Einführung in Windows 2000

Martin Werthmöller <mw@werthmoeller.de>

2. Dezember 2001

Copyright ©

Inhaltsverzeichnis

Teil I

Installation des Systems

Kapitel 1

Installation von W2K

1.1 Hardwareanforderungen

Um auf einem Rechner W2K zu installieren, bzw. diesen auf W2K zu aktualisieren muß zuerst überprüft werden, ob der Rechner der *Hardware Compatible List* (HCL) genügt. Eine weitergehende Überprüfung ist möglich, in dem auf dem upzugradenden Rechner das Setup-Programm `winnt32` mit dem Parameter `/checkupgradeonly` aufgerufen wird. Mit diesem Aufruf generiert das Programm einen Report, der auf etwaige Inkompatibilitäten hinweist. Falls vor dem Kauf einer Windows 2000 Lizenz entschieden werden soll, ob ein Upgrade möglich ist, kann auch das *Readiness Analyzer Tool* von der Microsoft Homepage heruntergeladen werden, mit dem die Tests ausgeführt werden können.

Windows 2000 benötigt minimal die folgende Hardware:

- i586 CPU,
- 32 MB Ram, 64 MB Ram empfohlen,
- 665 MB Festplattenplatz (W2K Workstation), 2 GB empfohlen

Bei der Kalkulation des Plattenplatzes ist zu beachten, daß bei einer Installation von einem Netzwerk-Share für temporären Dateien zusätzlich etwa 100 - 200 MB benötigt werden. Eine Partition, die mit FAT16 formatiert wurde, arbeitet mit 16 kB Blöcken, so daß im Mittel ca. 20 % des Plattenplatzes nicht genutzt wird. Dagegen arbeitet eine FAT32 Partition hier mit 4 KB Blöcken und ein NTFS Filesystem bei einer Partitonsgröße von 1 GB mit 1 KB Blöcken.

1.1.1 Max. Unterstützte Hardwareressourcen

Die unterschiedlichen Windows 2000 Versionen unterstützen maximal die folgenden Hardwareressourcen:

Version	RAM	Prozessoren
Professional	4 GB	2
Server	4 GB	4
Advanced Server	8 GB	8
Datacenter Server	64 GB	32

1.2 Aktualisierung auf W2K

Um ein bestehendes System auf W2K upzudaten können bzw. müssen je nach dem ursprünglichem System und dem System auf das upgedatet wird, verschiedene Updatepfade beschritten werden.

1.2.1 Update von Clientmaschinen

Für das Update von Clientmaschinen sollten folgende Updatepfade gewählt werden:

Windows 95 oder 98 Akutalisierung auf Windows 2000 Professional,

NT Workstation 3.51 oder 4.0 Akutalisierung auf Windows 2000 Professional.

Windows f. Workgroups 3.11 *Zuerst* auf NT 3.51 oder NT 4.0 akutalisieren, dann auf Windows 2000 Professional upzudaten.

Windows 3.1 Kann nicht direkt auf Windows 2000 Professional upgedatet werden, zuerst auf Win 9x updaten, dann auf W2K Workstation.

Für ein Update von Windows NT 3.51/4.0 Workstations auf Windows 2000 sollte die Datei `dosnet.inf` so konfiguriert werden, daß ein Update verweigert wird falls hinsichtlich der Hard- oder Software Inkompatibilitäten zu Windows 2000 bestehen.

1.2.2 Update von Servermaschinen

Das Update von Servern auf die W2K Serverserie erfolgt mit den folgenden Schritten:

PDC oder BDC unter NT 4.0 oder 3.51 Kann direkt auf W2K Server oder W2K Advanced Server in der Funktion eines Domänencontrollers aktualisiert werden.

Mitgliedsserver unter NT 4.0 oder 3.51 Mitgliedsserver unter W2K Server oder W2K Advanced Server.

Rechner unter NT 3.1 oder NT 3.5 Server Zuerst auf NT Server 3.51 bzw. NT Server 4.0, dann Aktualisierung auf W2K Server oder W2K Advanced Server.

Viele Maschinen die noch unter NT 3.1 oder NT 3.5 laufen sind in der Regel nicht mit ausreichenden Hardwareressourcen ausgestattet.

Ein Update von NT 4.0 Maschinen kann sehr einfach über das Netzwerk erfolgen, indem das Verzeichis */i386* auf den Server kopiert und freigegeben wird. Auf den Clientmaschinen wird sich jetzt mit hier gültigen lokalen Administratorrechten mit dem freigegebenen Verzeichnis auf dem Server verbunden und die Datei `winnt32` ausgeführt.

1.3 Möglichkeiten der Installation

W2K bietet mehrere Installationsmethoden an:

- CD
- Diskette
- Netzwerk
- Festplattenduplizierung
- Remote Installation (RIS)

Die Installationen können auch ohne manuelle Eingriffe automatisiert durchgeführt werden (unattendet Installation, s. Kap. 1.7).

Falls während der Installation oder eines Upgrades auf Windows 2000 eine Viren- Warnung erscheint, sollten alle Virenscanner von diesem Rechner entfernt werden und auch BIOS-Virenüberwachung deaktiviert werden. Bei der Installation schreibt das Installationsprogramm auf den Bootsektor, was von der BIOS-Virenwarnung erkannt wird (und eventuell verhindert wird). Ein Virenscanner verhält sich ähnlich. Er kann auch eine Fehlermeldung ausgeben, wenn er nicht für Windows 2000 entwickelt wurde, so daß er einen Fehlalarm ausgibt. Hier sollte der Virenscanner entfernt werden und eine für diese Windows-Version entwickelte Virenscannerversion angeschafft werden.

1.4 Installation von CD oder Diskette

Die Installations-CD ist Bootfähig nach dem *El-Torito-Standard*. Falls das CD-Rom Laufwerk bzw. das Bios des Rechners das Booten von CD nicht unterstützt, sollte der Zugriff unter DOS mit entsprechenden CD-Rom Treibern möglich sein. Die Installation kann jetzt vom Verzeichnis `i386` auf der CD durch Aufruf des Programms `winnt` gestartet werden. Sollte es Problemen unter W2K mit dem Zugriff auf das CD-Rom Laufwerk geben, ist alternativ auch das Kopieren des kompletten Verzeichnisses `i386` mittels `xcopy` auf die Festplatte möglich, so daß die Installation von hier gestartet werden kann.

Disketteninstallation

Für die Installation mittels Disketten werden 4 leere Disketten benötigt. Diese werden zum Booten des Rechners mit Zugriff auf das CD-Rom Laufwerk präpariert, indem das Programm `bootdisk\mkboot` von der CD aufgerufen wird.

Festplattentausch

Eine weitere Installationsoption ist die Vorbereitung einer Festplatte in einem anderen Rechner, die dann in die eingentliche zur Installation vorgesehene Maschine eingebaut wird. Hier wird die Festplatte zuerst in einen Rechner eingebaut, auf dem schon ein Win32-System läuft. Jetzt wird von der CD-Rom das Programm `winnt32` mit dem Parameter `/SYSPART:`*Laufwerk* aufgerufen. Die Angabe Laufwerk nennt den Laufwerksbuchstaben der Platte, die nachher in den neu zu installierenden Rechner eingebaut wird.

Die Installationsdateien werden komplett in ein temporäres Verzeichnis auf die neue Platte kopiert. Dann wird die Platte soweit vorbereitet, daß sie bootfähig ist (Partition aktiv schalten und Bootdateien übertragen) und kann dann in den neuen Rechner eingebaut werden. Dieser bootet direkt in das Setupprogramm, so daß Windows 2000 direkt installiert werden kann.

1.5 Installation über das Netzwerk

Zur Vorbereitung der Installation über das Netzwerk müssen die Installationsdateien auf einem Server in ein freigegebenes Verzeichnis kopiert werden, oder die CD auf dem Server direkt freigegeben werden. Der zu installierende Rechner muß die Möglichkeit bieten, auf eine (Windows-) Freigabe eines Windows- oder Samba-Servers zugreifen zu können. Nachdem sich der lokale Rechner mit der Freigabe verbunden hat, kann die Installation gestartet werden.

1.6 RIS

Mit Hilfe der Remoteinstallationsservices (RIS) können Kopien von W2K von einem zentralen Server aus auf alle Rechner im Netzwerk installiert werden. Von RIS werden CD-basierte und von RIPrep erstellte Festplattenimages unterstützt.

Zuerst wird eine Mutterinstallation mit allen gewünschten Programmen und der passenden Konfiguration auf einem Rechner vorgenommen. Dann wird mit Hilfe der entsprechenden Verwaltungstools (RIPrep) ein Diskimage dieses Rechners erstellt.

Der Clientrechner muß hierfür mit einer PXE kompatiblen Netzwerkkarte ausgerüstet werden. Diese NIC enthält ein entsprechend programmiertes

BOOT-Rom. Mit Hilfe des Tools `rbfg.exe` läßt sich die überprüfen, ob die Netzwerkkarte zu den RIS-Services kompatibel ist. Ein mit einer nicht PXE kompatiblen Netzwerkkarte kann unter Umständen mit Hilfe einer speziellen Startdiskette gebootet werden. Diese Diskette simuliert den Bootprozeß einer PXE-Netzwerkkarte und kann mit dem Utility *Remote Boot Disk Generator*
(`\\RIS_server\reminst\admin\i386\rbfg.exe`)
erstellt werden. Dieses Tool unterstützt eine Reihe von Netzwerkkarten, die mit Hilfe der Diskette für RIS genutzt werden können. Die so erstellte Diskette ist nicht an den speziellen Netzwerkkartentyp gebunden, für den sie erstellt wurde.

1.6.1 Installation über das Netzwerk

Die einzige über das Netz installierbare Version von Windows 2000 ist die Professional (Workstation) Version.

Der Installationsvorgang läuft wie folgt ab:

1. Beim Start generiert die Netzwerkkarte einen Broadcast um von einem DHCP-Server (s.a. **??**) eine IP-Adresse zu erhalten.

2. Nach Erhalt einer IP-Adresse wird der RIS (Remote Installation Services) Service auf dem DHCP-Server angesprochen.

Alternativ ist auch die Installation mit Hilfe einer Bootdisk möglich. Allerdings muß diese unter WinNT 4.0 erstellt werden. Auf dieser Diskette müssen die Dateien `a:\autoexec.bat` und `a:\net\system.ini` angepaßt werden:

```
[User Data]

Product ID = xxxx xxxx ...
```

Die Produkt-ID darf laut Lizensierungrichtlinien von MS für alle Installationen gleich sein. Allerdings müssen natürlich die Lizenzen für alle Installationen vorhanden sein ;-).

1.6.2 Festplattenduplizierung mit SYSPREP

Die Duplizierung spiegelt die Festplatte des Quellsystems, bietet allerdings Möglichkeiten für die Berücksichtigung von PNP-Geräten. Diese Installationsoption ist vor allem bei Installation einer Reihe ähnlicher Systeme äußerst schnell. Allerdings erfordert die Methode auf dem Mastersystem einige Vorarbeiten zur Vorbereitung des Quellsystems sowie Nacharbeiten auf dem geklonten System zur individuellen Anpassung.

Zunächst wird der Rechner mit der Referenzinstallation wird normal installiert und konfiguriert. Allerdings darf er keiner Domäne zugeordnet werden, somit darf auch kein Active Directory laufen. Jetzt wird das Quellsystem mit dem Tool `sysprep.exe`
(aus `INSTALL-CD\support\tools\deploy.cab`)
auf die Duplizierung vorbereitet. Sysprep verändert das Muttersystem so, daß es beim nächsten Aufruf ein kleines Installationsprogramm startet, daß einige rechnerspezifische Parameter wie Admin-Password und Hostname abfragt und konfiguriert. Die so vorbereitete Festplatte kann nun in ein anderes System eingebaut werden, oder – was wohl die häufigste Nutzung ist – mit Hilfe von Tools zur Erstellung eines Festplattenimages (z.B. *Ghost* von der Fa. Symantec oder *Drive Image* von der Fa. Powerquest) als komplettes Image auf ein anderes System kopiert werden.

