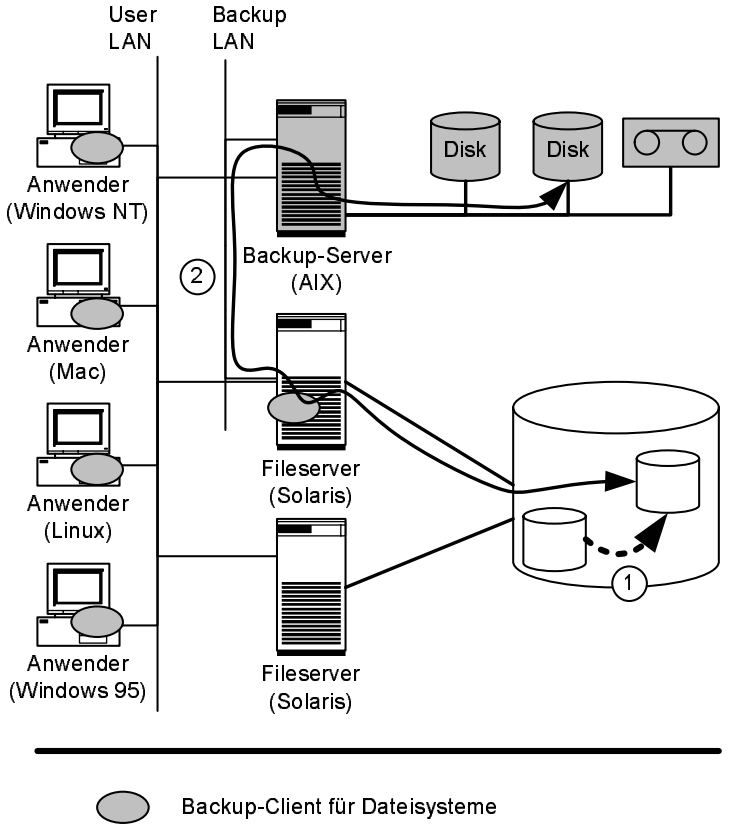

Abbildung 7.10
Application Server-free Backup nutzt die Funktionen eines intelligenten Disksubsystems aus. Für die Datensicherung wird die Anwendung für kurze Zeit so betrieben, dass sich auf den Festplatten ein konsistenter Datenzustand befindet, sodass die Daten mittels Instant Copy kopiert werden können (1). Die Anwendung kann sofort wieder auf Normalbetrieb umschalten; parallel dazu erfolgt die Datensicherung von der Instant Copy (2).

rekt über SCSI mit dem Disksubsystem verbunden; ein Speichernetz ist nicht unbedingt notwendig. Für die Datensicherung wird zunächst die Instant Copy wie oben 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 gesichert, ohne den Anwendungsserver zu belasten. Wird die Instant Copy im Disksubsystem aufgehoben, so können im Fehlerfalle die Daten mit dieser Kopie in wenigen Sekunden wiederhergestellt werden.

7.8.5 Datensicherung mit Remote Mirroring

Problem: Instant Copies schützen nicht vor Katastrophen.

Instant Copies helfen, die Daten bei Anwendungs- oder Bedienungsfehlern schnell wiederherzustellen, sie sind aber wirkungslos bei Katastrophen: Nach einem Brand nützt es nichts, dass sich auf einem Speichergerät mehrere Kopien der Daten befinden. Selbst ein Stromausfall kann so für einen 24x7-Betrieb zu einem Problem werden. Darüber hinaus gab es in den letzten Jahren auch einige europäische Beispiele für weiträumiger Störungen durch Stromausfälle, Überschwemmungen und Stürme. Bei solchen weiträumigen Katastrophen reicht es nicht aus, das eigene Rechenzentrum durch Notstromaggregate zu schützen, wenn von der Außenwelt keine Verbindung zu dem Rechenzentrum hergestellt werden kann. Global vernetzte Unternehmen verlieren so trotz Notstrom ihre Verbindung zu ihren Kunden.

Lösung: Remote Mirroring

Hier hilft nur, die Daten mittels Remote Mirroring auf zwei Disksubsysteme zu spiegeln, die zumindest durch eine Brandschutzmauer getrennt sind oder für den Schutz vor weiträumigen Ausfällen noch weiter voneinander entfernt stehen. Der Schutz von Anwendungen mittels Remote Mirroring wurde bereits in den Abschnitten 6.3.3 (»Ausfall eines Disksubsystems«) und 6.3.5 (»Ausfall eines Rechenzentrums am Beispiel ›Schutz einer wichtigen Datenbank‹«) besprochen.

Sicherung weiterhin erforderlich

Trotzdem müssen die Daten noch gesichert werden: Bei Remote Mirroring sind Ursprungsplatte und Kopie immer identisch. Das heißt, wenn durch einen Anwendungs- oder Bedienungsfehler Daten zerstört werden, so werden sie auch sofort auf der Kopie zerstört. Die Daten können mittels Instant Copy auf Festplatte oder mittels klassischer Netzwerk-Datensicherung auf Bänder gesichert werden. Da Speicherkapazität auf Festplatte teurer ist als Speicherkapazität auf Bändern, wird man nur die wichtigsten Daten mit Instant Copy und Remote Mirroring sichern. Für die meisten Daten dürfte die Sicherung auf Bänder nach wie vor am wirtschaftlichsten sein. In Abschnitt 9.5.4 werden wir die Kombination von Remote Mirroring und Datensicherung noch einmal aufgreifen und vertiefen.

7.8.6 Tape Library Sharing

Notwendigkeit für Tape Library Sharing

Manchmal besteht die Notwendigkeit, mehrere Backup-Server einzusetzen. In einigen Rechenzentren sind so viele Daten zu sichern, dass trotz der hier vorgestellten Techniken für die Datensicherung mit Speichernetzen mehrere Dutzend Backup-Server benötigt werden. In anderen Fällen werden wichtige Anwendungen netzwerktechnisch abgeschottet, um diese besser vor Angriffen von außen zu schützen. Hierbei möchte man gerne in jedem abgeschottenen Netzwerk einen separaten Backup-Server bereitstellen, wobei jeder Backup-Server mit einer eigenen kleineren Tape Library ausgestattet wird. Allerdings sind viele kleine Tape Libraries teurer in der Anschaffung und schwieriger zu verwalten als eine große, sodass häufig eine große Tape Library angeschafft wird, die dann alle Backup-Server über das Speichernetz mittels Tape Library Sharing (Kapitel 6.2.2) gemeinsam nutzen.

Tape Library Sharing für Netzwerk-Datensicherung

Abbildung 7.11 zeigt den Einsatz des Tape Library Sharings für die Netzwerk-Datensicherung: Hierbei agiert ein Backup-Server als Library-Master, alle anderen als Library-Client. Will ein Backup-Client

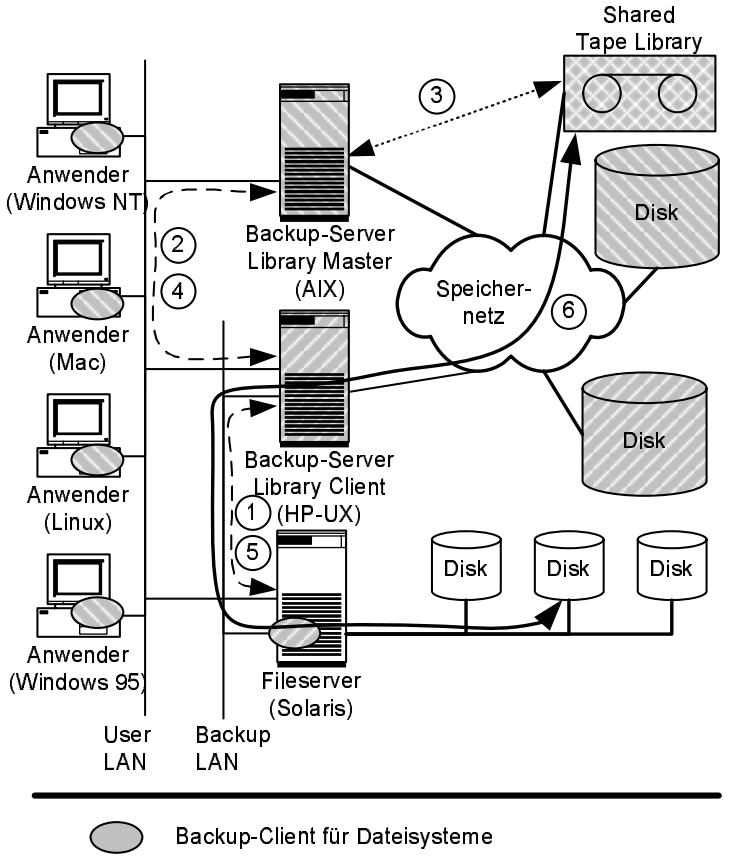

Abbildung 7.11
Beim Tape Library Sharing nutzen zwei Backup-Server eine gemeinsame Tape Library. Wenn ein Client beim zweiten Backup-Server (Library-Client) Daten direkt auf Band sichern will (1), so fordert dieser beim Library Master ein Band und ein Laufwerk an (2). Der Library Master legt ein freies Band in ein freies Laufwerk ein (3) und gibt die entsprechenden Informationen an den Library-Client zurück (4). Der Library-Client informiert nun den Backup-Client (5), dass er die Daten sichern kann (6).

zu einem Backup-Server Daten sichern, der als Library-Client konfiguriert ist, so fordert dieser zunächst vom Library-Master ein freies Band an. Der Library-Master wählt ein Band aus seinem Vorrat freier Bänder aus und legt dieses in ein freies Laufwerk ein. Danach vermerkt er in seiner Metadaten-Datenbank, dass dieses Band nun von dem Library-Client benutzt wird, und er informiert den Library-Client darüber, in welchem Laufwerk das Band liegt. Schließlich kann der Backup-Client die zu sichernden Daten über das LAN an den Backup-Server senden, welcher als Library-Client konfiguriert ist. Dieser schreibt die Daten anschließend über das Speichernetz direkt auf Band.

