Teil 6: Sicherheit der Daten

6/2 Datenschutz unter NetWare

Einer der Hauptgründe für den Einsatz eines Netzwerks liegt darin, eine mehr oder minder große Datenmenge speichern und für jeden Anwender zugänglich machen zu können. Aber gerade diese Eigenschaft der Netzwerke eröffnet die Möglichkeit des Mißbrauchs schützenswerter oder geheimer Daten, des Diebstahls von Informationen und der mutwilligen oder fahrlässigen Zerstörung von wertvollem Datenmaterial.

Sicherheit

Um einen umfassenden Schutz vor Datenmißbrauch zu gewährleisten, sind in Netzwerken umfassende Sicherheitsmaßnahmen vorzusehen. Novell bietet hier ein breites Spektrum an Schutzmaßnahmen, um sowohl das Eindringen Unbefugter in das Netz als auch den Datenmißbrauch von seiten der Anwender im Netz weitgehend zu verhindern.

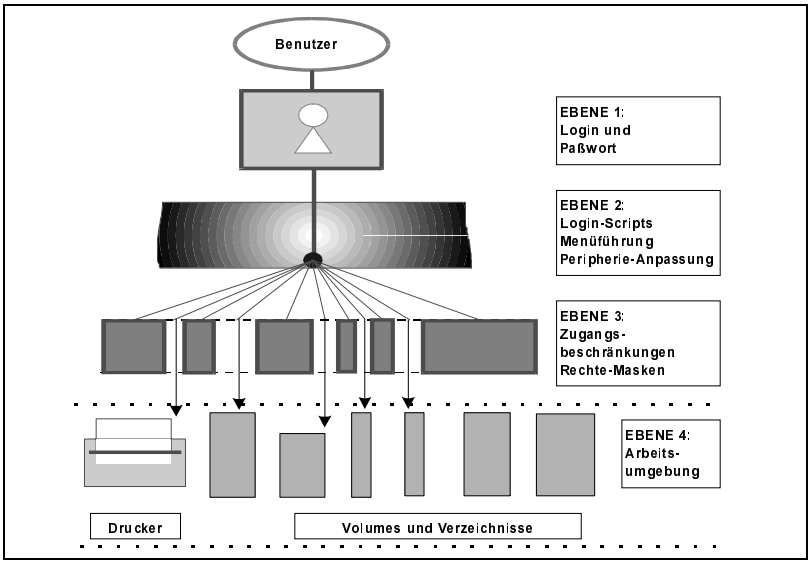

Abbildung 1: Allgemeiner Netzwerkzugang

Insgesamt hat Novell die Datenschutzmechanismen innerhalb von NetWare auf mehrere Ebenen verteilt. Wie in Abbildung 1 symbolisch dargestellt, läßt sich der Netzwerkzugang in 4 Ebenen gliedern, wobei die Ebenen 1 und 3 den Mechanismus des Datenschutzes definieren.

Netzwerkzugang

Ebene 1 repräsentiert die Zugangskennung (Benutzername) mit Paßwortschutz. Das Paßwort wird sofort bei Verlassen der Arbeitsstation in Richtung Server verschlüsselt. Damit kann ein Paßwort auch mit Abhörmaßnahmen nicht identifiziert werden. Diese Ebene stellt den Schlüssel zum Inneren des Servers dar, ohne den überhaupt kein Zugriff auf die Datenträger des Servers möglich ist.

Ebene 2 beinhaltet die relativ komplexe Steuerung der spezifischen Zugriffsrechte auf Verzeichnisse und Dateien der Volumes bezüglich der jeweiligen Benutzer. Des weiteren werden hier die Zugangseinschränkungen (am Beispiel von SYSCON) festgelegt:

- Volume/Disk Restrictions
- Account Restrictions
- Station Restrictions
- Time Restrictions

6/2.1 Benutzerkennung und Paßwortschutz

6/2.1.1 Benutzerkennung

Die Benutzerkennung – im Fachjargon Login-Name – stellt die erste Hürde für jeden Benutzers dar, der auf die verfügbaren Netzwerk-Ressourcen zugreifen möchte.

Hierbei wird nach dem Laden der NetWare-Shell bzw. nach der Aktivierung der entsprechenden Client-Software (DOS-Requester, 32-Bit-Client) und dem daraus resultierenden Serverkontakt das Programm LOGIN.EXE aufgerufen. Das Programm verlangt die Eingabe eines Login-Namens. Dieser Name – der (Kurz-)Name des Benutzers oder eine beliebige andere Zeichenfolge – muß auch in der NDS-Datenbank existieren. Dazu muß ein Systemverwalter mit den Dienstprogrammen NETADMIN oder NWADMIN den LOGIN-Namen anlegen. Bei der Erstellung eines neuen Namens werden dem Benutzer, der sich unter diesem Namen anmeldet, vom NetWare-System als Default-Einstellung gewisse „Grundrechte“ erteilt. Mit diesen Default-Rechten kann er folgende Minimalaktionen ausführen:

- Dateien in seinem Home-Verzeichnis erstellen und verändern, sofern die Erstellung dieses Verzeichnisses vom Systemverwalter nicht gesperrt wurde.
- Ein persönliches Login-Script (Anmeldescript) schreiben und abspeichern.
- NetWare-Dienstprogramme aus dem Verzeichnis SYS:PUBLIC aufrufen und mit ihnen Einstellungen treffen, die innerhalb seiner Rechtestruktur liegen.
- Unter Zuhilfenahme geeigneter Programme seinen eigenen Rechtestatus kontrollieren und überwachen – aber nicht verändern!

6/2.1.2 Paßwort

Der Paßwortschutz stellt bei einer Anmeldung nach der Benutzerkennung die zweite Hürde dar. Die Paßworteingabe verhindert, daß sich ein x-beliebiger Benutzer unter dem ihm bekannten Login-Namen eines anderen Benutzer den Netzwerkzugang „erschleicht", um dessen Zugriffsrechte im Netz zu mißbrauchen.

Paßwörter schützen

Das Paßwort selbst, das nach Eingabe der Benutzerkennung abgefragt wird, kann durch folgende Optionen zusätzlich geschützt werden:

- Beschränkung der Anzahl der Paßworteingaben
- Verfall des Paßworts nach einem bestimmten, festzulegenden Zeitraum
- Grace Logins (Fehlanmeldungen), die dem Benutzer nur eine bestimmte, festzulegende Anzahl von Paßworteingaben (altes Paßwort) bei abgelaufenem Paßwort erlauben.

6/2.1.3 Besonderheiten des Paßwortschutzes

In den NetWare-Versionen 2.x und 3.x wurden die Paßwörter teils verschlüsselt, teils unverschlüsselt über die Netzwerkkabel „verschickt". Ab der Version 4.0 von Novell NetWare wurde dieses Sicherheitsmanko beseitigt.

Benutzer-Autorisierung

Mit einem ausgeklügelten Verschlüsselungssystem erhält jeder Benutzer einen persönlichen Schlüssel, der die Benutzeridentifizierung (User Authentication) ermöglicht. Wenn ein Benutzer an einer Arbeitsstation seine Benutzerkennung (Anmeldename) eingibt, wird diese anschließend mit dem „Client Agent" des DOS-Requesters an die NDS-Datenbank übermittelt. Dort wird überprüft, ob die angegebene Ken-

nung im angegebenen oder im aktuellen Kontext überhaupt existiert. Wenn dies der Fall ist, wird der individuelle Benutzerschlüssel (private key) an die betreffende Arbeitsstation zurückgeschickt.