Beim Start dieses Rechners wird das kleine von `sysprep` erstellte Installationsprogramm ausgeführt. Dieses fragt wie oben beschrieben einige Konfigurationseinstellungen ab und generiert zusätzich eine einmalige *SID* (Security-ID), unter der der Rechner gegenüber anderen im Netzwerk auftritt.[1]

Die Hardware der Rechner auf denen das mit Sysprep vorbereitetet Image installiert werden soll, muß nur hinsichtlich des *HAL* (Hardware Abstraction Layer) gleich dem Rechner sein, der die Masterkopie erstellte. Dieses bezieht sich vor allem auf die folgenden Punkte:

- IDE- oder SCSI Festplattentreiber
- Standard- oder Multiprozessorsystem
- ACPI (Advanced Configuration and Power Interface, s. a. 27.0.6)

1.7 Unattended Installation

Die Installation von W2K läßt sich auch automatisiert durchführen. Hier liest das Installationsprogramm die Antworten auf Fragen während des Installationsvorgangs aus einer Textdatei. Diese Datei enthält nach Sektionen

[1] Die Security-ID identifiziert einen Windows-Rechner im (Windows-) Netzwerk eindeutig und muß daher garantiert einmalig sein. Bei mehreren gleichen SIDs könnte es zu Problemen kommen. Wenn nur ein einfaches Cloning der W2K Platte mit Hilfe eines Imaging-Tools ohne vorherige Vorbereitung durch `sysprep` durchgeführt wird, ist die SID nicht mehr eindeutig.
Man sollte sich über die Folgen und Möglichkeiten der eindeutigen Identifizierbarkeit des Rechners mit Hilfe der SID im Internet im klaren sein. In der Vergangenheit speicherte die Firma Microsoft "unabsichtlich" diese Daten ihrer Kunden (Stichwort: GUID Global Unique Identifier in MS-Office Dateien)

geordnete *Key - Value* Paare.[2]

Die Antwortdatei kann mit Hilfe des *Setup-Managers* erstellt werden. Er ist auf der W2K CD im Verzeichnis `Support\Tools` in der Datei `deploy.cab` zu finden. Mit Hilfe des *Setup-Managers* (setupmgr.exe) können Antwortdateien für die Installationsarten

- Unattendet Installation von Windows 2000
- Sysprep Installation
- Remote Installation Services (RIS)

erstellt werden.

Für unbeaufsichtigte Installation muß die Anwortdatei so gestaltet werden, daß alle Recherspezifischen Fragen automatisiert beantwortet werden. Hierzu ist in der Anwortdatei eine Sektion `[Data]` zu erstellen, die `Parameter = Value` einträge für diesen Rechner enthält. Auch im *Setup-Manager* läßt sich der Level einstellen, wie detailliert nach Parametern gefragt wird. Im Fenster mit zur Einstellung des Interaktionslevels stehen 5 Optionen zur Auswahl:

Provide defaults Hier wird der User gefragt, ob und wie der die in der Antwortdatei festgelegten Voreinstellungen ändern will.

Fully automated Bei der vollautomatischen Einstellung läuft des Setup vollautomatisch durch. Der User bekommt keine Möglichkeit die Parameter zu ändern.

Hide Pages Alle mit dem Setup-Assistenten erstellten Voreinstellungen der Antwortdatei können vom User nicht geändert werden.

Read only In der *nur lesen* Einstellung darf der User die Voreinstellungen sehen, kann diese aber nicht ändern. Falls für spezielle Einstellungen keine Voreinstellungen abgelegt wurden, können diese allerdings manuell eingegeben werden.

GUI attended Hier werden dem User nur während der grafischen Setupphase Fragen gestellt.

Installation per Diskette

Eine Installation mit Hilfe der Disketten, die vom Programm `makeboot.exe` der Installations-CD erstellt wurden, ist *nur* im Interaktiven Modus möglich.

[2]Eine genaue Beschreibung dieser Schlüssel ist in der Datei `unattended.doc` enthalten, die sich auf der Windows 2000 CD in der Archivdatei `support\tools\deploy.cab` befindet.

Um einen unbeaufsichtigte Installation durchführen zu können muß zuerst eine geeignete und angepasste Bootdiskette erstellt werden. Dieses ist nur mit Win9x oder NT4 möglich. Die Installation kann mit Hilfe der Bootdiskette über das Netzwerk oder von CDRom erfolgen. Für jede der beiden Alternativen muß die Startdiskette entsprechende Treiber bereithalten und installieren.

Installation per CD

Für eine unbeaufsichtigte Installation von CD müssen die Rechner in der Lage dazu sein von CD zu booten. Die Antwortdatei für eine unbeaufsichtigte Installation von CD wird als `winnt.sif` auf einer Diskette abgespeichert. Sie wird beim Start der Installation ohne vorherige Abfrage gesucht; die Diskette muß also nach dem Beginn des Bootvorgangs von CD in das Laufwerk eingelegt werden. Die Antwortdatei kann mit Hilfe des Setup-Managers `setupmgr.exe` erzeugt werden, in dem hier beim Speichern die Option zur Installation von CD gewählt wird.

Für eine unbeaufsichtigte Installation eines Rechners, der von Diskette oder von der Festplatte gebootet hat, wird das Setupprogramm mit einem passenden Parameter und dem Pfad zur Antwortdatei aufgerufen:
`winnt32 /unattend:` *Antwortdatei* (unter Win32)
`winnt /U:` *Antwortdatei* (unter DOS)

Innerhalb einer Batch-Datei kann der Aufruf wie folgt automatisiert werden:

```
set AnswerFile=.\unattend.txt
set SetupFiles=f:\i386

f:\i386\winnt /s:%SetupFiles% /unattend:%AnswerFile%
```

Weitere Kommandozeilenparameter für beide Programme sind in 26.8 aufgeführt.

Ein Beispiel einer Antwordatei ist auf Seite 20 aufgelistet. Zur automatisierten Installation weiterer Software kann der Parameter `OEMPreinstall = Yes` in der Sektion [Unattended] der Antwortdatei genutzt werden. Wenn dieser aktiviert ist, im Distributionsverzeichnis der Installationsdateien (z.B. eine Freigabe im Netz) nach dem Verzeichnis OEM gesucht. Die Dateien aus diesem Verzeichnis werden in ein temporäres Verzeichnis auf dem Zielcomputer kopiert. Wird im Verzeichnis OEM eine Datei mit dem Namen `cmdlines.txt` plaziert, werden die hier aufgeführten Befehle direkt nach der Installation ausgeführt. Mit Hilfe dieser Einstellung läßt sich die Installation weiterer Software automatisieren.

UDF-Dateien

In einer Antwortdatei sind die allgemeinen Einstellungen festgelegt, die ein System bei der Installation abfragt und die für alle Rechner gleich sind. Die Parameter, die für den einzelnen Computer gültig sind, wie z.B. der Computername werden in einer sogenannten *UDF*- Datei abgelegt. Bei Nutzung einer UDF-Datei wird das Setupprogramm mit dem Schalter `/udf` und folgender Syntax aufgerufen:
`winnt /unattended:unattended.txt /udf:SEKTION,unattended.udf`
Der Eintrag SEKTION verweist auf einen Sektion in der UDF-Datei, deren Paramter diejenigen der Datei `unattended.txt` überschreiben.

Eine *Uniqeness Database File (UDF)* für die Installation eines W2K Rechners ist wie der Name schon sagt, einzigartig. Sie muß für jeden Computer einzeln angepaßt werden, da sie z.B. auch den Computernamen enthält. Wenn bei der Installation mehrerer Rechner z.B. die Eingabe für den Computernamen manuell erfolgen soll, alle anderen Angaben ansonsten gleich sind, wird keine *UDP* Datei benötigt.

UDF-Dateien können mit `winnt.exe` und `winnt32.exe` genutzt werden. Die Nutzung einer UDF-Datei bei einer Installation mit einer bootfähigen W2K Installations-CD ist nicht möglich, diese Methode nur für die Installation eines einzelnen Rechners möglich ist.

Kapitel 2

Konfiguration von W2K

2.1 Hardware

Die Installation und Konfiguration von Hardwaregeräten kann unter W2K weitgehend automatisch durchgeführt werden. Die Plug and Play Implementierung arbeitet mittlerweile einigermaßen zuverlässig. Die einzelnen Hardwarekomponenten lassen sich lassen sich im Gerätemanager unter `Systemsteuerung-System-Hardware` konfigurieren, falls es dennoch Probleme gibt. Hier läßt sich ein Gerät per Software deaktivieren, so daß der Gerätetreiber beim nächsten Sytemstart nicht mehr geladen wird. Dieses wird z.B. benötigt wenn eine Komponenten nicht physikalisch aus dem Computer entfernt werden kann oder soll. Der Treiber bleibt in diesem Fall allerdings auf der Festplatte, so daß er bei Bedarf ohne Neuinstallation wieder aktiviert werden kann.

Plug and Play Komponenten

Bei Plug and Play Hardware wird der Treiber automatisch vom System gelöscht, wenn die Komponente ausgebaut wurde. Falls der Treiber einer solchen Hardware manuell gelöscht wurde, die entsprechende Komponente jedoch nicht ausgebaut wurde, erkennt das System beim nächsten Start das Fehlen der Treiber und fordert den Benutzer auf, diese zu installieren. Aus diesem Grunde sollte das Gerät auch nur per Gerätemanager deaktiviert werden, falls es im System verbleiben soll (oder nicht entfernt werden kann), die Treiber aber nicht geladen werden dürfen.

Nicht Plug and Play fähige Komponenten

Die Einstellungen für nicht Plug and Play fähige Geräte sind im Gerätemanager standardmäßig ausgeblendet. Um diese Einstellungen zu erreichen, muß der Menüpunkt `Ausgeblendete Geräte anzeigen` (`Show Hidden Devices`) angewält werden. Hier können dann bei Bedarf die entsprechenden Einstellungen für diese Geräte konfiguiert werden. Der Treiber kann auf der je-

weiligen Registerkarte gestartet oder gestoppt werden. Unter dem Punkt `Starten` kann der Treiber *deaktiviert* werden oder eine andere Startart wie z.B. (Start, Automatisch, System, Bedarf) gewählt werden.

2.2 Grafikkarten und Monitore

ISA-Grafikkarten werden definitiv *nicht* mehr unterstützt. Mit Hilfe der Multiheadfähigkeiten können mehrere Grafikkarten im Rechner angesteuert werden, von denen eine dieser Karten als primäre definiert wird. Die Bildschirmausgabe erfolgt auf diesen Monitor. Danach kann sie auf einen anderen Monitor geschoben werden. Die verschiedenen Monitore können mit Hilfe der Eingenschaften der Anzeige so eingestellt werden (drag and drop), daß die Reihenfolge hier der Reihenfolge der Monitore auf entspricht.

2.2.1 Hardwareprofile

Das nächste zu benutzende Hardwareprofil (s.a. 9.1) läßt sich nur als angemeldeter User einstellen, der Mitglied der Gruppe *lokale Administratoren* (also mit Admin-Rechten an der Maschine) ist. Eine Vorauswahl beim Bootvorgang ist *nicht* möglich. Die Einstellungen für das einzelne Hardwareprofile erfolgen unter `Systemsteuerung - System - Hardware`. Hardwareprofile werden bei Laptops, die z.B. temporär per Dockingstation genutzt werden gebraucht oder falls ein stationärer Rechner für verschiedene User unterschiedliche Hardwaregeräte nutzen können soll.