7.9 Sicherung von Dateisystemen

Weitere Gliederung des Kapitels

Fast alle Anwendungen speichern ihre Daten in Dateisystemen oder in Datenbanken. Deswegen schauen wir uns in diesem Abschnitt die Sicherung von Fileservern (Kapitel 7.9) und im nächsten Abschnitt die von Datenbanken (Kapitel 7.10) genauer an. Das Kapitel schließt dann mit organisatorischen Aspekten der Netzwerk-Datensicherung (Kapitel 7.11).

Gliederung des Unterkapitels

Dieses Kapitel bespricht zunächst grundlegende Anforderungen und Probleme der Sicherung von Fileservern (Abschnitt 7.9.1). Danach werden einige Funktionen moderner Dateisysteme vorgestellt, die die inkrementelle Sicherung von Dateisystemen beschleunigen (Abschnitt 7.9.2). Im Anschluss werden Einschränkungen bei der Sicherung von NAS-Servern diskutiert (Abschnitt 7.9.3). Schließlich wird mit dem Network Data Management Protocol (NDMP) ein Ansatz vorgestellt, der hilft, die Sicherung von NAS-Servern in ein bereits etabliertes Netzwerk-Datensicherungssystem zu integrieren (Abschnitt 7.9.4).

7.9.1 Sicherung von Fileservern

Definition: Fileserver

Unter Fileserver verstehen wir hier einen Rechner mit einem herkömmlichen Betriebssystem wie Windows oder Unix, der einen Teil seiner lokalen Dateisysteme über ein Netzwerk-Dateisystem exportiert oder einem Dienst (Novell, FTP, HTTP) zugänglich macht. Die Erläuterungen in diesem Abschnitt sind übertragbar auf alle Formen von Rechnern, vom Anwender-PC über den klassischen Fileserver bis hin zum Webserver.

Daten und Metadaten des Fileservers

Fileserver speichern drei Arten von Information:

- Daten in Form von Dateien,
- Metadaten über diese Dateien wie Dateiname, Erstellungsdatum und Zugriffsrechte und

- Metadaten über den Fileserver wie gegebenenfalls zugelassene Benutzer und deren Gruppen, Größe der einzelnen Dateisysteme, Netzkonfiguration des Fileservers sowie Namen, Bestandteile und Rechte der über das Netz exportierten Dateien oder Verzeichnissen.

Wiederherstellung von Dateien oder Dateisystemen

Je nach Fehlersituation müssen unterschiedliche Daten und Metadaten wiederhergestellt werden. Relativ einfach ist die Wiederherstellung einzelner Dateien oder gesamter Dateisysteme. Hier müssen nur die Dateiinhalte und die Metadaten der Dateien von dem Backup-Server auf den Fileserver zurückgespielt werden. Diese Funktion wird von den in Kapitel 7.4 vorgestellten Backup-Clients erbracht.

Wiederherstellung eines Fileservers

Schwieriger ist die Wiederherstellung eines gesamten Fileservers. Ist beispielsweise die Hardware des Fileservers nicht reparabel, sodass sie komplett ausgetauscht werden muss, sind folgende Schritte notwendig:

1. Beschaffung und Aufbau entsprechender Ersatz-Hardware,
2. Basisinstallation des Betriebssystems einschließlich notwendiger Patches,
3. Wiederherstellung der Basiskonfiguration des Fileservers, unter anderem LAN- und Speichernetz-Konfiguration des Fileservers,
4. gegebenenfalls Wiederherstellung von Benutzern und Gruppen sowie deren Rechte,
5. Anlegen und Formatieren der lokalen Dateisysteme unter Beachtung der notwendigen Dateisystemgrößen,
6. Installation und Konfiguration des Backup-Clients,
7. Wiederherstellung der Dateisysteme mit Hilfe des Netzwerk-Datensicherungssystems.

Schneller: Image Restore

Dieses Procedere ist sehr arbeits- und zeitaufwendig. Die Methode des sogenannten Image Restores beschleunigt die Wiederherstellung eines kompletten Rechners: Werkzeuge wie »mksysb« (AIX), »Web Flash Archive« (Solaris) oder diverse Disk Image Tools für Windows-Systeme erstellen eine komplette Kopie eines Rechners (Image). Man benötigt lediglich eine Boot-Diskette oder eine Boot-CD und ein entsprechendes Image, um einen Rechner komplett wiederherzustellen, ohne dass man die oben beschriebenen Schritte 2-7 durchexerzieren muss. Besonders vorteilhaft ist die Integration des Image Restores in ein Netzwerk-Datensicherungssystem. Dazu muss das Netzwerk-Datensicherungssystem das entsprechende Image erzeugen. Außerdem muss die Boot-Diskette beziehungsweise die Boot-CD eine Verbindung zum Netzwerk-Datensicherungssystem herstellen.

7.9.2 Sicherung von Dateisystemen

Sicherung von Dateisystemen

Für die klassische Netzwerk-Datensicherung von Dateisystemen wurde neben der Incremental-Forever-Strategie die Sicherung auf verschiedenen Ebenen (Blockebene, Dateiebene, Dateisystem-Image) besprochen. Mit der Einführung von Speichernetzen stehen für die Sicherung von Dateisystemen auch neue Methoden zur Verfügung wie Server-free Backup, Application Server-free Backup, LAN-free Backup, Shared-Disk-Dateisysteme, Instant Copies und Remote Mirroring.

Unterstützung durch das Dateisystem

Die Bedeutung der Sicherung von Dateisystemen zeigt sich darin, dass Hersteller von Dateisystemen neue Funktionen bereitstellen, die speziell auf die Beschleunigung der Datensicherung abzielen. Im Folgenden stellen wir mit dem sogenannten Archive Bit und dem Block Level Incremental Backup zwei dieser neuen Funktionen vor.

1. Archive Bit

Das Archive Bit unterstützt inkrementelle Sicherungen auf Dateiebene wie beispielsweise die Incremental-Forever-Strategie. Eine Schwierigkeit bei inkrementellen Sicherungen besteht darin, schnell festzustellen, welche Dateien sich seit der vorherigen Sicherung geändert haben. Zur Beschleunigung dieser Entscheidung erweitert das Dateisystem die Metadaten jeder Datei um das Archive Bit. Das Netzwerk-Datensicherungssystem setzt dieses Archive Bit unmittelbar, nachdem es eine Datei auf dem Backup-Server gesichert hat. Nach einer vollständigen Sicherung sind also die Archive Bits aller Dateien gesetzt. Wird nun eine Datei verändert, so setzt das Dateisystem automatisch deren Archive Bit zurück. Neu erzeugte Dateien erhalten ebenfalls kein Archive Bit. Bei der nächsten inkrementellen Sicherung weiß das Netzwerk-Datensicherungssystem, dass es nur die Dateien sichern muss, deren Archive Bits zurückgesetzt sind.

2. Block Level Incremental Backup

Das Prinzip des Archive Bits kann auch auf die einzelnen Blöcke eines Dateisystems angewendet werden, um den Aufwand für die Sicherung auf Blockebene zu reduzieren. In Kapitel 7.4 wurde ein vergleichsweise aufwendiges Verfahren für die Sicherung auf Blockebene vorgestellt: Der Aufwand für das Kopieren und Vergleichen der Dateien durch den Backup-Client wird stark vermindert, wenn das Dateisystem mit Hilfe des Archive Bit für Blöcke die Menge der veränderten Blöcke selber verwaltet und das Netzwerk-Datensicherungssystem diese über eine Schnittstelle abrufen kann.

Kombination von Archive Bits und Instant Copies

Das Prinzip der Archive Bits kann leider nicht ohne Weiteres mit dem Prinzip der Instant Copies kombiniert werden. Wird für die Datensicherung das Dateisystem mittels Instant Copy innerhalb des Disksubsystems kopiert (Abbildung 7.10 auf Seite 269), so setzt das Netzwerk-Datensicherungssystem die Archive Bits nur auf der Kopie des Dateisystems. In den Originaldaten bleibt also das Archive Bit zurückgesetzt, obwohl die Daten gesichert wurden. Folglich wird das Netzwerk-Da-

tensicherungssystem diese Daten bei der nächsten inkrementellen Sicherung erneut sichern, weil das Setzen des Archive Bits nicht zu den Originaldaten durchgedrungen ist.

7.9.3 Sicherung von NAS-Servern

Rahmenbedingungen

NAS-Server sind vorkonfigurierte Fileserver. Sie bestehen aus einem oder mehreren internen Servern, vorkonfigurierter Plattenkapazität und meist einem abgespeckten oder einem speziellen Betriebssystem (Abschnitt 4.2.2). NAS-Server bringen in der Regel eigene Werkzeuge für die Datensicherung mit. Diese Werkzeuge stellen jedoch genauso Insellösungen dar wie die Sicherungswerkzeuge, die Betriebssysteme mitbringen (Kapitel 7.1). Deshalb betrachten wir im Folgenden speziell das Einbinden der Sicherung von NAS-Servern in ein bestehendes Netzwerk-Datensicherungssystem.

Integration in Netzwerk-Datensicherungssystem schwierig

Optimal wäre es, wenn es für einen NAS-Server einen Backup-Client gäbe, der sowohl auf die Besonderheiten des NAS-Servers als auch auf die Besonderheiten des eingesetzten Netzwerk-Datensicherungssystems abgestimmt ist. Allerdings ist es in der Praxis sowohl für die Hersteller von NAS-Servern als auch für die Hersteller von Netzwerk-Datensicherungssystemen leider schwierig, einen solchen Backup-Client zu entwickeln.