Im Anschluß daran wird der Benutzer aufgefordert, sein Paßwort einzugeben. Dieses Paßwort wird danach mit Hilfe des Benutzerschlüssels an der Arbeitsstation dekodiert (entschlüsselt), wobei der Schlüssel (private key) anschließend wieder aus dem Arbeitsspeicher der Arbeitsstation entfernt wird. Der entschlüsselte Code wird zurück zur NDS-Datenbank geschickt, wo er überprüft wird. Wenn die Prüfung positiv ausfällt, kann der Benutzer auf das System zugreifen.

Somit wird das Paßwort selbst nicht mehr über die Hardware-Verbindung übertragen und ist daher auch nirgendwo mehr (unbefugt) „abzugreifen“ und zu entschlüsseln.

Hintergrund

Im übrigen läuft der Vorgang der Benutzeridentifizierung für die einzelnen Benutzer vollkommen unbemerkt im Hintergrund ab. Dies trifft im übrigen auch für die weitergehende Überprüfung zu, die bei jeder Anfrage des Benutzers an die Datenbank bzw. an die Server, also bei jeder Service-Anforderung (im Hintergrund) durchgeführt wird.

Hinter dem Verschlüsselungssystem von NetWare verbirgt sich ein kompliziertes mathematisches Verfahren, bei dem sowohl das Prinzip der symmetrischen als auch das der asymmetrischen Verschlüsselung zum Einsatz kommt. Dieses Prinzip hier weiter auszuführen, würde jedoch den Rahmen dieses Werkes „sprengen“.

6/2.2 Notwendigkeit von Zugriffsrechten

Wie in den vorhergehenden Abschnitten beschrieben, bestehen die ersten Sicherheitsmechanismen beim Netzwerkzugang aus der Benutzerkennung und dem Paßwortschutz. Nachdem sich ein bestimmter Benutzer nach positivem Ablauf der ersten Sicherheitsabfragen am Server eingeloggt hat, stehen ihm zwar gewisse Minimalrechte zur Verfügung, er kann jedoch noch keine sinnvolle Arbeit aufnehmen.

Ohne die zusätzliche Vergabe von Rechten durch den Systemverwalter oder einen ihm gleichgestellten Benutzer bleibt dem Anwender der Zugriff auf sämtliche Dateien auf dem Volume SYS: und den anderen Datenträgern versagt. Er kann existierende Verzeichnisse weder sehen (z. B. mit der DOS-Anweisung DIR) noch darauf zugreifen.

Nachdem von seiten des Systemverwalters bei der Netzwerkplanung ein sogenanntes Struktogramm (Organisationsstruktur) der betreffenden Firma erstellt wurde, können die benötigten Rechte bezüglich der einzelnen Benutzer festgelegt und zugewiesen werden.

Angenommen, ein Benutzer mit dem Login-Namen WEKALI soll unter der grafischen Oberfläche MS Windows mit dem Programm WINWORD arbeiten.

Die für diese Applikationen relevanten Daten stehen in folgenden Verzeichnissen:

- **SYS:WINDOWS**
  Hier stehen die Systemdateien, die vom Benutzer nicht verändert werden dürfen.

- **SYS:WINDOWS\WINUSER\WEKALI**
  In diesem Verzeichnis stehen neben den benutzerspezifischen Systemdateien konfigurierbare INI-Dateien, die in den meisten Fällen vom Benutzer verändert werden können.
  Des weiteren existieren unter dem Verzeichnis WEKALI noch weitere Unterverzeichnisse wie TEMP und DOC, auf die der betreffende Benutzer auf alle Fälle Schreibzugriff haben muß.
- **SYS:WINWORD**
  In diesem Verzeichnis stehen die Systemdateien von WINWORD, die ebenfalls nur geöffnet, aber nicht verändert werden dürfen.

Aus dieser Konstellation ergibt sich die erweiterte Rechtestruktur für den Benutzer WEKALI oder für die Gruppe, die dasselbe Tätigkeitsumfeld besitzt und deren Mitglied er ist.

Folgende Einträge sind mit den Dienstprogrammen SYSCON bzw. NETADMIN als Trustee Directory Assignments vorzunehmen:

```
SYS:WINDOWS                  [  R    F  ]

SYS:WINDOWS\WINUSER\WEKALI   [  RWCEMF  ]

SYS:WINWORD                  [  R    F  ]
```

Die Zeile SYS:WINDOWS\WINUSER\WEKALI darf natürlich nur in den Trustee Directory Assignments unter seinem Benutzernamen eingetragen sein – nicht in einer zugehörigen Gruppe –, da es sich hier ja um sein persönliches Verzeichnis handelt.

Verzeichnisrechte

Diese im obigen Beispiel aufgezeichnete Rechtezuweisung wird als Trustee Directory Assignment oder „Direkte Rechte-Zuweisung“ bezeichnet. Eine weitere Möglichkeit, Rechte zu erteilen, besteht in der Vergabe einer „rechtemäßigen Gleichstellung“, bei der einem Benutzer die Rechte eines anderen Benutzers erteilt werden. Dieser Vorgang wird als Security Equivalence (Sicherheitsgleichstellung) oder Indirekte Rechtezuweisung bezeichnet.

Sicherheitsgleichstellung

Die wichtigste indirekte Zuweisung ist die Sicherheitsgleichstellung mit dem Systemverwalter (ADMIN), durch die ein Benutzer alle Rechte auf dem System erhält. Dabei ist zu beachten, daß eine Rechte-Gleichstellung mit dem Systemverwalter nicht dasselbe bedeutet wie die Zuweisung des Rechts SUPERVISOR [S] an einen Benutzer.

Ein Benutzer mit dem [S]-Recht hat nur eingeschränkte Handlungsfreiheit. Er darf z. B. keine Konfigurationen vornehmen, die dem Systemverwalter vorbehalten sind.

Die Trustee Assignments können sowohl auf Verzeichnis- als auch auf Dateiebene vergeben werden.

Um eine komplette und übersichtliche Rechtestruktur aufbauen zu können, werden die Mechanismen von Trustee Assignments und Sicherheitsgleichstellung (Security Equivalence) ergänzt durch die Möglichkeit der Konfiguration des sogenannten Inherited Rights Filter.

Rechtevererbung

Diese „Filter für vererbte Rechte“ legen sich wie ein Sieb zwischen die verschiedenen Verzeichnisebenen. Rechte, die automatisch von einem Verzeichnis, dem sie zugewiesen wurden, in alle darunterliegende Unterverzeichnisse fließen (vererbt werden), können mit diesem Inherited Rights Filter verringert werden, falls dies notwendig erscheint. Als Default-Einstellung läßt der IRF alle Rechte ungehindert durch.

Nach dem Aufbau einer gezielten Rechtestruktur über diese drei erwähnten Mechanismen kann der ordnungsgemäße Zugriff auf Dateien weitgehend gewährleistet werden.