Teil II

Aufbau des Systems

Kapitel 3

Datenträger und Filesysteme

3.1 Datenträger

Mit W2K ist Hot-Plugging und Swapping von Festplatten mit entsprechender Hardware möglich. In W2K werden in der Regel immer noch Laufwerksbuchstaben vergeben. Die Vergabe richtet sich nach den Festplattenpartitionen und nach der Festplattenzuordnung am Controller.

1. Festplatten durchnummerieren,
2. pro Festplatte *Partitionen* durchnummerieren,
3. pro Festplatte bekommt die 1. primäre Partition einen Laufwerksbuchstaben,
4. pro Festplatte werden die Partitionen nacheinander durchnummeriert.

3.1.1 Zuordnung von Partitionsnummern

Die Partitionsnummern werden je Festplatte vergeben. Sie werden zugeordnet indem

1. Die *primären* Partitionen zuerst nacheinander nummeriert werden (max. 1-4).
2. Danach werden die sogenannten *logischen Laufwerke* in der erweiterten Partition durchnummeriert. *Achtung! Die erweiterte Partition selbst bekommt KEINE eigene Partitionsnummer.*

3.1.2 Zuordnung von Laufwerksbuchstaben

Die Laufwerksbuchstaben werden nach einem anderen Muster als die Partitionsnummern vergeben. Windows NT 4 und W2K ordnen die Laufwerksbuchstaben den Partitionen wie folgt zu:

1. Zuerst wird der 1. primäre Partition jeder physikalischen Platte nacheinander ein Laufwerksbuchstabe zugeordnet.
2. Dann werden den primären und logischen Partitionen jeder Platte Laufwerksbuchstaben zugeordnet. Die Zuordnung erfolgt also zuerst *komplett* auf der ersten Festplatte am ersten Controller, dann an der zweiten Festplatte, etc.
3. Dann werden die Buchstaben für weitere Festplatten vergeben.

3.2 dynamische Festplatten

W2K bietet zudem die Möglichkeit sogenannte dynamische Festplatten (dynamische Speicherung) zu erstellen. Hier wird auf der gesamten Festplatte eine Partition erstellt, die als *dynamische Festplatte* bezeichnet wird. Windows NT kann auf solches logisches *Volume* nicht zugreifen. Die dynamische Festplatte kann in mehrere Datenträger unterteilt werden. Diese können sich über mehrere Bereiche (Partitionen) einer oder mehreren physikalischen Festplatten erstrecken. Die dynamischen Datenträger werden also in der Ebene über den Partitionen angesprochen, so daß der Zugriff auf die Hardware und die Partitionen wird vom System koordiniert wird und für den Anwender völlig transparent erfolgt. Die Technik des dynamischen Datenträgers stellt also quasi ein eigenes Filesystem dar, welches unabhängig von Partitionstabellen arbeitet und direkt auf die Festplatte zugreift.

Dynamische Datenträger werden nicht durch die Partitionstabellen repräsentiert, daher sind diese nicht an Laufwerksbuchstaben gebunden. Ihre Zahl ist also auch nicht durch Laufwerksbuchstaben begrenzt. Falls Laufwerksbuchstaben für die Volumes vergeben werden, können diese den einzelnen Datenträgern frei zugeordnet werden .

Zu Beginn der Installation wird eine Basisplatte erstellt, die später in eine dynamische Festplatte konvertiert werden kann. Für das Konvertieren muß mindestens 1 MB freier Festplattenplatz vorhanden sein, um temporäre Daten abspeichern zu können. Die bereits vorhandene Partitionen bleiben in Form von Datenträgern erhalten. Die dynamischen Festplatten können ohne Tools von Drittherstellern nur noch von Windows 2000 Systemen gelesen werden.

Eine Konvertierung von einer dynamischen Festplatte in eine Basisplatte ist *nicht* mehr möglich.

3.2.1 Einfacher Datenträger (Simple Volume)

Ein einfacher Datenträger (Simple Volume) ist eine einfache Partition, die im System als einzelnes Laufwerk dargestellt wird. *Einfache Datenträger kommen nur bei dynamischen Festplatten vor.* Für größere Systeme, die z.B. mit Software-Raid arbeiten sind *dynamische Festplatten* eine sinnvolle Lösung.

3.2.2 Stripesets

Stripe Set-Datenträger werden durch Zusammenfassen von freien Speicherbereichen auf 2 bis 32 Festplatten zu einem logischen Datenträger erstellt. Die Daten werden in großen Blöcken in festgelegter Reihenfolge auf alle Festplatten des Arrays verteilt, wobei die einzelnen Blöcke quasiparallel geschrieben bzw. gelesen werden können. Diese Maßnahme bewirkt eine größere Zugriffsgeschwindigkeit. Die Ausfallsicherheit von Stripe Sets wird gegenüber einer einzigen Festplatte verschlechtert. Falls eine der in das Stripe Set eingebundenen Festplatten ausfällt sind alle Daten dieses Stripe Sets verloren. Mit Hilfe eines Stripe Sets wird die größte Systemleistung erreicht, daß verschiedene Festplatten (und ev. -Controller) parallel angesprochen werden.

3.2.3 Spanned Volumes

Beim *spanned Volume* bilden ebenso wie beim Stripeset mehrere Festplatten (bzw. Partitionen) ein logisches Volume ab. Allerdings werden die einzelnen Partitionen der Reihe nach komplett beschrieben. Ein (quasi-) paralleler Zugriff auf die einzelnen Platten findet also nicht statt, so daß die Performance dieser Lösung nur der der einzelnen Platte auf der gerade zugegriffen wird, entspricht.

Die Festplatten- und Partitionsoptionen wie Spiegelung, RAID-5, Datenträgersätze benötigen zwingend eine dynamische Festplatte. Falls einige Optionen (soweit implementiert) unter NT4 genutzt wurden können sie nach dem Konvertieren in eine dynamische Platte weiter genutzt werden.

Die Neuorganisation der Platte erfolgt nach folgendem Muster:

System- und Startpartitionen werden zu einfachen Datenträgern.

Primäre Partitionen werden zu einfachen Datenträgern.

Erweiterte Partitionen Alle logischen Laufwerke in der erweiterten Partition werden zu einfachen Datenträgern. Der gesamte freie Speicherplatz wird zu nicht zugeordnetem Speicherplatz.

Datenträgersatz aus NT wird zu einem übergreifendem Datenträger.

Stripe Sets aus NT werden zu einem Stripesetdatenträger.

Spiegelsätze aus NT werden zu einem gespiegeltem Datenträger.

Stripe Sets mit Parität aus NT werden zu einem *RAID-5-Datenträger*.

Falls Festplatten aus anderen Systemen eingebunden werden, müssen diese mit Hilfe der Datenträgerverwaltung importiert werden.

3.2.4 Laufwerkspfade

Unter W2K ist es möglich eine Festplattenpartition (bzw. ein Datenträger) in das Filesystem einzubinden, ohne daß hierfür ein Laufwerksbuchstabe vergeben werden muß. Bei Erstellung einer Partition in der `Computerverwaltung - Datenträgerverwaltung` kann festgelegt werden, daß daß dem zu erstellenden Datenträger kein Laufwerksbuchstabe zugeordnet wird, sondern daß er in das Filesystem auf ein Verzeichnis gemountet werden soll (Menüpunkt: Diesen Datenträger in einem leeren Verzeichnis bereitstellen, der Laufwerkpfade unterstützt.). Um ein Laufwerk in einen Verzeichnispfad zu mounten, muß die Festplatte allerdings als dynamische Festplatte verwaltet werden.

Das Mounten von Partitionen kann dazu genutzt werden um die Beschränkungen der Vergabe von Laufwerksbuchstaben zu umgehen. Auch bei Platzproblemen in vorhandenen Verzeichnistrukturen ist das hinzumounten von neuen Partitionen auf ein Verzeichnis sinnvoll.

3.3 Filesysteme

Microsoft unterscheidet zwischen der Systempartition und der Startpartition.

Systempartition Partition von der gebootet wird. Hier liegt auch die `boot.ini`.

Startpartition Partition auf der das Verzeichnis `%SystemRoot%` (Windows-Systmverzeichnis) liegt.

Die mittlerweile existierenden Microsoft-Filesysteme können nur teilweise von den Microsoft Betriebssystemversionen bzw. von anderen Systemen gelesen werden.

Zur Zeit (09.2000) können folgende Filesysteme genutzt werden:

FAT16 alle Microsoft Betriebssyteme, diverse Unix-Versionen (FreeBSD, OpenBSD, Linux, (Solaris, NetBSD, BeOS))

FAT32 Win95b, Win95c, Win98-1, Win98-2, W2K, andere ?

NTFS4 WinNT 4, W2K, (Linux, FreeBSD z.Zt. nur lesen, schreiben nicht stabil, andere ?)

NTFS5 alle W2K Versionen, NT4 ab Servicepack 4

3.4 RAID Systeme

RAID ist die Abkürzung für *Redundant Array of Inexpensive Disks*. Hiermit bezeichnet man ein Array von Festplatten, daß vom System gemeinsam zum

Zwecke der Ausfallsicherheit oder auch aus Performancegründen gemeinsam angesprochen wird. RAID-Systeme lassen sich als Hardware- oder als Softwaresysteme implementiern. Unter W2K muß mit dynamischen Festplatten gearbeitet werden um ein Software RAID-System aufzubauen.

W2K unterstützt softwareseitig einen Teil der RAID-Implementierungen wie

RAID 0 Auch als Striping bezeichnet. Die Daten werden auf mindestens zwei physikalischen Festplatten parallel gelesen und geschrieben. Mit Hilfe dieser Maßnahme wird die Performance des Festplattenzugriffs gesteigert. Allerdings steigt hiermit die Gefahr von Fehlern, daß bei Ausfall einer Platte das gesamte Array ausfällt und somit alle Daten verloren gehen. Unter W2K können 2-32 Platten für RAID 0 genutzt werden.

Der Speicherplatz der mit RAID 0 verknüpften Platten addiert sich.

RAID 1 bezeichnet die Spiegelung (Mirroring) von zwei Festplatten. Es steht hier nur der Speicherplatz einer Platte zur Verfügung. RAID 1 ist die einzige Möglichkeit die Startpartition (siehe 3.3) redundant anzulegen. Um bei Ausfall einer Platte ein System zu starten, muß in der Datei `boot.ini` (siehe 26.3) der Parameter für die Startpartition (rdisk(0)) entsprechend editiert werden um von der anderen Platte zu booten.

Eine Variante von RAID 1 ist die Duplizierung, bei der der Festplattencontroller redundant ausgeführt wird.

RAID 5 arbeitet mit mindestens drei physikalischen Platten. Es ist so aufgebaut, daß jeweils zwei Platten parallel zum Schreiben genutzt werden während auf die dritte Platte Paritätsinformationen geschrieben werden. Die Paritätsinformationen werden ebenso wie die Daten gleichmäßig auf alle Platten verteilt. Das System ist so aufgebaut, daß die Daten bei Ausfall einer Platte aus den Daten der anderen beiden Platten rekonstruiert werden können. Das RAID 5 Array kann als Softwarelösung unter W2K mit 3 bis 32 Platten genutzt werden. Allerdings darf *maximal eine Platte ausfallen*, da sonst die Daten nicht wieder hergestellt werden können. Somit steigt die Ausfallwarscheinlichkeit mit Anzahl der eingebundenen Platten. Neben der Sicherheit bietet RAID 5 noch eine Steigerung der I/O Performance der Platten. Allerdings wird das System hinsichtlich Prozessorleitung und Speicherverbrauch aufgrund der Berechnung der Paritätsinformationen zusätzlich belastet. Aufgrund der Struktur kann RAID 5 nicht zum redundanten Aufbau der Startpartitionen genutzt werden.