Probleme der Hersteller von Netzwerk-Datensicherungssystemen

Basiert der NAS-Server auf einem speziellen Betriebssystem, so fehlen dem Hersteller des Netzwerk-Datensicherungssystems unter Umständen die notwendigen Schnittstellen und Compiler, um einen solchen Client zu entwickeln. Selbst wenn die Rahmenbedingungen für die Entwicklung eines speziellen Backup-Clients gegeben wären, ist es fraglich, ob die Hersteller des Netzwerk-Datensicherungssystems für alle NAS-Server einen speziellen Backup-Client entwickeln würden. Der notwendige Entwicklungsaufwand für einen neuen Backup-Client ist noch zu vernachlässigen im Vergleich zu dem Testaufwand, der für jede neue Version des Netzwerk-Datensicherungssystems betrieben werden muss.

Probleme der Hersteller von NAS-Servern

Gleichermaßen ist es für die Hersteller von NAS-Servern schwierig, einen solchen Client zu entwickeln: Die Hersteller von Netzwerk-Datensicherungssystemen legen nämlich weder den Quellcode noch die Schnittstellen zwischen Backup-Client und Backup-Server offen, sodass sie keinen Client entwickeln können. Ja, selbst wenn ein solcher Backup-Client bereits existiert, weil der NAS-Server auf ein Standardbetriebssystem wie Windows, Linux oder ein anderes Unix aufsetzt, heißt das noch lange nicht, dass Kunden diesen Client einsetzen dürfen. Um die Plug&Play-Fähigkeit von NAS-Servern zu verbessern, dürfen Kunden nur die Software einsetzen, die von dem NAS-Hersteller getestet und zertifiziert wurde. Installiert der Kunde nichtzertifizierte Software, so verliert er unter Umständen den Support für den NAS-Server.

Aufgrund des Testaufwands können Hersteller von NAS-Servern zwar einige, sicherlich aber nicht alle Netzwerk-Datensicherungssysteme unterstützen.

Sicherung über Netzwerk-Dateisystem fraglich

Ohne weitere Maßnahmen bleibt nur die Möglichkeit, die Dateisysteme des NAS-Servers von einem Client des NAS-Servers aus zu sichern (Abbildung 7.12). Allerdings ist auch dieser Ansatz aus zwei Gründen fragwürdig.

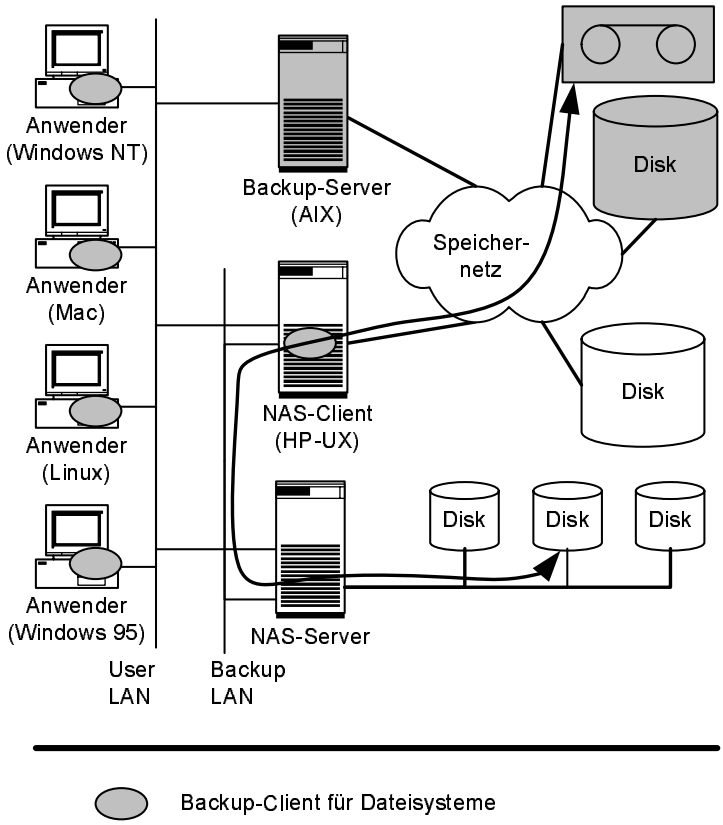

Abbildung 7.12
Bei der Sicherung eines NAS-Servers über ein Netzwerk-Dateisystem stellt die Verbindung zwischen dem NAS-Server und dem Backup-Client einen potenziellen Performance-Engpass dar. Das Backup über ein Netzwerk-Dateisystem erschwert die Sicherung und die Wiederherstellung von Metadaten des NAS-Servers.

Performance für große Datenmengen nicht ausreichend

Zum einem ist dieser Ansatz nur für kleinere Datenmengen praktikabel: Für die Datensicherung werden nämlich die Dateien des NAS-Servers über das LAN zu dem Netzwerk-Dateisystem-Client übertragen, auf dem der Backup-Client läuft. Erst der Backup-Client kann die Dateien mit fortgeschrittenen Methoden wie LAN-free Backup auf das Sicherungsmedium schreiben.

Sicherung von Metadaten schwierig

Zum anderen gestaltet sich die Sicherung von Metadaten als schwierig: Unterstützt ein NAS-Server den Export der lokalen Dateisysteme sowohl über CIFS als auch über NFS, so greift der Backup-Client nur über eines der beiden Protokolle auf die Dateien zu. Die Metadaten des anderen Protokolls gehen dabei verloren. NAS-Server

müssten also ihre Metadaten in speziellen Dateien ablegen, sodass das Netzwerk-Datensicherungssystem diese sichern kann. Es bleibt dann die Frage des Aufwands für die Wiederherstellung eines NAS-Servers oder eines Dateisystems. Die Metadaten von NAS-Server und Dateien müssen nämlich aus diesen Dateien wieder herausgezogen werden. Es ist fraglich, ob Netzwerk-Datensicherungssysteme diesen Vorgang automatisch anstoßen können.

Letzte Hoffnung: Standardisierung der Schnittstelle zur Datensicherung

Als letzter Ausweg zur Integration von NAS-Servern und Netzwerk-Datensicherungssystemen bleibt nur die Standardisierung der Schnittstelle zwischen dem NAS-Server und dem Netzwerk-Datensicherungssystem. Die Hersteller von NAS-Servern müssten so nur einen Backup-Client entwickeln und testen, der genau diese Schnittstelle unterstützt. Die Datensicherungssysteme verschiedener Hersteller könnten dann den NAS-Server über diese Schnittstelle sichern. In einem solchen Ansatz bestimmt die Reichhaltigkeit dieser Schnittstelle, wie gut die Sicherung von NAS-Servern in ein Netzwerk-Datensicherungssystem eingebunden werden kann. Der nächste Abschnitt stellt mit dem Network Data Management Protocol (NDMP) eine solche Schnittstelle vor.

7.9.4 Das Network Data Management Protocol (NDMP)

Das Network Data Management Protocol (NDMP)

Das Network Data Management Protocol (NDMP) definiert eine Schnittstelle zwischen NAS-Servern und Netzwerk-Datensicherungssystemen, die es ermöglicht, NAS-Server zu sichern, ohne für sie einen speziellen Backup-Client bereitzustellen. NDMP bietet somit einen Lösungsansatz für die im vorherigen Abschnitt beschriebene Integration von NAS-Servern und Netzwerk-Datensicherungssystemen.

Stand der Standardisierung

Immer mehr Hersteller, sowohl von NAS-Servern als auch von Netzwerk-Datensicherungssystemen, unterstützen NDMP, sodass NDMP als De-Facto-Standard anzusehen ist. Zu NDMP Version 4 liegt seit längerem ein Internet Draft vor. Des Weiteren existiert ein Anforderungskatalog für NDMP Version 5. NDMP Version 4 hat einige Lücken wie die Sicherung von Snaphots, die einige Hersteller über sogenannte Extensions schließen. Extensions sind herstellerspezifische Erweiterungen von NDMP Version 4. Dennoch hat sich NDMP in der Praxis bewährt, sodass NDMP als Mittel zur Integration von NAS-Servern und Netzwerk-Datensicherungssystemen eine breite Zustimmung findet.

Architektur

NDMP bezeichnet die Sicherung und die Wiederherstellung von Daten als Data Management Operations. Eine sogenannte Data Management Application (DMA), in der Regel ein Datensicherungssystem, initiiert und steuert die Data Management Operations, wobei die Ausführung einer Data Management Operation als NDMP Session bezeichnet wird. Die DMA kann dabei nicht direkt auf die Daten zugreifen. Sie benötigt die Unterstützung von Diensten, den sogenannten

NDMP Services (Abbildung 7.13). NDMP Services verwalten die jeweiligen Datenspeicher wie Dateisysteme, Sicherungsmedien und Tape Libraries. Die DMA stellt für die Steuerung einer NDMP Session zu jedem beteiligten NDMP Service eine NDMP Control Connection her. Für den eigentlichen Datenfluss zwischen Ursprungsmedium und Sicherungsmedium wird zwischen den entsprechenden NDMP Services eine sogenannte NDMP Data Connection etabliert. Letztendlich beschreibt NDMP eine Client-Server-Architektur, wobei die DMA die Rolle des NDMP Clients einnimmt. Ein NDMP Server setzt sich aus einem oder mehreren NDMP Services zusammen. Schließlich bezeichnet NDMP Host einen Rechner, der einen oder mehrere NDMP Server beherbergt.