6/2.3 Separater Datei- und Verzeichnisschutz

Während die oben beschriebenen Trustee Directory Assignments die Zugriffsrechte für Verzeichnisse und Unterverzeichnisse regeln, bezieht sich die Rechtezuweisung über die Trustee File Assignments auf einzelne Dateien.

Obwohl diese Art der Rechtezuweisung direkt auf Dateien in der Praxis weniger häufig verwendet wird, kann sie in speziellen Fällen für den Aufbau einer passenden Rechtestruktur durchaus von Vorteil sein. Zusammen mit der Inherited Rights Mask bzw. dem Inherited Rights Filter (NetWare) ist es somit möglich, komplexe Rechtestrukturen auf ein relativ überschaubares Gebilde zu reduzieren.

Der Benutzer WEKALI hat z. B. im Verzeichnis SYS:WINDOWS\WINUSER\WEKALI alle Rechte außer **Supervisor** und **Access Control**. Da sich jedoch in diesem Verzeichnis auch Systemdateien befinden, die durch unsachgemäße Behandlung zerstört werden könnten, ist es durchaus sinnvoll, die allgemeine Rechtezuweisung über Trustee Directory Assignments mittels Trustee File Assignments bezüglich der betreffenden Dateien einzuschränken.

Eine elegantere Lösung bietet jedoch eine weitere Option bezüglich des Zugriffs auf Dateien: Die Verzeichnis- und Dateiattribute. Sowohl Verzeichnisse als auch Dateien besitzen sogenannte Attribute, die als „letzte Instanz“ die Zugriffsmechanismen vervollständigen.

Sie überlagern die mit NETADMIN erteilten Zugriffsrechte einzelner Benutzer oder Gruppen und sind allgemeingültig, also nicht benutzer- oder gruppenbezogen. Sie können nicht additiv wirksam werden, d. h. sie können die durch direkte oder indirekte Zuweisung vergebenen Rechte nicht erweitern.

Im obigen Beispiel könnten also die betreffenden Dateien über das READ-ONLY-Attribut vor einem Schreibzugriff geschützt werden, statt hier das Trustee File Assignment einzusetzen. Allerdings wäre es in diesem Fall notwendig, dem Benutzer WEKALI das MODIFY-Recht zu entziehen, da er damit die Möglichkeit hat, Dateiattribute zu ändern.

6/3 Datensicherung

Es ist heute genau wie vor 20 Jahren: Die größten Probleme im gesamten EDV-Bereich entstehen immer dann, wenn wichtige Daten unwiderruflich zerstört werden, was unter Umständen zum wirtschaftlichen Ruin einer Firma führen kann. Mit weiteren, in der Regel sehr kostenintensiven Problemen ist ein Unternehmen dann konfrontiert, wenn das Netzwerk, auf dessen ständigem Betrieb die gesamte Arbeitsstruktur basiert, für einen längeren Zeitraum ausfällt.

Kosten

Aus den o. a. Gründen besitzt das Thema Datensicherung hohe Priorität bei der Planung eines Netzwerks. Und so ist es eine Frage des Verantwortungsbewußtseins des Netzwerkberaters, hier den nötigen Nachdruck aufzubringen, zumal ein Maximum an Sicherheit nicht unerhebliche Kosten verursacht. Weiterhin muß sich der Systemverwalter eines Netzwerks umfangreiche Kenntnisse in diesem Bereich aneignen, um die vorhandenen Sicherungsmaßnahmen korrekt anwenden zu können.

So reicht es in der Regel nicht aus, die Daten nur korrekt zu sichern, d. h. in regelmäßigen Abständen nach einem bestimmten System auf ein Sicherungsmedium zu kopieren. Genau so schnell muß es im Bedarfsfall möglich sein, die gesicherten Daten wieder auf das normale Speichermedium zurückkopieren zu können.

Dazu ist es jedoch unbedingt nötig, nach der Installation der Sicherungseinrichtung sowohl das BACKUP (Sicherungskopie) als auch das RESTORE (Zurückholen der gesicherten Daten) ausführlich zu testen. Gerade das „Restore“ (Durchspielen des Katastrophenfalls) wird in der Praxis oft stiefmütterlich behandelt.

Bei der Auswahl eines möglichen Sicherungsverfahrens sind einige Dinge zu beachten, von denen die wichtigsten in der

nachfolgenden Tabelle in Form entsprechender Fragen aufgeführt sind.

Sicherungsverfahren

Auswahlfaktoren für ein Sicherungsverfahren
■ Wie groß ist die Datenmenge? (Ist genügend Speicherplatz auf dem Backup-Medium vorhanden?)
■ Wohin soll gesichert werden? (Auf eine andere Server-Festplatte oder auf gesonderte Speichermedien wie z. B. Tapes, Wechselplatten etc.?)
■ Was soll gesichert werden? (Nur Systemdaten oder das gesamte System incl. NDS-Server und Arbeitsstationen?)
■ Wie komfortabel soll der Sicherungsmechanismus sein? (WINDOWS- oder DOS-Anwendungen; Möglichkeit eines rollierenden Verfahrens; Quick File Access – QFA; automatischer Ablauf der Sicherung im Hintergrund ohne Belastung einer Arbeitsstation?)
■ Wie schnell soll das System arbeiten? (Wichtig bei großen Datenmengen)
■ Wie groß wäre der Schaden eines Datenverlusts im Katastrophenfall? (In der Praxis kommt es immer wieder vor, daß nach einem Crash der Server-Platte Sicherungskopien nicht mehr zurückgeholt werden können; begründet durch falsche Handhabung oder durch Hardware-/Software-Versagen bei Billigprodukten. Eine exakte Planung und Bedienung kann dies weitgehend verhindern.)

6/3.1 Formen der Datensicherung

Speicher-medium

Als Form einer Datensicherung wird die Art und Weise verstanden, wie und wohin Daten kopiert werden, um sie im Bedarfsfall (z. B. Verlust der Originaldaten durch Defekt des Speichermediums) wieder zurückkopieren zu können. Dabei sind folgende Möglichkeiten zu unterscheiden:

- Einfache Sicherung von Daten
  Meist werden die Daten auf der Festplatte einer Arbeitsstation, auf Disketten durch einfaches Kopieren oder mit Einsatz des DOS-Backup-Programms gesichert. Dieses Verfahren ist relativ antiquiert und für größere Datenmengen nicht verwendbar.
- Sicherung der Daten auf nicht auswechselbare Datenträger
  Darunter fallen Sicherungen auf eine andere Festplatte in einer Arbeitsstation oder in einem Server. Diese Sicherungen werden in der Regel von der systemeigenen Backup-Software ausgeführt. Die Methode besitzt den Vorteil, daß keine zusätzlichen Software- und Hardware-Module benötigt werden, ist jedoch z. B. beim Einsatz einer zweiten Server-Festplatte unter Umständen kostspielig und umständlich. Zudem sind damit optimale Archivierungskonzepte nicht realisierbar.
- Sicherung der Daten auf auswechselbare Datenträger
  Hier sind in erster Linie Streamer (Bandlaufwerke) anzuführen, die große Datenmengen auf kleine Magnetbänder übertragen. Diese Bänder sind relativ billig und problemlos zu lagern. Gute Archivierungssysteme arbeiten ausschließlich mit Streamer-Laufwerken.

