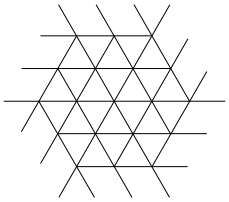
URZ-BERICHTE

Studie zur Eignung von Windows NT für den Einsatz in Universitätsverwaltungen

(Bericht an die DFG)

Guido A. Hölting
Email: guido.hoelting@rz.uni-ulm.de
Oktober 1996



Universität Ulm
Universitätsrechenzentrum
Leiter: Prof. Dr. H.P. Großmann
Albert-Einstein-Allee 11
89081Ulm

Inhaltsverzeichnis

Vorwort

Die Universität Ulm legt hiermit eine Studie vor, in der untersucht wird, inwieweit Windows-NT als Plattform für die EDV-Verfahren in den Universitätsverwaltungen geeignet ist und damit zu UNIX-Lösungen konkurrenzfähig wird. Die Studie beruht auf praktischen Erfahrungen, die über einen längeren Zeitraum in einer realistischen Testumgebung gewonnen werden konnten. Die vorliegende Ausarbeitung behandelt nicht nur mehr EDV-technische Aspekte, sondern untersucht insbesondere die konzeptionelle Eignung von NT — auch im Vergleich zu UNIX — für das vorgesehene Anwendungsfeld. Es wird darauf eingegangen, wie die Nutzer- und Rechteverwaltung in verschiedenen Domänenmodellen realisiert werden kann und welche Sicherheitsmechanismen zur Verfügung stehen. Sehr ausführlich wird auch auf die für die betriebliche Praxis wichtige System- und Netzadministration eingegangen, wobei hier — mangels Verfügbarkeit geeigneter NT-tools — auch Drittprodukte erwähnt werden.
Im Verlauf der Studie wurde sehr klar, daß die gewonnenen Erkenntnisse nicht nur für den Anwendungsfall: Verwaltungs-EDV, gelten, sondern ohne weiteres auch auf andere Anwendungsgebiete übertragen werden können. Im universitären Umfeld wären dies beispielsweise die Bibliotheks-EDV oder auch Bereiche der DV für Forschung und Lehre.
Als ein Ergebnis der Studie kann man festhalten, daß Windows-NT in vielen wichtigen Bereichen (z.Bsp. Nutzerverwaltung, Sicherheit) überzeugende und auch UNIX überlegene Systemeigenschaften besitzt. Die zunehmend starke Verbreitung von NT und die Tatsache, daß es auf einem wesentlich moderneren Betriebssystemkonzept basiert, wird schnell dafür sorgen, daß noch vorhandene Nachteile (z.Bsp. Systemverwaltungsroutinen, Eignung für Hochleistungs-DB Server) beseitigt werden. Als Zwischenlösungen gibt es zum Teil hierfür leistungsfähige third-party Produkte. Was den vermuteten Preisvorteil der NT-Lösung gegenüber einer UNIX-Lösung angeht, so entpuppt sich dieser bei genauem Hinsehen als wenig signifikant oder als gar nicht vorhanden, sofern man qualitativ äquivalente Systeme vergleicht. Bezieht man den manpower Bedarf für den laufenden Betrieb in diese Betrachtung mit ein, so sind heute Vorteile für die NT-Lösung sichtbar.

Die Studie wurde von meinem Mitarbeiter Herrn Dipl. oec. Guido Hölting durchgeführt und verfaßt. Er konnte während seiner Tätigkeit hierfür auf die Kompetenzen vieler weiterer Mitarbeiter im Universitätsrechenzentrum zurückgreifen und dabei nahezu alle „Glaubensrichtungen“ kennenlernen.

Ich danke allen Mitarbeitern, die zum Gelingen der Studie beigetragen haben.

Ulm, den 2.10.1996

Hans Peter Großmann

1. Zusammenfassung

Die am Rechenzentrum der Universität Ulm durchgeführten Untersuchungen zum Betriebssystem Microsoft Windows NT[1] wurden in einer möglichst **praxisnahen Testumgebung** realisiert, die den tatsächlichen Einsatzbedingungen eines Produktionssystems nahekommt. Es ging dabei weniger um die Erprobung und Bewertung einzelner Softwareprodukte für den Endanwender, sondern vor allem um die Frage der **Eignung von NT als Netzwerkbetriebssystem für Client-/Serverumgebungen im universitären (Verwaltungs-)bereich. Zentrale Untersuchungskriterien der Tests waren:**

- realisierbare und geeignete Netzwerkkonzepte, die ggf. auch universitätsweit tragfähig und zukunftssicher sein sollen
- Betriebsstabilität
- Datensicherheit auf Ebene des Betriebssystems
- Integration und Kompatibilität zu bestehenden PC-Systemen
- Möglichkeiten des netzwerkweiten Systemmanagements und Bewertung ihrer Effizienz
- Einschätzung möglicher Kostenvorteile durch den Einsatz von NT

Den durchgeführten Untersuchungen am Universitätsrechenzentrum zufolge steht NT an Universitäten bei der Erneuerung überalterter, mainframebasierter EDV-Strukturen in Konkurrenz zu UNIX-Lösungen. NT muß sich daher an den von UNIX gesetzten Leistungsstandards messen.

Die in den Testumgebungen erprobten **Domänenmodelle** konnten den Anforderungen genügen, besonders das ***Master Domain Modell*** (vgl. 3.1.2.) würde sich nach unserer Einschätzung für Universitäten eignen, da es einerseits genügend Leistungsreserven bereithält und andererseits wegen der zwar möglichen, aber dennoch nicht zwingenden zentralen Administration gegenüber individuellen Konfigurationen flexibel ist. Ebenso wie im UNIX ist bei größeren NT-Lösungen eine sorgfältige Vorüberlegung und Planungsphase unbedingt erforderlich. Dies gilt besonders dann, wenn eine effiziente Administration und **der Einsatz von Managementtools wie dem *Microsoft SMS*** (**S**ystems **M**anagement **S**erver) angestrebt wird.

---

1 Im folgenden nur noch als *NT* bezeichnet.

Die von NT standardmäßig mitgebrachten Verwaltungswerkzeuge wirken in ihrer Vielfalt und funktionalen Aufteilung zersplittert und teilweise unlogisch; sie können in dieser Form noch nicht recht überzeugen und eignen sich nur für kleinere, nicht sehr komplexe Systeme. Für den professionellen Einsatz sollte unbedingt zusätzliche Managementsoftware verwendet werden, die von *Microsoft* selbst mit dem SMS oder nahezu von allen großen Markenherstellern von NT-Systemhardware angeboten wird (z.Bsp. *DEC Assett Works, HP OpenView*).

Speziell das SMS wurde in den Testumgebungen erprobt und führte besonders bei der Softwaredistribution und Konfiguration von Clients sowie der Inventarisierung (installierte Programme, Hardwareausstattung) und Problemdiagnose zu einer besseren Effizienz. Trotz der recht großen Komplexität des SMS ist der Umgang damit vergleichsweise einfach. Allerdings erschien SMS in einigen Details noch etwas unfertig, was sich beispielsweise in fehlerhaften Installationsskripten für Standardapplikationen äußerte. Derartige Fehlerbehebungen und Workarounds erfordern von administrativer Seite einen erhöhten Aufwand, der mit der SMS Philosophie nicht recht vereinbar ist.

Insgesamt darf der erstmalige Planungs- und Installationsaufwand zusammen mit dem meist erforderlichen Know-How-Aufbau bei der Einführung eines NT-Systems nicht unterschätzt werden, ist aber sicher auch nicht höher als bei einem neuen UNIX-System. Der laufende Betrieb dagegen gestaltet sich im direkten Vergleich unkomplizierter und könnte auch in größeren Netzen überwiegend von Operateuren abgewickelt werden. Unter günstigen Bedingungen ist die Betreuung von 100 Clients incl. den erforderlichen Servern durch einen hauptamtlichen Administrator sicher nicht unrealistisch.

Die Betriebsstabilität von NT ist insgesamt als sehr gut zu bewerten und kann sich ohne weiteres mit der vergleichbarer UNIX-Systeme messen. Ein fataler Systemabsturz war bei richtig konfigurierten Testsystemen auch nach wochen- bzw. monatelangem Dauerbetrieb nicht aufgetreten. Probleme mit hängenden Prozessen u.ä. ließen sich in der Regel im laufenden Betrieb lösen. In Kombination mit geeigneten Failoverkonzepten kann die Verfügbarkeit und Stabilität von NT sowohl beim Einsatz auf Servern wie Clients als geeignet für Produktionssysteme angesehen werden.

Einen positiven Eindruck hinterlassen haben die mit *NTFS*[2] realisierten Mechanismen zur benutzerspezifischen Zugriffsberechtigung auf Dateien, die weitaus flexibler und umfassender sind als die von UNIX bekannte *owner/group/everyone*-Variante. Durch die Vielfalt leidet allerdings die Übersichtlichkeit, so daß bei der Vergabe von Verzeichnis-, Datei- und Systemrechten unbedingt netzwerkweite Administrationsrichtlinien aufzustellen sind; dies gilt besonders dann, wenn eine ganze Reihe von Personen mit der Systemverwaltung betraut sind, was in größeren Einrichtungen fast immer der Fall ist. **Der mit NT realisierbare Sicher-**

---

2 NTFS: *New Technology File System*; das NT-eigene Dateisystem

heitsstandard ist gerade für den Verwaltungsbereich mit seinen datenschutzrechtlichen Anforderungen interessant; für PC-Clients gibt es hier zu NT nach unserer Einschätzung keine Alternative!

Durch die Portierung von Datenbanksystemen wie *ORACLE* und *Sybase* auf die NT-Plattform wurden die *Voraussetzungen* zur Realisierung von NT-basierter Verwaltungssoftware geschaffen. Nach dem augenblicklichen Stand der, allerdings sehr dynamischen, NT-Entwicklung, kann aber im High-Endbereich der *Datenbankanwendungen* weder auf seiten der Software noch der Hardware (derzeit Systeme mit bis zu vier Prozessoren) ein Performance-Gleichstand mit UNIX erreicht werden; dies wird sich aller Voraussicht nach innerhalb der nächsten zwei Jahre ändern.

Der Aspekt der möglichen Kostensenkung sollte in der Diskussion *NT vs. UNIX* nicht allzu hoch bewertet werden. Sofern wirklich vergleichbar gute und leistungsfähige Hardware zum Einsatz kommen soll, bei einem Produktionssystem eigentlich selbstverständlich, kann bei NT nicht mehr von einer Low-cost-Lösung gesprochen werden. Die tatsächlichen Investitions- und Betriebskosten hängen im übrigen sehr von jeweils individuellen Parametern ab, so etwa der vorhandenen und weiter nutzbaren (Client-)hardware sowie den personellen Ressourcen. Gegenüber UNIX ist eine allgemein weniger aufwendige und leichter erlernbare Administration eines NT-Systems zu erwarten; dadurch könnten eventuell Kosten im personellen Bereich eingespart werden. Eine allgemeingültige Empfehlung kann jedoch an dieser Stelle nicht gegeben werden.

Klare Vorteile von NT gegenüber UNIX bleiben das modernere Betriebssystemkonzept, eine in Details höhere Managementeffizienz, eine dem Benutzer eher vertraute GUI sowie die Verfügbarkeit einer großen Zahl von Standardapplikationen, auf die man in kaum einem EDV-System mehr verzichten will (Bürokommunikation, Office-Anwendungen etc.).

2. Erläuterung der Testumgebungen

Die Tests wurden mit insgesamt drei NT-Domänen durchgeführt, wobei sowohl das *Standalone* wie das *Master Domain Modell* zur Anwendung kamen. An Servern wurden im einzelnen eingesetzt:

NT-Domäne	*Prozessor*	*RAM*	*Bus*	*Harddisk*	*CD-ROM*	*Streamer*	*Serverfunktionen*
Rechenzentrum	Pentium 133 MHz	96 MByte	SCSI-2	2 + 4 GByte	4-fach	DAT	PDC, WINS, SQL, SMS, File, Print, FTP, WWW, Telnet
Rechenzentrum	i486 50 MHz	16 MByte	SCSI	500 Mbyte	4-fach	-	BDC, WINS, SMS, Mac-File, Mac-Print, Telnet
Rechenzentrum	Pentium 100 MHz	64 MByte	E-IDE	1 GByte	4-fach	-	Server mit NCD Win-Center für X-Terminals
Bibliothek	Pentium 166 MHz	64 MByte	SCSI-2	4 GByte	6-fach	DAT	PDC, SQL, SMS, File, Print, FTP, WWW, Telnet
Verwaltung	Pentium 166 MHz	64 MByte	SCSI-2	4 + 4 GByte	6-fach	-	PDC, WINS, SQL, SMS, File, Print, FTP, WWW

Abb.1: Übersicht der im Testfeld eingesetzten Server, ihrer Ausstattung und Verwendung; Abkürzungen: PDC (Primary Domain Controller), BDC (Backup Domain Controller), WINS (Windows Internet Name Service), SMS (Systems Management Server)

Die Domäne im Rechenzentrum bildete dabei die Master Domäne für die Subdomain in der Bibliothek. Das System in der Universitätsverwaltung blieb wegen der Trennung des Verwaltungsnetzes vom restlichen Uni-LAN durch einen Firewall eine Standalone-Domäne. Auf den Servern wurde das Betriebssystem *NT3.51* mit *Service Pack 4* und dem *Resource Kit* eingesetzt.

In diesen Domänen wurden insgesamt etwa 25 Clients unter den Betriebssystemen *Windows 3.x*[3]*, NT3.51, NT4.0 Beta 2, MacOS* und vor allem *Windows95*[4] versorgt. Alle Clients waren Mitarbeiterarbeitsplätze, an denen täglich intensiv gearbeitet wird. Durch die sich im Rahmen der Untersuchungen ergebende Nutzung der Serverdienste, sind einige der Maschinen zu defacto Produktionssystemen geworden.

---

3 Im folgenden nur noch als *Win3.x* bezeichnet.

4 Im folgenden nur noch als *Win95* bezeichnet

Auf den Servern bzw. Clients wurde folgende Software installiert und im Praxiseinsatz erprobt:

- MS SQL Server Vers. 6.0
- MS SMS Server Vers. 1.1
- MS Internet Information Server (IIS) Vers. 1.0
- MS Frontpage Beta (in Zusammenhang mit dem MS IIS)
- MS Office95 Vers. 7.0
- Netscape Navigator Vers. 3.0
- Legato NetWorker Client Pak für NT Vers. 4.2.1
- NCD WinFrame und WinCenter: Ein spezielles Multiuser-NT, das es gestattet, sich mit X-Terminals oder UNIX-Workstations auf dem Server einzuloggen und die NT-Applikationen zu nutzen.

Die Aufstellung von Servern und Clients erfolgte über mehrere durch Router getrennte Subnetze in unterschiedlichen Standorten auf dem Universitätscampus.

3. NT Domänenkonzept

Ein wesentlicher Vorteil des Einsatzes von NT als Server- und Clientbetriebssystem besteht, verglichen mit anderen PC-Betriebssystemen, in seiner weitaus höheren Sicherheit im Netzwerk, die jedoch auch immer eine entsprechende Administration voraussetzt. Bei Anwendung einer geeigneten Konzeption können mit NT die Anforderungen des C2-Sicherheitsstandards erfüllt werden.

Wesentlicher Bestandteil des NT Sicherheitskonzepts ist die *Domäne* , deren Grundidee bereits früher in Form der *Yellow Pages* im UNIX-Bereich oder beim *LAN-Manager* realisiert wurde.

Grundsätzlich ist die NT Domäne eine logische Struktur, die sich über mehrere physische Subnetze erstrecken kann und innerhalb eines Subnetzes auch mehrere Domänen gestattet. Ihr großer Vorteil gegenüber dem von *Windows for Workgroups* (WfW) bekannten Arbeitsgruppenmodell mit einer Anzahl vernetzter und gleichberechtigter PCs (Peer-to-Peer) besteht darin, daß hier für alle Server und Clients, die Mitglied der Domäne sind, eine gemeinsame Benutzermenge in Form einer *Benutzerkontendatenbank* definiert wird. Die Authentisierung der Benutzer erfolgt immer aufgrund der in dieser Datenbank hinterlegten Informationen bezüglich Paßwörtern, Anmeldeskripten, Umgebungsprofilen, Systemrechten und Gruppenzugehörigkeit, und zwar nur einmal zu Beginn einer Sitzung. Eine neuerliche Authentisierung beim Zugriff auf die Ressourcen anderer Maschinen der Domäne braucht der Benutzer dann nicht mehr vorzunehmen. Der Vorteil des Domänenkonzepts liegt auf der Hand: Bei einer Vielzahl von Rechnern, die nur berechtigten Usern Zugriff gestatten sollen, vereinfacht sich die Administration erheblich, da die Accounts nur ein einziges Mal für die gesamte Domäne an zentraler Stelle geführt und verwaltet werden müssen.