Die gesamte Kapazität des RAID 5 Arrays errechnet sich aus der Summe der Kapazitäten der einzelnen Platten abzüglich der Größe einer

Platte (n*k-k).

Neben den Software-RAID Implementierungen ist auch das Spanning (übergreifende Datenträger) möglich. Hierbei werden mehrere Partitionen zu einem Datenträger zusammengefaßt. Hierfür wird eine dynamische Festplatte benötigt. Auf einem Basislaufwerk ist die Implementierung eines übergreifenden Datenträgers nicht möglich.

Kapitel 4

Das NTFS Filesystem

W2K nutzt das NTFS-Filesystem Version 5. Das heißt, daß dieses von NT4 nicht gelesen werden kann.

4.1 Dateisystemrechte

Die Dateisystemsicherheit wird mit Hilfe von Berechtigungen eingestellt. Diese können Usern und Gruppen zugewiesen werden. Berechtigungen an einem Objekt verhalten sich kummulativ (d.h. sie werden addiert). Einzig das Recht *no access* (kein Zugriff, "Verweigern") bildet hier eine Ausnahme.*Allerdings sollte das* Verweigern *Recht in einer gut geplanten Umgebung nicht benötigt werden.*
(siehe auch 19)

4.2 Erweiterte Möglichkeiten des Filesystems

4.2.1 Komprimierung auf Filesystemebene

Das NT Filesystem bietet die Möglichkeit zur automatischen Komprimierung von Dateien. In den erweiterten Dateieigenschaften kann eingestellt werden, ob eine Datei oder ein Verzeichnis komprimiert werden soll. Werden Dateien in einem Verzeichnis mit dieser Einstellung abgelegt, werden diese automatisch komprimiert. Falls sich zum Zeitpunkt der Einstellung schon Dateien im Verzeichnis befinden, kann ausgewählt werden ob auch diese schon komprimiert werden sollen oder weiterhin unkomprimiert bleiben. *Diese Möglichkeit kann nur auf alle Dateien im Verzeichnis gleichzeitig angewandt werden.*

Zur Komprimierung auf Konsolenebene läßt sich der Befehl `compact.exe` nutzen, der allerdings *nur* auf NTFS Dateisystemen arbeitet. Er setzt die Dateiattribute dieser Datei auf *komprimiert Speichern.* Zu beachten ist hier, daß für die Berechnung der Disk-Quotas die *unkomprimierte* Datenmenge

berücksichtigt wird. Mit einer Komprimierung auf Filesystemebene läßt sich die Menge der zu speichernden Daten hinsichtlich der Quota-Limits also nicht vergrößern (s.a. 27.0.52).

Zur Komprimierung einer Datei für den Transport z.B. auf Diskette kann der Befehl *compress.exe* genutzt werden. Er komprimiert eine Datei auf jedem beliebigen Filesystem (unter Windows) komprimieren. Mit dem Schalter `-r` wird der Befehl veranlaßt, die komprimierte Datei umzubenennen, so daß der letzte Buchstabe der Dateiendung zu einem _ (Underscore) wird. Eine Datei mit einem Dateinamen *.??_ ist also meist eine mit `compress` komprimierte Datei. Das Expandieren der Datei erfolgt mit dem Befehl `expand.exe`.[1]

4.2.2 Verschlüsselung auf Filesystebene

Daneben kann eine Datei auch verschlüsselt auf der Festplatte gespeichert werden. Das heißt, das jemand anderes als der Besitzer die Datei selbst zwar sehen, den Inhalt aber nicht lesen kann. Die Eigenschaft des Filesystems eine Datei verschlüsselt abzuspeichern, wird als *EFS* (Encryption File System) bezeichnet.

Die Dateien werden mit symmetrischer Verschlüsselung blockweise verschlüsselt. Hierbei wird je Block ein anderer Schlüssel verwandt. Die Schlüssel für die einzelne Datei werden auf dem Filesystem im Vorspann der Datei im Datenverschlüsselungfeld (Data Decryption Field, DDF) und im Datenwiederherstellungfeld (Data Recovery Field, DRF) gespeichert. Der automatisch generierte Schlüssel wird für jede Datei individuell ermittelt.

Bei Aktivierung der Verschlüsselung kann gewählt werden, ob für das aktuelle Verzeichnis eingestellt werden soll, daß alle Dateien und Unterverzeichnisse die hier erstellt werden automatisch verschlüsselt werden. Beim Kopieren einer Datei aus einem verschlüsselten Verzeichnis in ein anderes sind folgende Möglichkeiten zu beachten:

1. Wird die Datei in ein anderes Verzeichnis kopiert, das auch *mit dem NTFS Filesystem Version 5 (W2K)* formatiert ist, wird die Datei *auf jeden Fall* verschlüsselt abgespeichert, auch wenn das Verzeichnis nicht dementsprechend konfiguriert ist.

2. Wird die Datei in ein anderes Filesystem kopiert (z.B. FAT) wird sie hier im Klartext abgespeichert. Dieses darf allerdings nur der Ei-

[1] In der Praxis wird man jedoch in der Regel mit einem der weit verbreiteten Packprogramme wie `ZIP, ARJ, SHA, RAR, GZIP` arbeiten, da diese sehr weit verbreitet sind und auf vielen Hard- und Softwareplattformen (auch abseits der Microsoft-Systemfamilie) verfügbar sind. Zudem können die mit diesen Tools erzeugten komprimierten Dateien so gestaltet werden, daß sie unter DOS/Windows (bei RAR zusätzlich unter Linux und *BSD) selbstextrahierend sind.

gentümer der Datei. Selbst der Administrator darf eine verschlüsselte Datei nicht (auf ein FAT-Filesystem) verschieben oder kopieren.

Falls jemand anderes auf eine verschlüsselte Datei zugreifen will, bekommt er lediglich eine Meldung, daß die Datei nicht geöffnet werden kann. Falls eine verschlüsselte Datei auf ein anderes Filesystem kopiert wird, bleibt die Verschlüsselung erhalten, so daß der Verschlüsselungsschutz hiermit nicht umgangen werden kann.

Die Verschlüsselung überschreibt die NTFS Filesystemrechte, so daß außer dem Besitzer niemand den Inhalt der Datei sehen kann. Eine Ausnahme bildete hier lediglich die Person, die in der Policy *Wiederherstellungs-Agent* (Encrypted Data Recovery Agents) eingetragen ist. Dieses ist in der Standardeinstellung der *Administrator der lokalen Domäne*, zu der der Computer gehört. Diese Benutzer können neben dem Besitzer die verschlüsselte Datei noch öffnen. Der Wiederherstellungs-Agent hat sozusagen einen Generalschlüssel. Werden alle Benutzer aus der o.g. Policy entfernt, haben die Benutzer innerhalb dieses Group Policy Objektes keine Möglichkeit mehr, die Verschlüsselung auf Filesystemebene anzuwenden. Um die Verschlüsselung endgültig zu sperren, sollte hierfür noch die *No Override* Option aktiviert werden.

Auch wenn der zugreifende die Berechtigung hat, den Besitz der Datei zu übernehmen kann er die Datei auch nach der Besitzübernahme nicht entschlüsseln. Dieses ist nur dem eigentlichen Besitzer oder dem *Recovery Agent* erlaubt. Darüber hinaus ist das Kopieren der Datei auch nicht möglich. Soll ein anderer Useraccount (*User B*) die Dateien von *User A* lesen können, ohne ein Wiederherstellungs-Agent zu werden, so muß der Useraccount von *User A* in *User B* umbenannt werden. In diesem Falle bleibt die *SID* des Accounts gleich, mit der der Eigentümer der Datei identifiziert wird, der diese auch entschlüsseln kann.

Zur weitergehende Sicherung des EFS Systems sollte der Private Recovery Schlüssel vom Rechner entfernt, und auf Diskette gesichert werden (allerdings ist hierbei zu beachten, daß Disketten ein unzuverlässiges Speichermedium darstellen). In den Exportoptionen für die Schlüsselverwaltung kann eingestellt werden, daß der Schlüssel nach erfolgreichem Export gelöscht wird.

Sicherung der Schlüssel

Zur Sicherung des Schlüssels müssen entsprechende Rechte bestehen. Diese hat in der Regel der jeweilige Administrator, so daß die Sicherung des Schlüsselsatzes eines Einzelrechners der Administratoraccount benötigt wird und bei Sicherung der Domäne der Account des Domänenadministrators.

Die Verschlüsselung und die Komprimierung können *nicht* gleichzeitig angewandt werden.

4.3 Distributed File System

Das *Distributed File System* ist ein Netzwerk-Filesystem. Es erlaubt Redundanz und Load Balancing, da ein (freigegebenes) Verzeichnis auf einem Server erlaubt es, ein Verzeichnis auf einem Server auf mehrere gleichartige Verzeichnisse auf anderen Maschinen zu mappen. Der Client, der auf diese Freigabe zugreift wird transparent auf eine der eigentlichen Freigaben umgeleitet. Diese Maßnahme erlaubt den Aufbau von redundanten Netzwerkressourcen, da die Anfragen bei Ausfall einer Maschine, die Zugriffe auf die Freigaben der anderen Maschinen weitergeleitet werden können. Des Weiteren läßt sich ein einfaches Load-Balancing implementieren, indem die Zugriffe per Zufallsprinzip auf die Maschinen im Hintergrund verteilt werden.

Die Installation des DSF erfordert in der Regel, daß die Verzeichnisse auf den Rechnern mit den eigentlichen Ressourcen des DSF untereinander identisch sind. Daher wird hier eine automatische Replikation eingestellt, so daß Unterschiede in den einzelnen Verzeichnissen nach einiger Zeit ausgeglichen werden.

Bei Schreibzugriffen auf eine Freigabe im DFS ist darauf zu achten, daß eine Versionskontrolle nicht gewährleistet ist. Der User der zuletzt speichert überschreibt u.U. die Änderungen der anderen User. Je nach zeitlichem Abstand der einzelnen Replikationen sind die Verzeichnisse eine zeitlang nicht mehr synchron zueinander.

Kapitel 5

Schutz gegen Systemausfall (Notfallabsicherung)

5.1 USV-Systeme

Die USV (Unterbrechungsfreie Stromversorgung, auch UPS - Uninterruptable Power Supply) beliefert den Rechner mit weiter mit Strom falls die Netzversorgung wegfällt. Sie ist mit Akkus und einem Wandler auf 230V/50 Hz ausgerüstet. Bei den USV-Anlagen unterscheidet man zwischen

Offline USV Diese Variante schaltet bei Ausfall der Netzspannung innerhalb von einigen Millisekunden auf Netzversorgung um. Dieses kann u.U. zu Problemen führen falls nicht schnell genug umgeschaltet wird.

Online USV Hier wird der Rechner durchgehend über die USV versorgt. Die Netzversorgung sorgt dafür daß die Akkus dauerhaft aufgeladen wird. Ein Wegfall der Netzversorgung bewirkt keinen Spannungsausfall auf der Sekundärseite.

Wenn die Akkus im USV-Betrieb erschöpft sind, muß der Rechner automatisch heruntergefahren werden. Hierzu wird die USV mit Hilfe eines seriellen Kabels mit dem Rechner verbunden, auf dem sie signalisiert wenn die Akkus erschöpft sind. Der Shutdownvorgang sollte gerade bei Servern früh genug eingeleitet werden, da dieses u.U. einige Zeit in Anspruch nehmen kann.