Streamer, sogenannte Backup-Geräte, sind Speichermedien, die beim Sicherungsvorgang als Ziel der Datenübertragung fungieren. Als Auswahlfaktoren sollten bei Streamern folgende Punkte Beachtung finden:

Auswahlfaktoren für Streamer

- Interface
  Hier stehen 3 verschiedene Methoden zur Auswahl:
  – SCSI Controller (SCSI 1, 2, 3)
  – QIC-Standard
  – Parallele Schnittstelle
- Datenübertragungsrate
  Abhängig vom Aufzeichnungsverfahren und vom Interface werden Geschwindigkeiten von 100 kB/s bis 5 MB/s erreicht.
- Speicherkapazität
  Abhängig vom Preis und vom technischen Aufwand der Geräte liegen die Kapazitäten bei 150 MB bis 16 GB pro Band.
- Kompatibilität der Backup-Software
  Natürlich eignet sich nicht jeder Streamer für jede Software und umgekehrt. Es ist die Aufgabe des Systemverwalters, hier eine passende Zusammenstellung zu finden

6/3.2 Datensicherung in der Praxis

Die Datensicherung bzw. die Datensicherheit unter NetWare 4.x/5.x kann in 2 Kategorien unterteilt werden.

1. Systeminterne Datensicherung
2. Zusätzliche Archivierungssysteme

System-intern

Zur systeminternen Datensicherung zählt der Umstand, daß gelöschte Dateien unter bestimmten Bedingungen physikalisch weiter auf der Platte existieren und nur eine sogenannte „Löschmarkierung“ erhalten. Damit sind sie nicht mehr sichtbar, und der betreffende Speicherplatz wird freigegeben. Diese Dateien lassen sich unter anderem mit der PURGE-Anweisung physikalisch entfernen. Solange dies nicht erfolgt, bleiben die Daten erhalten und können restauriert werden. Dies gilt allerdings nur für Daten, die durch normale Löschprogramme gelöscht wurden und nicht durch einen Plattendefekts oder korrupte Software beschädigt wurden.

FILER

Mit Hilfe des Dienstprogramms FILER werden die betreffenden Dateien in das Verzeichnis zurückgeschrieben, aus dem sie entfernt wurden (**Zurückholen gelöschter Dateien**). Wurde ein ganzes Verzeichnis mit Inhalt gelöscht, so wird dieses Verzeichnis nicht automatisch restauriert, sondern die betreffenden Dateien in das System-Verzeichnis DELETED.SAV zurückgeholt, von wo aus sie dann entsprechend weiter behandelt werden können (**Zurückholen von Dateien aus gelöschten Verzeichnissen**).

Obwohl die systeminterne Datensicherung ausreichend erscheint, ist es sinnvoll, zusätzliche Sicherungssysteme (Archivierungssysteme) zu erwägen. Eine komfortable und übersichtliche Handhabung bei Sicherung und Rücksicherung sowie die freie Auswahl, wo das Speichermedium zur Sicherung plaziert werden soll, sind nicht zu unterschätzen.

6/3.2.1 Vorbereitende Maßnahmen

Um ein Sicherungskonzept zu entwickeln, sind einige grundsätzliche Überlegungen anzustellen, wobei die Kenntnis der diversen Archivierungsmethoden eine wichtige Rolle spielt.

Archivierungssysteme dienen dazu, bestehende Daten in komprimierter oder unkomprimierter Form auf ein anderes Medium bzw. ein anderes Laufwerk zu übertragen. Die zwei wesentlichen Gründe für den Einsatz solcher Systeme sind:

- Auslagerung von Daten, die über einen längeren Zeitraum nicht benutzt wurden. Diese Daten werden dabei auf dem Ziellaufwerk (Target) gelöscht
- Regelmäßiges Kopieren wichtiger Daten zur Sicherung gegen Datenverlust im Fall der Zerstörung von Originaldaten.

Planung

Bei der Planung von Archivierungssystemen sollten die folgenden Kriterien beachtet werden:

Archivierungsmethoden

1. Archivierungsmethode

Hier sind zwei grundlegende Verfahren zu unterscheiden:

a) MS-DOS-gestützte Backup-Systeme

Diese Systeme arbeiten auf den Arbeitsstationen, wobei die Daten auf einen Streamer mit DOS-Device-Treiber kopiert werden. Je nach Ausführung der Software können alle Daten des Servers (mit Ausnahme der NDS-Struktur) und die der Arbeitsstation selbst übertragen werden.

Vorteile

- geringer finanzieller Aufwand
- relativ problemlose Installation

Nachteile

- Da DOS als sogenanntes „monolithisches Betriebssystem“ wegen unkontrollierter Hardware-Zugriffe der verschiedenen Prozeduren im Kernel-Mode bisweilen abstürzt, ist die Sicherheit dieser Methode begrenzt.
- Begrenzte Geschwindigkeit.
- Die Arbeitsstation kann während des Sicherungsvorgangs keine anderen Arbeiten ausführen.
- Die Daten anderer Arbeitsstationen können nicht mitgesichert werden.

b) Server-gestützte Backup-Systeme

Bei diesen Sicherungssystemen sind die Hardware und ein Teil der Software im Server integriert. Die Software-Module und die entsprechenden Gerätetreiber werden als NLMs an der Serverkonsole (oder über die entsprechende NCF-Datei) geladen. Das Management wird, abhängig vom jeweiligen Archivierungssystem, entweder von der Arbeitsstation oder von der Server-Konsole aus übernommen.

Vorteile

- Ausreichende Zuverlässigkeit und Datenintegrität.
- Hohe Übertragungsgeschwindigkeiten.
- Große Auswahl an komfortabler Software.
- Alle Arbeitsstationen können mitgesichert werden.
- Die NDS kann übertragen werden.
- Der Sicherungsvorgang läuft nur am Server, somit ist keine Arbeitsstation belastet.

Bei der Server-gestützten Sicherung sind keine relevanten Nachteile bekannt.

2. Speichermedien (Backup-Devices)

Backup-Geräte

Um zwischen den möglichen Medien auswählen zu können, sollte Klarheit bezüglich folgender Punkte bestehen:

- Benötigte Datenmenge (genügend Platz auf dem Speichermedium?)
- Wohin sollen die Daten gesichert werden (zweite Server-Festplatte – Bandlaufwerk – Wechselplatten – Disketten)?
- Welche Daten sind für die Sicherung relevant (nur Server-Daten – die Daten zusätzlicher Arbeitsstationen)?
- Wie schnell soll das System arbeiten (wichtig bei großen Datenmengen)?

Da die niederwertigen Backup-Methoden (DOS-Backup, Komprimierungssoftware LHA etc) als bekannt vorausgesetzt werden und nicht NetWare-spezifisch sind und die DOS-Backups nicht dem benötigten Sicherheitsstandard entsprechen, soll hier als Beispiel nur eine bewährte, servergestützte Kombination angeführt werden:

STREAMER	DDS-2 DAT-Streamer SCSI-II
CONTROLLER	Adaptec SCSI-II
SOFTWARE	Systeminternes SBACKUP ArcServe für NetWare von Cheyenne

6/3.2.2 Spezielle Speicher-Verwaltungsdienste

Mit dem internen Speicher-Verwaltungssystem (Storage Management System, SMS) bietet NetWare einen ausreichend flexiblen Mechanismus zur Sicherung von Daten. SMS ist von der Speicher-Hardware sowie vom Dateisystem (DOS, OS/2, UNIX bzw.Windows) unabhängig.