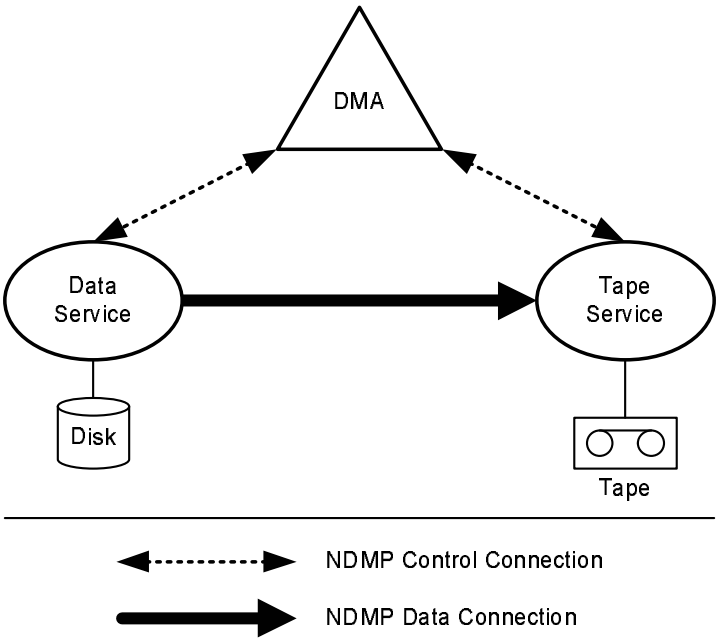

Abbildung 7.13
NDMP ist ein wichtiges Protokoll für die Sicherung von NAS-Servern. Es standardisiert die Kommunikation zwischen der Data Management Application (DMA), in der Regel ein Datensicherungssystem, und den NDMP Services (NDMP Data Service, NDMP Tape Service), die die Speichergeräte repräsentieren. Nicht standardisiert ist die Kommunikation zwischen den NDMP Services und den Speichergeräten.

NDMP Services

NDMP definiert verschiedene Formen von NDMP Services. Allen ist gemeinsam, dass sie nur ihren lokalen Zustand verwalten. Einem NDMP Service bleibt der Zustand anderer NDMP Services verborgen. NDMP Version 4 definiert im Einzelnen die folgenden NDMP Services:

NDMP Data Service

- *NDMP Data Service*
  Der NDMP Data Service bildet die Schnittstelle zu Primärdaten wie einem Dateisystem auf einem NAS-Server. Es ist die Quelle von Backup- und das Ziel von Restore-Operationen. Für die Sicherung eines Dateisystems wandelt der NDMP Data Service den Inhalt des Dateisystems in einen Datenstrom um und schreibt diesen in eine NDMP Data Connection, die in der Regel über eine TCP/IP-Verbindung hergestellt wird. Zur Wiederherstellung ei-

nes Dateisystems liest er den Datenstrom aus einer NDMP Data Connection und rekonstruiert daraus den Inhalt eines Dateisystems. Der Data Service ermöglicht nur die Sicherung kompletter Dateisysteme; das Sichern einzelner Dateien ist nicht möglich. Hingegen lassen sich neben kompletten Dateisystemen auch einzelne Dateien oder Verzeichnisse wiederherstellen.

Wiederherstellung einzelner Dateien

Die Wiederherstellung einzelner Dateien oder Verzeichnisse wird auch als »Direct Access Recovery« bezeichnet. Dazu stellt der Data Service ein sogenanntes File History Interface bereit, über das er während der Datensicherung die notwendigen Metadaten an die DMA weiterleitet. Die File History speichert die Positionen der einzelnen Dateien innerhalb des gesamten Datenstroms. Diese sogenannte File Locator Data ist für die DMA nicht lesbar. Sie kann diese aber bei einem Restore an den NDMP Tape Service übergeben, der auf Grundlage dieser Information an die entsprechende Bandposition spult und die entsprechende Datei ausliest.

- *NDMP Tape Service*

  NDMP Tape Service

  Der NDMP Tape Service bildet die Schnittstelle zum Sekundärspeicher. Sekundärspeicher im Sinne von NDMP sind Rechner mit angeschlossenem Bandlaufwerk, angeschlossener Tape Library oder einem CD-Brenner. Der Tape Service verwaltet das Ziel einer Datensicherung beziehungsweise die Quelle der Wiederherstellung von Daten. Der Tape Service schreibt für die Datensicherung einen über die NDMP Data Connection einkommenden Datenstrom auf Band. Für die Wiederherstellung liest er den Inhalt eines Bands und schreibt diesen als Datenstrom in eine NDMP Data Connection. Der Tape Service hat nur die Informationen, die er zum Lesen und Schreiben benötigt, wie Bandgröße oder Blockgröße. Er hat keine Kenntnisse über das Format des Datenstroms. Für das Wechseln von Bändern in einer Tape Library benötigt er die Hilfe der DMA.

- *NDMP SCSI Pass Through Service*

  NDMP SCSI Pass Through Service

  Der SCSI Pass Through Service ermöglicht es einer DMA, SCSI-Befehle an ein SCSI-Gerät zu senden, das an einen NDMP Server angeschlossen ist. Die DMA benötigt diesen Dienst beispielsweise für das Wechseln von Bändern in einer Tape Library.

Data Management Application (DMA)

Die DMA hält die Fäden einer NDMP Session zusammen. Sie verwaltet alle Zustandsinformationen der beteiligten NDMP Services, übernimmt die Verwaltung der Sicherungsmedien und leitet im Fehlerfall entsprechende Recovery-Maßnahmen ein. Dazu hält die DMA zu den beteiligten NDMP Services je eine NDMP Control Connection aufrecht, die wie die NDMP Data Connections in der Regel auf TCP/IP aufsetzt. Innerhalb einer NDMP Session können beide Seiten, DMA wie NDMP

Services, aktiv werden. So sendet beispielsweise die DMA Befehle zur Steuerung der NDMP Services, die NDMP Services wiederum schicken Meldungen, wenn ein Kontrolleingriff der DMA erforderlich ist. Hat beispielsweise ein NDMP Tape Service ein Band vollgeschrieben, so informiert er die DMA. Diese kann dann über einen NDMP SCSI Pass Through Service einen Wechsel der Bänder initiieren.

Backup-Szenarien mit NDMP

Aus der Tatsache, dass sowohl NDMP Control Connections als auch NDMP Data Connections auf TCP/IP aufsetzen, ergeben sich flexible Konfigurationsmöglichkeiten für die Datensicherung mit NDMP. Diese Vorgehensweise unterstützt die Sicherung auf ein lokal angeschlossenes Bandlaufwerk (Abbildung 7.14) ebenso wie auf ein Band-

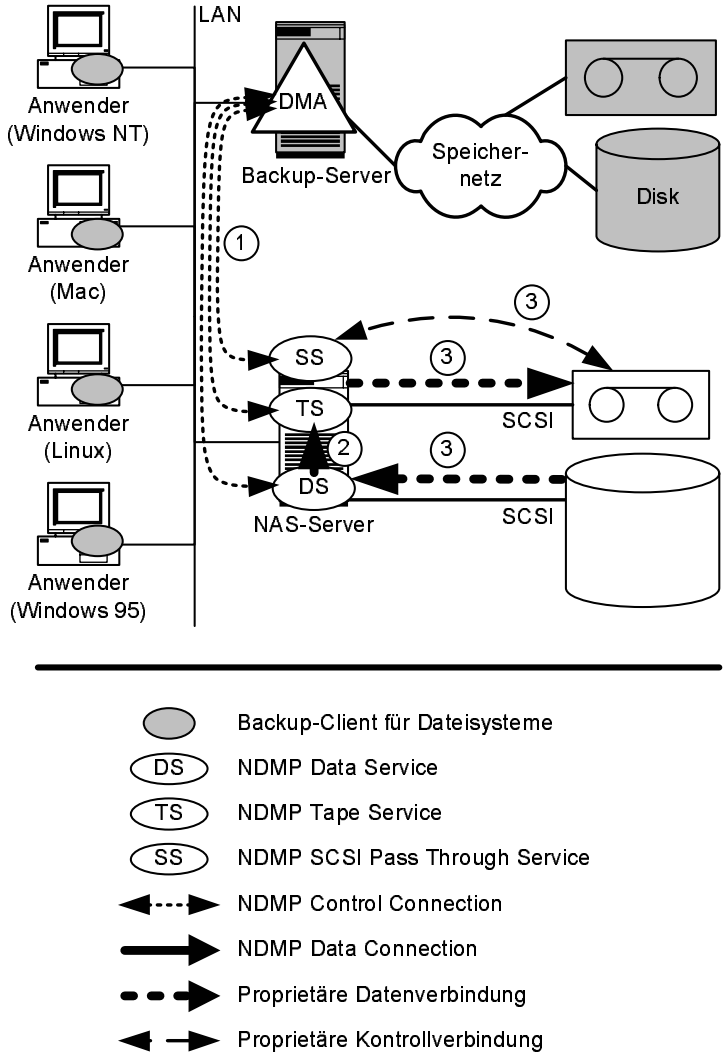

Abbildung 7.14
Bei der lokalen Sicherung (Local Backup) laufen NDMP Data Service, NDMP Tape Service und NDMP SCSI Pass Through Service auf demselben Rechner. NDMP definiert die Protokolle für die NDMP Control Connection (1) und die NDMP Data Connection (2). Die Kommunikation zwischen den NDMP Services und den Speichergeräten ist nicht standardisiert (3).

laufwerk, das an einem anderen Rechner, beispielsweise einem zweiten NAS-Server oder einem Backup-Server, angeschlossen ist (Abbildung 7.15). Dieses sogenannte Remote Backup hat den Vorteil, dass kleinere NAS-Server nicht mit einer Tape Library ausgestattet werden müssen. Weitere Einsatzgebiete von Remote Backup sind das Replizieren von Dateisystemen (disk-to-disk remote backup) und von Sicherungsbändern (tape-to-tape remote backup).