Unter Umständen kann es zu Problemen kommen, daß eine per seriellem Kabel an das System angeschlossene USV als Maus erkannt wird. Hierzu wird in der Datei `boot.ini` (s.a. 26.3)der Parameter `/noserialmice:com1` an das Ende der jeweiligen Zeile gesetzt werden um z.B. auf dem COM-Port 1 nicht nach einer Maus zu suchen [1].

[1] `multi(0)disk(0)rdisk(0)partition(1) \''WINNT=Microsoft Windows 2000 Advanced Server'' /fastdetect /noserialmice:com1`

5.2 Backup und Restore

Das Backup- und Restoreprogramm kann unter `Zubehör - Systemprogramme - Sicherung` aufgerufen werden. Hier lassen sich Art der Sicherung sowie die Zeitplanung der Backupläufe einstellen. Der Backupprozeß kann von einem Sicherungsoperator konfiguriert werden.

Das Backup kann unter W2K auf drei verschiedene Arten erfolgen:

- Gesamtes System sichern
- nur ausgewählte Dateien sichern
- Systemdaten sichern (Active Directory wird hier gesichert)

Beim Sichern der Systemdaten (System State) werden die Boot-Dateien, alle durch die *Windows File Protection* geschützten Dateien,[2] die Registry und die COM+ Klassenregistrationsdatenbank gesichert. Diese Komponenten nehmen einen Raum von ca. 200MB auf dem zu sichernden Medium ein.

Beim Backup werden nur die Dateien gesichert bei denen das Archivbit gesetzt ist. Die verschiedenen Backupstrategieen unterscheidn sich in erster Linie dadurch, ob und wann bei einer Sicherung das Archivbit gelöscht wird oder nicht.

Komplettsicherung Alle Daten werden gesichert, wobei die erfolgte Sicherung durch Löschen des Archivbits angezeigt wird.

inkrementelle Sicherung Es werden nur geänderte Daten gesichert, wobei durch Löschen des Archivbits die erfolgte Dateisicherung angezeigt wird. Beim Restore wird daher die letzte Vollsicherung sowie alle zwischenzeilich erfolgten inkrementellen Sicherungen benötigt.

Die inkrementelle Sicherung hat beim Sichern den Vorteil, daß ein Zwischenbackup sehr schnell läuft, ist aber mit dem Nachteil des langwirigen und komplizierten Restore verbunden.

differenzielle Sicherung Es werden die seit der letzten Vollsicherung geänderten Daten gesichert. Das Archivbit der gesicherten Daeien wird *nicht* gelöscht, so daß mit jedem Sicherungslauf *alle* Files gesichert werden, die seit der letzten Vollsicherung (mit Löschen des Archivbits) geändert wurden. Beim Restore muß daher nur die letzte Vollsicherung und die letzte Differentielle Sicherung zurückgespielt werden.

Die differentielle Sicherung ist daher beim Restore recht einfach zu handhaben, allerdings mit dem Nachteil daß das Zwischenbackup von Mal zu Mal erheblich wachsen kann.

[2] WFP-geschützte Datein sind Systemdateien, die durch das System vor dem Überschreiben geschützt sind, um die Probleme früherer Windows-Versionen diesbezüglich zu vermeiden.

Kopiersicherung Eine komplette Sicherung (Abzug) des Systems, allerdings wird das Archivbit *nicht* gelöscht. Der nächste Backuplauf nimmt wieder eine komplette Sicherung aller Dateien mit gesetztem Archivbit vor.

tägliche Sicherung Sicherung auf Grundlage des Datums, so daß nur die an diesem Tag erstellten Daten gesichert werden.

Beim Restore wird zuerst der Katalog der Sicherung importiert. Hier besteht auch die Möglichkeit einen katalog von anderen Backupprogrammen zu importieren und die Daten dann eventuell zurückzuspielen. Das Restore kann auf ein FAT Laufwerk erfolgen, so daß hier eine Sicherheitslücke entsteht, da Dateien auf ein Filesystem ohne die Möglichkeit der Rechtevergabe gespielt werden. Um diese Gefahr zu umgehen, darf die Gruppe der Sicherungsoperatoren nur das Recht zu sichern bekommen. Die Möglichkeit des Restores bleibt dann den Administratoren vorbehalten.

Zusammenfassung

Sicherungstyp	Archivbit löschen?
Komplettsicherung (Normal Backup)	Ja
inkrementelles Backup	Ja
differenzielles Backup	Nein
Kopierbackup	Nein
tägliches Backup (Datumsbasis)	Nein

5.3 Disaster Recovery

Ein echtes Disaster Recovery ist mit den Bordmitteln von W2K nur möglich, indem W2K neu installiert wird. Diese Neuinstallation kann in das orginale WINNT-Verzeichnis erfolgen. Mit Hilfe des neuen Systems kann das letzte Backup wieder eingespielt werden.

Ohne Neuistallation sind mehrere Möglichkeiten der Fehlerbehebung bei einem nicht startenem System möglich.

1. Last Known Good Configuration
2. Recoverykonsole
3. Safe Mode
4. Startdiskette
5. Emergency Repair Process
6. ERD (Emergency Repair Disk)

5.3.1 Last Known Good Configuration

Der erste, nichtgrafische Startbildschirm läßt evenutell die Auswahl zum Starten verschiedener Betriebssysteme zu. Hier ist auch ein Punkt, mit dem man die letzte, als funktionierend bekannte Konfiguration des Systems starten kann. Mit dieser Konfiguration ist die Konfiguration gemeint, mit der das letzte mal eine erfolgreiche Anmeldung am System möglich war.[3] Eventuelle Probleme, die das System *nach der Anmeldung* zum Stehen bzw. Absturz bringen, können mit dieser Auswahl nicht behoben werden, da das System immer mit der Fehlkonfiguration startet.

5.3.2 Recoverykonsole

Bei Startproblemen kann alternativ eine rudimentäre Konsole gestartet werden, um Reparaturen durchführen zu können. Die Konsole kann nach Start eines `Setups` (i386/winnt32) mit der Installationsoption `R` (Reparatur-Modus) aufgerufen werden. Alternativ kann sie dauerhaft auf dem System installiert werden, indem das Setupprogramm mit winnt32 /cmdcons aus dem Verzeichnis `i386` von der Setup-CD aufgerufen wird. Nach der Installation steht im Boot-Menü ein Eintrag für die Recovery Console zur Verfügung. Der Aufruf kann dann auch mit `F8` erfolgen.

Beim Ausführen der Recovery Console wird eine Anmeldung als Administrator gefordert, so daß das Administrator-Passwort benötigt wird. Eine Auflistung der Befehle der Recovery Console ist unter 26.6 zu finden.

An der Recoveryconsole kann auch eine Sicherung der Registry zurückkopiert werden.[4]

5.4 Startdiskette

Ein Windows 2000 Rechner läßt sich nicht allein von Diskette starten! Zum primären Booten des Systems von Diskette werden die hierfür notwendigen Dateien von der Diskette geladen. Der Rechner kann dann bis zum Bootmenü hochgefahren werden. Die beim Setup erstellte Disktette ist hierzu nicht in der Lage, so daß eine extra Startdiskette erstellt werden muß. *Zum kompletten Systemstart wird auf jeden Fall zusätzlich das System von Festplatte benötigt,* da beispielsweise ein Zugriff auf das NTFS Filesystem ohne Drittanbieter-Tools nicht möglich ist.

[3] Hier werden lediglich die Registry-Informationem wiederhergestellt, die unter dem Registry-Schlüssel
HKLM\System\CurrentControlSet
abgelegt worden sind. Konfigurationseinstellungen, die einen anderen Subzweig der Registry betreffen werden durch diese Startmethode nicht berührt.

[4] Diese befindet sich im Verzeichnis:
%SYSTEMROOT%\repair\regbak\

Zum Erstellen der Startdiskette wird wie folgt vorgegangen:

1. Diskette unter Windows 2000 formatieren. Hierdurch wird ein initialer Bootcode auf die Spur 0 der Diskette geschrieben. (Wichtig: Die Diskette *muß* unter W2K formatiert werden.

2. Folgende Dateien werden auf die Diskette kopiert:

   ntldr Bootloader von Windows,

   boot.ini Pfade zur Startpartition (s.a. 26.3),

   ntdectec.com Erkennung von Hardware-Komponenten beim Hochfahren des Systems.

   bootsect.dos Bootsektor für DOS-System bei Dual-Boot-Systemen

   ntbootdd.sys Treiber für SCSI-Controller ohne Bios.

5.4.1 Emergency Repair Process

Der Emergency Repair Process (ERP) kann nach dem Booten mit der W2K Installations-CD oder den Installationsdisketten als eine Option des *Repair-Modus* bei der Installation gewählt werden. Der ERP dient dazu, Fehler mit einer defekten `ntldr` oder einem fehlerhaften Bootsektor zu korrigieren. Falls der Fehler hiermit nicht behoben werden kann, wird die Recoverykonsole genutzt um einen bootfähigen Systemzustand wieder herzustellen.

5.4.2 Emergency Repair Disk

Eine W2K *Installation* selbst läßt sich unter Umständen mit Hilfe einer einer sogenannten ERD (Emergency Repair Disk) wiederherstellen. Allerdings ist es mit dieser Diskette *nicht* möglich ein nicht bootendes System zu reparieren, da die Diskette die Dateien `boot.ini` und `ntldr.exe` nicht enthält. Sie enthält nur Dateien, die dazu dienen die installierten Systemdateien wieder auf das System zurückspielen zu können. Um die Diskette zu erstellen wird das Sicherungsprogramm (Backupprogramm) von W2K gestartet. Am "Willkommen"-Prompt wird dann die Option `Notfalldiskette erstellen` (auch unter dem Menü `Extras` zu erreichen) gewählt. Das Programm kopiert jetzt die Dateien

autoexec.nt Kopie von %SYSTEMROOT%\system32\autoexec.nt

config.nt Kopie von %SYSTEMROOT%\system32\config.nt

setup.log Protokoll der installierten Dateien (der Installation!)

auf die Diskette. Die so erzeugte Diskette ist rechnerspezifisch; sie kann nicht auf einem anderen System genutzt werden. Die Registry selbst wird *nicht* mit auf Diskette gesichert. Beim Erstellen der Diskette kann jedoch

als Option angegeben werden, daß die Registry des Rechners als Kopie im Verzeichnis
%SYSTEMROOT%\repair\regbak\
gespeichert werden soll.

Wiederherstellung mittels der ERD

Für die Systemwiederherstellung mittels der ERD muß zuerst das Setup Programm von W2K von CD-Rom oder der ersten Installationsdiskette gestartet werden. Zu Beginn des Zeichenbasierten Teils des Installationsvorgangs wird die Taste `R` gedrückt, um die Reparatur vornehmen zu können. Nach Wählen der Optionen für manuelle Reparatur oder automatische Reparatur wird die Notfalldiskette eingelegt. Das System überprüfut jetzt u.a. die Installationslogs und kopiert eventuell fehlende Dateien von CD auf die Platte.

Bei der automatische Reparatur (Schnellreparatur) wird zusätzlich zur manuellen Reparatur noch eine Überprüfung der Struktur-Dateien der Registry durchgeführt. Dieses wird auch als ERD (Emergency Repair Process) bezeichnet. Die Registrydateien können sich im Laufe der Zeit erheblich von den gesicherten unterscheiden. In diesem Falle muß eine aktuelle Sicherung der Registry wiederhergestellt werden. Die zwischenzeitliche Sicherung der Registry[5] erfolgt automatisch, wenn mit Hilfe des Sicherheitsprogramms von W2K eine Sicherung der Systemstatusdateien durchgeführt wurde.