Je nach Größe und den an das Netz gestellten Anforderungen, lassen sich durch die Kombination von Domänen verschiedene Domänenmodelle realisieren.

3.1. Domänenmodelle

3.1.1. Standalone Domäne

Die einzelne Domäne eignet sich vor allem für kleinere Netze mit einer überschaubaren Anzahl von Benutzern, obwohl man nicht eine feste Obergrenze angeben kann. Dies hängt auch sehr von der Anzahl Server und der Art der angebotenen Dienste innerhalb der Domäne ab.

Die Grundkomponenten der Standalone Domäne finden sich jedoch in jedem der anderen Modelle wieder, nämlich Domänencontroller, „einfache“ Server und Clients.

Zentraler Bestandteil jeder Domäne ist der *Primary Domain Controller* (PDC), der genau einmal vorhanden sein muß. Er führt das Original der Benutzerkontendatenbank. Alle Änderungen an den Accounts werden durch die entsprechenden Administrationswerkzeuge automatisch auf dieser Maschine durchgeführt. Im Unterschied zu anderen Servern und Workstations innerhalb der Domäne führt der PDC keine separaten lokalen Benutzerkonten, oder anders ausgedrückt: seine lokale Datenbank fungiert als Domänendatenbank. Lokale Gruppen wie Administratoren oder Serveroperatoren lassen sich aber prinzipiell definieren. Diese Gruppen haben dann nur auf den Domänencontrollern Gültigkeit.

Neben dem PDC kann es einen oder mehrere *Backup Domain Controller* (BDC) geben, auf denen sich jeweils ein genaues Duplikat der originalen Benutzerkontendatenbank befindet, die auch nach Änderungen in einstellbaren Zeitabständen wieder repliziert wird. Durch dieses Konzept werden zum einen mögliche Inkonsistenzen zwischen verschiedenen Versionen der Datenbank vermieden sowie zum anderen eine höhere Verfügbarkeit des Systems erreicht: Ohne BDCs wäre bei einem Ausfall des primären Controllers ansonsten kein Domänenlogon mehr möglich, im allgemeinen könnte also auf den Clients nicht mehr oder nur noch eingeschränkt gearbeitet werden, selbst wenn alle anderen Server funktionsbereit wären.

Nach eigenen Erfahrungen empfiehlt es sich schon alleine aus diesem Grund, mindestens einen BDC für jede Domäne aufzusetzen. Gleichzeitig wird dadurch unter Umständen eine höhere Performance erreicht, da sich PDC und BDCs die benutzerspezifischen Logonprozeduren mit der Authentisierung und Übermittlung von Skripten und Umgebungsprofilen teilen, womit bei Stoßzeiten, wie etwa dem morgendlichen Arbeitsbeginn, längere Wartezeiten vermieden werden können.

Dieses Verfahren der „Arbeitsteilung“ gestattet auch die Zusammenfassung von Clients in verschiedenen, nur durch WAN-Strecken mit geringer Bandbreite verbundenen Netzen zu einer logischen Domäne. Bei nur einem Logonserver wäre sonst die Übermittlung der teils etliche hundert Kilobyte großen Umgebungsprofile für jeden Benutzer praktisch nicht möglich.

Im Falle des Ausfalls des PDCs kann ein BDC auch gänzlich dessen Aufgaben wahrnehmen, indem er zum PDC hochgestuft wird. Ist der alte PDC wieder am Netz, dann kann eine Zurückstufung durchgeführt werden. Die Umwidmung eines normalen Servers zu einem PDC oder BDC ist allerdings ohne Neuinstallation *nicht* möglich. In der Praxis wird dieser Fall nicht allzu oft auftreten, der Sachverhalt an sich bleibt aber zu kritisieren und ist grundsätzlich nicht verständlich.

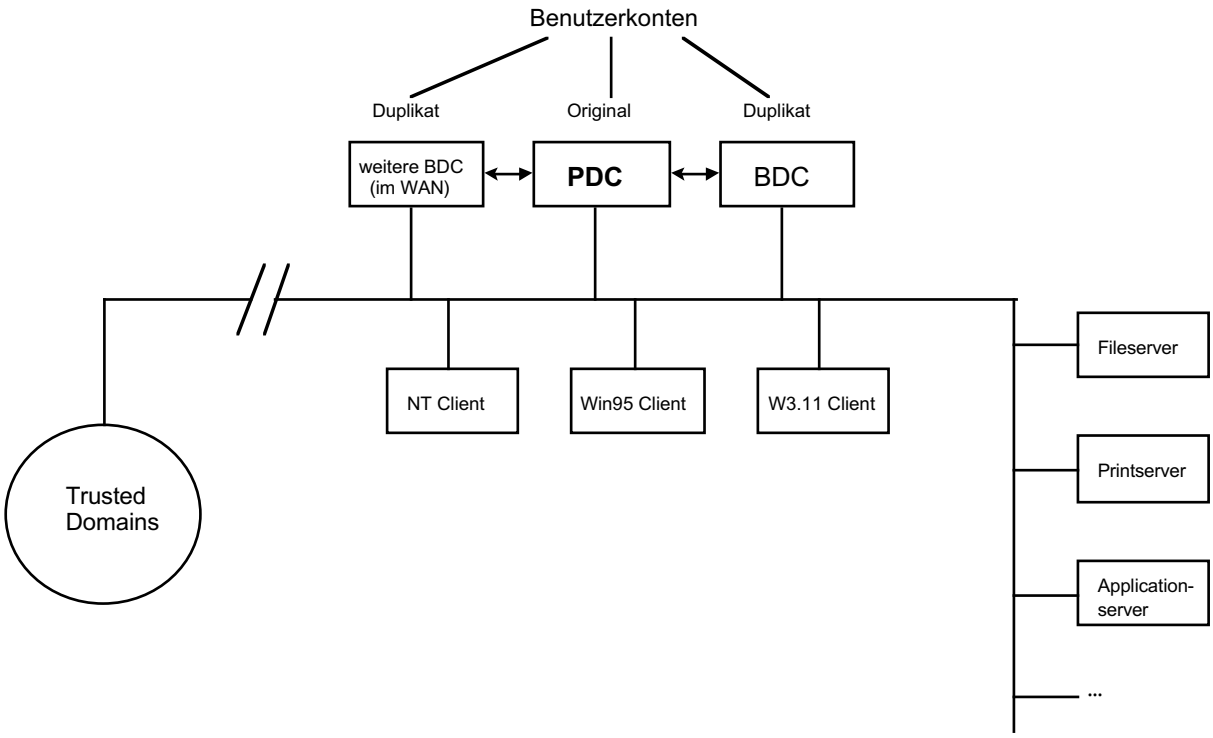


Abb.2: Komponenten der Standalone Domäne

Die Domänencontroller können prinzipiell auch alle anderen Netzwerkdienste bereitstellen, also beispielsweise File-, Print- und Applicationservices, im Extremfall genügt eine *All-in-one*-Maschine, was jedoch seine Grenzen in der enormen Abhängigkeit von diesem einzigen Gerät und der eher geringen Anzahl Clients, die damit versorgt werden können, findet. In den Testumgebungen an der Universität Ulm erwies sich aber eine Versorgung von etwa 20 Clients durch zwei zentrale, nicht übermäßig leistungsfähige Server noch als absolut ausreichend. Allerdings wurde durch die Vielfalt der angebotenen Services für die Hauptmaschine ein Speicherausbau auf knapp 100 MByte zwingend erforderlich, ein für Server allerdings auch nicht besonders hoher Wert, weder in der NT-, noch in der UNIX-Welt. In dieser Ausbaustufe wäre den Auslastungsstatistiken zufolge selbst die doppelte Anzahl Clients noch problemlos zu bedienen gewesen. Als begrenzender Faktor erwies sich eher die für heutige Verhältnisse geringe Bandbreite des Ethernet von 10 Mbit/s; für Hochleistungsserver sollte deswegen auch bei NT die Verwendung eines schnelleren Übertragungsverfahrens erwogen werden (ATM).

Die an einer Domäne und ihren Diensten partizipierenden Clients können grundsätzlich unter ganz verschiedenen Betriebssystemen arbeiten; NT unterstützt beispielsweise das Netzwerkprotokoll *Appletalk* und UNIX-Anwender können zumindest via FTP und Telnet auf die Domäne zugreifen. Eine optimale, volle Funktionalität bietende Unterstützung ist jedoch nur bei Microsoft-Betriebssystemen gegeben und dort vor allem bei einer *NT Workstation* (ein im Grunde etwas abgespeckter *NT Server*). Sie ist in einer NT Domäne zweifellos das ideale

Frontend, stellt jedoch auch die höchsten Hardwareanforderungen. Auf den Aspekt der Wahl des „richtigen“ Clientbetriebssystems wird weiter unten ausführlich eingegangen.

3.1.2. Master Domain Modell

Bei diesem Modell werden mehrere Domänen miteinander verknüpft. Voraussetzung dafür ist die Möglichkeit der Definition globaler Benutzergruppen und Trusts.

Globale Gruppen werden auf den Domänencontrollern definiert und dienen der Zusammenfassung von Benutzern aufgrund von Rollen innerhalb der Organisation. Jeder Domänenaccount ist standardmäßig Mitglied der globalen Gruppe der Domänenbenutzer. Diese globalen Gruppen können dann den lokalen Gruppen zugeordnet werden, die für *jede* Maschine separat definiert werden müssen und auf deren Basis dann die Rechte auf Datei- und Verzeichnisebene vergeben werden. Dieses Verfahren läßt sich zwar logisch einwandfrei strukturieren, führt jedoch auch zu einer gewissen Redundanz, die entsprechend administriert werden will, in der Regel aber nur auf den (relativ wenigen) Servern. Der Vorteil globaler Gruppen ist, daß sie über Domänengrenzen hinaus *exportiert* werden können (ebenso wie Domänenaccounts). Damit können Benutzern in anderen Domänen Rechte zugewiesen werden.

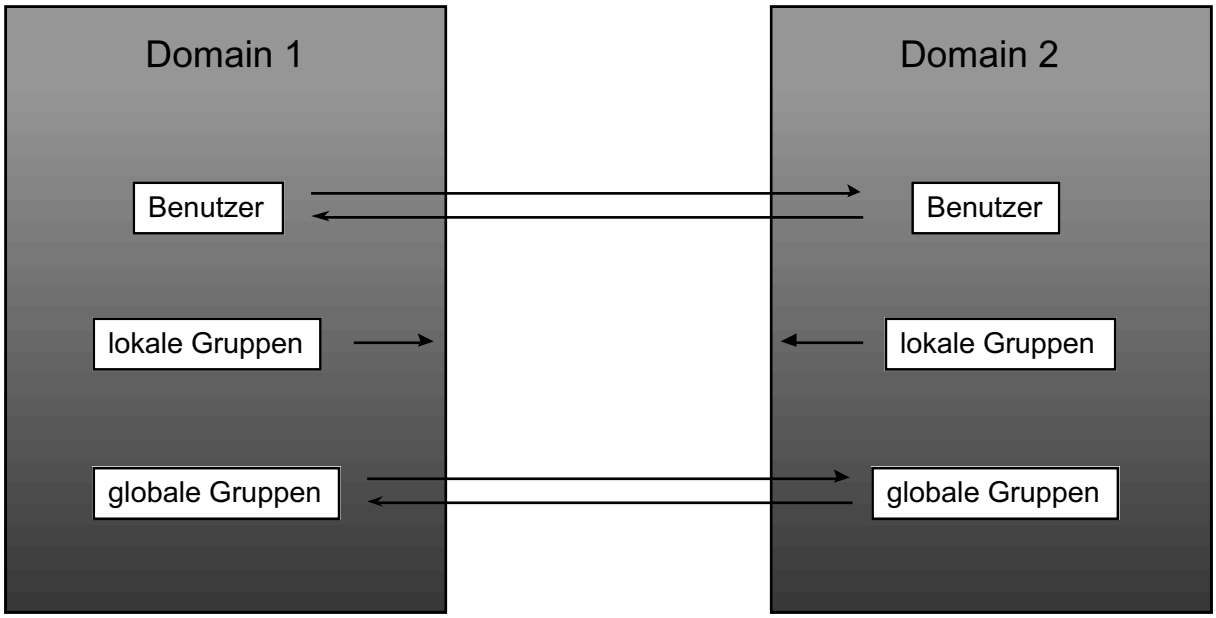


Abb.3: Reichweite von Benutzeraccounts und Gruppenzuordnungen

Damit dies funktioniert, sind zunächst *Trusts* zwischen den zu verknüpfenden Domänen zu definieren, was die Administratoren mit Hilfe des *Benutzermanagers* auf Ebene der PDCs tun können.

Die dahinter stehende Idee ist, daß die Authentisierung des Benutzers nur genau einmal in der Domäne erfolgen muß, die seinen Account führt. Ein Zugriff auf die Ressourcen anderer Domänen kann dann ohne neuerliche Authentisierung erfolgen, wenn zwischen den Domänen Vertrauensbeziehungen definiert werden. Diese Trusts können wechselseitig oder einseitig sein. Im ersten Fall vertrauen die Domänen sich gegenseitig, sind also gleichberechtigt, im zweiten Fall wird eine hierarchische Struktur geschaffen: Accounts aus der übergeordneten, der vertrauten Domäne können in die untergeordnete, vertrauende Domäne importiert werden bzw. ihnen können Rechte zugewiesen werden, jedoch nicht umgekehrt.

Die Möglichkeit einer hierarchischen Strukturierung erlaubt in größeren Netzen bis zu einigen tausend Benutzern verteilt über mehrere Domänen die Verwaltung der Accounts und Gruppen in einer gemeinsamen *Master Domain*, der alle untergeordneten Domänen einseitig vertrauen. Die Master Domain übernimmt dann ausschließlich die Authentisierung und das Usermanagement, während die Subdomains die eigentlichen File-, Application- und Printressourcen zur Verfügung stellen, inclusive der entsprechenden Rechteadministration. Die Accounts werden also nur einmal an zentraler Stelle angelegt, und ihre Administration kann relativ einfach mit einer einheitlichen Policy geschehen.

Dieses Modell wurde in den Testumgebungen an der Universität Ulm erprobt, da es sich schon von der theoretischen Konzeption her für die spezifischen Bedingungen an Hochschulen am besten eignet, wo zentrale Einrichtungen wie Verwaltung, Bibliothek und Rechenzentrum jeweils eigene PC-Netze und Server betreiben. Hier macht es unter Umständen gerade für die Zukunft Sinn, die Accounts zentral in einer Master Domain zu verwalten, die darüber hinaus auch bestimmte andere Dienste wie *WINS* (**W**indows **I**nternet **N**ame **S**ervice) und *SMS* anbieten kann, die universitätsweit von Interesse sind.

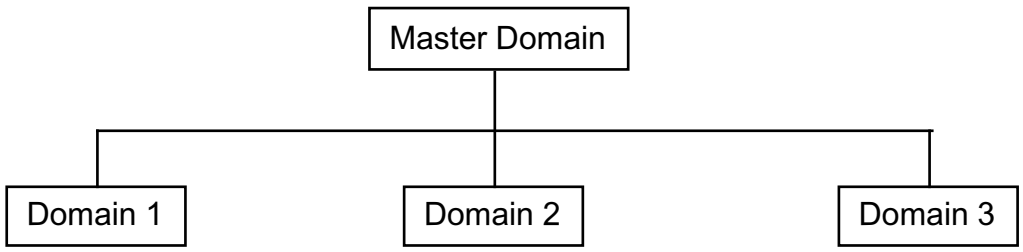


Abb.4: Schematische Darstellung des Master Domain Modells

Positiv bei der konkreten Implementation dieses Modells in NT ist aufgefallen, daß die in der Master Domain authentisierten Benutzer nicht automatisch Rechte in den Subdomains besitzen, sondern jeweils explizit zugeordnet werden müssen. Dies gilt gleichfalls für die globalen Gruppen der Master Domain. Allerdings können die globalen Gruppen einer übergeordneten Domain nicht gleichzeitig Mitglied der globalen Gruppen der untergeordneten Domain sein, was es erforderlich macht, sie jeweils den lokalen Gruppen auf *allen* Servern *manuell* zuzu-

weisen, auf die sie Zugriff haben sollen. Bei vielen Servern, die zu administrieren sind, kann sich dies als lästig und umständlich erweisen.

Das Master Domain Modell schließt im übrigen nicht aus, daß in den untergeordneten Domänen weiterhin Benutzeraccounts definiert werden. Diese haben dann aber *nur* dort Gültigkeit. Welche Accountpolicy im Einzelfall verfolgt wird, hängt nicht zuletzt von den konkreten individuellen Anforderungen der Institution ab. Für die Universitätsverwaltungen mag es durchaus ein Securityproblem sein, nicht nur datenschutzrechtlich, die Accounts in einer mit anderen Einrichtungen gemeinsamen Benutzerkontendatenbank zu führen. Technisch schwierig wird die Realisierung dieses Modells, wenn einzelne Domänen durch Firewalls geschützt sind. Andererseits wird dann eine enge Verknüpfung dieser Systeme im allgemeinen ohnehin nicht gewünscht.