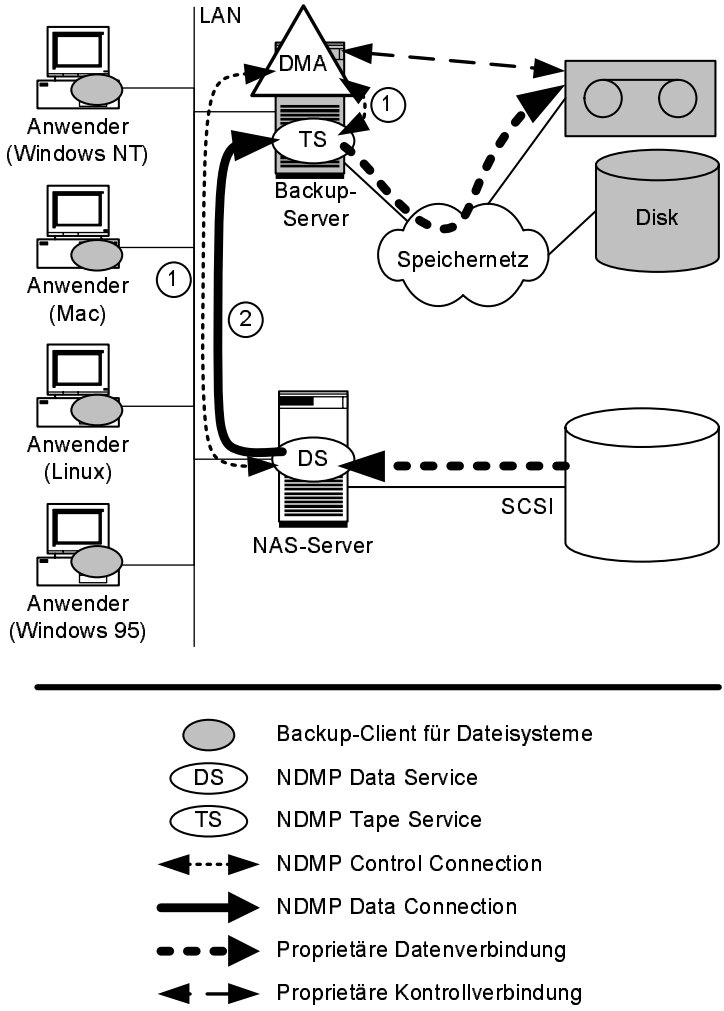

Abbildung 7.15
Bei der Sicherung über das LAN (Remote Backup) läuft der NDMP Tape Service auf dem Rechner, an dem das Sicherungsmedium angeschlossen ist. Die Kommunikation zwischen den entfernten Diensten ist dadurch gewährleistet, dass NDMP Control Connections (1) und NDMP Data Connections (2) auf TCP/IP aufsetzen. Der Backup-Server spricht die Tape Library lokal an, sodass der NDMP SCSI Pass Through Service hier nicht benötigt wird.

LAN-free Backup mit NDMP

Beim Remote Backup hat der Administrator mit den gleichen Performance-Engpässen zu kämpfen wie bei der herkömmlichen Netzwerk-Datensicherung über LAN (Kapitel 7.6). Erfreulicherweise ergänzen sich NDMP Local Backup und LAN-free Backup von Netzwerk-Datensicherungssystemen ausgezeichnet (Abbildung 7.16): Ein NAS-

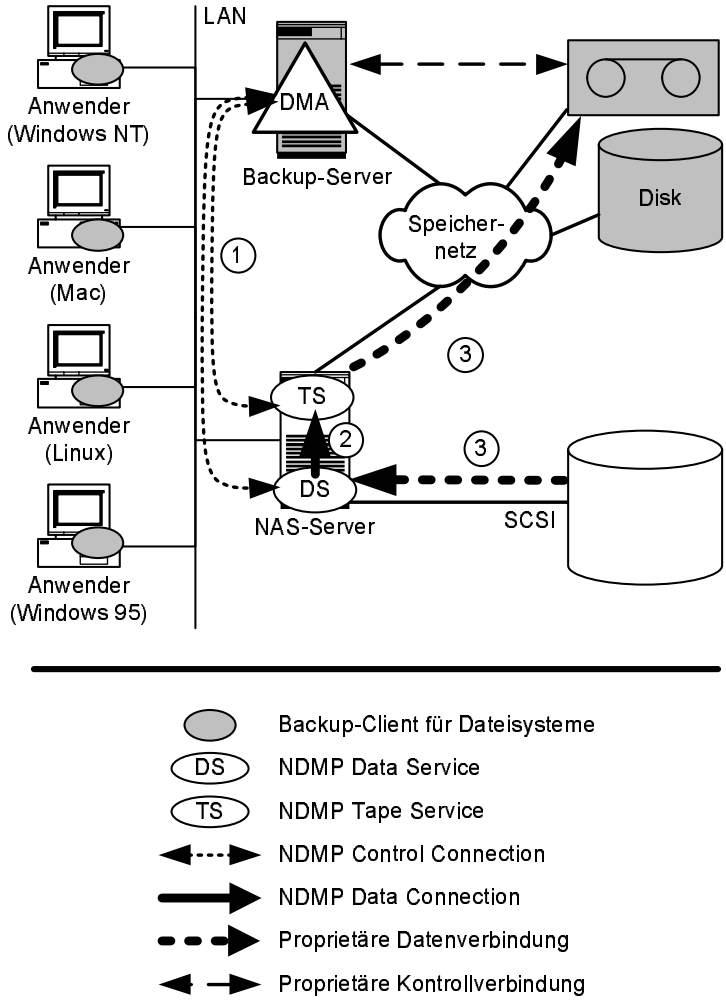

Abbildung 7.16
NDMP Local Backup kann hervorragend mit dem LAN-free Backup von Netzwerk-Datensicherungssystemen kombiniert werden.

Server kann auf ein im Speichernetz verfügbares Bandlaufwerk sichern, wobei das Netzwerk-Datensicherungssystem den Zugriff auf das Bandlaufwerk außerhalb von NDMP mittels Tape Library Sharing koordiniert.

NDMP Version 4: Extensions

NDMP Version 4 bietet über sogenannte Extensions die Möglichkeit, die Funktionalität des Protokolls zu erweitern. Dies wird von einigen Herstellern genutzt, um wichtige fehlende Funktionen von NDMP Version 4 bereitzustellen – beispielsweise das Sichern und die Verwaltung von Snapshots. Leider sind diese Extensions herstellerspezifisch, sodass man im Einzelfall genau prüfen muss, ob beispielsweise ein bestimmtes Netzwerk-Datensicherungssystem die Snapshots eines bestimmten NAS-Servers sichern kann.

Ausblick auf NDMP Version 5: Translator Services

Mit Version 5 erhält NDMP weitere Funktionen wie Multiplexing, Komprimierung und Verschlüsselung. Dazu erweitert NDMP Version 5 die Architektur um den sogenannten Translator Service (Abbildung 7.17). Translator Services bearbeiten den Datenstrom (Data Stream Processor): Sie können einen oder mehrere Datenströme lesen und verändern. Die Implementierung der Translator Services ist dabei konform zu den bisherigen NDMP Services. Das heißt, die Kontrolle des Translator Services liegt bei der DMA. Für andere beteiligte NDMP Services ist nicht erkennbar, ob ein einkommender Datenstrom von einem Translator Service oder einem anderen NDMP Service erzeugt wurde. NDMP Version 5 definiert die folgenden Translator Services:

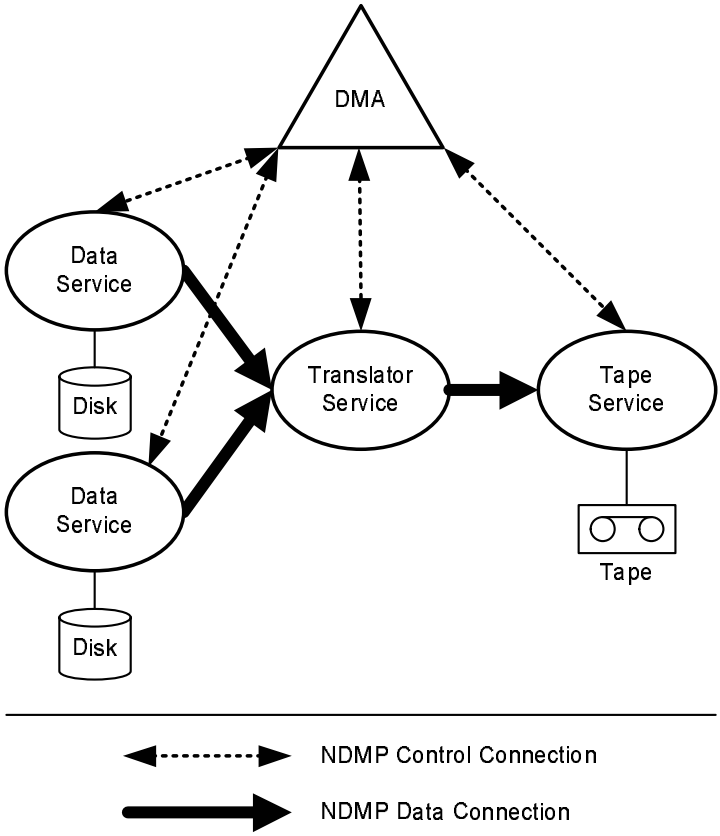

Abbildung 7.17
NDMP Version 5 erweitert die NDMP Services um Translator Services, die Funktionen wie Multiplexing, Verschlüsselung und Komprimierung bereitstellen.

Data Stream Multiplexing

- *Data Stream Multiplexing*
  Beim Data Stream Multiplexing geht es darum, mehrere Datenströme in einem Datenstrom zu bündeln (N:1-Multiplexing) oder aus einem Datenstrom mehrere zu erzeugen (1:M-Multiplexing). Beispiele hierfür sind die Sicherung mehrerer kleiner, langsamer

Dateisysteme auf ein schnelles Bandlaufwerk (N:1-Multiplexing) oder die parallele Sicherung eines großen Dateisystems auf mehrere Bandlaufwerke (1:M-Multiplexing).

Data Stream Compression

- *Data Stream Compression*
  Bei der Data Stream Compression liest der Translator Service einen Datenstrom, komprimiert ihn und gibt ihn wieder aus. Damit können die Daten bereits von der Festplatte komprimiert werden, sodass das Netz zwischen ihr und dem Sicherungsmedium entlastet wird.