5.5 Defekte Festplatten

Wenn ein Sektor einer Festplatte als defekt erkannt wird, markiert das System diesen als defekt und verlagert die Informationen sowei noch zu rekonstruieren in einen anderen Sektor. In der Regel verläuft dieses transparent im Hintergrund. Wenn die Anzahl der defekten Sektoren jedoch größer wird, zeigt das System E/A (I/O) Fehler an. Hier besteht die Gefahr, daß bald die ganze Festplatte unbrauchbar wird. Um Datenverlust vorzubeugen sollte die Festplattem möglichst schnell ausgetauscht werden.

Eine defekte Festplatte wird i.d.R. in der `Datenträgerverwaltung` als offline oder fehlend angezeigt. Um die hier noch verfügbaren Daten möglichst noch zu sichern sollte zuerst versucht werden die Festplatte zu reaktivieren (Menübefehl). Falls die Festplatte so eingelesen werden kann, sollten die Daten sofort gesichert und die Festplatte dann ausgetauscht werden.

[5] In das Verzeichnis:
%SYSTEMROOT%\repair\regbak\

5.5.1 Fehlerbehebung bei dynamischen Festplatten

Wenn eine Platte eines gespiegelten Datenträgers I/O Fehler aufweist, wird sie in der Datenträgerverwaltung als Offline gekennzeichnet. Wenn der Fehler nur temporär aufgetreten und die Platte wieder ansprechbar ist, kann das gespiegelte Volume mit Hilfe des Befehls `resynchronize` wieder aktiviert werden.

Falls der Fehler noch besteht sollte zuerst versucht werden die defekte Platte zu reaktivieren. Wenn dieses zu keinem Erfolg führt, muß die Platte getauscht werden. Um den Betrieb vorläufig wiederherzustellen, kann die zweite Platte des Mirrors allein genutzt werden. Hierzu wird zuerst der Befehl `Remove Mirror` aufgerufen um den defekten Teil des Mirrors zu entfernen. Der Befehl wandelt den Plattenplatz in unallozierten Speicherplatz um. Dann kann der Befehl `Remove Disk` genutzt werden, um dem System mitzuteilen, daß die Platte nicht mehr angesprochen werden soll. Nach Herunterfahren des Rechners wird die Platte getauscht.

Kapitel 6

Überwachen des Systems

Ein W2K System läßt eine laufende Überwachung des Systems hinsichtlich zweier verschiedener Aspekte zu. Zum einen kann protokolliert werden, welche Benutzer oder Programme welche Aktionen starten und auf welche Ressourcen zugreifen. Daneben kann die Systemleistung überwacht und aufgezeichnet werden um z.B. Tendenzen abzulesen oder zeitweilig Auftretende Probleme einzukreisen.

6.1 Zugriffsüberwachung (Auditing)

W2K ermöglicht die Überwachung (Auditing) und Protokollierung des Zugriffs auf Systemressourcen. Die Überwachung läßt sich spezifisch für jede einzelne Maschine mit Hilfe von Richtlinien konfigurieren. Diese Richtlinien werden den einzelnen Rechnern der Domäne zugewiesen und können auch nur für einen Computer und nicht für einzelne User gelten. Die Protokollierung der Überwachten Ereignisse erfolgt im Ereignisprotokoll, genauer gesagt im Sicherheitsprotokoll. Hier werden Informationen über

- den ausgeführten Vorgang,
- den Benutzer, der den Vorgang initiert hat,
- Zeitpunkt, Erfolg oder Fehlschlag des Ereignisses,
- zusätzliche Informationen wie Rechnername von dem aus der Vorgang initiert wurde.

6.2 Überwachung und Optimierung des Systems

Zur Überwachung des Systems lassen sich Überwachungsrichtlinien festlegen. Hier kann eingestellt werden, welche Ereignisse überwacht werden sollen. Die Ereignisse werden in einem von drei Protokollen festgehalten.

Systemprotokoll Enthält von Systemkomponenten protokollierte Ereignisse. Die zu protokollierenden Ereignistypen sind vom System voreingestellt.

Anwendungsprotokoll Hier werden die Ereignisse von Anwendungsprogrammen protokolliert. Die zu protokollierenden Ereignisse werden in der Anwendung festgelegt. Vom Programm "Dr. Watson" generierte Ereignisse können hier mitprotokolliert werden.

Sicherheitsprotokoll Zeichnet Ereignisse hinsichtlich Sicherheit und Überwachung des Systems auf wie z.B.

- gültige und ungültige Anmeldeversuche,
- Ereignisse im Zusammenhang mit der Ressourcenverwendung wie Erstellen, Löschen und Öffnen von Dateien.

Die hier aufzuzeichnenden Ereignisse werden vom Administrator festgelegt.

Die Anwendungs- und Systemprotokolle können von allen Usern eingesehen werden, während die Sicherheitsprotokolle nur vom Systemadministrator gelistet werden können. Eine Einsicht in Protokolle von anderen Maschinen über das Netzwerk ist möglich. Hierzu wird in der Ereignisprotokollanzeige per Kontextmenü eine Verbindung zu einem Remote-Computer hergestellt.

Hinsichtlich der Anwendungs- und Systemereignisse unterscheidet man noch zwischen

Informationen (i-Symbol) zeigen die erfolgreiche Ausführung einer Anwendung oder eines Treibers an.

Warnung (!-Symbol) Ereignis, welches wichtig ist und möglicherweise in der Zukunft zu Problemen führen kann wie z.B. vollaufende Platten.

Fehler (x-Symbol) Bedeutendes Problem wie fehlgeschlagenes Laden eines Teibers oder Dienstes.

Innerhalb der Ereignisanzeige kann nach Ereignissen gesucht werden sowie eine Filterung auf bestimmte Ereignisquellen erfolgen (`Kontextmenü -> Ansicht -> Filter`).

6.2.1 Überwachung der Festplattenleistung

Mit Hilfe des Befehls `diskperf` lassen sich physikalische Leistungsindikatoren für die Festplatten oder für einzelne Partitionen aktivieren.

```
DISKPERF [-Y[D|V] | -N[D|V]] [\\Computername]

  -Y  Startet alle Leistungsindikatoren, wenn das System
      neu gestartet wird.

  -YD Aktiviert die Leistungsindikatoren für die physikalischen
      Laufwerke, wenn das System neu gestartet wird.

  -YV Aktiviert die Leistungsindikatoren für die logischen
      Laufwerke oder Datenträger, wenn das System neu gestartet
      wird.

  -N  Deaktiviert alle Leistungsindikatoren, wenn das System
      neu gestartet wird.

  -ND Deaktiviert die Leistungsindikatoren für die
      physikalischen Laufwerke.

  -NV Deaktiviert die Leistungsindikatoren für die logischen
      Laufwerke.

  \\Computername
  Der Name des Computers, für den Leistungsindikatoren
  angezeigt oder festgelegt werden sollen.
```

Kapitel 7

Druckerdienste

Beim Drucker muß zwischen dem *Druckgerät* (physikalischer Drucker) und dem *Drucker* ("virtueller Drucker", der die Druckausgabe auf einem Druckgerät vornimmt. Einem Druckgerät lassen sich mehrere Drucker zuweisen, die verschiedene Konfigurationen des Druckgerätes (z.B. DIN A3, DIN A4, Querformat, verschiedene Prioritäten) darstellen.

Ein Drucker kann auf verschiedene Arten über das Netzwerk genutzt werden:

direkt am Server Der Drucker wird direkt am Server angeschlossen. MS empfielt hierfür die Standard-Serverversion von W2K.

als Netzwerkdrucker Der Drucker wird mit einer Netzwerkkarte ausgerüstet, bzw. mit einer Printbox mit dem Netzwerk verunden. Der jeweilige Druckjob beim Absender lokal gespoolt (zwischengespeichert). Um den Netzwerkdrucker nutzen zu können, muß die Netzadresse (z.B. IP-Adresse) des Druckers bekannt sein. Um Drucker im Netzwerk finden zu können wird u.U. (NT4) spezielle Zusatzsoftware benötigt. In W2K ist eine Software integriert, die in der Lage ist die Drucker im Netzwerk zu finden. Ein im Netzwerk freigegebener Drucker kann zusätzlich im AD freigegeben werden.

lokaler Arbeitsplatzdrucker Hier wird der Drucker lokal an einer Workstation angeschlossen. Der Nachteil hierbei ist, daß nur gedruckt werden kann, wenn die Workstation in Betrieb ist und daß die lokalen Ressourcen der Workstation belegt werden. Unter Umständen kann es zu Problemen führen, da *max. 10 Netzwerkzugriffe* auf die Workstation erlaubt sind.

Bei gemeinsamer Nutzung ist der Druck einer Trennseite sinnvoll, da die Übersicht sonst schnell verloren gehen kann. Den Ausdruck der Trennseite kann man in den Eigenschaften des Druckgerätes einstellen.

Auf einen im Netzwerk freigegebenen Drucker kann von Clients aus mittels des UNC-Pfades zugreifen. Die Defaulteinstellung (Standardfreigabe) der Freigabe ist *Drucken*. Mit dieser Freigabe können keine Druckaufträge geändert werden.

Beim W2K-Drucker läßt sich einstellen, daß der Drucker im AD eingetragen wird. In diesem Falle läßt sich im AD nach dem Drucker suchen. Die Suche im AD kann zudem nach Druckerspezifikationen (Fähikgkeiten, z.B. A3, Farbe, ...)eingegrenzt werden.

7.1 Ablauf des Druckvorgangs

1. Der Druckauftrag wird auf der lokalen Maschine vom Spooler entgegengenommen.

2. Der lokale Spooler überträgt die Druckdaten zum Serverspooler.

3. Der Druckserver sendet die Daten an den Druckerspeicher (physikalischer Speicher im Drucker).

7.1.1 Spoolverzeichnis

Der Spooler speichert die Druckjobs im Spoolverzeichnis zwischen. In der Defaulteinstellung ist dieses das Verzeichnis: `%SYSTEMROOT%`\system32\spool\printers Diese Einstellung kann geändert werden, in dem im Fenster *Drucker* unter dem Menüpunkt `Datei - Servereigenschaften` der Reiter *Erweiterte Optionen* gewählt wird und hier ein neues Spoolverzeichnis eingestellt wird. Auf der Serverversion von W2K muß jetzt noch der Druckservice neu gestartet werden, damit die Einstellungen eingelesen werden. (?RICHTIG? BITTE RÜCKMELDUNG an ¡doku@werthmoeller.de¿)

7.2 Installation und Konfiguration

7.2.1 Druckertreiber

Falls W2K als Druckserver eingesetzt wird, kann es so eingesetzt werden, daß die Druckertreiber automatisch auf dem Client installiert werden. Hierzu werden die Treiber auf dem Server installiert (Drucker - Eigenschaften - Freigabe). Zusätzlich zu den Treibern für W2K können auch NT4, NT3.51 und Win9x Treiber installiert werden. Alle Treiber werden im Verzeichnis `%SYSTEM_ROOT%\system32\spool\drivers` installiert. Dieses Verzeichnis wird als `drivers$` freigegeben.

Die Clientsysteme, die auf einen Druckserver zugreifen sollen verhalten sich z.T. unterschiedlich bei der Installation der Druckertreiber.

MSDOS, OS/2, 3.x Die Druckertreiber müssen *manuell* installiert werden.

Win 9x Die Treiber werden nur *einmal* automatisch installiert. Ein automatisches Treiberupdate ist nicht möglich, es muß also manuell erfolgen, indem der Drucker dann gelöscht und neuinstalliert wird.

NT 4.0 Die NT 4.0 Treiber auf den Clients werden automatisch aktualisiert, wenn die Treiber auf dem Server aktualisiert werden.

W2K siehe NT 4.0

Fremdhersteller Die File and Printservices für Netware (Add-On) liegen nicht auf der Server CD und müssen zusätzlich geordert werden.