3.1.3. Multiple Master Domain Modell

Bei diesem Modell handelt es sich um eine Variante des Master Domain Modells, das sich vor allem für sehr große *Corporate Networks* eignet und für Universitäten weniger brauchbar ist. Der Vollständigkeit halber soll es dennoch kurz erläutert werden: Hier kommt wieder eine hierarchische Domänenstruktur zur Anwendung, jedoch existieren *mehrere* Master Domänen, zwischen denen wechselseitige Vertrauensbeziehungen angelegt sind. Die Subdomains vertrauen über einseitige Trusts allen Master Domains, in denen wiederum alle Benutzeraccounts und alle globalen Gruppen genau einmal erstellt werden. Der Vorteil dieses Konzepts liegt darin, daß in sehr großen Systemen das Usermanagement gerade *nicht* von einer einzigen zentralen Stelle aus erfolgen muß, sondern verteilt durchgeführt werden kann. Die einzelnen Benutzerkontendatenbanken in den Master Domains bleiben überschaubar. Zudem wird der Replikationsaufwand zwischen den einzelnen Domain Controllern geringer ausfallen, als bei nur einer einzigen Master Domain.

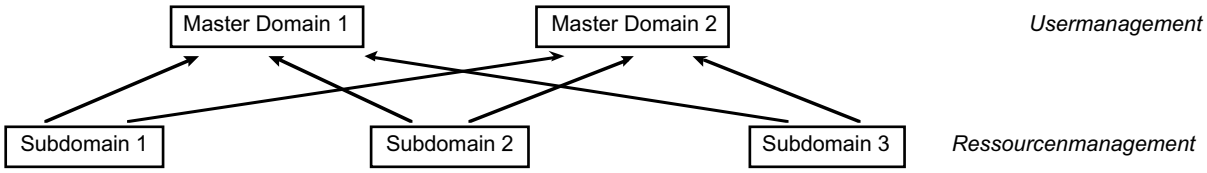


Abb.5: Schematische Darstellung des Multiple Master Domain Modells

3.2. Netzwerkprotokolle

Die Wahl des geeigneten Netzwerkprotokolls ist von einer ganzen Reihe von Randbedingungen abhängig:

- der Anzahl zu vernetzender Systeme

- der Einbindung in ein heterogenes Umfeld mit einer großen Vielfalt von verwendeten Betriebssystemen auf Servern und Clients
- der physischen Netzinfrastruktur

Gerade an Universitäten werden NT-Systeme auf eine bereits bestehende EDV-Umgebung stoßen, einerseits aus dem UNIX- und Mainframebereich und andererseits aus dem WfW- und Novell-Umfeld. In vielen Fällen ist eine völlige Substitution dieser Systeme durch NT nicht möglich oder wünschenswert. Es ist also von erheblicher praktischer Bedeutung, daß NT auch eine gute Connectivity zu den vorhandenen Systemen bietet. Diesem Umstand hat *Microsoft* durch die Unterstützung aller gängigen Netzwerkprotokolle Rechnung getragen. Im einzelnen sind dies:

- das microsofteigene (und veraltete) *NetBeui*, das bereits von WfW bekannt ist,
- Novells *IPX* mit einem passenden Client für Novell Netware Netze,
- *Appletalk* für die Benutzer von MacIntosh Computern,
- *TCP/IP*.

Alle Protokolle und Netzwerkclients wurden in dem heterogenen Umfeld an der Universität Ulm getestet. Zur Vernetzung der Clients unter den verschiedenen Windows Versionen und zu ihrer Anbindung an NT Server eignet sich dabei vor allem TCP/IP, das, wenn irgend möglich, als Standardprotokoll oder sogar ausschließlich gefahren werden sollte. Die Integration dieses Protokolls bietet über einen entsprechenden Client für das *Microsoft Netzwerk* volle Funktionalität und gestattet darüber hinaus die Anbindung an die UNIX-Welt über Dienste wie Telnet, FTP und NFS. Sofern die NT Domäne ausschließlich über NT- und Win95-Clients verfügt, genügt TCP/IP als alleiniges installiertes Netzwerkprotokoll, zumal auch hierüber die populären und vielgenutzten Internetdienste *WWW*, *Mail* und *News* abgewickelt werden. Im Gegensatz zu allen anderen genannten Protokollen (bis auf, in eingeschränkter Weise, IPX) ist TCP/IP in vollem Umfang routingfähig, was für Universitäten mit ihren großen, meist aus diversen Subnets bestehenden Netzen und der in den meisten Fällen gegebenen und erforderlichen Internetanbindung ein wesentliches Kriterium darstellt. Im Prinzip könnten NT Domänen damit auch relativ problemlos über WAN-Strecken ausgedehnt werden.

Bei der Anbindung von WfW-Clients kann zwar grundsätzlich auch TCP/IP gefahren werden, allerdings ist hier eher das proprietäre und nicht routbare NetBeui als Client für Microsoft Netzwerke verbreitet, während zur Nutzung der Internet Services gerne das Sharewareprodukt *Trumpet Winsock* als TCP/IP Stack verwendet wird. Mit dieser Konfiguration muß auch ser-

verseitig NetBeui installiert sein, um den Clients eine volle Funktionalität bietende Domänennutzung zu gestatten, allerdings notwendigerweise auf das lokale Netzwerk beschränkt.

Das IPX Protokoll ist in jedem Fall erforderlich, wenn Clients und Server der NT Domäne auf bestehende *Novellserver* und deren File- bzw. Printservices zugreifen sollen. Bei entsprechender Konfiguration läßt sich ein komfortabler Zugriff auf diese Maschinen inclusive der Authentisierung erreichen.

Durch die Unterstützung von Appletalk können Benutzer von MacIntosh Computern File- und Printservices auf NT Servern nutzen, sofern sie dort einen Useraccount besitzen. Dabei sind allerdings spezielle Mac-Volumes zu definieren. Der umgekehrte Weg ist nicht möglich: Clients unter irgendeinem der Windows Betriebssysteme können auf die Ressourcen von MacIntosh Computern nicht zugreifen (Standardservices wie etwa FTP natürlich ausgenommen).

Immer unter Berücksichtigung der jeweiligen Erfordernisse empfiehlt sich nach unseren Erkenntnissen zum Betrieb einer NT Domäne in erster Linie TCP/IP. Hiermit gab es im praktischen Einsatz die wenigsten Probleme, die sich auch durch die gute Dokumentation und die bekannten Eigenschaften dieses Protokolls leicht beheben ließen.

3.3. Nameservice

Computer in einem Netzwerk werden letztlich identifiziert durch die eindeutige Hardwareadresse ihrer Netzwerkkarte bzw. auf Ebene des TCP/IP Protokolls durch ihre IP-Adresse. Diese Art der Adressierung ist für die Benutzer durch ihre Kompliziertheit praktisch unbrauchbar. Anwenderseitig wünscht man sich einen Zugriff auf andere Rechner über einen leichter zu merkenden Namen. Damit dies möglich ist, muß grundsätzlich eine Verbindung zwischen dem Rechnernamen und seiner (IP-)Adresse hergestellt werden, wofür es unterschiedliche Techniken gibt.

Das einfachste Verfahren zur name resolution ist das Versenden von *Broadcasts* (RFC 1001/1002), die ein System 1. nach dem Einschalten an alle anderen Rechner verschickt, die die Namens-IP Zuordnung dann in ihre lokale Tabelle aufnehmen (sofern der Name nicht doppelt auftaucht) und 2. reagieren die Systeme auf Broadcasts, in denen ein Name gesucht wird. Dies Verfahren führt insgesamt zu einer hohen Netzbelastung, weswegen Broadcasts im allgemeinen von Routern nicht weitergegeben werden. Diese Lösung funktioniert also immer nur für das lokale Subnetz, mithin für kleinere Arbeitsgruppen.

Einen besseren und bewährten Weg beschreitet man mit *Hosts-Dateien*, in denen die Namen den IPs zugeordnet sind. Im einfachsten Fall liegen diese Tabellen auf jedem einzelnen Rech-

ner, oder, in weiter entwickelter und leichter zu administrierender Form, auf einem zentralen Nameserver (UNIX DNS, **D**omain **N**ame **S**ervice). Grundsätzlich müssen Änderungen an der oder den Namenstabellen manuell vorgenommen werden. In größeren Netzen kann der dazu nötige Aufwand beträchtlich sein.

NT gestattet zur name resolution grundsätzlich alle genannten Verfahren, wobei aber zwischen den *UNIX Namen* und den Windows bzw. *Netbios Namen* unterschieden werden muß. Beide sind in den meisten Fällen aus Vereinfachungsgründen identisch, was aber nicht zwangsläufig so sein muß. Die name resolution des UNIX Namens geschieht entweder über eine lokale Host-Datei oder über einen DNS-Server. Das Pendant für den Netbios Namen, über den Windows Rechner miteinander kommunizieren, ist die *LMHOSTS-Datei*. Bei der Nutzung eines zentralen Namensservers hat man jetzt aber die Wahl zwischen einem eventuell schon bestehenden und in der Regel unixbasierten DNS Server (sofern UNIX und Netbios Name identisch sind) oder einer NT-spezifischen Nameserver-Variante, dem *WINS* (**W**indows **I**nternet **N**ame **S**ervice).

Hierbei handelt es sich um eine verteilt zu gestaltende Datenbank, in der den IP-Adressen die Netzwerknamen dynamisch zugeordnet werden. Durch die *automatische Registrierung* der WINS Clients in dieser Datenbank, die Änderungen an den Zuordnungen sofort „verbucht“, wird das Führen statischer Tabellen weitgehend überflüssig, wiewohl auch dies mit WINS möglich ist. Sofern weder DNS noch lokale Hosttabellen zum Einsatz kommen sollen, ist WINS das Mittel der Wahl, ein NT Netz über Routergrenzen auszudehnen. Nur so kann auch der *Browserdienst*, der eine Liste der gerade aktiven Rechner bereitstellt, korrekt funktionieren. Durch das skalierfähige Konzept können sich mehrere WINS Server ihre Aufgabe teilen und gegenseitig ihre Datenbanken in konfigurierbaren Zeitabständen austauschen. Für den Administrator gestaltet sich die Einrichtung und laufende Pflege der WINS Daten denkbar einfach, da es sich hier um ein weitgehend automatisiertes und selbstwartendes System handelt. So werden beispielsweise Clients, die ihre Registrierung über einen längeren Zeitraum nicht mehr erneuert haben, als veraltet gekennzeichnet und schließlich nach einem bestimmbaren Intervall gänzlich gelöscht. Diese Zeitspannen lassen sich allesamt vom Administrator an die individuellen Erfordernisse anpassen, stellen aber neben der Wahl der zu verknüpfenden Server und der (eigentlich überflüssigen) Definition statischer Einträge auch praktisch die einzige Eingriffsmöglichkeit dar, zumal die Datenbank in einem speziellen Format abgelegt ist und nur mit dem mitgelieferten *WINS Manager* verwaltet werden kann.

In den Testumgebungen wurde WINS über einen Zeitraum von mehreren Monaten betrieben und hat die ihm zugedachten Funktionen erfüllt. Durch die Möglichkeit, den WINS Dienst auch domänenfremden Clients zur Verfügung zu stellen, was ebenfalls erprobt wurde, sind die Datenbestände relativ rasch angewachsen, wobei sich zeigte, daß die vom WINS Manager

präsentierte Darstellung der Inhalte sehr unübersichtlich und zudem noch schlecht dokumentiert ist. Zusammen mit den ohnehin beschränkten Eingriffsmöglichkeiten ist dieses Tool für die Diagnose oder gar Lösung eventuell auftretender Probleme im Zusammenhang mit der name resolution kaum geeignet.

Es erscheint zudem völlig unklar, wie mit dem derzeitigen WINS eine dem DNS vergleichbare Domänenhierarchie realisiert werden soll, die wirklich weltweite Eindeutigkeit gewährleistet und somit internettauglich ist. Der Einsatz von WINS ist im Augenblick eher für „Intranets“ geeignet, wo dann auch für größere NT Netze eindeutige Zuordnungen durch die Weisungsbefugnisse einer zentralen EDV-Einrichtung garantiert werden können (ansonsten sind Netzwerkprobleme früher oder später unvermeidlich). Diese Rahmenbedingung ist für den universitären Bereich in der Regel gegeben oder läßt sich dort doch wenigstens realisieren, so daß dem Einsatz von WINS hier keine prinzipiellen Einwände entgegenstünden. An der Erweiterung dieses Konzepts muß jedoch noch gearbeitet werden.

Voraussetzung für die Nutzung von WINS ist immer der Einsatz von TCP/IP als Netzwerkprotokoll. Da *Microsoft* kein anderes wirklich zeitgemäßes Verfahren zur name resolution anbietet, das heutigen Anforderungen hinsichtlich einfacher Administrierung und Unabhängigkeit von physischer Netzstruktur entgegenkommt,[5] unterstreicht dies die Bedeutung von TCP/IP. Es ist zu erwarten, daß die zukünftige Entwicklung von NT ganz in diese Richtung und fort von proprietären Netzstandards gehen wird.

---

5 Ab der Version 4.0 enthält NT einen DNS Server; ein Indiz dafür, daß *Microsoft* um einen Anschluß an etablierte Internet-Standards bemüht ist.

4. Sicherheitsmechanismen

Die sicherheitstechnischen Anforderungen an ein Betriebssystem in datenschutzrechtlich sensiblen Bereichen wie der Verwaltung sind heute sehr hoch. Sicherheit in dem hier verstandenen Sinne bezieht sich dabei auf zwei Aspekte:

- Ausfallsicherheit und Betriebsstabilität des Systems (Datensicherheit)
- Zugriffssicherheit auf Benutzerebene (Datenschutz)

Zu beiden Bereichen bietet NT Lösungen an, die im folgenden erläutert werden sollen.

4.1. Dateisysteme und Festplattenverwaltung

Der Betriebssicherheit eines Datenverarbeitungssystems kann durch die Wahl geeigneter Hardware Rechnung getragen werden. Dies schützt in der Praxis aber nicht vor den Fehlern schlecht programmierter und instabiler Software. Wesentlich für die Sicherheit der wertvollen Datenbestände ist daher auch die Frage, wie ein Betriebssystem Files auf den Datenträgern ablegt und welche Mechanismen zur Wahrung der Konsistenz und zur Fehlertoleranz vorgesehen sind.

NT unterstützt zur Erzielung größtmöglicher Kompatibilität drei verschiedene Dateisysteme auf Festplatten:

- FAT (**F**ile **A**llocation **T**able)
- HPFS (**H**igh **P**erformance **F**ile **S**ystem); nur bis Version 3.51
- NTFS (**N**ew **T**echnology **F**ile **S**ystem)

Das HPFS wird von NT vorrangig wegen der Abwärtskompatibilität zu Dual-Boot Systemen wie OS/2 unterstützt, während es FAT gestattet, ein älteres DOS bzw. Windows auf derselben Partition zu betreiben wie NT sowie auf Disketten und entsprechend formatierte Wechselplatten zuzugreifen. Grundsätzlich muß auf einem leeren Computersystem auch mindestens eine Partition unter FAT eingerichtet sein, um NT von einem Installationsserver aus einzurichten. Für den ernsthaften Einsatz von NT ist dieses betagte Dateisystem wegen seiner technischen Defizite und fehlenden Vergabemöglichkeit von Benutzerrechten jedoch ungeeignet, obgleich sich NT damit durchaus betreiben läßt. Wesentliche Vorteile, aus denen heraus man ja gerade NT einsetzt, gehen dabei allerdings verloren.

Aus diesen Gründen empfiehlt sich der Einsatz des NTFS Dateisystems. Es bietet eine schnelle Ausführung von Standardoperationen wie Lesen, Schreiben und Suchen auch auf sehr großen Festplatten sowie die Wiederherstellung des Dateisystems nach einem Systemversagen.

Jede Datei eines NTFS Datenträgers wird durch einen Eintrag in der MFT (**M**aster **F**ile **T**able) repräsentiert, die in dem attributbasierten Dateisystem, das alle Dateien als Objekte mit benutzer- und systemdefinierten Attributen behandelt, wiederum als Datei geführt wird. Neben einer Redundanz z.Bsp. für den Bootsektor, führt die MFT eine Logdatei, mit deren Hilfe unvollständige oder fehlerhafte *Transaktionen*, als die NTFS jede E/A-Operation auf einem NTFS Datenträger betrachtet, wiederholt oder rückgängig gemacht werden können. Nach einem Systemabsturz können dadurch Inkonsistenzen im *Dateisystem* sehr schnell und zuverlässig beseitigt werden.