SMS-Architektur

NetWare bietet folgende Software-Module und NLM-Programme für SMS an, die auf dem Server ablaufen können:

- SBACKUP
  Programm, das Sicherungs- und Zurücksicherungsfunktionen bietet.
- SMDR (Speicher-Management-Daten-Requester)
  Leitet Befehle und Informationen zwischen SBACKUP und Ziel-Service-Agenten weiter.
- SMSDI (SMS-Speichergeräte-Schnittstelle)
  Speichergeräte-Schnittstelle, die Befehle bzw. Informationen zwischen SBACKUP und den Speichergeräten-bzw. Medien weiterleitet.
- Gerätetreiber (IDE.DSK, TAPEDAI.DSK, AHAxxxx.DSK)
  Steuern den mechanischen Betrieb von Speichereinheiten entsprechend den Befehlen, die sie über SBACKUP und SMSDI erhalten.
- NetWare Server-Ziel-Service-Agenten (z. B. TSA*)
  Leiten (von SBACKUP generierte) Datenanforderungen an den NetWare-Server weiter, auf dem sich die Daten befinden. Anschließend leiten sie die angeforderten Daten an SBACKUP zurück.

- Datenbank-Ziel-Service-Agenten (z. B. TSANDS)
  Leiten Befehle und Daten zwischen dem HOST-Server (auf dem sich SBACKUP befindet) und der Datenbank weiter, in der sich die zu sichernden Daten befinden. Anschließend leiten sie die geforderten Daten über SMDR an SBACKUP zurück.
- Arbeitsstation-Ziel-Service-Agenten (z. B. TSADOS)
  Leiten Befehle und Daten zwischen dem HOST-Server (auf dem sich SBACKUP befindet) und der Arbeitsstation (auf der sich die zu sichernden Daten befinden) weiter und liefern die angeforderten Daten über den SMDR an SBACKUP zurück.
- Arbeitsstation-Manager-Programm
  Empfängt „I am alive"-Meldungen von Arbeitsstationen, die zum Sichern verfügbar sind. Das Programm zeichnet die Namen dieser Stationen in einer internen Liste auf.

Per definitionem ist das Ziel (Target) der zu sichernden Daten dasjenige Medium, auf dem sich diese Daten befinden.

6/3.2.3 Datensicherung mit SBACKUP

SBACKUP

Die internen Sicherungsmechanismen von SBACKUP setzen auf der SMS-Architektur von NetWare auf. Folgende Speichergeräte und Treiber werden unterstützt:

- TAPEDAI.DSK
  Der von Novell erstellte generische Gerätetreiber für Bandlaufwerke. Er funktioniert unter den meisten ASPI-kompatiblen SCSI-Controllern.

- MNS16S.DSK, MNS8MM.DSK, MNSDAT.DSK
  Arbeiten mit Mountain Network Solutions SCSI-Controllern und Bandlaufwerken.
- PS2SCSI.DSK
  Arbeitet mit IBMs 2.2-GB-Bandgeräten, die PS2-SCSI-Controller verwenden.
- AHAxxxx.DSK, ASPITRAN.DSK
  Können bei Adaptec-Controllern verwendet werden.

Backup-Quellen

Die Daten zur Sicherung und Wiederherstellung mittels SBACKUP können aus folgenden Quellen stammen: NetWare-2.x-, -3.x-, -4.x- und -5.x-Server (einschließlich NDS, Bindery und Datenträgereinschränkung), OS/2-Netzwerk-Server, Arbeitsstationen oder andere ausgewählte Services. Darüber hinaus ermöglicht SBACKUP

- Auswahl von 4 Sicherungstypen: Volle, inkrementale, differentielle und angepaßte Sicherung,
- die Sofortige Ausführung der Sicherung oder die Festlegung eines späteren Sicherungs-Zeitpunkts,
- Sicherung der Daten von Servern oder Arbeitsstationen, auch wenn diese gerade verwendet werden,
- Sicherung und Wiederherstellung innerhalb mehrerer Name-Space-Formate, die auf einem Datenträger definiert sind (einschließlich DOS, FTAM, MacIntosh, NFS und OS/2),
- Wiederherstellung aller Daten oder eines Teils der Daten auf dem ursprünglichen Standort oder auf einem anderen Standort in der Verzeichnisstruktur.

Wahlmöglichkeiten

Da jede Netzwerkumgebung anders ist, bietet SBACKUP viele verschiedene Möglichkeiten für die Datensicherung. Im folgenden sollen die drei grundlegenden Umgebungen dargestellt werden:

1. Server-Datensicherung
Host-Server ist gleichzeitig Target-Server

SMDR

Der Systemverwalter startet SBACKUP. Dieses Modul verwendet SMDR für den Zugriff auf den Ziel-Service-Agenten des NetWare-Servers. Der Server-Ziel-Service-Agent (z. B. TSA410.NLM) holt die angeforderten Daten und leitet sie anschließend über SMDR an SBACKUP weiter, das die Daten an die SMSDI übergibt.

In der folgenden Abbildung ist diese Form der Datensicherung in einem vereinfachten Diagramm dargestellt.

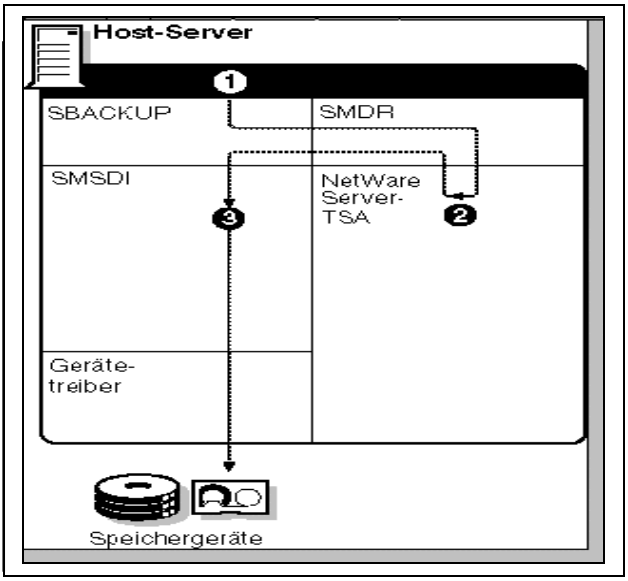

Abbildung 1: Datensicherung beim Host-Server

2. Datensicherung bei einem Target- und einem Host-Server

Die folgende Abbildung zeigt in vereinfachter Form die Verhältnisse bei einem (analog auch bei mehreren) TARGET-(Ziel-)Server(n) und einem HOST-Server.