Data Stream Encryption

- *Data Stream Encryption*
  Data Stream Encryption arbeitet vom Prinzip her genauso wie Data Stream Compression, wobei es die Daten nicht komprimiert, sondern verschlüsselt. Verschlüsselung ist beispielsweise sinnvoll für die Sicherung kleiner NAS-Server in Außenstellen über ein öffentliches Netz zu einem Backup-Server in einem Rechenzentrum.

Fazit

NDMP bietet viele Möglichkeiten, NAS-Server in ein Netzwerk-Datensicherungssystem einzubinden. Voraussetzung ist die NDMP-Unterstützung auf beiden Seiten. NDMP Data Services decken annähernd die Funktionen ab, die Backup-Clients von Netzwerk-Datensicherungssystemen bereitstellen. Eine Schwachstelle von NDMP ist die Sicherung von Metadaten des NAS-Servers, was die Wiederherstellung eines NAS-Servers nach dem kompletten Austausch der Hardware deutlich erschwert (Abschnitt 7.9.1). Des Weiteren werden die Sicherung von Dateisystemen mit Hilfe von Snapshots oder Instant Copies nur über herstellerspezifische Extensions ermöglicht. Schließlich wäre eine formale Standardisierung von NDMP, beispielsweise durch die IETF, wünschenswert. Trotz dieser Mängel hat NDMP sich als Industriestandard etabliert.

7.10 Sicherung von Datenbanken

Gliederung des Unterkapitels

Datenbanken sind neben den im vorherigen Kapitel besprochen Dateisystemen die zweite wichtige Organisationsform für Daten. Trotz der in Abschnitt 6.3.5 (»Ausfall eines Rechenzentrums am Beispiel ›Schutz einer wichtigen Datenbank‹«) vorgestellten Maßnahmen ist es manchmal erforderlich, eine Datenbank von einem Sicherungsmedium wieder zurückzuspielen. Für die Sicherung der Metadaten eines Datenbankservers ergeben sich die gleichen Fragen wie für die Sicherungen von Fileservern (Abschnitt 7.9.1). Dagegen gibt es deutliche Unterschiede

zwischen der Sicherung von Dateisystemen und Datenbanken. Für die Sicherung von Datenbanken ist ein grundlegendes Verständnis der Arbeitsweise von Datenbanken notwendig (Abschnitt 7.10.1). Kenntnisse über die Arbeitsweise von Datenbanken helfen, sowohl die herkömmliche Sicherung von Datenbanken ohne Speichernetze (Abschnitt 7.10.2) als auch die Sicherung von Datenbanken mit Speichernetzen und intelligenten Speichersystemen (Abschnitt 7.10.3) effizienter zu gestalten.

7.10.1 Arbeitsweise von Datenbanksystemen

Forderung: Atomizität von Transaktionen

Eine Anforderung an Datenbanksysteme ist die Atomizität von Transaktionen, wobei Transaktionen mehrere Schreib- und Lesezugriffe auf die Datenbank zu logisch zusammenhängenden Einheiten zusammenfassen. Atomizität von Transaktionen besagt, dass eine Transaktion mit Schreibzugriff vollständig durchgeführt werden soll oder überhaupt nicht.

Problem: Stromausfall während Transaktion

Transaktionen können den Inhalt einer oder mehrerer Blöcke verändern, die über mehrere Festplatten oder mehrere Disksubsysteme verteilt sein können. Transaktionen, die mehrere Blöcke verändern, sind problematisch für die Atomizität. Wenn das Datenbanksystem einige zu ändernde Blöcke bereits auf Festplatte geschrieben hat und andere noch nicht und anschließend der Datenbankserver wegen eines Stromausfalls oder eines Hardware-Fehlers ausfällt, dann wurde die Transaktion nur teilweise durchgeführt. Ohne zusätzliche Maßnahmen kann die Transaktion nach einem Reboot des Datenbankservers weder vollendet noch zurückgesetzt werden, weil die dazu notwendigen Informationen nicht mehr vorhanden sind. Die Datenbank wäre also inkonsistent.

Lösung: Logdateien

Das Datenbanksystem muss also neben der eigentlichen Datenbank zusätzlich Informationen über noch nicht abgeschlossene Transaktionen auf Festplatte speichern. Das Datenbanksystem verwaltet diese Informationen in sogenannten Logdateien. Es vermerkt jede anstehende Änderung der Datenbank zunächst in einer Logdatei, bevor es dann die Änderungen der Blöcke in der Datenbank selbst vornimmt. Fällt nun der Datenbankserver während einer Transaktion aus, so kann das Datenbanksystem nach einem Reboot des Servers noch nicht abgeschlossene Transaktionen mit Hilfe der Logdateien wahlweise vollenden oder zurücksetzen.

Aufgaben von Datenbanksystemen

Abbildung 7.18 zeigt stark vereinfacht die Architektur von Datenbanksystemen. Das Datenbanksystem erfüllt im Wesentlichen zwei Aufgaben:

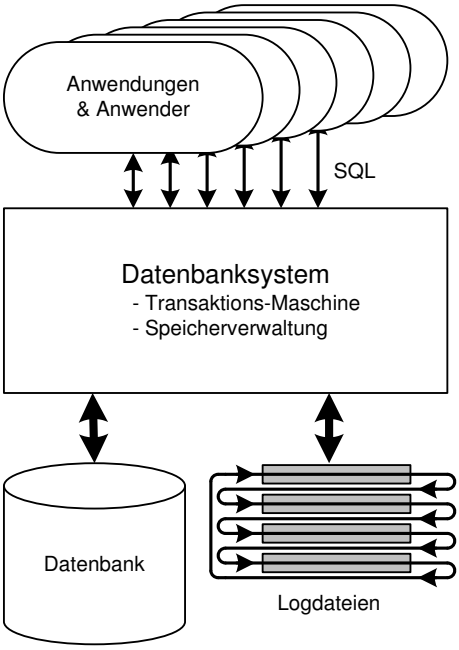

Abbildung 7.18
Anwender starten über die Datenbanksprache (SQL) Transaktionen, um Daten zu lesen oder zu schreiben. Das Datenbanksystem speichert die Anwendungsdaten in blockorientierten Daten (Datenbank) und gewährleistet mit Hilfe der Logdateien die Atomizität der Transaktionen.

Datenbank: Abbildung der logischen Datenstruktur auf blockorientierten Speicher

- *Datenbank: Speichern der logischen Datenstruktur auf blockorientierten Speicher*
  Zum einen organisiert das Datenbanksystem die Daten in einer den Anwendungen adäquaten Struktur und legt diese auf dem blockorientierten Festplattenspeicher ab. In heutigen Datenbanksystemen wird hierzu vor allem das relationale Datenmodell benutzt, das Informationen in miteinander verknüpften Tabellen speichert. Genau genommen speichert das Datenbanksystem die logischen Daten unter Umgehung eines Dateisystems direkt auf den Festplatten oder in großen Dateien. Die Vor- und Nachteile dieser beiden Alternativen wurden bereits im Abschnitt 4.1.1 diskutiert.

Transaktions-Maschine: Veränderung der Datenbank

- *Transaktions-Maschine: Veränderung der Datenbank*
  Zum anderen realisiert das Datenbanksystem Methoden für die Veränderungen der gespeicherten Informationen: Dazu stellt es eine Datenbanksprache und eine Transaktions-Maschine (transaction engine) bereit. In einer relationalen Datenbank initiieren Anwender und Anwendungen über die Datenbanksprache SQL Transaktionen und rufen so die gespeicherten Informationen ab oder verändern sie. Transaktionen auf der logischen, anwendungsnahen Datenstruktur bewirken also, dass die physikalischen Blöcke auf Festplatten verändert werden. Das Transaktionssystem sorgt unter anderem dafür, dass die durch eine Transakti-

on verursachten Änderungen des Datenbestandes entweder vollständig oder überhaupt nicht durchgeführt werden. Wie oben beschrieben, kann diese Bedingung mit Hilfe von Logdateien auch bei Rechner- oder Datenbanksystemabstürzen gewährleistet werden.

Organisation der Logdateien

Das Datenbanksystem verändert Blöcke im Datenbereich »wild durcheinander«, so wie es sich aus den Transaktionen ergibt. Die Logdateien dagegen werden grundsätzlich sequenziell beschrieben, wobei jede Logdatei eine gewisse Anzahl von Änderungen speichern kann. Datenbanksysteme werden in der Regel mit mehreren Logdateien konfiguriert, die nacheinander beschrieben werden. Wurden alle Logdateien vollgeschrieben, so überschreibt das Datenbanksystem zunächst diejenige Logdatei, die zuerst beschrieben wurde, danach die nächste und so weiter.

Archivierte Logdateien (Archive Logfiles)

Eine weitere wichtige Funktion für die Sicherung von Datenbanken ist die Sicherung der Logdateien. Dazu kopiert das Datenbanksystem vollgeschriebene Logdateien als Dateien in ein Dateisystem und nummeriert diese durch: logfile1, logfile2, logfile3 und so weiter. Diese Kopien der Logdateien werden auch als archivierte Logdateien (Archive Logfiles) bezeichnet. Das Datenbanksystem muss mit ausreichend Logdateien konfiguriert sein, damit ausreichend Zeit vorhanden ist, den Inhalt einer gerade vollgeschriebenen Logdatei in eine archivierte Logdatei zu kopieren, bevor sie erneut überschrieben wird.

7.10.2 Klassische Sicherung von Datenbanken

Wichtig: Konsistenz der Sicherung

Wie bei allen Anwendungen muss auch bei Datenbanken auf die Konsistenz der gesicherten Daten geachtet werden. Bei Datenbanken bedeutet Konsistenz, dass die Eigenschaft der Atomizität der Transaktionen aufrechterhalten bleibt. Nach dem Wiedereinspielen (Restore) einer Datenbank muss also sichergestellt sein, dass sich im Datenbestand nur die Ergebnisse von vollständig abgeschlossenen Transaktionen befinden. In diesem Abschnitt besprechen wir verschiedene Methoden der Datensicherung, die genau dies gewährleisten. Im Anschluss erläutern wir, wie Speichernetze und intelligente Speichersysteme helfen, die Sicherung von Datenbanken zu beschleunigen (Abschnitt 7.10.3).