Anders als im FAT oder seiner Win95 Variante VFAT werden kleine Dateien (bis 1.5 kByte) im NTFS sehr effizient verwaltet, da sie komplett in die MFT passen, was einen sehr schnellen Zugriff auf ihre Inhalte erlaubt. Generell wird auch der Inhalt einer Datei vom Filesystem als ein Attribut behandelt. Bei den Attributen unterscheidet man zwischen residenten (innerhalb der MFT) und nicht-residenten (außerhalb der MFT) Attributen. Dieses Verfahren gestattet es, die Liste der Attribute in der Zukunft beliebig zu erweitern.

Die bisher unter DOS/Windows gebräuchliche *„8+3“*-Namenskonvention ist im NTFS obsolet. Dateinamen dürfen bis zu 255 Zeichen und beliebig viele Interpunktionen wie Punkte und Kommata enthalten. Bestimmte Sonderzeichen wie Backslashes sind allerdings nicht möglich. Neben diesen neuen Dateinamen führt aber NTFS *automatisch* generierte *„8+3“*-Namen, die sicherstellen, daß DOS/Windows Clients, die über Shares auf einen solchen Datenträger zugreifen, die Dateien auch lesen können.

Einer der größten Vorteile des NT-eigenen Filesystems besteht jedoch darin, für Verzeichnisse und sogar einzelne Dateien sehr differenziert Benutzerrechte auf Basis der Benutzerkontendatenbank zu vergeben (vgl. dazu Abschnitt 4.2.).

Zur Festplattenverwaltung bietet NT eine Reihe von Techniken, mit denen sich die Sicherheit und Verfügbarkeit der Daten erhöhen läßt:

- Bildung von *Datenträgersätzen*: Zusammenfassung freier Flächen auf einer oder mehreren Festplatten zu einer logischen Festplatte.

- *Stripe Sets ohne Parität*: Erhöhung der Lese- und Schreibgeschwindigkeit durch optimierte Anordnung der Datenblöcke.

- *Stripe Sets mit Parität*: Die Daten werden in Stripes über alle Partitionen des Sets geschrieben, wobei ein Paritäts-Stripe angelegt wird. Bei Ausfall einer Platte können die Dateninhalte restauriert werden (fehlertolerantes System; vgl. Abb.6)
- *Festplattenspiegelung*: Dateien der primären Platte werden auf die sekundäre Platte gespiegelt (gemeinsamer Controller).
- *Festplattenduplikation*: wie Festplattenspiegelung, jedoch zur Erzielung einer höheren Ausfallsicherheit mit zwei Controllern.

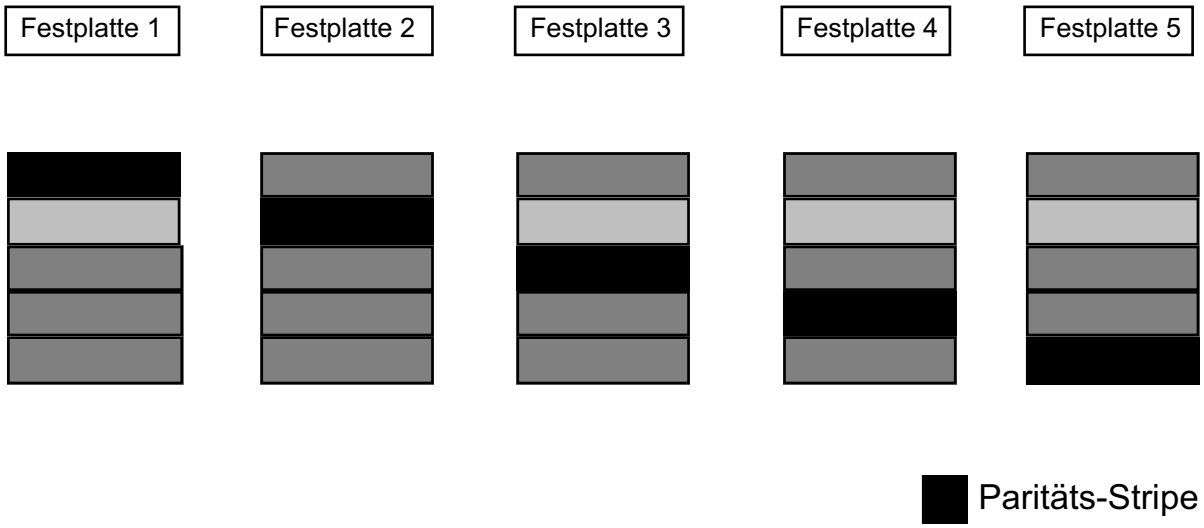


Abb.6: Stripe Sets mit Parität unter NT

Die Möglichkeit, mit NT rein auf Softwarebasis ein RAID-System aufzubauen, ist sicher ein bemerkenswertes Feature, darf jedoch nicht darüber hinwegtäuschen, daß dies nur eine Low-cost Alternative zu einem hardwaremäßig realisierten RAID-Array darstellt, das bezogen auf Verfügbarkeit und Performance gerade für ein Produktionssystem in einer mittleren bis größeren Netzwerkumgebung die bessere Wahl darstellt. Dies wird auch grundsätzlich für den Einsatz von NT in Universitätsverwaltungen empfohlen, wo sich ohnehin eine Lösung von mehreren Servern mit einem gemeinsamen RAID anbietet (vgl. später auch *NT Cluster*). Zweifellos erhöht ein solches Vorgehen die reinen Hardwarekosten, jedoch sollte man dies immer in Relation zu dem entstehenden Schaden bei einem vorübergehenden Ausfall des Gesamtsystems oder gar einem Datenverlust sehen. **Ein NT System sollte mindestens die gleiche Sicherheit bieten, wie bestehende Lösungen, auch wenn dies teilweise die Preisgabe eines zunächst offensichtlichen Kostenvorteils bedeutet.**

Im praktischen Testbetrieb hat das NTFS keine erkennbaren Schwächen offenbart, sowohl Performance wie Zuverlässigkeit ließen nichts zu wünschen übrig. Ein erfreuliches Detail ist

die Möglichkeit der sehr schnellen Konvertierung von FAT Partitionen zu NTFS, was ohne Datenverlust möglich ist. Somit können auch ältere Festplatten problemlos übernommen werden, wobei natürlich noch die Verzeichnis- und Dateiberechtigungen angepaßt werden müssen, die FAT ja nicht kennt. Der umgekehrte Weg, also von NTFS zu FAT, ist nur durch eine komplette Neuformatierung möglich, ein Nachteil, dem in der Praxis aber kaum große Bedeutung zukommt.

4.2. Benutzermanagement

Jede Organisation, die datenschutzrechtlich relevante Informationen auf ihren EDV-Systemen verarbeitet, muß gewährleisten, daß diese Daten gegen unberechtigten Zugriff gesichert sind.

NT bietet die Möglichkeit, ein System auf den Sicherheitsstandard C2 des US-Verteidigungsministeriums zu administrieren. Die wichtigsten Ansprüche dieses Standards sind:

- Gewährung von Eigentümerprivilegien für eine Ressource wie etwa eine Datei, d.h. der Benutzer muß die volle Kontrolle haben.
- Das Betriebssystem muß Objekte dergestalt schützen, daß andere Prozesse diese nicht nach Belieben verwenden können.
- Jeder Benutzer unterliegt beim Zugriff auf das System einer Authentisierungspflicht durch Username und Paßwort.
- Administratoren müssen den Zugriff auf Ressourcen überwachen können.
- Das System muß gegenüber externen Störungen und Eingriffen geschützt sein.

Unter NT ist in jedem Fall eine Authentisierung des Benutzers zwingend erforderlich. Dies gilt sowohl für eine nicht vernetzte standalone Workstation mit eigener lokaler Benutzerkontendatenbank wie für die gesamte NT Domäne. Im Normalfall werden die Accounts auf dem PDC bzw. seinen BDCs geführt. Der Logon erfolgt deswegen auch immer an der Domäne, wobei der Benutzer dann nicht wissen muß, welcher der Domänencontroller letztlich die Authentisierung übernimmt. Die Übermittlung von Username und Paßwort erfolgt dabei nicht im Klartext. Die anfangs allerdings nur mäßig brauchbare Verschlüsselung wurde inzwischen von *Microsoft* überarbeitet und soll auch höchsten Ansprüchen genügen. Gegenüber dem immer noch verbreiteten, nicht verschlüsselten Login in UNIX-Systemen, bei dem ein Ausspionieren der Paßwörter durch Hacker relativ leicht möglich ist, bietet NT hier klare Vorteile. Allerdings ist zu bedenken, daß dies für die Nutzung unixkonformer Dienste wie FTP und Telnet nicht gilt. Wenn auf Sicherheit höchster Wert gelegt wird, dann dürfen diese Dienste

auf NT Servern nicht aktiviert sein. Gleichermaßen sollte der standardmäßig angelegte Gastaccount deaktiviert werden.

Soll ein NT Server öffentliche Dienste wie etwa WWW bereitstellen, und zwar nicht nur für eine Gruppe von Benutzern, die in der Domäne einen Account besitzen, dann muß natürlich ein anonymer Logon möglich sein. Allerdings existieren auch hier Mittel und Wege, diese Zugriffe unter einer Security-ID mit genau definierten Rechten abzuwickeln (vgl. 5.6.1.).

Die für das Netzwerk vorgesehenen Ressourcen eines Systems wie Files, Directories und Printer, werden über *Shares* realisiert. Abgesehen von den ausschließlich Administratoren zugänglichen Shares, die die gesamte Verzeichnisstruktur umfassen, gestatten die Freigaben nur Zugriff auf das explizit angegebene Directory und seine Subdirectories. Individuellen Benutzern oder Gruppen (s.d.) können für diese Shares differenziert Rechte gewährt werden. In der Konsequenz bedeutet dies, daß normale User keinen direkten Zugriff auf Systemverzeichnisse oder andere vom Administrator nicht gewünschte Bereiche haben; nach außen hin sind nur die Shares (also die exportierten Ressourcen) sichtbar. Somit wirken sich ungenau oder gar fahrlässig gesetzte Rechte in den Systemverzeichnissen nicht gleich fatal aus, obgleich eine solche Denkweise natürlich nicht empfohlen werden kann.

Während die Shares und die ihnen zugeordneten Berechtigungen den Netzwerkzugriff regeln, können auf Datei- und Verzeichnisebene ganz andere Rechte gesetzt sein, die in jedem Fall die höhere Priorität haben. Faktisch wird aus beiden Bereichen der größte gemeinsame Nenner gebildet. Dadurch können für die ansonsten eher global arbeitenden Shares (geben den Verzeichnisbaum komplett mit einheitlicher Berechtigung frei) ganz individuelle Rechte für Gruppen und einzelne User realisiert werden.

Die auf Datei- und Verzeichnisebene definierbaren Rechte umfassen:

- Lesen [R]
- Schreiben [W]
- Löschen [D]
- Verzeichnis ansehen [X]
- Besitz am Objekt übernehmen (Ownership)
- Berechtigungen des Objekts ändern

Die Berechtigungen *RWXD* werden unter dem Begriff *Ändern* zusammengefaßt, der komplette Funktionsumfang als *Vollzugriff*.

Jedem Verzeichnis und sogar jeder Datei lassen sich nun einzelne Benutzer oder Benutzergruppen zuordnen, für die die oben genannten Berechtigungen individuell gesetzt werden können. Anders als beim UNIX ist der Administrator hier nicht mehr auf die Dreiteilung *owner/group/everyone* beschränkt, sondern kann beliebig viele Individuen und Gruppen zuordnen. Für neu angelegte oder kopierte Dateien bzw. Verzeichnisse werden standardmäßig die Rechte des übergeordneten Verzeichnisses vererbt.

Über den Dateimanager kann der Administrator oder ein dazu berechtigter Benutzer den Zugriff auf Objekte protokollieren und ggf. sperren.

All diese Features setzen einen NTFS Datenträger voraus, sind also nur auf einer NT Workstation oder einem NT Server verfügbar. Werden in der Netzwerkumgebung auch Clients unter anderen Betriebssystemen (DOS, Win3.x, Win95, MacIntosh) eingesetzt, dann unterliegen diese beim Zugriff auf NT Maschinen zwar den dortigen Restriktionen, für den Client selber sind diese Schutzmechanismen jedoch mangels NTFS nicht möglich. So kann auch in einer NT Domäne beispielsweise ein Win95 Client grundsätzlich lokal von jedermann verwendet bzw. leicht „geknackt“ werden, selbst wenn die Domänenanmeldung scheitert. **Bei einem so gestalteten Netz sollten zur Wahrung der Datensicherheit und des Datenschutzes alle relevanten Dateien auf den NTFS Datenträgern der Server abgelegt werden.** Sofern die Clients unter NT Workstation betrieben werden, ist dies an sich nicht erforderlich, jedoch aus Gründen der einfacheren Administration und der Implementierung von Backupstrategien zu empfehlen.

Bei der Gewährung von „Vollzugriff“ kann ein Benutzer prinzipiell die Rechte ändern, also zum Beispiel Dateien und Directories in seinem Homeverzeichnis für andere Benutzer zur Verfügung stellen. Dies setzt jedoch voraus, daß der Benutzer auf einer Maschine unter NT arbeitet. Andere Betriebssysteme können zwar über Shares auf einen NTFS Datenträger zugreifen, unterstützen dieses Dateisystem jedoch nicht aktiv. Die Berechtigungen müssen also so akzeptiert werden, wie sie gesetzt sind. In der Praxis kann sich dies in großen Netzen schon nachteilig auswirken, da der Administrator dann alle Benutzerwünsche zur Änderung von Dateirechten selbst ausführen muß. Sowohl unter Sicherheits- wie Praktikabilitätsaspekten empfiehlt sich deswegen auch für Clients wann immer möglich der Einsatz von NT.

Wie in anderen Netzwerkbetriebssystemen gestattet NT die Zusammenfassung von Benutzern zu Gruppen, wobei ein Benutzer gleichzeitig Mitglied beliebig vieler Gruppen sein kann.

In der NT Domäne werden zwei Arten von Gruppen unterschieden:

- *Globale Gruppen* zur Zusammenfassung von Benutzern zu Gruppen. Hierin sollen sich organisatorische Strukturen (Dezernate in der Verwaltung) oder Rollen in der

Organisation widerspiegeln sowie temporäre Strukturen wie etwa Arbeits- oder Projektgruppen.

- *Lokale Gruppen* werden definiert, um den Benutzern oder globalen Gruppen Berechtigungen zur Nutzung der Ressourcen zuzuordnen.

Die globalen Gruppen haben dabei die Eigenschaft, domänenübergreifend verwendet werden zu können, während lokale Gruppen an die lokale Benutzerkontendatenbank der Workstation bzw. des Servers gebunden sind. Mitglieder der globalen Gruppe können nur Benutzer der Domäne sein, in der sie definiert wurde. Allerdings kann sie in andere Domänen exportiert (sofern die Trustrelationships entsprechend eingerichtet sind) und dort lokalen Gruppen und somit Ressourcen zugeordnet werden.

Über die Berechtigungen für Shares und Dateien hinaus lassen sich den Accounts noch weitere Attribute zuordnen. Dazu gehören:

- Systemrechte wie lokale Anmeldung (Konsole), Shutdown, Treiberkonfiguration, Backup etc.
- Account Policy:
  - ◊ Maximales und minimales Paßwortalter
  - ◊ Minimale Länge von Paßwörtern
  - ◊ Paßworthistory
  - ◊ Sperrung von Accounts unter bestimmten Bedingungen (z.Bsp. wiederholtes vergebliches Einloggen)
  - ◊ zeitliche Eingrenzung der Zugriffsberechtigung (z.Bsp. nicht nachts oder an Wochenenden)
  - ◊ Ablaufdatum
  - ◊ Eingrenzung, von welchen Maschinen aus der Logon erfolgen darf.

Einschränkend muß allerdings angemerkt werden, daß nicht alle diese Einstellungen benutzerindividuell vorgenommen werden können. So ist die Account Policy grundsätzlich eine globale Einstellung, die es beispielsweise nicht gestattet, die Paßwortlebensdauer für einzelne Benutzergruppen unterschiedlich zu setzen oder Administratorenaccounts nach einer geringeren Anzahl von vergeblichen Logons zu sperren als andere. Es wäre wünschenswert, wenn NT hier in der Zukunft flexiblere Möglichkeiten eröffnen würde.