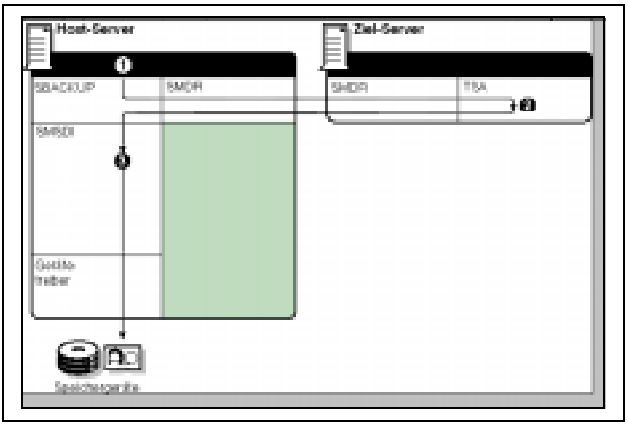

Abbildung 2: Datensicherung beim Ziel-Server

Die Erklärung zu den einzelnen Punkten entspricht der vorhergehenden Abbildung.

3. Datensicherung einer DOS-Arbeitsstation

Arbeitsstation Der Systemverwalter startet SBACKUP am HOST-Server. Nach dem Laden des DOS-Ziel-Service-Agenten (TSASMS) auf der Arbeitsstation nimmt dieser Verbindung mit dem betreffenden Managerprogramm des HOST-Servers (TSADOS.NLM) auf.

TSADOS SBACKUP setzt TSADOS für den Zugriff auf das Arbeitsstation-Manager-Programm ein, das die zu sichernden Daten von TSASMS.COM holt und an SBACKUP zurückliefert. Schließlich werden die Daten an SMSDI weitergeleitet. SMSDI setzt die entsprechenden Gerätetreiber ein, um die Daten an das ausgewählte Sicherungsgerät zu senden.

Die folgende Abbildung zeigt die Verhältnisse bei der Sicherung einer Arbeitsstation.

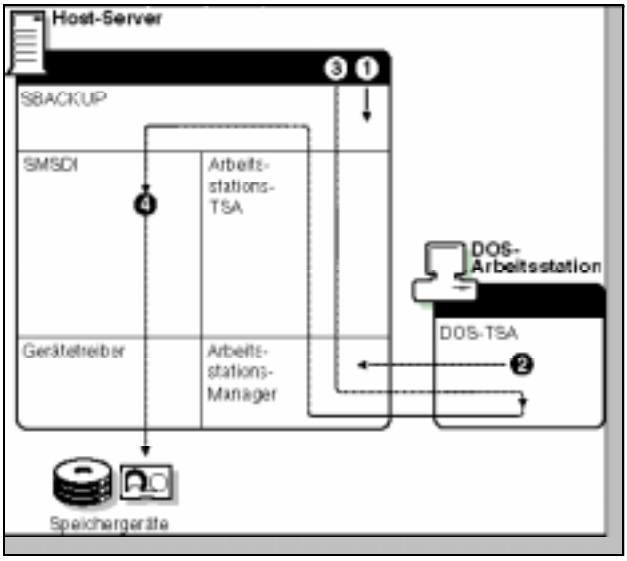

Abbildung 3: Datensicherung bei einer DOS-Station

Das Arbeitsstationen-Manager-Programm, das auf dem Host-Server läuft, führt eine interne Liste aller Target-Service-Agenten, die mit ihm Verbindung aufgenommen haben. Somit erscheinen auch alle Arbeitsstationen, an denen TSASMS.COM geladen wurde.

6/3.2.4 NDS-Datenbank

Recovery

Die Wiederherstellung (Recovery) einer NDS-Datenbank mit SBACKUP sollte nur bei einem Gesamtverlust der Daten einschließlich eventueller Reproduktionen erfolgen. Befindet sich in einem Netzwerk nur ein einziger Server, so ist dringend zu empfehlen, den Inhalt der NDS zu dokumentieren,

denn in diesem Fall kann keine Reproduktion der NDS-Struktur abgespeichert werden.

In diesem Zusammenhang gibt es eine Ausnahme: Falls die aktive Server-Festplatte einen physikalischen Defekt erleidet oder die FAT bzw. DET irreversibel zerstört wird, bleiben bei einem gespiegelten System die Daten einschließlich der NDS-Datenbank erhalten.

Die sicherste Möglichkeit, die vollständige Wiederherstellung der Novell-Verzeichnisdienste (NDS) zu garantieren, ist das Erstellen von Reproduktionen der Partitionen mit dem NDS-Manager und ihre Speicherung auf weiteren Servern.

Der Vollständigkeit halber soll hier jedoch die Sicherung der NDS mittels SBACKUP kurz beschrieben werden. Ergänzend zu den sonstigen Targets muß zur Sicherung das Modul TSANDS.NLM geladen werden, damit die NDS als Target in der Sicherungsliste erscheint.

Backup NDS

Für die Sicherung müssen in SBACKUP die Punkte **Change Target to Backup From or Restore TO** und **NetWare Directory** ausgewählt werden. Daraufhin erfolgt die Anmeldung mit der Benutzerkennung (ADMIN-Äquivalenz!). Nach Aktivieren der Punkte **Backup** (Hauptmenü) und **FULL: All Data On Target** kann optional eine Beschreibung erfolgen. Nach der Entscheidung, ob die Sicherung an eine bestehende Session angehängt oder das Band überschrieben werden soll, wird mit <F10> das Backup gestartet. Beim Überschreiben muß noch ein neuer Medium-Name eingegeben werden.

Restore NDS

Um die gesicherten Daten zurückzuschreiben, müssen im SBACKUP-Menü die Punkte **Change Target to Backup From or Restore TO** und **NetWare Directory** ausgewählt werden. Daraufhin erfolgt die Anmeldung am System. Nach Aktivierung von **Restore** muß der Punkt **Restore Without Session File** angewählt werden. Hierbei muß das Band mit

der geeigneten NDS-Datenbank eingelegt sein. Nach der Aktivierung von **Restore an Entire Session** kann das Wiederherstellen der NDS-Struktur anlaufen. Falls anstelle von **Restore an Entire Session** die Option **Custom Restore** gewählt wird, kann das Überschreiben bestehender Strukturen verhindert werden.

6/3.2.5 Sicherung und Wiederherstellung

Zur Sicherung bzw. Wiederherstellung der Daten müssen an der Server-Konsole folgende Programme und Treiber geladen bzw. aktiviert werden:

1. Laden der Treiber für Controller und Speichergeräte

Bei Verwendung eines Adaptec-Controllers und eines unter 8/4.3.3 beschriebenen Bandlaufwerks sind an der Serverkonsole folgende Anweisungen einzusetzen:

```
AHA1540
TAPEDAI
```

2. Bandlaufwerk im System eintragen

Dazu ist an der Konsole folgendes einzugeben:

```
SCAN FOR NEW DEVICES
```

3. Laden der SBACKUP-Module

Anschließend werden dann die entsprechenden SBACKUP-Treiber geladen (z. B. TSA410.NLM).

Ein Netzwerk besteht aus einem NetWare-4.x-Server, in dem ein HP-Streamer installiert ist. Außer diesem Server soll noch ein weiterer 3.x-Server und zusätzlich die NDS-

Datenbank mitgesichert werden. Für den Betrieb der Server-Platte ist ein SCSI-Controller eingebaut.