Cold Backup

Die einfachste Sicherungsmethode für Datenbanken ist das sogenannte Cold Backup. Für Cold Backup wird die Datenbank heruntergefahren, sodass alle Transaktionen abgeschlossen sind, und dann werden die entsprechenden Dateien oder Volumes gesichert. Dabei werden Datenbanken genauso gesichert wie Dateisysteme. Hier ist es einfach, die Konsistenz der gesicherten Daten zu gewährleisten, weil während der Sicherung keine Transaktionen stattfinden.

Bewertung: Cold Backup

Cold Backup ist eine einfach zu realisierende Methode für die Sicherung von Datenbanken. Sie hat aber zwei Nachteile. Zum einen kann man es sich in einer 24x7-Umgebung nicht leisten, Datenbanken für die Datensicherung herunterzufahren, zumal die Sicherung großer Datenbanken mit herkömmlichen Methoden einige Stunden dauern kann. Zum anderen sind ohne weitere Maßnahmen bei Ausfall des Disksubsystems alle Änderungen seit der letzten Sicherung verloren. Wird eine Datenbank beispielsweise nachts gesichert und fällt das Disksubsystem am nächsten Abend aus, so sind alle Änderungen des letzten Arbeitstages verloren.

Forward Recovery mit archivierten Logdateien

Mit Hilfe der archivierten Logdateien lässt sich zumindest das zweite Problem lösen. Mit der letzten Sicherung der Datenbank und allen danach gesicherten archivierten Logdateien sowie den aktiven Logdateien kann man den letzten Stand der Datenbank wiederherstellen. Dazu muss man zunächst die letzte Sicherung der Datenbank vom Sicherungmedium wieder einspielen, im Beispiel oben die Sicherung der letzten Nacht. Danach spielt man alle archivierten Logdateien, die seit der letzten Sicherung erstellt wurden, sowie alle aktiven Logdateien noch einmal in den Datenbestand ein. Diese Vorgehensweise, die auch als Forward Recovery von Datenbanken bezeichnet wird, ermöglicht es, selbst lange nach der letzten Sicherung der Datenbank den neuesten Stand wiederherzustellen. Je nach Größe der archivierten Logdateien kann dies allerdings einige Zeit in Anspruch nehmen.

Sicherung der archivierten Logdateien

Die Verfügbarkeit der archivierten Logdateien ist also eine wichtige Voraussetzung für das erfolgreiche Forward Recovery einer Datenbank. Deshalb sollte das Dateisystem für die archivierten Logdateien auf anderen Festplatten abgelegt werden als die Datenbank selbst (Abbildung 7.19) und zusätzlich durch ein redundantes RAID-Verfahren abgesichert werden. Zudem sollte man auch die archivierten Logdateien regelmäßig sichern.

Hot Backup

Logdateien und archivierte Logdateien bilden die Grundlage von zwei weiteren Sicherungsmethoden für Datenbanken: Hot Backup und Fuzzy Backup. Beim Hot Backup schreibt das Datenbanksystem anstehende Änderungen der Datenbank nur in die Logdateien. Die eigentliche Datenbank bleibt in dieser Zeit unberührt, sodass die Konsistenz der Sicherung gewährleistet ist. Nach Beenden der Sicherung wird das Datenbanksystem wieder in den Normalzustand zurückgeschaltet. Es kann dann die in den Logdateien vermerkten Änderungen in die Datenbank einbringen.

Bewertung von Hot Backup

Hot Backup eignet sich für Situationen, in denen rund um die Uhr Zugriff auf die Daten benötigt wird. Allerdings sollte Hot Backup nur in Phasen eingesetzt werden, in denen relativ wenige Schreibzugriffe stattfinden. Dauert beispielsweise die Sicherung der Datenbank zwei Stunden und steht die Datenbank unter Volllast, so müssen die Log-

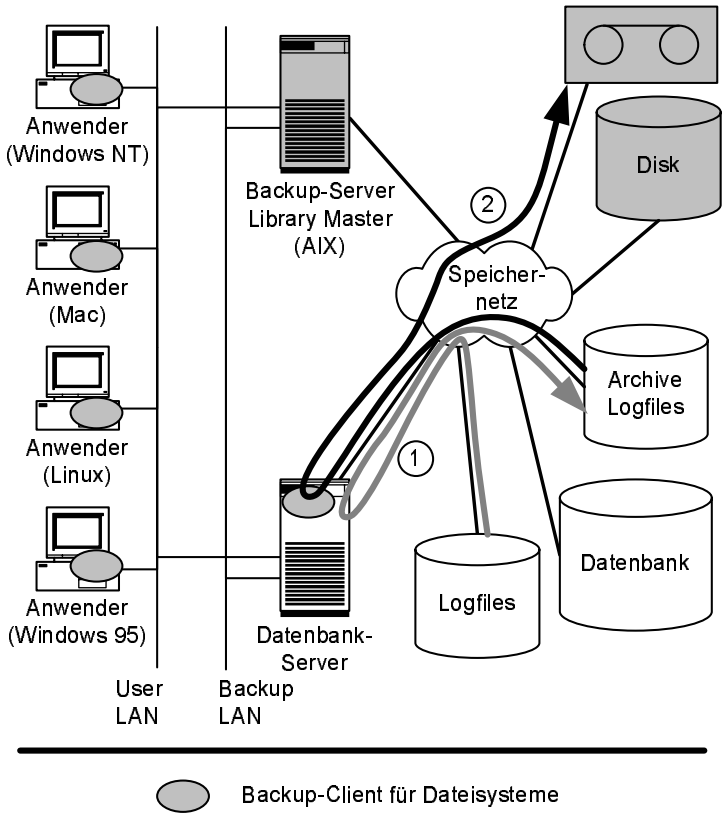

Abbildung 7.19
Das Datenbanksystem kopiert die archivierten Logdateien in ein Dateisystem, das auf einem anderen Speichersystem platziert ist als die Datenbank und deren Logdateien (1). Die archivierten Logdateien können von dort aus mit fortgeschrittenen Techniken wie dem LAN-free Backup gesichert werden (2).

dateien groß genug dimensioniert sein, um alle während der Sicherung durchgeführten Änderungen speichern zu können. Außerdem muss das System nach der Sicherung zusätzlich zu den aktuell anstehenden auch die aufgeschobenen Transaktionen nachziehen. Beides zusammen kann zu Performance-Engpässen führen.

Fuzzy Backup

Fuzzy Backup schließlich lässt Änderungen der Datenbank während ihrer Sicherung zu, sodass ein inkonsistenter Zustand der Datenbank gesichert wird. Das Datenbanksystem ist dennoch in der Lage, mit Hilfe der archivierten Logdateien, die während der Sicherung geschrieben wurden, den inkonsistenten Zustand zu bereinigen.

Fazit

Mit Cold Backup, Hot Backup und Fuzzy Backup stehen drei Methoden für die Sicherung von Datenbanken zur Verfügung. Netzwerk-Datensicherungssysteme stellen Backup-Clients für Datenbanken bereit, sodass alle drei Sicherungsmethoden gut mit einem Netzwerk-Datensicherungssystem automatisiert werden können. Nach dem Prinzip, Systeme so einfach wie möglich zu halten, sollten Cold Backup oder Hot Backup eingesetzt werden, wann immer es möglich ist.

7.10.3 Sicherung von Datenbanken mit Speichernetzen

Sicherung von Datenbanken mit Speichernetzen

Die im vorherigen Abschnitt vorgestellten Methoden zur Datensicherung (Cold Backup, Hot Backup und Fuzzy Backup) können hervorragend mit Speichernetzen und intelligenten Speichersystemen kombiniert werden. Im Folgenden zeigen wir, wie dies nun effizienter gestaltet werden kann.

Sicherung mit Instant Copies

Die Verknüpfung von Hot Backup mit Instant Copies ist ein nahezu perfektes Werkzeug für die Sicherung von Datenbanken. Im Einzelnen sind folgende Schritte auszuführen:

1. Umschalten der Datenbank in den Hot-Backup-Modus, sodass sich ein konsistenter Datenbestand im Speichersystem befindet,
2. Erstellen der Instant Copy,
3. Zurückschalten der Datenbank in den Normalmodus,
4. Sicherung der Datenbank von der Instant Copy.

Diese Vorgehensweise hat zwei Vorteile: Zum einen ist während der gesamten Zeit ein Zugriff auf die Datenbank möglich. Zum anderen dauern die Schritte 1 bis 3 nur wenige Sekunden, sodass das Datenbanksystem nach dem Zurückschalten in den Normalmodus nur vergleichsweise wenige Transaktionen nachziehen muss.

Application Server-free Backup

Application Server-free Backup erweitert die Sicherung mit Instant Copies, um zusätzlich den Datenbankserver von der Last der Sicherung zu befreien (Abschnitt 7.8.4). Das in Abbildung 7.10 auf Seite 269 dargestellte Konzept eignet sich auch sehr gut für Datenbanken. Aufgrund der großen Datenmenge bei der Sicherung von Datenbanken wird – anders als in der Abbildung gezeigt – häufig LAN-free Backup eingesetzt, um die mit Instant Copy erzeugten Daten zu sichern.

Anforderung: Erhöhung der Frequenz der Datenbanksicherungen

Im vorherigen Abschnitt (Abschnitt 7.10.2) wurde erläutert, dass der Zeitpunkt der letzten Sicherung entscheidend ist für die Zeit, die benötigt wird, um eine Datenbank auf dem letzten Datenstand wiederherzustellen. Liegt die letzte Sicherung schon lange zurück, so müssen sehr viele archivierte Logdateien nachgespielt werden. Um die Wiederherstellungsszeit einer Datenbank zu verkürzen, ist es also notwendig, die Frequenz der Datenbanksicherungen zu erhöhen.