Insgesamt konnte das Benutzermanagement unter NT mit seiner differenzierten Rechtevergabe für Shares, Verzeichnisse, Dateien und andere Ressourcen wie Printer jedoch überzeugen. Lediglich die Übersichtlichkeit läßt notgedrungen etwas zu wünschen übrig, denn anders als etwa im UNIX, wo die Berechtigungen (rwx) problemlos in Verzeichnislistings hinter dem Namen angebracht werden können, ist dies bei NT durch die jeweils völlig unterschiedlich gestaltbaren Einstellungen nicht möglich. Sollen Berechtigungen angezeigt oder geändert werden, dann ist das betreffende Objekt zu selektieren und eine umfangreiche Dialogbox zu öffnen. Dies wirkt zunächst umständlich, erweist sich in der Praxis jedoch als einigermaßen gut handhabbar, da Berechtigungsänderungen auch rekursiv vorgenommen werden können. Zur vollständigen Remote Administration des Filesystems ist allerdings eine grafische Benutzeroberfläche mit dem Dateimanager erforderlich (nicht von UNIX aus über Telnetsessions).

5. Administration und Remote Management

Bei einem Vergleich mit anderen Netzwerkbetriebssystemen und vor allem unter dem Kostenaspekt ist die Frage nach der Realisierung eines netzwerkweiten Remote Managements für Clients und Server in einem NT-basierten PC-Umfeld von großem Interesse. Anders als im UNIX-Bereich, wo in der Regel auf relativ wenigen, an zentraler Stelle aufgestellten Maschinen gearbeitet wird, an die lediglich (X-)Terminals angeschlossen sind, sind im PC-Bereich auch die Benutzerarbeitsplätze vollwertige Computer mit eigener Prozessorleistung und in der Regel eigenem Massenspeicher, der zumindest die Betriebssysteminstallation, oftmals aber auch Anwendungsprogramme enthält. Für die Administration wäre es außerordentlich aufwendig, Konfigurationen, Helpdeskfunktionen etc. jeweils vor Ort wahrnehmen zu müssen.[6] Ein Effizienzverlust und unnötig hoher Personalaufwand wären damit zwangsläufig verbunden. Die bisherigen PC-basierten Netze mit WfW hatten mehr oder weniger alle mit diesem Problem zu kämpfen. Für die heutige Verbreitung von PCs in großen Institutionen wie Universitäten, die nicht selten großflächig über diverse Standorte verteilt sind, ist dieses Konzept nicht nur überholt, sondern praktisch untragbar.

Unter Berücksichtigung dieses Problems wurde dem Aspekt der effizienten Administration bei den Tests besondere Bedeutung beigemessen.

5.1. Tools im Lieferumfang

Gemäß der Windowsphilosophie sind die Administrationswerkzeuge, die NT standardmäßig mitbringt, rein grafisch orientiert. Im einzelnen sind dies:

- Systemsteuerung
- NT Backup
- NT Diagnose

---

6 Es gibt allerdings auch Lösungen von Fremdherstellern wie etwa *WinCenter* von *NCD*, bei denen die Anmeldung an eine NT Domäne auch mit X-Terminals oder von UNIX Workstations aus möglich ist. Es können dann alle auf dem WinCenter Server oder anderen NT Servern installierten Applikationen und alle Netzwerkressourcen verwendet werden. Eine Konfiguration der Clients entfällt dann natürlich. Voraussetzung zum Betrieb von WinCenter ist ein spezielles Multiuser-NT, das von NCD mitgeliefert wird. Es wird vom Hersteller empfohlen, diesen Terminalserver nicht gleichzeitig als Domänencontroller zu verwenden, was einerseits Performance- und Stabilitäts-, aber sicher auch Kompatibilitätsgründe hat. Im Testumfeld an der Universität Ulm bestand Gelegenheit, dieses Produkt zu erproben. Die Ausstattung des Testservers gestattete die gleichzeitige Benutzung durch fünf angemeldete User, ohne daß die Systemleistung erkennbar nachließ. Bei leistungsfähigerer Hardware können entsprechend mehr Terminals bedient werden. Sofern eine größere Anzahl bereits vorhandener X-Terminals weiterverwendet werden soll, ist diese Terminallösung eine brauchbare Alternative zu der Neuanschaffung von PC-Hardware; in der Praxis dürfte das allerdings eher selten der Fall sein.

- Registrierungseditor
- Festplattenmanager
- Systemmonitor
- Benutzermanager für Domänen
- Ereignisanzeige
- Druckmanager
- Servermanager

5.1.1. Systemsteuerung

Gegenüber den älteren Windowsversionen gibt es hier keine wesentlichen Änderungen oder Verbesserungen. Die Systemsteuerung gestattet einmal die Veränderung von benutzerspezifischen Einstellungen (Farben, Maus, Desktop, Console) und zum anderen von systemspezifischen Einstellungen (Treiber, Netzwerk, Dienste, Geräte, USV). Im allgemeinen betrifft die Systemsteuerung immer nur den lokalen Computer bzw. das Profil des gerade eingeloggten Benutzers. Ein Remote Management anderer Maschinen ist damit nicht möglich. Allerdings finden alle hier vorgenommenen Einstellungen ihre Entsprechung in der lokalen *Registrierungsdatenbank*, die unter NT die früheren *ini*-Files ablöst. Diese Registrierung ist durch andere Tools auch über das Netzwerk zugänglich (vgl. 5.1.4.).

5.1.2. Backup

Das hier von Microsoft mitgelieferte Tool ist eine abgespeckte Version des bekannten *Arcadabackup* und genügt allerhöchstens sehr bescheidenen Ansprüchen. Unterstützt werden an den Floppycontroller angeschlossene Tapestreamer (nur der Vollständigkeit halber genannt) und lokale DAT-Laufwerke. Das grafische Interface dieses Programms gestattet *keine* Automatisierung, alle Einstellungen bezüglich der zu sichernden Laufwerke und Verzeichnisse, der Art des Backups (vollständig, inkrementell,...), der Komprimierung, der Protokollierung etc. müssen bei jeder Sitzung neu vorgenommen werden, da jegliche Möglichkeit zum Abspeichern der Konfiguration fehlt. Dieser Minimalismus läßt die NT-eigene Backuplösung für ein größeres professionelles Netzwerk weitgehend unbrauchbar werden. Da das Backupprogramm unter der Security-ID des eingeloggten Benutzers ausgeführt wird, können damit immerhin auch Netzlaufwerke gesichert werden, allerdings eben nur manuell und ohne die entscheidend wichtige Registrierungsdatenbank der Ferncomputer. Warum das so ist, bleibt un-

klar, da die lokale Registrierung ohne Probleme gesichert werden kann, obgleich es sich hierbei auch um geöffnete Dateien mit besonderen Berechtigungen handelt.

Das NT-eigene Backupprogramm kann auch nicht-interaktiv über Batches gestartet werden, wobei die jeweils gewünschte Konfiguration in einer Kommandozeile angegeben werden kann. Wird dieser Batch einem AT-job[7] zugeordnet, dann ist damit ein automatisiertes, regelmäßiges Backup möglich, allerdings nur, wenn die Datenmengen die Kapazität des Bandes nicht überschreiten und, gravierender noch, nur von den lokalen Laufwerken, denn das Backupprogramm wird als Batch nur unter der Security-ID des lokalen Rechners ausgeführt, die keine Netzwerkzugriffe gestattet.

Insgesamt läßt sich mit diesem Tool keine Backuplösung für Produktionsumgebungen realisieren. In der Praxis wird man auf Programme von Third-party Anbietern angewiesen sein. Am Rechenzentrum der Universität Ulm wird derzeit die Integration der NT Server in das unixbasierte Backupsystem auf eine DLT-Jukebox mit der *Legato Networker* Software in Angriff genommen (vgl. Abschnitt 5.5.1.).

5.1.3. NT Diagnose

Dieses Tool zeigt Informationen an über die Hardwareausstattung, die aktiven Dienste, Treiber, Speicherauslastung, Geräte, IRQs etc. Es dient einzig diagnostischen Zwecken, gestattet keine interaktiven Änderungen und ist auf die lokale Maschine beschränkt, was es für den Administrator eines NT Netzes wiederum recht unbrauchbar werden läßt.

5.1.4. Registrierungseditor

Unter NT werden an sich keine programmspezifischen *ini*-Dateien oder Systemdateien wie etwa *autoexec.bat*, *config.sys*, *system.ini* oder *win.ini* mehr verwendet (außer aus Kompatibilität zu alten Programmen). Alle Einstellungen sind in einer *Registrierungsdatenbank* eingetragen, so etwa auch die Benutzerkonten. Auf Domänencontrollern, die zusätzlich noch diverse Serverfunktionen wahrnehmen, kann diese Datenbank sehr umfangreich werden und hat für das ganze Netz **absolut** funktionsentscheidende Bedeutung. Aus diesem Grund sind hier verschiedene Sicherheitsvorkehrungen getroffen:

- Die Datenbankdateien können auch von Administratoren nicht versehentlich gelöscht werden.

---

7 Die AT-jobs entsprechen den cron-jobs im UNIX. Mit ihnen können zu bestimmten Zeitpunkten einmalig oder wiederkehrend Kommandos ohne Benutzereingabe ausgeführt werden. Anders als bei UNIX ist dies bei NT **nur** für Administratoren und Serveroperatoren möglich.

- Die vitalsten Daten sind in mehrfacher Redundanz vorhanden, zusätzlich wird bei jedem erfolgreichen Systemstart eine Kopie der letzten Systemkonfiguration angelegt, die im Falle des Verlusts der gerade aktiven Einstellungen wiederhergestellt werden kann.

- Das Format der Registrierungsdateien gestattet kein Editieren oder Ansehen mit herkömmlichen Texteditoren.

Alle auf einem grafischen Interface basierenden Administrationstools greifen letztlich auf die Einträge in der Registrierungsdatenbank zurück, verändern, löschen oder legen sie neu an, ohne daß der Benutzer von ihrem Aufbau oder ihrer Syntax etwas verstehen muß. Jedoch beinhaltet die Registry auch sehr viele Einträge, zu deren Modifikation es schon aus Sicherheitsgründen kein grafisches Tool gibt. Meist handelt es sich dabei um sehr spezielle Parameter, deren Anpassung unter Umständen die Systemperformance erhöhen kann und den Betrieb eines großen NT Netzes überhaupt erst effizient ermöglicht. In der Praxis von noch größerer Bedeutung ist sicher, daß ein Administrator durch direkte Bearbeitung der Registry System- und Konfigurationsfehler im laufenden Betrieb beheben kann, die anders nur viel aufwendiger etwa durch Neuinstallation oder das Einspielen von Backups umgangen werden können.

NT bringt zur Bearbeitung der Registry einen speziellen *Registrierungseditor* mit, der jedoch standardmäßig nicht auf dem Desktop installiert wird, sicher als Vorsichtsmaßnahme gedacht, um experimentierfreudige aber laienhafte Benutzer von seiner Verwendung auszuschließen. Der eigentliche Schutz der Datenbank wird darüber hinaus durch Sicherheitsdeskriptoren der einzelnen Einträge realisiert, die ähnlich wie im *Dateimanager* grafisch als Verzeichnisbaum dargestellt werden und mit benutzer- bzw. benutzergruppenspezifischen Zugriffsberechtigungen versehen sind. So kann ein „normaler“ NT Benutzer zwar sein eigenes Profil bearbeiten und ggf. zerstören, jedoch nicht die gerätespezifischen Einstellungen. Sie sind nur Administratoren zugänglich, allerdings auch hier mit einer Ausnahme: der Benutzerkontendatenbank. Diese kann weder mit dem Registry-Editor bearbeitet noch angesehen werden. Jede Veränderung an diesen Daten muß mit dem *Benutzermanager* (s.d.) vorgenommen werden.

Mit dem Registrierungseditor lassen sich aber nicht nur die praktisch gesamten Hard- und Softwarekonfigurationen der lokalen Maschinen bearbeiten und einsehen, sondern die von allen NT Computern im Netz — immer unter der Voraussetzung, daß der Benutzer dafür die erforderliche Berechtigung besitzt. Win95 Computer, die gleichfalls über eine Registrierungsdatenbank verfügen, lassen sich damit leider nicht bearbeiten, da hier ein anderes Format verwendet wird. Sie bringen ihren eigenen Editor mit.

Die Zusammenfassung aller Konfigurationen in einer voll in die NT Sicherheit integrierten Datenbank ist eine saubere und zeitgemäße Lösung, die es auf der anderen Seite aber auch mit sich bringt, daß der Administrator zur Systemverwaltung auf die Verfügbarkeit und die Möglichkeiten spezieller Tools angewiesen ist. Gerade in der Funktionalität muß der Registrierungseditor noch überarbeitet werden. Ebenso ist beispielsweise ein Zugriff auf die Registry von anderen Betriebssystemplattformen aus nicht so ohne weiteres möglich. Im *NT Resource Kit* wird zwar ein Kommandozeilenutility mitgeliefert, mit dem man die Registry auch über eine Telnetsession bearbeiten könnte, doch dies ist eine riskante Sache, die zudem noch völlig unkomfortabel ist. Ein solches Vorgehen kann im allgemeinen nicht empfohlen werden.[8]

5.1.5. Festplattenmanager

Ähnlich wie beim NT Backup bietet auch dieses Tool im Grunde nur eine Basisfunktionalität. Es ist in seiner Anwendung ausschließlich auf die lokale Maschine beschränkt und bietet folgende Möglichkeiten:

- Partitionen erstellen und löschen
- Laufwerke bzw. Partitionen formatieren (FAT, NTFS)
- Partitionen benennen und Laufwerksbuchstaben zuordnen (kann nachträglich geändert werden)
- Einrichtung von Stripe Sets und Spiegelsätzen

Für ein kleines NT Netz mit wenigen zentralen Servern und einer mittleren Anzahl von in ihren Festplattenkonfigurationen nur selten zu verändernden Clients ist der Festplattenmanager in seiner Funktionalität ausreichend, durch die fehlende Möglichkeit des Remote Managements in größeren, verteilten Systemen mit umfangreichen Disk Arrays jedoch unbrauchbar. Allerdings liefern praktisch alle Markenhersteller von professionellen NT Lösungen hier geeignetere eigene Tools mit (z.Bsp. *Compaq* mit dem *Insight Manager*).

5.1.6. Systemmonitor

Der Systemmonitor ist weniger ein Tool zur aktiven Administration, sondern dient vor allem der Information und Diagnose. Hiermit lassen sich netzwerkweit (!) sehr viele Statusinforma-

---

8 Zu den besonderen Problemen bei Telnetsessions vgl. 5.3.

tionen von NT Maschinen grafisch oder als Report darstellen; auch ein Abspeichern und zeitversetztes Auswerten ist möglich.

Zu den angebotenen Informationen gehören z.Bsp. Prozessorauslastung sowie Netz- und Festplattenbelastung. Insgesamt hat der Administrator oder auch der interessierte Benutzer die Wahl unter einer Fülle von Meßgrößen, die es manchmal schon erschwert, die wirklich wesentlichen Daten herauszufinden.

5.1.7. Benutzermanager (für Domänen)

Mit dem Benutzermanager, einem grafischen Tool, kann die Benutzerkontendatenbank von NT Maschinen bearbeitet werden. Es gibt ihn in zwei Varianten: Der einfache Benutzermanager, wie er bei NT Workstation mitgeliefert wird, erlaubt nur den Zugriff auf die lokalen Benutzerkonten, während der bei NT Server enthaltene *Benutzermanager für Domänen* diese Beschränkung nicht aufweist und sogar das Editieren der Benutzerkonten von vertrauenden Domänen gestattet. Da ohnehin der Sicherheitsstatus des aktiven Benutzers bestimmt, ob und welche Konten er bearbeiten darf, erscheint die Trennung zwischen NT Server und NT Workstation unsinnig, ja sogar lästig, da der Administrator oftmals das Netz nicht von einem Server, sondern von seiner Workstation aus managen wird; in diesem Fall muß er auf der Workstation den Domänenbenutzermanager manuell installieren.

Das Anlegen neuer Benutzer kann ohne weiteres von mehreren Operateuren parallel durchgeführt werden, da der Fokus des Benutzermanagers immer auf der Originaldatenbank auf dem PDC liegt. Änderungen werden bei Bedarf automatisch auf die BDCs repliziert; anders herum bedeutet dies natürlich auch, daß ohne einen aktiven PDC die Accounts nicht bearbeitet werden können; eine vertretbare Lösung, um mit wenig Aufwand die Konsistenz der Datenbank zu gewährleisten.

Das Anlegen neuer Benutzerkonten muß generell für jeden Account manuell erfolgen. Bestimmte Einstellungen wie z.Bsp. die Zuordnung von (persönlichen) Profilen, Homedirectories, Anmeldeskripten und Gruppen lassen sich aber auch recht einfach, ggf. unter Verwendung von Variablen, für eine größere Zahl von Accounts auf einen Streich durchführen. Dies empfiehlt sich sogar, um die Einheitlichkeit solcher Zuordnungen zu gewährleisten.