Ladevorgang am 4.x-Server (Host = Target)

```
Load TAPEDAI
SCAN FOR NEW DEVICES
Load TSANDS
Load TSA410
Load SBACKUP
```

Ladevorgang am 3.x-Server (TARGET)

```
Load TSA312
```

Damit stehen in der Target-Liste des Hauptmenüs drei Ziele (Targets) zur Auswahl:

- NetWare File System des 4.x-Servers
- Novell Directory Services des 4.x-Servers
- NetWare File System des 3.12-Servers

Nachdem alle benötigten Module im Host und in den Targets installiert wurden, kann mit dem eigentlichen Sicherungslauf begonnen werden. Dazu ist am Host das Modul SBACKUP.NLM zu aktivieren (LOAD SBACKUP).

Der Begriff „Target“ bezieht sich in der gesamten Sicherungsthematik immer auf das Objekt, dessen Daten gesichert bzw. auf das die Daten zurückkopiert werden sollen. Target – im Sinne von Ziel – gilt nie als Bezeichnung für das Objekt, auf das die zu sichernden Daten kopiert oder von dem die zurückzusichernden Daten geholt werden. Diese Definition wird hier deshalb so nachdrücklich aufgezeigt, da vor allem bei Backup-Systemen mit deutscher Übersetzung eine heillo-

se Sprachverwirrung herrscht und der Benutzer trotz der gut konstruierten Menüführungen dadurch oft verwirrt wird.

Mehrere Targets

Falls wie im obigen Beispiel mehrere Targets gesichert werden sollen, kann bei der Aktivierung jedes einzelnen Backup-Vorgangs die Option **Start the Backup Later** eingestellt werden. Für die weitere Konfiguration ist der Menüführung zu folgen.

Aktivierung

Nach der Abfrage des Benutzernamens und des entsprechenden Paßworts (falls vorhanden) erscheint das einleitende Menü, in dem der passende Streamer-Treiber ausgesucht werden muß. Ist hier kein geeigneter Treiber zu finden, so muß der benötigte Treiber in das Systemverzeichnis kopiert werden. Dieser Treiber muß außerdem in die Datei *DIBI2$DV.DAT* eingetragen werden.

SBACKUP-Menü

Sobald der passende Treiber ausgewählt wurde, wird das Hauptmenü von SBACKUP angezeigt. Im folgenden sind die wesentlichen Merkmale der einzelnen Menüpunkte aufgeführt. Die etwas unverständlichen Formulierungen werden zusätzlich näher erläutert.

Select TARGET to Backup/Restore

Nach der Aktivierung dieses Menüpunkts bietet SBACKUP eine Liste der Server und Workstations an, die das Kommunikationsmodul SMDR aufgrund der TSA-Module erkennt (TSA*.NLM bzw. TSA_SMS.COM müssen geladen sein).

BACKUP-Menü

Ein Backup-Lauf wird als Session bezeichnet. Auf einem Tape können verschiedene Sessions hintereinander gespeichert werden, falls es „multisession“-fähig ist. Nachfolgend sollen die wichtigsten Fachbegriffe, die in diesem Zusammenhang auftreten, erläutert werden.

Working Directory

Ein „Working Directory“ kann beliebig ausgewählt werden. Es enthält nach dem Backup die Error.log- und die Backup.log-Files.

Full Backup

„Full Backup“ bedeutet, daß die gesamten Daten eines Target (z. B. eines Servers) gesichert werden.

Nach dem Sichern sollte das Attribut **„**Archive Needed“ bei allen Dateien am Target gelöscht werden. Dies ist wichtig für die folgenden Backup-Methoden.

Incremental Backup

Bei diesem Verfahren werden nur Dateien gesichert, die das Attribut „Archive Needed“ (A) besitzen. Dieses Backup ist natürlich nur sinnvoll, wenn vorher ein Full Backup erfolgte, bei dem die sogenannten „Modify Bits“ zurückgesetzt wurden. Wird dann eine Datei auf dem Target verändert, so wird das Attribut „A“ wieder gesetzt, wobei diese Datei beim nächsten Backup gesichert wird. Auch hier muß der Menüparameter „Clear Modify Bit“ auf „Yes“ gesetzt werden.

Differential Backup

Der Unterschied zum Incremental Backup besteht beim „Differential Backup“ darin, daß zwar nach einem Full Backup auch alle Archivbits gelöscht werden, um veränderte Dateien markieren zu können, aber beim Konfigurieren des Differential Backup der Parameter „Clear Modify Bit“ auf „No“ gesetzt werden muß. Dies hat zur Folge, daß bei jedem Differential Backup alle Dateien, die seit dem Full Backup verändert wurden, gesichert werden.

Beim „Differential Backup“ wird zwar mehr Platz auf dem Band benötigt, ein Zurücksichern der kompletten, aktuellen Daten kann dadurch jedoch wesentlich beschleunigt werden.

Custom Backup

Das „Custom Backup“ dient dazu, nur ausgesuchte, spezifische Daten zu sichern. Im Untermenü **Select List Options** können bestimmte Teile der Daten eines Target ausgeschlossen werden. Dies geschieht über die sogenannten Major TSA

Resources, also die verschiedenen Volumes und Binderies eines Target-Servers.

System-Backup

In manchen Fällen (z. B. bei einer gewissen Form des Upgrade) sollen nur die Systemdatenbanken (Binderies) gesichert werden. Da diese Binderies während des laufenden Betriebs ständig geöffnet sind, können sie nicht einfach kopiert werden. SBACKUP bietet die Möglichkeit, die Binderies trotzdem zu sichern. Dies geschieht mittels des o. e. Custom Backup, indem bei den Major TSA Resources alle Volumes (Datenträger) ausgeschlossen werden.

RESTORE-Vorgang

Prinzipiell entspricht die Vorgehensweise beim Restore der beim Backup. Es existieren jedoch einige unterschiedliche Definitionen der Restore-Konfiguration.

Session-Dateien

Um beim Restore-Prozeß die richtigen Daten zurückzusichern, muß die entsprechende Session ausgewählt werden. Diese Session-Dateien wurden beim Backup-Vorgang im Working Directory angelegt (Backup/Restore Session Log bzw. Backup/Restore Error Log).

Diese Dateien werden nicht unbedingt benötigt, da es ja vorkommen kann, daß sie sich nach dem Totalverlust von Serverdaten nur auf dem Backup-Device befinden, wo sie nichts nützen. Die Verfügbarkeit dieser Dateien gewährleistet jedoch einen erheblich schnelleren Rücksicherungslauf.

Methode

Das Vorgehen beim Restore hängt von der vorher gewählten Backup-Methode ab. Beim „Full Backup“ im Zusammenhang mit „Differential Backup“ sind das letzte „Full Backup“ und das letzte „Differential Backup“ die relevanten Sessions. Sind nach einem „Full Backup“ mehrere „Incremental Backups“ gelaufen, so müssen, um die neuesten Daten zu-

rückzuerhalten, alle Sessions für das Restore verwendet werden.

Overwrite Existing Parent

Wenn nur die Daten eines einzelnen Unterverzeichnisses gesichert wurden, werden alle Verzeichnisse, die über diesem Verzeichnis liegen, als „Parent" angesehen. Die Trustee-Rechte bzw. Verzeichnistabellen für diese Parent-Verzeichnisse werden beim entsprechenden Backup-Vorgang mitgesichert. Dabei stellt sich die Frage, ob diese Rechte und Tabellen bei einem Restore die momentan vorhandenen überschreiben sollen. Falls in der Zwischenzeit eine Änderung der Rechte bzw. der Verzeichnisstruktur stattgefunden haben sollte, würde sie dadurch wieder rückgängig gemacht werden. In diesem Fall ist der Parameter „Overwrite Existing Parent" auf „No" zu setzen.