Problem: Große Datenmenge

Das Problem dabei: Bei der vollständigen Sicherung von Datenbanken werden große Datenvolumina bewegt. Dies ist sehr zeitaufwendig und verbraucht viele Ressourcen, sodass die Frequenz der Sicherungen nur bedingt erhöht werden kann. Ebenso sind das verzögerte Nachfahren der Logdateien auf einem zweiten System (Abschnitt 6.3.5) und das Vorhalten mehrerer Kopien des Datenbestandes auf dem Disksubsys-

tem mittels Instant Copy aufgrund des hohen Hardware-Bedarfs und der damit verbunden Kosten nur selten wirtschaftlich zu rechtfertigen.

Lösung: Block-Level Incremental Backup für Datenbanken

Um die Frequenz der Sicherung einer Datenbank dennoch zu erhöhen, muss also das zu übertragende Datenvolumen reduziert werden. Dies ist über eine inkrementelle Sicherung der Datenbank auf Blockebene möglich. Die wichtigsten Datenbanksysteme bieten hierzu Sicherungswerkzeuge an. Viele Netzwerk-Datensicherungssysteme stellen spezielle Adapter (Backup Agents) bereit, die auf die Sicherungswerkzeuge der jeweiligen Datenbanksysteme zugeschnitten sind. Allerdings bleibt der Backup-Software das Format der Inkremente verborgen, sodass die Incremental-Forever-Strategie auf diesem Weg nicht realisiert werden kann. Die Hersteller von Datenbanksystemen müssten dazu das Format der Inkremente bekanntmachen.

Incremental Forever für Datenbanken

Für die Sicherung von Datenbanken mit der Incremental-Forever-Strategie muss die Backup-Software also das Format der inkrementellen Sicherungen kennen, damit sie daraus die Vollsicherungen berechnen kann. Hierzu muss man den Speicherplatz der Datenbank über ein Dateisystem bereitstellen, das mit dem entsprechenden Backup-Client auf Blockebene inkrementell gesichert wird. Nun ist der Backup-Software das Format der Inkremente bekannt, sodass über den Umweg Dateisysteme die Incremental-Forever-Strategie für Datenbanken realisiert werden kann.

7.11 Organisatorische Aspekte der Datensicherung

Datensicherung ist personalintensiv.

Neben den erforderlichen technischen Ressourcen wird auch der Personalaufwand für die Datensicherung allzu oft unterschätzt. Es wurde bereits besprochen, dass (1.) die Datensicherung immer wieder an die sich ständig verändernde IT-Landschaft angepasst werden muss und dass (2.) permanent überwacht werden muss, ob die Datensicherung tatsächlich wie geplant ausgeführt wird. Beides zusammen erfordert einfach Zeit, wobei der Zeitaufwand für diese Tätigkeiten oft unterschätzt wird.

Personalkosten verglichen mit Kosten für Datenverluste

Wie bei jeder Tätigkeit sind auch bei der Datensicherung handwerkliche Fehler nicht zu vermeiden, insbesondere wenn wegen Personalmangels permanenter Zeitdruck herrscht. Im Bereich der Datensicherung bedeuten handwerkliche Fehler aber immer einen potenziellen Datenverlust. Die Kosten für einen Datenverlust können enorm sein: Beispielsweise nennt Marc Farley (Building Storage Networks, 2000) allein 1.000 US-Dollar pro Angestellten als Kosten für verlore-

ne E-Mail-Datenbanken. Deshalb sollte der Personalbedarf für die Datensicherung zumindest jährlich begutachtet werden. Dabei müssen die Personalkosten immer mit den Kosten für verlorene Daten verglichen werden.

Probleme bei der Wiederherstellung von Daten

Das Wiederherstellen von Daten scheitert manchmal daran, dass bei der Datensicherung die Daten nicht vollständig gesichert wurden, dass aus Versehen Bänder mit aktuellen Daten überschrieben wurden oder dass zur Sicherung Bänder benutzt wurden, die schon abgenutzt und überaltert waren. Der Media Manager kann gegen die meisten dieser Probleme vorbeugen.

Eine erfolgreiche Datenwiederherstellung erfordert eine fehlerfreie Konfiguration der Backup-Software.

Er bleibt aber wirkungslos, wenn die Backup-Software nicht richtig konfiguriert wird. Einer der Autoren kann sich noch gut an eine Situation erinnern, die heute fast zwanzig Jahre zurückliegt: Nach einer geplanten Repartitionierung einer Festplatte konnte er die Daten nicht wiederherstellen. Im Skript zur Datensicherung befand sich nur einziger Tippfehler. Dadurch wurde statt der Partition mit Daten eine leere Partition gesichert.

Datenwiederherstellung muss geübt werden.

Die Wiederherstellung von Daten sollte regelmäßig geübt werden, um Fehler bei der Datensicherung vor dem Ernstfall festzustellen, um die Ausführung solcher Aufgaben einzuüben und um die zu veranschlagende Zeit zu messen. Die Zeit für die Datenwiederherstellung ist eine wichtige Kostengröße: Beispielsweise kann ein mehrstündiger Ausfall einer zentralen Anwendung wie SAP erhebliche Kosten nach sich ziehen.

Diese Szenarien sollten immer wieder geübt werden!

Deshalb sollten zum Beispiel folgende Szenarien regelmäßig trainiert werden:

- Wiederherstellung eines wichtigen Servers inklusive aller Anwendungen und Daten auf äquivalenter Hardware,
- Wiederherstellung eines wichtigen Servers inklusive aller Anwendungen und Daten auf neuer Hardware,
- Wiederherstellung eines Unterverzeichnisses in einen anderen Bereich des Dateisystems,
- Wiederherstellung eines wichtigen Dateisystems oder einer wichtigen Datenbank,
- Wiederherstellung mehrerer Rechner mit den Bändern aus dem Off-Site-Lager,
- Wiederherstellung alter Archive (Gibt es noch Bandlaufwerke für die alten Medien?).

Der Zeitaufwand für solche Übungen ist bei der Berechnung des Personalbedarfs für die Datensicherung ebenfalls zu berücksichtigen.

7.12 Zusammenfassung und Ausblick

Fazit

Speichernetze und intelligente Speichersysteme eröffnen neue Möglichkeiten, Performance-Probleme der Netzwerk-Datensicherung zu lösen. Allerdings sind diese neuen Techniken erheblich teurer als die klassische Netzwerk-Datensicherung über das LAN. Deshalb sollte man sich zunächst überlegen, wie schnell Daten wirklich gesichert beziehungsweise wiederhergestellt werden müssen. Erst dann kann man sich überlegen, welche Alternative am wirtschaftlichsten ist: Die neuen Techniken wird man vor allem für schwergewichtige Clients und für 24x7-Anwendungen einsetzen. Einfache Clients werden nach wie vor mit klassischen Methoden der Netzwerk-Datensicherung gesichert, und für mittelschwere Clients bietet sich immer noch die Möglichkeit, ein separates LAN für die Datensicherung zu installieren. In heutigen realen IT-Systemen wird man deshalb oft alle drei Techniken finden.

Zusammenfassung des Kapitels

Datensicherung ist ein schwieriges und ressourcenintensives Geschäft. Mit Netzwerk-Datensicherungssystemen kann die Datensicherung auch in heterogenen Umgebungen weitgehend automatisiert werden. Die Automatisierung entlastet Systemverwalter und hilft Fehler wie das unbeabsichtigte Überschreiben von Bändern zu vermeiden. Der Einsatz von Netzwerk-Datensicherungssystemen ist in großen Umgebungen unerlässlich. Er lohnt sich aber auch in kleineren Umgebungen. Trotzdem darf der Personalaufwand für die Datensicherung nicht unterschätzt werden.

Zusammenfassung des Kapitels im Detail

Ausgangspunkt des Kapitels waren die Rahmenbedingungen für die Datensicherung: starkes Wachstum der zu sichernden Datenmenge, kontinuierliche Anpassung der Datensicherung an sich ständig wandelnde IT-Systeme und die Verkleinerung des Zeitfensters für die Datensicherung durch Globalisierung. Der Übergang zur Netzwerk-Datensicherung erfolgte mit der Beschreibung der Dienste Datensicherung (Backup), Archivierung und hierarchische Speicherverwaltung (HSM). Dann wurden die für die Implementierung dieser Dienste notwendigen Serverkomponenten (Job Scheduler, Error Handler, Media Manager und Metadaten-Datenbank) sowie die Backup-Clients besprochen. Im Zentrum standen die Incremental-Forever-Strategie und die Speicherhierarchie innerhalb des Backup-Servers. Weiter wurde die Netzwerk-Datensicherung in Hinblick auf die Performance betrachtet. Zunächst wurde gezeigt, wie Netzwerk-Datensicherungssysteme dazu beitragen können, die bestehende Infrastruktur effizienter zu nutzen. Als Performance-Engpässe waren die CPU-Auslastung, die Verstopfung der internen Busse und die Ineffizienz des Mediums TCP/IP/Ethernet hervorzuheben. Anschließend wurden Lösungsansätze zur Performance-

Steigerung diskutiert, die innerhalb einer serverzentrierten IT-Architektur möglich sind einschließlich deren Einschränkungen. Es folgten Lösungsansätze zur Überwindung der Performance-Engpässe in einer speicherzentrierten IT-Architektur. Abschließend wurden die Sicherung großer Dateisysteme und Datenbanken sowie organisatorische Fragestellungen der Netzwerk-Datensicherung angerissen.

Bezug zu den folgenden Kapiteln

Das nächste Kapitel (Kapitel 8) betrachtet mit der Archivierung ein weiteres wichtiges Einsatzfeld von Speichernetzen. Im Gegensatz zur Datensicherung geht es bei der Archivierung darum, Daten »einzufrieren« und über Jahre oder gar Jahrzehnte aufzuheben. In dem darauf folgenden Kapitel (Kapitel 9) werden wir die Datensicherung als wichtigen Baustein der Business Continuity wieder aufgreifen.