Vollautomatisierte Batches zur Generierung von Accounts sind mit diesem Tool allerdings nicht möglich, obwohl in der Praxis dafür durchaus ein Bedarf vorhanden sein kann, so z.Bsp. wenn Benutzer gleichzeitig Accounts unter NT und UNIX haben, ihre Daten aber nur einmal mit einem dafür geschriebenen Tool erfaßt werden sollen. Dann müßte es möglich sein, auch ASCII-Daten in die Datenbank zu importieren. Im *Resource Kit* zu NT wird dazu ein Programm mitgeliefert, das direkt von der Kommandozeile verwendet werden kann und eine

bessere Batchverarbeitung bietet, in der wenigstens die wichtigsten der individuellen Einstellungen vorgenommen werden können. Ausgegangen wird dabei von einer ASCII-Datei, die die Daten in einem genau festgelegten Format enthält. Unter Sicherheitsaspekten außerordentlich bedenklich ist jedoch, daß in dieser Datei die Anfangspaßwörter im *Klartext* stehen müssen. Bei der Verwendung dieses Zusatztools sollte daher beachtet werden:

- Die ASCII-Datei sollte nur von Administratoren und Kontenoperateuren lesbar sein.
- Bei der Verwendung des Tools über Telnet sollten sich Programm und ASCII-Datei auf derselben Maschine (dem PDC) befinden, da ansonsten wieder das Problem auftaucht, daß alle Daten im Klartext übertragen werden.
- Die Benutzer müssen die Anfangspaßwörter bei ihrer ersten Anmeldung ändern.

Das Entfernen bzw. Löschen von Accounts ist im Gegensatz dazu eine unter Umständen aufwendigere Angelegenheit. Zwar ist der Eintrag aus der Datenbank rasch entfernt, aber alle sonstigen benutzerspezifischen Dateien bleiben auf den Datenträgern unangetastet, so etwa die Profildateien (Zentralprofile und lokale Kopien) und das Homedirectory. Wenn man auf Ordnung im System bedacht ist, müssen erstere explizit und manuell auf jeder Maschine gelöscht werden, obgleich ihr Vorhandensein außer Platzverschwendung keine weiteren Nachteile aufweist. Das Entfernen der Homedirectories ist eine umständliche Angelegenheit, die nicht mit einem einfachen Knopfdruck erledigt ist, da sich der Operateur hier erst die Zugriffsberechtigung aneignen muß.

In einem Einsatzbereich, wo die Accounts wenig verändert werden müssen, ist die Funktionalität des Benutzermanagers absolut ausreichend, in anderen Bereichen mit hoher Fluktuation, etwa Studenten PC-Pools, jedoch noch zu umständlich. Gegebenenfalls müssen hier andere Tools zum Einsatz kommen.

Neben der Verwaltung von Benutzern, Gruppen und der Account Policy dient der Benutzermanager auch zur Definition von Vertrauensstellungen zwischen Domänen, mit denen man dann die im Kapitel über Domänenkonzepte beschriebenen Hierarchien realisieren kann. Diese Einstellungen müssen von berechtigten Usern auf beiden PDCs vorgenommen werden.

5.1.8. Ereignisanzeige

Anders als etwa UNIX geht NT bei der Protokollierung von Ereignissen den Weg, diese wiederum in Datenbanken zu organisieren, wobei zwischen den drei Logbereichen *System, Sicherheit* und *Anwendung* differenziert wird und dort nochmals zwischen den Ereigniskategorien *Information*, *Warnung* und *Fehler*. Der Umfang der Protokollierung läßt sich teilweise

individuell konfigurieren. So kann zum Beispiel bestimmt werden, ob alle Zugriffe auf den Server aufgezeichnet werden (ggf. auf bestimmte Verzeichnisse und Dateien) oder nur die gescheiterten (in der Praxis wohl die bessere Wahl).

Allerdings wird das Konzept der zentralen Protokolldatenbank oft dadurch unterwandert, daß viele Programme entweder zusätzlich oder ausschließlich eigene Logfiles anlegen, darunter auch microsofteigene Produkte wie das *NT Backup* und der *Internet Information Server* (s.d.); in Anbetracht der hierbei anfallenden Datenmengen ist das aber im Einzelfall durchaus sinnvoll, wobei dem Administrator dann natürlich das gelegentliche Aufräumen der Logdirectories selber zufällt, während dies in der Protokolldatenbank, je nach Einstellung, automatisch geschehen kann.

Die Ereignisanzeige gestattet den Zugriff auf die Protokolldatenbanken aller NT Maschinen in der Domäne bzw. in den vertrauenden Domänen. Die Ansicht kann durch Filterfunktionen zeit- und themenmäßig reduziert und grundsätzlich auch als ASCII-Datei abgespeichert werden. Leider ist das nicht automatisierbar, sondern macht einen manuellen Eingriff erforderlich. Wiederum im *Resource Kit* wird ein auch in Batchprogrammen verwendbares Utility mitgeliefert, das diesen Mangel teilweise behebt, jedoch nicht die volle Funktionalität bietet.

Mit dem windowsbasierten Tool *Crystal Reports* können direkt aus der Protokolldatenbank individuell formatierte und optisch aufbereitete Reports erstellt werden, womit ohne den Aufwand der Abfassung von beispielsweise *Perlskripten* auch ein Accounting der diversen NT Services möglich ist.

5.1.9. Druckmanager

Mit dem Druckmanager, der sich bei NT Server und NT Workstation nicht unterscheidet, können lokale und Netzwerkdrucker verwaltet werden, d.h. sie können eingerichtet, entfernt, konfiguriert und überwacht werden und zwar von einer zentralen Arbeitsstation aus für die ganze Domäne.

Neben den üblichen Ports (seriell, parallel) werden auch *lpr*, *LanMan* und *Digital Network* unterstützt, womit die Einbindung in eine heterogene Printserverumgebung prinzipiell möglich ist.

Im Testfeld an der Universität Ulm wurde der für die Domänenprintservices vorgesehene NT Server voll in das unixbasierte und von Operateuren betreute Printsystem aus diversen Laserdruckern (Farbe und s/w) und Plottern integriert. Dies ließ sich mit der lpr-Unterstützung auf der NT Seite recht einfach realisieren, indem lediglich der Name des für das Accounting zuständigen UNIX-Hosts zusammen mit der richtigen Queue angegeben wurde. Der eingerich-

tete Drucker wurde dann als Windows Netzwerkdrucker der Domäne und ihren Benutzern zur Verfügung gestellt, wobei sich natürlich die Berechtigung zum Drucken nach Benutzern oder Gruppen differenzieren läßt; eine volle Unterstützung des NT Sicherheitskonzepts ist gewährleistet. Weniger erfreulich war allerdings die Suche und Konfiguration der richtigen Treiber für die Printer, da erstens die Auswahl an mitgelieferten Treibern nicht besonders groß und aktuell ist, und zweitens diese Treiber oftmals nicht alle Druckerfunktionen optimal unterstützen. Die bei Win95 enthaltenen Treiber konnten hier mehr überzeugen. Es bleibt abzuwarten, ob NT 4.0 hier Abhilfe schaffen kann.

Obwohl der Druckmanager grundsätzlich den Zugriff auf alle NT Maschinen gestattet, ist die Remote Installation neuer Drucker nur unbefriedigend gelöst. So kann zum Beispiel über das Netz kein lpr-Port eingerichtet werden; dies ist nur von der Konsole der betreffenden Maschine aus möglich. Die Einschränkung, der der Druckmanager in diesem Fall unterliegt, erscheint völlig unnötig, da ein erfahrener Administrator die in der Registry abgelegten Einstellungen für den neuen Port auch manuell hinzufügen kann, ohne daß dies technische Schwierigkeiten bringt. Warum kann das der Druckmanager nicht?

Das Hinzufügen neuer Drucker und Ports wird keine tägliche Übung sein, sondern eher gelegentlich vorkommen, aber eine funktionelle Erweiterung des Druckmanagers wäre schon eine wünschenswerte Verbesserung.

5.1.10. Servermanager

Der Servermanager ist Bestandteil von NT Server und bei der Workstation Variante nicht im Lieferumfang enthalten, kann aber ohne weiteres von der Server-CD oder vom *Resource Kit* installiert werden.

Das Tool bietet zunächst eine übersichtliche, alphabetisch sortierte Liste aller Maschinen einer Domäne, allerdings nur, soweit sie unter NT oder Win95 betrieben werden. Clients unter anderen Betriebssystemen wie WfW oder MacOS werden hier nicht angezeigt.

Sofern ein entsprechender Trust besteht und der Benutzer die erforderliche Berechtigung besitzt, kann der Fokus des Servermanagers auch auf eine andere Domäne gesetzt werden.

Mit dem Servermanager kann ein gewisses Remote Management von NT Maschinen (nicht Win95 !) realisiert werden. Im einzelnen sind das:

- freigegebene Verzeichnisse (Shares) und Drucker inclusive der Berechtigungen hierfür
- aktuell verwendete Ressourcen, mit der Option, Benutzer zu trennen

- Warnmeldungen, Verzeichnisreproduktion (automatische Replizierung eines Verzeichnisses auf andere Server; sinnvoll etwa für die Verteilung von Anmeldeskripten auf alle Anmeldeserver)

- Dienste starten, beenden, anhalten, fortsetzen und konfigurieren (nicht jedoch: installieren)

- Konfiguration des bei NT mitgelieferten FTP Servers, dessen Einsatz wegen des geringen Funktionsumfangs jedoch nicht zu empfehlen ist, falls man einen „richtigen“ FTP Server für die Öffentlichkeit betreiben will. Hier ist Microsofts *Internet Information Server* besser geeignet (s.d.).

- Synchronisation der Domäne sowie Herauf- bzw. Herabstufen von BDCs zu einem PDC (bei dessen Ausfall).

5.1.11. Zusammenfassung

Insgesamt sind die bei NT mitgelieferten Administrationswerkzeuge für den Einsatz in kleineren Domänen eine brauchbare und meist ausreichende Sache, aber für den wirklich professionellen und vor allem zeit- und kosteneffizienten Einsatz in großen, verteilten und heterogenen Client-/Server Umgebungen bieten sie noch eine im Detail zu geringe Funktionalität. Teilweise kann dies durch die im preisgünstigen *Resource Kit* enthaltenen Tools umgangen werden, aber eine wirklich umfassende, integrierte Administrations- und Managementumgebung bietet NT in der Grundausstattung nicht. Manche wünschenswerten Funktionen sucht man vergebens, und die Vielzahl der Tools führt auch zu einer gewissen Zersplitterung und Unübersichtlichkeit, zumal die Zuordnung der Funktionen zu den Tools manchmal inkonsistent ist. Was hat etwa die Entfernung von Benutzerprofilen im NT Setup zu suchen?

Zahlreiche Firmen, darunter *Compaq*, *HP* und sogar *Microsoft* selbst, bieten spezielle Administrationspakete für NT an, die aber natürlich separat zu erwerben sind.

5.2. SMS und Assett Works

Mit dem *Systems Management Server* (SMS) bietet Microsoft ein plattformübergreifendes Administrationswerkzeug für den Einsatz in größeren Netzen an. Überblicksartig zusammengefaßt hat SMS folgende Funktionen:

- Inventarisierung von Hardware und Software aller in das NT Netz integrierten Maschinen

- Verteilung und Einrichtung neuer Software auf den Clients

- Verwaltung gemeinsam genutzter Anwendungen, die von Servern aus gestartet werden
- Netzwerkprotokollanalysen
- Helpdeskfunktionen für Clients unter DOS, Win3.x und Win95 (nicht jedoch NT Clients!)

Voraussetzung zum Betrieb von SMS ist die Verfügbarkeit eines *MS SQL Servers*, auf dem die SMS Datenbank läuft. Beide Systeme können natürlich, so wie in der Testumgebung, auf einer Maschine installiert sein. Vor dem Einsatz des SMS in einem größeren NT Netz, das aus mehreren Domänen besteht, sind sorgfältige Überlegungen anzustellen, damit auch auf längere Sicht die gewünschte Funktionalität gewährleistet ist. So ist das SMS ein hierarchisch strukturierbares System, das unter einer sogenannten *Central Site* diverse untergeordnete bzw. *Attended Sites* (Primary und Secondary Sites) besitzen kann. Nur die Primary Sites müssen dabei eine eigene SQL Datenbank haben, die aber zusammen mit denen anderer Sites denselben SQL Server nutzen kann. Kommt das NT *Master Domänenmodell* zur Anwendung, dann wäre es naheliegend, die dort zum Ausdruck gebrachte hierarchische Struktur auch im SMS abzubilden und die Master Domäne als Central Site zu konfigurieren. Dies muß aber nicht zwangsläufig so sein, da auch Aspekte wie die räumliche Verteilung und die Netzbandbreite zu berücksichtigen sind. Da bei SMS teilweise sehr umfangreiche Softwarepakete auf die Distributionsserver und später die Clients verteilt werden, kommt dem letztgenannten Aspekt bei der Planung und Konzeption einige Bedeutung zu.

Recht schön gelöst ist bei SMS die Administration, die ohne Problem für das gesamte System von zentraler Stelle mit dem *SMS Administrator* erfolgen kann, der auch auf einer NT Workstation installiert sein darf. Damit lassen sich Domänen, Distributionsserver und untergeordnete Sites dem System auch später hinzufügen. Lediglich zur Einrichtung eines neuen SQL Servers und ggf. einer separaten Central Site ist ein Konsolenlogin an der betreffenden Maschine erforderlich.

Damit die Clients das SMS nutzen können, müssen auf jeder Maschine bestimmte Komponenten lokal installiert werden, die auf Inventarisierungsanfragen reagieren, die Distributionsserver nach neuen Softwarepaketen abfragen und die Abwicklung von Installationsaufträgen übernehmen. Diese Komponenten werden in der Regel automatisch über ein Anmeldeskript installiert, das den Benutzeraccounts über den Benutzermanager zugeordnet wird; eine zeit- und ressourcenaufwendige Konfiguration vor Ort entfällt.

Prinzipiell können die Clients unter den Betriebssystemen DOS, Win3.x (bzw. WfW), Win95, NT, OS/2 und MacOS betrieben werden, wobei es naturgemäß durch die großen Unterschiede

zwischen diesen Systemen nicht in jedem Fall die volle Funktionalität gibt. Ein Kuriosum in diesem Zusammenhang ist, daß die Helpdeskoption zwar unter DOS, Win3.x und Win95, nicht jedoch unter NT verfügbar ist. Dies wäre aber doch wünschenswert, da NT eben auch als Client wegen seiner unbestreitbaren Vorzüge (Sicherheit, Stabilität) zunehmende Verbreitung findet bzw. finden wird. In den hier verwendeten Testumgebungen wurden ausschließlich Clients unter Win95 und NT über SMS inventarisiert und mit Software versorgt.

Die Inventarisierung hat von Anfang an mit den mitgelieferten Skripten problemlos funktioniert, und die dabei gesammelten Daten über die Hardwareausstattung der Geräte und ihre Konfiguration können im Einzelfall für die Administratoren von großem Nutzen sein (Bsp.: Welche Netzwerkkarte ist eingebaut und welchen Interrupt belegt diese?). Da alle Informationen in der SQL Datenbank abgelegt werden, können auch Abfragen der Art wie „Zeige mir alle Rechner, deren Festplatte zu 90% voll ist“ realisiert werden. Allerdings werden die Inventarisierungsdaten nicht online, sondern nur in regelmäßigen Zeitabständen aktualisiert. Die Default-Einstellung führt die Aktualisierung bei jedem Userlogin durch, was sich zumindest in der Testumgebung als lästig erwies, da sich die Benutzer häufig mehrmals am Tag anmelden und durch die Inventarisierung die Anmeldung erheblich länger dauert (zumindest fällt dies bei Win95 auf). Das Intervall wurde deswegen auf einmal pro Woche heraufgesetzt.

Weniger problemlos gestaltete sich die Definition von Softwarepaketen, während ihre Distribution wiederum sehr einfach war. Für Microsoftprodukte wie etwa das *Office Paket* werden Skriptdateien mitgeliefert, mit denen SMS die verschiedenen Installationsoptionen steuern kann. Interessant ist dabei die Möglichkeit, Pakete als Netzwerkinstallation auf einem Server zu hinterlegen, oder sie automatisiert und ohne Benutzerinteraktion lokal auf den Clients zu installieren. Leider jedoch sind weder die mitgelieferten Skriptdateien immer fehlerlos (gerade die uns zur Verfügung stehende Version von *Office95* hat dies gezeigt; sie brach die automatisierte Clientinstallation regelmäßig mit Fehlermeldungen ab), noch läßt jede Software eine solche Prozedur zu. Zwar kann man diese Skripte auch selber entwickeln, eine mitunter außerordentlich aufwendige Angelegenheit, aber Voraussetzung ist immer, daß das Setupprogramm der Applikation diese auch auswertet. Sind die Programme nicht von *Microsoft*, dann hat man in dieser Hinsicht im Augenblick noch schlechte Karten. Zumindest die netzwerkweite Zurverfügungstellung der originalen Installationsdateien, so wie sie vom Hersteller auf CD-ROM oder Diskette vertrieben werden, ist mit SMS aber immer möglich. So entfällt das Transportieren der Originalmedien zu den Clients, und die Benutzer bekommen außerdem immer die neuesten Softwarepakete und Updates zur Installation vorgeschlagen. Es läßt sich aber auch realisieren, diesen Vorschlag nach einer bestimmten Zeit verbindlich werden zu lassen.