UN*X Um von UN*X-Clients auf den Server ausdrucken zu können müssen die TCP/IP Druckdienste (lpd) installiert werden.

Apple Macintosh Rechner können mit Hilfe der *Services für Macintosh* über den W2K Druckserver drucken.

Die Druckertreiber können manuell installiert werden, indem das Fenster *Drucke* vom Startmenü aus geöffnet wird. Hier ist ein Icon *Neuer Drucker* vorhanden, mit dem ein neuer Druckertreiber installiert werden kann. Ein im Netzwerk freigegebener Drucker kann installiert werden, indem das Drucker-Icon der Freigabe per Drag-and-Drop in das *Drucker*-Fenster gezogen wird. Falls das Druckgerät lokal am System angeschlossen ist, kann der Drucker auch mit Hilfe des Hardwareassistenten installiert werden.

7.2.2 Einstellungen am Drucker

Für einen (virtuellen) Drucker kann einen Priorität festgelegt werden, mit der er auf ein physisches Druckgerät drucken darf. Um auf ein und demselben Druckgerät Druckjobs mit verschiedenen Prioriäten auszudrucken, sollten mehrere Drucker hierfür installiert werden, die alle auf den gleichen Port (Druckanschluß) verweisen. Den einzelnen virtuellen Druckern werden jetzt verschiedene Prioritäten zugeordnet.

In den Eigenschaften für einen Drucker kann darüber hinaus festgelegt werden, wann der Druckvorgang gestartet wird.

Drucken beginnen nachdem die letzte Seite gespoolt wurde Diese Einstellung ermöglicht es der Applikation den Druckdialog nach Abschicken des Druckjobs direkt zu beenden. Allerdings verlängert sich hier die Zeit, bis mit dem eingentlichen Druck begonnen wird, da erst alle Seiten gerendert werden, bevor der Drucker angesprochen wird.

Drucken unmittelbar beginnen Hier wird der Druck sofort nach Anstoßen des Druckauftrages begonnen. Allerdings kann es einige Zeit dauern bis die Anwendung, die den Druckjob initiierte wieder reagiert.

Direkt zum Anschluß drucken Mit dieser Einstellung wird festgelegt, daß der Druckjob auf der lokalen Maschine gerendert wird. Die Rechenleistung wird also lokal aufgebracht. Da bei dieser Einstellung keine Druckerqueue benötigt wird, lassen sich auch keinerlei Prozeßprioriäten festlegen. Die Druckjobs werden in der Reihenfolge abgearbeitet in der sie einlaufen.

7.2.3 Druckumleitung

Im Falle eines Defektes (Papierstau) läßt sich der Drucker auf ein anderes (Druck-)Gerät umleiten. Hierzu wird der Drucker angehalten, eventuell ein neuer Druckerport (TCP/IP-Port auf Netzwerkdrucker) erstellt und der neue Druckerport dem Drucker zugewiesen. Ein schon begonnener Druckauftrag läßt sich u.U. noch einmal neu anstoßen (Restart printing), so daß dieser auf dem neuen Gerät noch einmal ausgedruckt wird.

7.2.4 Trennseiten

Der Drucker läßt sich einstellen, daß zwischen den Aufträgen Trennseiten gedruckt werden sollen, oder der Drucker in einen anderen Druckmodus umgeschaltet werden soll. Diese Einstellung läßt sich unter *Erweitert-¿Trennseite* vornehmen. Folgende Trennseitendateien stehen in der Standardinformation zur Verfügung:

sysprint.sep Druckt eine Trennseite,

pcl.sep schaltet den Drucker in den PCL-Modus (HP Druckersprache), druckt allerdings keine Trennseite,

pscript.sep schaltet den Drucker in den Post-Script Modus (Adobe Seitenbeschreibungssprache, in vielen hochwertigen Druckern integriert [1]), druckt keine Trennseite.

7.3 Verwalten von Druckjobs

Ein User, der die Berechtigungen zum Verwalten von Dokumenten besitzt, darf für jedes Dokument oder für alle zu druckenden Dokumente verschiedene Eigenschaften einstellen. Die Einstellungen können eimal für alle zu

[1] Eine Post-Script Datei kann mit dem frei erhältlichen Tool GhostScript auch auf nicht Post-Script fähigen Druckern ausgedruckt bzw. angesehen werden.

druckenden Dokumente im Fenster des Druckers unter dem Menüpunkt *Dokument* erfolgen oder für jedes Dokument einzeln. Der Menüpunkt ist erst erreichbar, wenn ein Dokument zum Drucken bereitliegt.

Priorität Die Priorität, mit der die Dokumente gedruckt werden.

Druckzeit Die Uhrzeit in der die Dokumente gedruckt werden.

Benachrichtigung Der User, der benachrichtigt werden soll, falls der Druckauftrag beendet ist. Dieser Vorgang wird eingeleitet, nachdem der Printserver eine Rückmeldung vom *Druckgerät* erhalten hat. Die Konfiguration kann daher nur auf der Maschine aktiviert werden, die als Printserver fungiert, also physikalisch mit dem Drucker verbunden ist.

Die Benachrichtigung erfolgt über den Netzwerkbenachrichtigungsdienst, der auch von dem Befehl `net send` genutzt wird. Dieser ist defaultmäßig schon installiert und aktiviert. Ansonsten erfolgt die Aktivierung in der Systemsteuerung unter `Verwaltung:Dienste`.

Die Benachrichtigung des Users ist auf die direkte Rückmeldung des Druckers angewiesn. Sie kann daher nur auf der Maschine aktiviert werden, die als Printserver fungiert, also physikalisch mit dem Drucker verbunden ist.

7.4 Webbasiertes Drucken

Das Webbasierte Drucken ermöglicht es einem Client einen Drucker per Webbrowser zu nutzen. Hierzu wird auf dem Client ein Browser benötigt, der Frames unterstützt, wie z.B. Netscape Navigator oder Internet Explorer ab Version 4. Auf der Servermaschine werden ein freigegebener Drucker und die Peer Web Services benötigt, die die HTML-Seiten für den Webbasierten Zugriff erzeugen. Falls der Server als Printserver für das gesamte firmenweite Intranet dienen soll *muß* hier allerdings der komplette *Internet Information Server* installiert werden. Dieser stellt in der Standardeinstellung ein *virtuelles* Verzeichis `Drucker` dar. In diesem Verzeichnis sind weitere Links zu allen auf *diesem* Printserver freigegebenen Drucker aufgelistet. Über diese Links wird eine weitere Page generiert, auf der die User die Druckjobs *anstoßen, anhalten, weiterlaufen* oder ganz *löschen* können.

Der Druckauftrag kann per Webinterface abgeschickt werden, indem im Browser die URL `http://SERVERNAME/Drucker` des Druckservers angegeben wird. Hier wird dann der Link für den passenden Drucker ausgewählt. Auf der Page des ausgewählten Druckers kann der User den Ausdruck starten, indem er die lokale Datei auswählt, die ausgedruckt werden soll.

Kapitel 8

Terminaldienste

In W2K sind die Terminaldienste integriert, mit der ein Client auf eine andere Maschine zugreifen kann um sich deren Desktop anzeigen zu lassen bzw. auf der Maschine zu arbeiten. Die Kommunikation erfolgt über das für diesen Zweck entwickelte "Remote Desktop Protocol (RDP). Die Installation dieser Funktionalität erfolgt unter `Sytemsteuerung - Software - .. Terminaldienste`. Während der Installation wird auch der Einsatzzweck – Remoteadministration oder Applikationsserver – festgelegt, so daß *der Server nicht gleichzeitig im Applikationsserver- und im Remote Administration Modus laufen kann.* Des Weiteren ist eine Nutzung der Terminaldienste gleichzeitig mit den Offline-Foldern 20.1 ist ebenso *nicht* möglich.

Die Clientmaschinen können auch unter älterern (16 und 32 Bit) Windows-Clients laufen um die Terminalservices eines W2K Terminalservers zu nutzen.

8.1 Terminalserver als Applikationsserver

Im Anwendermodus arbeitet der Terminalserver als Applikationsserver. *Die Auswahl, daß der Terminaldienst für einen Applikationsserver genutzt werden kann ist nur während der Installation möglich, so daß eine parallele Nutzung für Adminzugriffe nicht mehr eingestellt werden kann.* Im *Application Server Modus* können sich die Thin Clients mit dem Server verbinden und die Applikationen auf dem Server ausführen. Dem Administrator ist es hier möglich, die Benutzersessions kontrollieren. Diese kann wahlweise passiv (Reine Überwachung) oder aktiv (z.B für User-Support) erfolgen. Die Einstellungen der Berechtigungen für den Remotezugriff auf eine Terminalsession lassen sich unter den Eigenschaften für jeden einzelnen User konfigurieren. Hier kann z.B. eingestellt werden, daß der User vor Einblick in die Session um Erlaubnis gefragt werden muß, oder daß der Remotezugriff die volle Kontrolle über Tastatur und Maus übernimmt. Hierzu muß diesem auf dem Terminal Server das *Full Control* Recht für *RDP* (Remo-

te Desktop Protocol) Verbindungen zugewiesen werden. Bei Nutzung der Terminaldienste für einen Terminalserver sind unbegrenzt viele Clientzugriffe auf die Servermaschine möglich. Die Clientsessions laufen auf dieser Maschine ab, so daß für jede geplante Session ca. 4-10 MB Hauptspeicher eingeplant werden müssen. Jedem User kann für ein eigenes Profil für die Session zugewiesen werden.

Die Client-Software für die Terminaldienste kann von:
`%SYSTEMROOT%/System32/CLIENTS/TSCLIENTS`
installiert werden.

Die Nutzung der Terminaldienste im Anwendermodus ist ohne zusätzliche Lizensierung auf 90 Tage beschränkt. Danach wird vom Terminaldienst der Terminaldienst-Lizensierungsserver gesucht, der von der Setup-CD nachinstalliert werden kann. Die Terminaldienste für den Applikationsserver sind dann nach entsprechender Lizensierung (und Zahlung!) weiter nutzbar.

Das Setup von Anwendungen auf dem Terminalserver muß im sogannten Installationsmodus erfolgen. Hier wird die Installation protokolliert, um die Änderungen am Profil (Icons auf dem Desktop) bei allen Usern durchführen zu können. Der Installationsmodus wird automatisch bei der Installation mittels Setup-Programmen gefordert. Allerdings sollte die Softwareinstallation mittels `Systemsteuerung - Software` erfolgen, um eine protokollierte Installation zu gewährleisten.

Eine Installation lässt sich manuell in den protokollierten Modus schalten, indem innerhalb einer Terminalserversession mit entsprechenden Rechten an der Konsole der Befehl `change user /install` eingegeben wird. Nach erfolgter Installation wird in den Standardmodus zurückgeschaltet: `change user /execute`.

8.1.1 Remoteadministration

Der *Remote Administration Modus* ist zur Remoteverwaltung für alle Arten von Windows 2000 Servern und Clusterdiensten vorgesehen. In diesem Modus können *keine* Terminaldienste für Thin Clients angeboten werden. Der Benutzer, der den Server remote verwalten will, verbindet sich mit dem Server und bekommt dessen Benutzeroberfläche in einem Fenster präsentiert, so daß er hiermit volle Kontrolle über den Server erhält.

8.2 Alternativen

Alternativ zur oben beschriebenen Methode läßt sich ein einfacher Remote-Zugriff über das Neztwerk auch mit Hilfe des Tools *VNC*, das von den *At&T Laboratories Cambridge* entwickelt wurde, realisieren. Mit Hilfe von VNC wird der Desktop über das Netzwerk übertragen und kann remote bedient werden. Das Tool hat m.E. mehrere Vorteile:

Open Source VNC ist Open Source Software, so daß der Quellcode vorliegt. Versierte Programmierer können es nach belieben anpassen, etwaige Fehler beseitigen und sich an der Weiterentwicklung beteiligen.