Overwrite Existing Child

Sollen – wie im vorhergehenden Absatz beschrieben – nur die Parent-Rechte und die Verzeichnisstruktur zurückkopiert werden, ohne daß die Backup-Daten im betreffenden Child-Verzeichnis (ursprünglich gesichertes Unter-/Endverzeichnis) berücksichtigt werden, so ist der Parameter „Overwrite Existing Child" auf „No" zu setzen.

Destination Path

Wenn die Daten auf ein anderes als das ursprüngliche Verzeichnis zurückkopiert werden sollen, ist bei „Destination Path" das entsprechende Laufwerk bzw. der gewünschte Pfad anzugeben.

Nach Fertigstellung der geeigneten Restore-Konfiguration – unter Berücksichtigung der entsprechenden TSA-Module – braucht nur noch das Tape mit den richtigen Sessions eingelegt und das Backup mit <Esc> gestartet zu werden.

6/3.2.6 Daten einer Arbeitsstation sichern

Um die Daten einer Arbeitsstation sichern zu können, müssen folgende Voraussetzungen erfüllt sein:

1. Die Treiber für Controller und Speichergerät am Host-Server müssen geladen werden.
2. Das Speichergerät muß mittels des Befehls SCAN FOR NEW DEVICES im System eingetragen werden.

Geräte-Erkennung

3. Die weitere Vorgehensweise stellt sich dann wie folgt dar:

   Sicherung einer DOS-Arbeitsstation:
   LOAD TSADOS (Server)
   TSASMS (Arbeitsstation)

   Sicherung einer OS/2-Arbeitststation:
   LOAD SBACKUP (Server)
   LOAD TSAPROXY (Server)
   TSAOS2 (Arbeitsstation)

Das Laden der aufgelisteten Module muß in der angegebenen Reihenfolge geschehen. Außerdem muß an der zu sichernden Arbeitsstation der Empfang von Nachrichten abgestellt werden, da sonst die SPX-Verbindung abgebrochen wird. Dies geschieht unter NetWare 4.x/5.x mit der Anweisung SEND /A=N an der Befehlszeile der Arbeitsstation.

Zum Laden des Target-Service-Agenten sollte an der Arbeitsstation in das Verzeichnis NWCLIENT gewechselt werden.

Eingabe-Syntax:

```
TSASMS  /SE={l}  /P={m}  /D={n}  /N={o}
```

wobei die Parameter folgende Bedeutungen haben:

l HOST-Server-Name

m Paßwort der Arbeitsstation (beliebig)

n Laufwerksbuchstabe der zu sichernden Laufwerke (bei 2 Laufwerken c:\ und d:\ muß hier z. B. „D=cd“ eingegeben werden.

o Name der Arbeitsstation (beliebig)

Falls nur TSASMS ohne Parameter eingegeben wird, erscheint ein Hilfefenster mit den möglichen Parametern. Anschließend erscheint diese Arbeitsstation unter dem spezifizierten Namen in der Target-Liste von SBACKUP und kann zur Sicherung aktiviert werden.

Vor dem Laden von TSASMS an der Arbeitsstation muß am HOST-Server das Arbeitsstationen-Management-Modul TSADOS.NLM geladen werden.

6/3.2.7 Programme von Fremdanbietern

Im Gegensatz zu dem in den vorigen Kapiteln besprochenen NetWare-internen Datensicherungsmodul SBACKUP, bei dem das gesamte Sicherungsmanagement (außer dem Laden von TSASMS.COM) an der Server-Konsole stattfindet, gibt es zahlreiche Archivierungssysteme, die von der Arbeitsstation aus gesteuert werden.

Zu unterscheiden sind hier:

- Systeme, die auf das Betriebssystem DOS gestützt sind und die Arbeitsstation dediziert beanspruchen. Das bedeutet, daß das Speichermedium als DOS-Device in der betreffenden Arbeitsstation eingebaut ist und alle Steuerprogramme auf diesem Rechner laufen.

- Systeme, die Server-gestützt arbeiten. Das bedeutet, daß die Hauptmodule am Server im Hintergrund arbeiten und nur die Konfigurationen und die Startvorgänge von einer (Windows-)Arbeitsstation aus gesteuert werden. Das Speichermedium ist hier im Server eingebaut.

Anders als bei NetWare 3.x, das mit dem Modul NBACKUP eine Möglichkeit bietet, von einer Arbeitsstation aus Server- und Client-Daten zu sichern, besteht z. B. in NetWare 4.x für diese Art der Datensicherung keine integrierte Möglichkeit.

Das Sichern von Daten (Server-Daten und Daten der eigenen und anderer Arbeitsstationen) von einer Arbeitsstation aus kann dort also nur mittels externer Archivierungssysteme erfolgen. In Frage kommen hier eigentlich nur Systeme, die von Novell zertifiziert sind, da hier eine weitgehende Kompatibilität gewährleistet ist. Diese Systeme arbeiten ausschließlich mit Server-gestützter Software, wobei das hauptsächliche Management an einer (oder an mehreren) Arbeitsstation(en) unter Windows stattfindet. Zu nennen sind hier die Software-Pakete ArcServe und Palindrome. ArcServe wird nachfolgend etwas ausführlicher beschrieben.

ArcServe

Während die ArcServe-Version 4.x für NetWare-Versionen vor 4.02 durchaus relevant war, können für den Einsatz in 4.x-Netzwerken nur noch die von NetWare dafür zertifizierten Version 5.x bzw. 6.x empfohlen werden.

Die System-Steuermodule von Arcserve laufen als NLMs auf dem Server, während das Management von einer Arbeitsstation unter Windows 3.x/95/NT aus stattfindet. Die dazugehörigen Manager-System-Dateien können wahlweise auf die Festplatte der Arbeitsstation oder des Servers kopiert werden.

Ob ein kleines Netzwerk mit einem Server oder eine Multi-Server-Umgebung – Arcserve sichert alle NetWare-Server sowie DOS-, Windows-, OS/2-, UNIX- und Macintosh-Arbeitsstationen ebenso wie Datenbank-Server und NDS-Datenbanken. Arcserve unterstützt dabei die meisten SCSI- und QIC-02-Bandlaufwerke nach dem Industriestandard und eine große Anzahl von Host-Adaptern.

Parallel Streaming

Als eine der wichtigsten Zusatzoptionen bietet ArcServe das sogenannte Parallel Streaming. Dies bedeutet, daß bis zu 7 Bandlaufwerke an einem SCSI-Bus simultan an einer Sicherung bzw. an einer Rücksicherung beteiligt sein können.

Ebenso erwähnt werden sollte die Möglichkeit eines QFA (Quick File Access). Dieser Schnellzugriff auf einzelne Dateien oder Dateigruppen wird über BTRIEVE-Datenbanken gesteuert und beschleunigt die Wiederherstellung einzelner Dateien erheblich.

ArcServe nutzt dabei die vielfältigen Möglichkeiten der grafischen Benutzeroberfläche Windows voll aus, um dem Benutzer möglichst viel Komfort und Übersichtlichkeit zu bieten.