Was SMS noch vermissen läßt, ist ein vernünftiges Konzept zur Vergabe von *Floating Licences*. Zwar kann der Administrator, sofern richtig konfiguriert, aus den Inventurdaten entnehmen, welche der definierten (!) Softwarepakete auf den einzelnen Clients installiert sind, aber das sind natürlich nur statische Informationen, die über die tatsächliche Verwendung nichts aussagen. Nachdem auf anderen Plattformen Floating Licences schon länger kein Fremdwort mehr sind, sollte man erwarten können, daß dies in zukünftigen SMS Versionen implementiert wird. Für den Anwender wäre das ein geeignetes Mittel, nicht nur um den Überblick über die installierte Software zu bewahren, sondern auch, um unnötig hohe Lizenzierungskosten zu vermeiden und diese mehr am tatsächlichen Bedarf zu orientieren.

Durch die Unterstützung von *SNMP* und *NetView* kann der Systems Management Server mit bestehenden Management Systemen integriert werden. Dadurch kann SMS mit SNMP-basierenden Konsolen (*DEC Polycenter*, *HP OpenView*) sowie *IBM* Mainframe Konsolen zusammenarbeiten.

Digital bietet mit dem *PolyCenter Asset Works* eine auf SMS basierende Erweiterung an, die zusätzlich Unterstützung für Desktops unter *OpenVMS*, *SunOS*, *AIX*, *Solaris*, *HP-UX* und *ULTRIX* bringt. Die Server können dabei nicht nur unter *NT*, *NetWare 3.x* und *LAN Manager 2.x*, sondern auch in einer *PATHWORKS* Umgebung betrieben werden.

Insgesamt kann SMS vom Konzept her überzeugen, aber es läßt sich auch nicht leugnen, daß sich dieses System noch in einer Phase rascher Entwicklung und Entwicklungsbedürftigkeit befindet. Die Forderung nach breiterer Softwareunterstützung und Standardisierung betrifft nicht nur den Hersteller *Microsoft*, sondern ebenso die zahlreichen Softwarehäuser, die ihre Produkte so ausliefern sollten, daß sie die Möglichkeiten von SMS optimal nutzen.

5.3. Quotas und Telnetserver

Im Lieferumfang von NT ist kein Tool vorhanden, mit dem Benutzern für definierte Verzeichnisse *Quoten* zugeordnet werden können. Anders als bei *VMS* ist dies also kein integraler Bestandteil des Betriebssystems. In vielen Fällen ist das Setzen von Beschränkungen jedoch unverzichtbar (nicht nur in Studentenpools), da sonst die Festplattenkapazitäten zu schnell erschöpft werden.

Diesen offensichtlichen Mangel decken diverse Quotamanager von Drittanbietern ab. Getestet wurde hier stellvertretend ein Produkt im Vertrieb von *Sunbelt*, das sich serverseitig als Dienst installiert (und somit über die üblichen Tools zur Dienstkontrolle gesteuert werden kann). Die den jeweiligen Verzeichnissen zugeordneten Quoten werden nicht durch Manipulationen am Filesystem gesetzt (genausowenig wie Zugriffssperren beim Überschreiten der Quote), sondern durch Einträge im Registry-Zweig dieses Dienstes. Alle Benutzer, die der

Quotenregelung unterworfen werden sollen, sind einer besonderen Gruppe „Quota“ zugeordnet. Vom Konzept her eine saubere Sache, die der NT Philosophie entspricht.

Für die Administration steht ein grafisches Tool zur Verfügung, das sowohl unter NT wie Win95 lauffähig ist (ggf. auch direkt über das Netz aus einem freigegebenen Verzeichnis; eine spezielle Version für Win 3.x gibt es daneben gleichfalls). Mit dem Tool kann der Quotendienst auf einem beliebigen Server im Netz konfiguriert werden, ebenso ist ein Monitoring der aktuellen Auslastung der Quoten möglich. Für den normalen User gibt es darüber hinaus ein reines Inquirytool, mit dem er sich den Quotenstatus der von ihm aktuell verwendeten Ressourcen anzeigen lassen kann.

Insgesamt eine runde Sache, die etwa vergleichbares wie die Konkurrenzprodukte bietet. Alle Quotenlösungen für NT haben jedoch den Nachteil, daß sie eben zusätzlich zu erwerben sind und preislich überteuert erscheinen (beim Quotenmanager von *Sunbelt* etwa DM 1.500,00 pro Server).

Ebenso auffallend und in der Praxis dann doch ärgerlich ist das Fehlen eines *Telnetservice*, mit dem man auf unproblematische Weise auch von völlig unterschiedlichen Plattformen aus auf NT Maschinen zugreifen und zumindest Kommandozeilenprogramme ausführen könnte. Dies ist durchaus in einzelnen Fällen sinnvoll, da die grafischen Tools zur Remote Administration nicht sämtliche Funktionen, die von der Kommandozeile aus erreichbar sind, abdekken. Besonders gilt dies für die vielen im *Resource Kit* mitgelieferten Befehlserweiterungen.

Einen eigenen Telnetservice für NT hat *Microsoft* zwar bereits für das *Resource Kit* in Aussicht gestellt, bislang aber nicht verwirklicht. Da auch in der Version 4.0 kein solches Produkt enthalten sein wird, ist der Anwender hier wiederum auf Drittanbieter verwiesen. Getestet wurden im Rahmen unserer Untersuchungen die Telnetservices *Ataman* und der in Hummingbirds *Exceed* mitgelieferte, die beide die vorgesehene Funktion erfüllen und beide ähnliche Einschränkungen und Mängel aufweisen, die zum Teil jedoch auch NT-spezifisch sind: Da NT nicht im selben Sinne ein Multiusersystem ist wie UNIX, sind Telnet- und Konsolensitzungen auf einer Maschine nicht völlig getrennt; so können Umgebungseinstellungen wie Pfade und Netzverbindungen nur für alle eingeloggten Benutzer gemeinsam vorgenommen werden.

Lästig ist weiterhin, daß grundsätzlich nicht verhindert werden kann, daß der Benutzer von der Kommandozeile ein Programm mit grafischem Interface startet, dessen Fenster dann auf einem virtuellen Desktop des Servers geöffnet wird und für jedermann damit unerreichbar bleibt. Ein solcher Prozess muß dann zwangsläufig vom Administrator manuell aus dem Speicher entfernt werden.

Da der Benutzer sich bei einer Telnetsession direkt auf dem Server einloggt, bekommt er natürlich im Prinzip alle Laufwerke und Verzeichnisse dieser Maschine zu sehen und nicht nur die explizit für das Netz freigegebenen Shares. Dies ist bei UNIX zwar auch nicht anders, bedeutet aber in gewisser Weise den Verlust eines Sicherheitsbonus, da nun für alle Directories unbedingt die Zugriffsberechtigungen sauber zu administrieren sind (das sollte allerdings sowieso selbstverständlich sein).

Insgesamt wirft der Telnetdienst unter NT, so wie er derzeit realisiert ist, in der Praxis zu viele Unschönheiten und Sicherheitsprobleme auf (auch: Paßwortübertragung im Klartext), so daß eine Freigabe für eine breite Benutzerbasis kaum empfohlen werden kann. In den Testsystemen wurde der Telnetzugang daher auf Administratoren beschränkt.

5.4. Benutzerprofile

Durch die zentrale Benutzerkontenverwaltung in einer NT Domäne ist es grundsätzlich für jeden Benutzer möglich, sich von jedem beliebigen Rechner aus an der Domäne anzumelden und ihre Ressourcen gemäß den ihm zugeordneten Berechtigungen zu nutzen. NT bietet darüber hinaus aber noch die Möglichkeit, dem Benutzer an jedem Arbeitsplatz immer seine gewohnte, ggf. individuell angepaßte Arbeitsoberfläche mit Farben, Fensteranordnung, Icons etc. zu präsentieren. Realisiert wird dieses schöne Feature durch *Benutzerprofile*. Bei NT3.51 ist dies eine einfache Datei, bei NT4.0 etwas aufwendiger ein spezieller Profilordner für jeden User mit zahlreichen Dateien und Unterordnern. Diese Profile werden generell immer auf der lokalen Maschine gespeichert, bei entsprechender Einstellung aber auch noch zusätzlich auf einem Server; in der Regel wird das einer der Anmeldeserver sein, also ein Domänencontroller; zwingend ist das jedoch nicht.

Das Zentralprofil kann somit beim Logon immer vom Server geladen werden, bei Ausfall des Netzes wird die lokale Kopie verwendet. Sofern diese an der Arbeitsstation nicht vorliegt (etwa, wenn es die erste Anmeldung dort ist), bekommt der Anwender eine Defaulteinstellung.

NT unterscheidet vier Arten von Profilen:

- *Verbindliche Profile*: Sie können einer Gruppe von Benutzern zugeordnet werden und bleiben von Sitzung zu Sitzung erhalten. Individuelle Veränderungen werden nicht gespeichert, die Arbeitsumgebung wird vom Administrator eingerichtet.

- *Persönliche Profile* : Abhängig von den im Profil festgelegten Berechtigungen können diese Profile vom Benutzer verändert und individuell angepaßt werden.

- *Benutzerstandardprofil*: Dieses Profil liegt grundsätzlich lokal auf jeder Maschine (unter NT: UserDef) und wird einem User zugewiesen, der sich das erste Mal anmeldet und dem kein anderes Profil zugeordnet ist bzw. dessen Zentralprofil aus irgendwelchen Gründen nicht geladen werden kann.

- *Systemstandardprofil*: Dies Profil wird ausgeführt, wenn kein Benutzer an der Konsole angemeldet ist (wie bei Servern in der Regel der Fall).

Da NT standardmäßig für einen Benutzer ein Profil führt, das dieser verändern und mit „Einstellungen speichern“ fixieren kann, könnte man damit bereits Profile gestalten und nach Bedarf die Dateien umbenennen und kopieren. Geeigneter zur Profiladministration ist der bei NT mitgelieferte *Benutzerprofileditor*, mit dem noch weitere Einstellungen wie etwa die Sperrung von Programmgruppen oder bestimmten Menübefehlen vorgenommen werden können.

Zweckmäßigerweise sollte der Administrator für jeden Typ von Benutzerprofil einen eigenen Verwaltungsaccount mit Superuserrechten anlegen, dem er dieses Profil zuordnet. Zur Editierung des Profils meldet er sich an dem betreffenden Konto an, führt die Änderungen durch und speichert sie mit dem Profileditor ab. Bei der Gestaltung von Profilen ist unbedingt zu berücksichtigen, daß sie unterschiedliche Hard- und Softwareausstattungen antizipieren müssen. Programme beispielsweise, die nur auf einigen wenigen Clients lokal installiert sind (etwa Spezialanwendungen mit ungewöhnlichen Hardwareanforderungen), sollten über allgemeine Programmgruppen gestartet werden, da diese Bestandteil der lokalen Maschinenregistry sind und nicht im Benutzerprofil abgespeichert werden. Einen Sonderfall in diesem Zusammenhang bilden Programmgruppen, die beim Logon vom SMS generiert und angezeigt werden: Sie betreffen Programme, die als Serveranwendungen vom SMS verteilt werden. Eine Integration ins Benutzerprofil ist hierbei nicht nötig.

In der Praxis problematisch ist, daß im Benutzerprofil, das beim Anmelden eigentlich Bestandteil der aktiven Registry wird (und auch mit dem Registry-Editor dann manuell bearbeitet werden kann !), von vielen Programmen benutzerspezifische Einstellungen abgelegt werden. Beispiele für diese Programme sind etwa *Microsofts Officeprodukte* und *Netscapes Navigator*. Sollen solche Programme dem Benutzer sofort beim ersten Logon als ausführbar präsentiert werden, dann müssen diese Registry-Einträge bereits vorliegen. Das Problem besteht nun darin, daß ein Vorgabeprofil allgemeingültig gehalten sein muß, manche Einträge für Programme aber benutzerindividuell sein sollen, wie etwa Pfade, die ins Homedirectory verweisen. Ein prinzipielles Workaround wäre die Verwendung von NT-spezifischen Variablen, die aber leider von vielen Programmen nicht verstanden werden.

Für bestimmte Softwarepakete, wie gerade *Netscape*, ist es daher die praktikabelste Lösung, den Anwender die Software selbst „aktivieren“ zu lassen, indem sie ihm über das SMS als Installationsbefehl (ggf. mit Skripten bereits vorkonfiguriert) angeboten wird. Die Tests haben gezeigt, daß die Softwarepakete sich leider bezüglich ihrer Installation ganz unterschiedlich verhalten, weswegen hier keine generelle Empfehlung ausgesprochen werden kann. Es bleibt nur, jede Software vor ihrem Einsatz auf die optimale Distributionsmethode (vorkonfiguriert, customizable, lokale oder serverzentrierte Installation) zu untersuchen.

5.5. Datensicherung und Failover

5.5.1. Legato Networker

Die durch das NT Backup gebotene Minimallösung zur Datensicherung erwies sich bereits im Testumfeld an der Universität Ulm als unzureichend, einmal wegen der mangelnden Automatisierbarkeit und Netzwerkunterstützung, aber auch wegen der recht geringen Speicherkapazität eines lokalen DAT-Streamers. Da das Universitätsrechenzentrum unter dem *Networker* von *Legato* bereits seit einiger Zeit eine zentrale DLT-Backuplösung mit einem *Digital Alpha Server* in Betrieb hat, war es naheliegend, dieses System für die NT Server zu nutzen. Getestet wurde der *Networker Client für NT* (eine Serverversion ist ebenfalls erhältlich, setzt dann natürlich an der NT Maschine ein entsprechendes Backupmedium voraus), dessen Installation problemlos mit zwei zusätzlichen Services (REXEC und PORTMAPPER) erledigt ist. Auf der Seite des Alpha Servers war zunächst ein besonderer Patch von *Legato* einzuspielen, ohne den alle Backupversuche scheiterten.

Eine Datensicherung kann auf zwei Weisen erfolgen: Der normale Weg führt über ein *scheduled Backup* auf dem Networker Server, in dem alle gewünschten Clients in regelmäßigen Abständen abgefragt werden und dann eine vollständige bzw. inkrementelle Datensicherung angestoßen wird. Die andere Variante ermöglicht es dem Administrator oder Backupoperator eines Clients (in diesem Sinne auch ein NT Server), eine Datensicherung benutzerdefiniert und manuell zu starten bzw. ein komplettes oder selektives Restore vorzunehmen.

Da die Legato Clientsoftware für NT erst kurz vor Ende der Tests zur Verfügung stand, können noch keine Erfahrungen aus einem längeren Erprobungszeitraum vorliegen. Es deutet aber einiges darauf hin, daß die Integration von NT in dieses System noch nicht stabil und fehlerfrei gelöst worden ist. So wurden die nächtlichen Datensicherungen gelegentlich nicht komplettiert und brachen mit Fehlermeldungen ab. Eine genaue Erforschung der zugrunde liegenden Ursachen war bislang nicht möglich, es scheint sich aber nicht um prinzipielle Mängel des Networker oder von NT zu handeln, sondern um eine noch nicht ausreichend von Bugs befreite Implementation.

5.5.2. Clustering

Mit geeigneten Backupkonzepten kann Vorsorge vor dem Verlust von Daten getroffen werden. Das schützt aber nicht vor dem Produktivitätsverlust und dem Ärger bei einem Serverausfall. Wie bei allen Produktionssystemen, so kommt es auch beim Einsatz in Universitätsverwaltungen heute auf höchste Verfügbarkeit der zentralen Maschinen an. Zur Vermeidung von Ausfällen durch Festplattendefekte lassen sich Vorkehrungen treffen mit Festplattenspiegelung, dem in NT integrierten „Soft-RAID“ durch die Bildung von Stripe Sets und für den größeren professionellen Rechenzentrumsbetrieb mit echten RAID-Systemen. Ein Versagen des Servers an sich, etwa durch Defekte an Netzwerkkarte oder Motherboard, ist dadurch aber noch nicht abgedeckt. Hier muß ein möglichst automatisches *Failoverkonzept* greifen, das bei Ausfall eines Servers dessen Aufgaben sofort an ein Backupsystem delegiert.

NT in der von *Microsoft* gelieferten Standardversion bietet derzeit nur unzulängliche Möglichkeiten zum Failover, die sich nur relativ aufwendig und nicht unterbrechungsfrei realisieren lassen. Lediglich die Dauer der Offline-Zeit wird vermindert.

Die optimale Failoverlösung wäre die Zusammenfassung von mindestens zwei NT Servern zu einem *Cluster*, die gemeinsam auf ein RAID-Diskarray zugreifen. Nach außen hin erscheint der Cluster allen Benutzern im Netz als eine Maschine, die tatsächliche Distribution der Prozesse ist eine ausschließlich für den Administrator relevante Frage.

Zwar arbeitet *Microsoft* nach eigenem Bekunden an einer solchen Clusterlösung, aber in der derzeitigen Version ist NT *nicht* clusterfähig. Allerdings bieten Hersteller wie *HP* und *Digital* zusammen mit ihren Servern spezielle Clusterkonzepte für NT an.

Bei *Digitals* Clusterlösung, die hier stellvertretend für alle anderen kurz vorgestellt werden soll, sind zwei Server zusammengefaßt, die mit drei Arten von Anschlüssen ausgestattet sind:

- einem gemeinsamen SCSI-Bus (oder mehreren Bussen), an die auch das RAID-Speichersystem angeschlossen ist,
- dem eigentlichen Netzwerkanschluß an das LAN (Ethernet oder FDDI),
- einer speziellen Netzwerkverbindung zwischen den Clustermaschinen, die zwar nicht zwingend erforderlich ist, aber empfohlen wird, um den steten Kommunikationsfluß zwischen den NT Servern auch im Fall externer Netzwerkfehler zu gewährleisten.

Ein Vorteil von Clustern ist neben dem Failover aber auch die Skalierbarkeit und eine effizientere Verteilung des Workload. Derzeit hat *Digital* allerdings beim Zugriff auf das gemeinsame RAID nur ein *Partitioned Data Model* realisiert, bei dem jede Disk im gemeinsamen

SCSI-Subsystem zu einer Zeit immer nur einem der beiden Server zugeordnet ist. Besser wäre ein symmetrisches *Data Access Model*, wie es *OpenVMS* Cluster bieten, und das diese Beschränkung nicht aufweist. *Digital* beabsichtigt, dies in der Zukunft auch mit NT zu realisieren.

Im Augenblick unterstützt *Digital Clusters* ein Failover für:

- NTFS Fileservices und Netzwerkshares (mit den Protokollen NetBeui, TCP/IP und IPX/SPX),
- Microsoft SQL Server V6.5,
- Oracle7 Workgroup Server V7.1, V7.2,
- sowie alle anderen Applikationen, die mit einem Skript gestartet und beendet werden können.

Ein Failover für Clientverbindungen ist möglich, durch Besonderheiten bei der Verwendung von *Named Pipes* jedoch nicht für offene Dateien. Hier müssen die verwendeten Applikationen so programmiert sein, daß sie nach dem Failover die Verbindung ohne Benutzerinteraktion wiederherstellen.

5.6. Benutzerservices

5.6.1. Internet Services

Die Möglichkeiten, mit NT Internet Services bereitzustellen, sollen hier nur der Vollständigkeit halber kurz erläutert werden, denn es handelt sich dabei zweifellos nicht um einen für Universitätsverwaltungen zentralen Anwendungsbereich. Allerdings mag ein WWW-basierendes Inhouse-Informationssystem, über das den einzelnen Instituten und Abteilungen Zugriff auf ihre Konten gewährt wird, durchaus von Interesse sein. Ein solcher, in der Verwaltung angesiedelter WWW-Service muß selbstverständlich bestimmten Sicherheitskriterien genügen, da die angebotenen Daten nicht jedermann zugänglich sein dürfen.

Für NT sind von verschiedenen Anbietern Webserver verfügbar, so von *Netscape*, *Oracle* und *Microsoft*. Getestet wurde im Rahmen dieses Projekts der *Internet Information Server (IIS) Vers. 1.0* von *Microsoft*. Neben WWW bietet der IIS auch einen FTP und Gopher Server, die alle mit einem gemeinsamen Tool, dem *Internet Dienstmanager*, konfiguriert und verwaltet werden können. Es ist ohne weiteres auch möglich, netzwerkweit mehrere solcher Services zu verwalten.

Sehr angenehm fällt auf, daß sich der IIS nahtlos in das NT Sicherheitskonzept einfügt. Unter diesem Aspekt untersucht wurden der FTP und WWW Service; wegen seiner schon heute geringen Bedeutung wurde Gopher außer acht gelassen.

Sowohl FTP wie WWW lassen sich im IIS entweder für anonymen oder authentisierungspflichtigen Zugriff konfigurieren. Im ersten Fall wird der Zugang zu den vorgesehenen Verzeichnisstrukturen dann über einen besonderen Gastaccount abgewickelt, dessen zugeordnete Berechtigungen ausschlaggebend dafür sind, was der anonyme Benutzer mit den Dateien machen darf, etwa neben Lesen auch Ändern o.ä. Beim authentisierungspflichtigen Zugang muß der Benutzer sich grundsätzlich mit Username und Paßwort identifizieren, wobei hierzu das normale NT Domänenkonto mit allen zugeordneten Privilegien verwendet wird. Mit einem neueren Webbrowser wie *Microsofts Internet Explorer* oder dem *Netscape Navigator* kann die Paßwortübermittlung auch verschlüsselt erfolgen, während etwa ein Standard FTP Programm dazu nicht in der Lage ist. Die Nutzung eines nicht anonymen FTP Dienstes auf einem NT Server ist deswegen genauso ein Security-Problem wie ein Telnet Server unter NT, da hier alle Sicherheitsvorkehrungen von NT bei der Authentisierung konterkariert werden. Für anonyme Dienste gilt das nicht in gleichem Maße, da diese ja über ein und dasselbe Konto mit ohnehin nur minimaler (Lese-)berechtigung abgewickelt werden. Mit dem IIS läßt sich ohne weiteres in Universitätsverwaltungen ein zugriffsgeschütztes Konteninformationssystem realisieren.

Alle Zugriffe auf den IIS können mitprotokolliert werden, entweder in der üblichen Form einer ASCII-Datei oder in einer SQL-Datenbank, womit nicht nur aussagekräftige Statistiken erstellt, sondern ein zusätzliches, allerdings nicht besonders gewichtiges, Kontrollinstrument zur Verfügung steht.

Die mit WWW oder FTP angebotenen Verzeichnisstrukturen lassen sich durch *Aliasing* nach Belieben aus verstreuten Verzeichnissen zusammensetzen, die auch auf anderen Servern liegen dürfen. Diese „Links“ werden aber, anders als im UNIX, im Directory nicht angezeigt, obwohl sie durch ein „cd“-Kommando ohne weiteres angesprochen werden können; eine Unschönheit gerade für den FTP Server. Ein akzeptables Workaround ist das Anlegen eines leeren Verzeichnisses mit dem Namen des entsprechenden Alias. Aus sicherheitstechnischen Überlegungen ein echter Bug ist die Möglichkeit, die für die Dienste vorgesehenen Verzeichnisse zu verlassen und Zugang zu übergeordneten oder nebengeordneten Verzeichnissen zu erlangen. Auch hier gelten natürlich immer die Berechtigungen des Kontos, unter dem der Zugang gerade abgewickelt wird, aber eine potentielle Sicherheitslücke ist das trotzdem. Mit einem Servicepack für die Version 1.0 des IIS soll das Problem behoben sein.

Der Zugang zu den Diensten des IIS läßt sich darüber hinaus nicht nur nach Benutzern sondern auch nach IPs und kompletten Subnetzen limitieren (etwa: anonyme Zugriffe nur von Maschinen aus dem eigenen Subnetz).

In der Version 4.0 von NT Server wird der im Augenblick noch kostenlos als Zusatzprodukt installierbare IIS integriert sein. Damit dürfte er zumindest unter dem Kostenaspekt die Konkurrenz aus dem Felde schlagen. Sofern *Microsoft* den IIS von Bugs befreit, ist er wegen seiner einfachen Handhabung und der Integration in die NT Sicherheit durchaus auch für den Einsatz in Verwaltungen mit ihren besonderen datenschutzrechtlichen Anforderungen geeignet.

5.6.2. Mail

Die Zurverfügungstellung eines Email-Dienstes muß heute unter jedem modernen Betriebssystem eine Selbstverständlichkeit sein. NT bildet hier keine Ausnahme, bringt dabei aber leider einen eigenen Mailstandard mit, der nicht internettauglich ist. Das Microsoft Mailsystem arbeitet mit einem serverseitig angesiedelten Arbeitsgruppen-Postoffice, dessen Namensgebung schon auf den eher für kleinere Corporate Networks gedachten Einsatz hindeutet. Wie andere bei NT mitgelieferte Tools, ist das Microsoft Mail gleichfalls eine Minimallösung, die für den weltweiten Email-Versand ungeeignet ist und für die ernsthafte Verwendung im universitären Umfeld nicht empfohlen werden kann.

Microsoft selbst bietet hier mit dem *Exchange Server* eine bessere Lösung an, die einerseits zum eigenen Standard kompatibel ist und andererseits einen *Internet Mail Connector* für SMTP-basierte Mailsysteme enthält. Dadurch könnte ein NT Exchange Server auch von Clients unter MacOS und UNIX verwendet werden.

Sofern bereits ein gut funktionierendes SMTP Mailsystem betrieben wird, zum Beispiel an zentraler Stelle vom Universitätsrechenzentrum, macht es nur dann Sinn, hier eine eigene NT Lösung aufzubauen, wenn eine zusätzliche Funktionalität gewünscht wird, so etwa die Integration eines Faxdienstes oder die Nutzung des Microsoft Office Programms *Schedule*, mit dem die gemeinsame Terminplanung bzw. Terminabstimmung aller am Netz teilnehmenden Benutzer möglich ist.

6. Kostenaspekte

Die zur Zeit und in der absehbaren Zukunft eher knapp bemessenen öffentlichen Mittel erfordern auch bei der Beschaffung von EDV-Systemen für universitäre Einrichtungen ein verstärkt an Wirtschaftlichkeits- und Kostenkriterien orientiertes Denken: Das Problem, nämlich die EDV-gestützte Abwicklung laufender Arbeiten, soll mit dem geringstmöglichen Aufwand an Kosten für Material und Personal gelöst werden.

Im einzelnen lassen sich folgende Kostenkategorien ausmachen:

- Reine Hardwarekosten für Server, Clients, Netzinfrastruktur etc. Diese Kosten fallen typischerweise zu Beginn als Investitionskosten an, aber u.U. auch später bei Erweiterungen und Reparaturen.

- Pflege- und Supportkosten, etwa für Softwareupdates und Dienstleistungen seitens der Hersteller bzw. Vertriebspartner.

- Reine Softwarekosten für Betriebssysteme, Serveranwendungen und Benutzerapplikationen.

- Personalkosten für Schulungen und die Aufrechterhaltung des normalen Rechenzentrumsbetriebs.

In der breiten Diskussion wird gerade der Kostenaspekt als ein starkes Argument *für* den Einsatz von NT genannt. Dabei wird ein Vergleich, etwa mit UNIX, leider oftmals unter unpassenden Voraussetzungen geführt. So kommen in einem UNIX-System in der Regel hochwertige Server und Terminals von Markenherstellern (*Sun*, *HP*, *NCD*,...) zum Einsatz, die von den Investitionskosten her die in NT-Systemen nicht selten verwendeten Noname-Geräte bei weitem übertreffen. Allerdings bieten sie dann eine höhere Qualität und damit Ausfallsicherheit sowie einen vom Hersteller über kostenpflichtige Wartungsverträge realisierbaren Support mit kurzen Reaktionszeiten, wie sie für den professionellen Bereich und Produktionssysteme unverzichtbar sind; ebenso ist in der Regel die längerfristige, dann aber teurere, Versorgung mit Ersatzteilen gewährleistet, während dies bei Noname-Systemen eher Glückssache ist. Ein Kostenvergleich von NT mit anderen Systemen (vor allem UNIX) muß daher unbedingt auf der Basis äquivalenter Hardware bezüglich Qualität und Leistung vorgenommen werden. Die Vielfalt der auf dem Markt verfügbaren Systeme in unterschiedlichsten Konfigurationen macht es unmöglich, an dieser Stelle konkrete Zahlen zu nennen, die wirklich realistisch sind.

Da NT wegen seiner recht guten Abwärtskompatibilität sehr viel näher am Massenmarkt plaziert ist als UNIX, sind die Lizenzkosten zumindest für gängige Standardapplikationen, Serverdienste und das Betriebssystem vergleichsweise niedrig, womit sich, unter Berücksichtigung der Aufrechterhaltung bzw. Verbesserung der angebotenen Funktionalität, durch den Einsatz von NT die reinen Softwarekosten in vielen Fällen senken lassen. Für Spezialanwendungen gilt dies allerdings nicht. Für den individuellen Fall sollte ein Anforderungsprofil bzw. Pflichtenheft erstellt werden, auf dessen Basis Vergleichsangebote zwischen NT und UNIX bzw. Novell (den beiden nennenswerten Konkurrenten) eingeholt werden.

Novellsysteme arbeiten auf derselben Hardwareplattform wie NT, so daß ein Vergleich sich hier, bei ansonsten gleichen Ansprüchen an die Hardware, vor allem auf die Merkmale des Betriebssystems selbst beziehen muß. Beim geplanten Einsatz von Novell sollte allerdings immer berücksichtigt werden, daß es sich hier um ein reines Netzwerkbetriebssystem handelt, das in einem PC-Netz Print- und Fileressourcen zur Verfügung stellt; es ist dann immer noch die Wahl des Clientbetriebssystems zu treffen: Win3.x ist ganz klar veraltet und sollte für ein neu einzurichtendes System keine Verwendung mehr finden, da es weder von der Stabilität noch der Leistung und dem Zugriffsschutz her heutigen Anforderungen genügt; ähnliches gilt für Win95, das nach allgemeiner und realistischer Einschätzung nur einen Zwischenschritt darstellt, obgleich es zur Zeit als Clientbetriebssystem durchaus noch geeignet erscheint. Auf mittlere oder längere Sicht geht die Entwicklung von PC-Betriebssystemen aber ganz klar in Richtung des sehr stabil laufenden und modern konzipierten NT, dessen Vorteil für den Verwaltungsbereich gerade auch in seinem besseren Schutz vor unberechtigtem Zugriff auf die Datenbestände liegt. Nur, wenn man schon NT auf den Clients einsetzt, warum sollte dann die Wahl für die Server auf Novell fallen? Erstens bietet Novell keine Vorzüge gegenüber NT, die man unbedingt haben müßte, noch läßt es eine ähnliche Entwicklungsdynamik erkennen. Lediglich die breite installierte Basis und das oftmals bereits bei den Administratoren vorhandene Know How sprechen für dieses System.

Der Einsatz von NT, besonders von NT Server, erfordert zunächst gewiß eine Einarbeitung und Schulung der Administratoren, aber auch der Benutzer. Dies gilt selbstverständlich allgemein für die Einführung neuer Systeme. Der Aufwand bei der Mitarbeiterschulung fällt dann besonders gering aus, wenn früher schon mit Win3.x gearbeitet wurde, da NT sich hier mit derselben Oberfläche (ab Vers. 4.0 mit der Win95 GUI) präsentiert und auch die Standardapplikationen gleich zu bedienen sind. Ganz anders sieht dies aus, wenn die Mitarbeiter früher an Terminals gearbeitet haben; dann ist mit höherem zeitlichen und finanziellen Aufwand für die Schulung zu rechnen. Auf der administrativen Seite stellt sich ebenfalls die Frage nach dem bereits vorhandenen Know How. So ist sicher die Neueinweisung eines UNIX-Administrators etwas aufwendiger als bei NT, aber gerade an Universitäten bestehen meist schon langjährige Erfahrungen im Umgang und dem Betrieb von UNIX-Systemen, während

NT meist Neuland ist. Der mühselige Prozeß des erstmaligen Aufbaus von Know How mag durch die bei NT-Systemen relativ geringe laufende Administration aufgewogen werden, die in der Regel (bei hinreichend homogenen Hard- und Softwareumgebungen) weniger personalintensiv ist.

Eine Domäne für UNIX konnte von NT allerdings bislang nicht eingenommen werden: Für Highperformance-Datenbanken stellt UNIX zur Zeit noch die bessere Plattform dar. Vermutlich wird NT hier in absehbarer Zeit gleichziehen; die Multiprozessorsysteme und Clusterlösungen einiger Hersteller deuten in diese Richtung, liegen dann aber auch preislich auf dem UNIX-Niveau.

Abkürzungsverzeichnis

BDC	Backup Domain Controller
bzw.	beziehungsweise
etc.	et cetera
ggf.	gegebenenfalls
GUI	Graphical User Interface
i.d.R.	in der Regel
i.a.	im allgemeinen
LAN	Local Area Network
o.ä.	oder ähnliches
PDC	Primary Domain Controller
s.d.	siehe dort
SMS	Systems Management Server
u.ä.	und ähnliches
u.U.	unter Umständen
WAN	Wide Area Network
WINS	Windows Internet Name Service
z.Bsp.	zum Beispiel

Abbildungsverzeichnis

Universitätsrechenzentrum
Universität Ulm

Oktober 1996