Schlank VNC ist relativ schlank. Der Client ist nur einige 100 kByte groß und kann auf einer Diskette transportiert werden. Er kann ohne Installation direkt gestartet werden, so daß auch die Gefahr von Systemfehlern durch überschriebene Dateien entfällt.

Plattformunabhängig VNC ist relativ plattformunabhängig. Es sind binäre Distributionen für die Plattformen Windows (9x, NT, 2000, CE), Linux, Solaris (Sparc), Macintosh (68k und PPC), DEC Alpha OSF1 sowie entsprechende Sourcen für diese Plattformen und Java downloadbar.

VNC kann von `http://www.uk.research.att.com/vnc` geladen werden.

Kapitel 9

Betrieb von mobilen Computern

Bei mobilen Computern müssen für den mobilen und stationären Betrieb jeweils andere Einstellungen gewählt werden. Im Mobilbetrieb besteht kein Zugang zum Netzwerk, so daß die Netzwerkkarte nicht initialisiert werden muß. Die unterschiedlichen Betriebsweisen lassen sich mittels Hardwareprofilen einstellen.

9.1 Hardwareprofile

In einem Hardwareprofil läßt sich einstellen, welche (Hardware-) Geräte und anderen Konfigurationseinstellungen (z.B. IP-Adresse) der Rechner in diesem speziellem Profil läd und aktiviert. Mit dieser Maßname lassen sich z.B. die Startzeiten eines Laptops im mobilen Betrieb verringern, da nicht mehr versucht wird die Gerätetreiber für diese Geräte zu laden. Bei Erstellung eines Profils läßt sich einstellen, mit welchem Profil defaultmäßig gebootet wird, wenn innerhalb einer angegebenen Zeitspanne keine Auswahl getroffen wird. Ein Hardwareprofil wird in `Systemsteuerung - Hardware - Gerätemanager` eingestellt. Das aktuelle Profil kann hier aufgrund einer Markierung (current profile, aktuelles Profil) erkannt werden.

9.2 Powermanagement

Unter W2K lassen sich verschiedene Energiemanagementfunktionen einstellen und konfigurieren. Für das Powermanangement gibt es verschiedene Standards, die vom BIOS des Rechnerns unterstützt werden müssen.

ACPI Advanced Configuration and Power Interface (s. a. 27.0.6)

APM Advanced Powermanagement (älterer Standard)

Das Powermanagement läßt eine Einstellung verschiedener Optionen vor, die als Energieschemata bezeichnet werden.

Desktop Konstante Energieversorgung des Systems und der Festplatte wenn der Rechner an Dockingstation / Netz angeschlossen ist.

Tragbar/Laptop Schaltet alle Einstellungen nach 5-30 Min. inaktivität ab.

Präsentation Gewärleistung einer konstanten Energieversorgung des Monitors im Akkubetrieb, sowie eine konstante Energieversorgung der Festplatte bei Anschluß an Dockingstation / Netz.

Dauerbetrieb Konstante Energieversorgung des gesamten Gerätes im Batterie oder Netzbetrieb.

minimaler Energieverbrauch Konstante Energieversorgung von Festplatte oder System nur im Netzbetrieb.

minimale Batteriebeleistung Konstante Energieversorgung der ausschließlich der Festplatte nur im Netzbetrieb.

Hibernate Schlafmodus

Für alle Schemata kann die Zeitdauer eingestellt werden, nach der sich Festplatte oder Monitor ausgeschaltet werden.

Teil III

Windows 2000 im Netzwerk

Kapitel 10

WINS

10.1 NetBIOS und WINS

Zur Beibehaltung der Rückwärskompatibilität mit älteren Microsoft-Sytstemen unterstützt W2K immer noch die NetBIOS (über TCP/IP, auch NetBT) Namensauflösung im Netzwerk. Auch hier darf ein Rechnername im Netzwerk nur einmal vorkommen. Er kann jedoch für einen einzelnen Compter gelten oder auch für eine ganze Gruppe (sogenannter Scope, der aber selbst von Microsoft nicht empfohlen wird). Daneben können für einen einzelnen Rechner verschiedene NetBIOS Namen vergeben werden, die verschiedene Dienste darstellen, die auf diesem Rechner laufen. Das System ist in *dieser* Hinsicht mit dem DNS-System vergleichbar. Die Registrierung der Rechnernamen und somit die Abbildung auf IP- (bzw. MAC-Adressen) kann hier verschiedene Arten erfolgen.

Namenscache Jeder Rechner baut einen eigenen Cache auf, in dem das Mapping von NetBIOS Namen auf IP-Adressen festgehalten wird. Diese Methode der Namensauflösung ist die schnellste, da sich der Cache komplett im Speicher befindet. Um die Einträge im Namenscache zu überprüfen wird der Befehl `nbtstat -c` genutzt. Diese Art der Namensauflösung wird unabhängig von der Konfiguration zuallererst durcheführt.

Broadcast Ein neu ins Netzwerk eingefügter Rechner versendet einen Broadcast im Netzwerksegment. Hiermit teilt er allen Rechnern mit, welchen Rechnernamen er belegen möchte. Falls kein anderer Rechner im Netz diesen Namen belegt hat, bekommt er von allen anderen Rechnern eine Bestätigung in der ihm die Namen der anderen Rechner mitgeteilt werden. Diese fügt er in seinen lokalen Cache ein. Falls ein Rechner diesen Namen schon belegt hat, bekommt er von diesem eine negative Rückmeldung. Die neue Maschine gibt eine Fehlermeldung aus, aus der zu erkennen sein sollte, daß der Name schon vergeben ist.

LMHOSTS Mit Hilfe der Datei %SYSTEMROOT%\system32\drivers\etc\lmhosts kann eine statische Namensauflösung festgelegt werden. Hier werden die die Rechnernamen den IP-Adressen zugeordnet. Diese Art wird z.B. genutzt, wenn sich einige Rechner in anderen Netzwerksegmenten befinden und daher keine Auflösung per Broadcast erfolgen kann.

WINS-Server Im Netzwerk wird ein sogenannter WINS-Server eingesetzt, der ähnlich einem DNS-Server die Namensauflösung vornimmt. Die IP-Adresse des Wins-Servers wird auf den Client-Maschinen in der IP-Adresskonfiguration festgelegt, bzw. bei der Adressfestlegung mittels DHCP übermittelt.

Statisches Mapping Auf dem WINS-Server kann zusätzlich noch ein statisches Mapping von IP-Adressen auf Rechnernamen erfolgen. Dieses bietet sich dann an, wenn die Namen von Clients aufgelöst werden sollen, die keine Clients *dieses* WINS Servers sind.

Die Freigabe erfolgt automatisch, falls der Rechner ordnungsgemäß heruntergefahren werden kann.

Die einzelnen Rechner, die auch Konten oder Nodes genannt werden können zur Namensauflösung auf unterschiedliche Arten konfiguriert werden. Der sogenannte Knotentyp legt fest, auf welche Art die Namensauflösung bei der jeweiligen Maschine erfolgt. Die Einstellungen erfolgen in der Regel automatisch, können jedoch in der Registry (unter dem Schlüssel ...`NodeType`) editiert werden oder dem Client in der DHCP Konfiguration übergeben werden.

b-Knoten Die Namensauflösung erfolgt allein über **B**roadcasts. Dieser Knotentyp wird automtisch eingestellt, falls sich *kein* WINS Server im Netzwerk befindet. Der Registry-Schlüssel wird hierfür auf den Wert 1 eingestellt.

p-Knoten Der Name wird mit Hilfe einer **P**oint-to-Point Verbindung zu einem WINS Server aufgelöst. Dieser Typ wird automatisch eingestellt, wenn mindestens ein WINS Server im Netzwerksegment vorhanden ist.

m-Knoten Diese Einstellung kombiniert den B- und den P-Knoten mit der Defaulteinstellung der Namensauflösung per Broadcast. Falls der Name so nicht aufgelöst werden kann, wird eine Auflösung per WINS Server versucht. Der Registryeintrag muß hierfür auf 4 gesetzt werden.

h-Knoten Beim h-Knoten (Hybrid-Knoten) erfolgt auch eine kombinierte Auflösung der Rechnernamen. Allerdings ist hier die Defaulteinstellung die WINS Auflösung. Der Schlüssel in der Registry wird hier auf 8 gesetzt.

Der h-Knotentyp wird auf einer Maschine automatisch als Default eingestellt, wenn in den Netzwerkeinstellungen ein WINS-Server angegeben wird.

10.1.1 Namensauflösung per WINS und WINS Proxy

Wird das Netzwerk mit WINS konfiguriert, versucht der Client die Namensauflösung per default über den primären WINS Server. Falls dieses dreimal hintereinander fehlschlägt, wird versucht einen eventuell vorhandenen sekundären WINS Server zu erreichen. Falls dieses auch keinen Erfolg hat, wird ein Broadcast versandt. Zu allerletzt sieht der Client in seine LMHOSTS Datei, ob sich der Name hier auflösen läßt. Falls sich im lokalen Netzwerksegmet kein WINS Server befindet und auf den Clients auch keine WINS-Server Adresse konfiguriert wurde kann ein *WINS-Proxy* eingesetzt werden. Dieses ist ein entsprechend konfigurierter Server, der den Broadcast eines Clients aufnimmt und direkt an einen WINS Server in einem anderen Netzwerksegment weiterleitet. Er arbeitet als transparenter Proxy, so daß der Client gar nicht bemerkt, daß die Anfrage an den WINS-Server weitergeleitet wird. Die positive oder negative Antwort vom WINS-Server wiederum wird vom Proxy an den Client zurückgesandt. Der Proxy speichert den Namen des neuen Clients und die IP-Adresse in seinem lokalen Cache, so daß er zukünftig auch Anfragen von Clients für diesen Namen direkt beantworten kann. Pro Netzwerksegment darf nur ein WINS-Proxy installiert werden um eine doppelte Namensvergabe zu verhindern.

10.1.2 WINS Namensauflösung per DNS

Im W2K Netzwerk ist der Namensauflösung per DNS die eigentlich eingesetzte Methode. Die NetBIOS Namensauflösung existiert nur noch für die Kompatibilität mit den alten Microsoft Systemen. Falls jetzt ein W2K Rechner einen NetBIOS Namen einer IP-Adresse zuordnen soll, stellt er eine Anfrage an den DNS Server. Der für die jeweilige Zone primär zuständige Server kann so konfiguriert werden, daß er für diese Zone ein WINS-Lookup durchführt, falls er den Namen nicht auflösen kann.[1] Die Anfrage wird dann an den für diese Zone konfigurierten WINS-Server gerichtet. Falls ein nicht W2K Server für die Zone zuständig ist, muß auf dem W2K DNS-Server eingestellt werden, daß nur die dem Standard entsprechenden Records mit den anderen Servern abgeglichen werden.

[1] Achtung! Dieses ist eine Erweiterung des DNS-Systems von Microsoft, die *nicht* im Standard festgelegt ist.

Primäre nicht W2K DNS-Server und WINS

Falls im Netzwerk primäre DNS-Server eingesetzt werden, die dem Standard entsprechen, kann ein WINS-Lookup nicht direkt auf diesen Servern konfiguriert werden. Hier erfolgt die Konfiguration so, daß einen extra Zone direkt unterhalb der Hostnames erstellt wird, für die WINS-Clients zuständig ist. Hierfür wird eine W2K DNS-Server aufgestetzt, auf dem das WINS-Lookup für diese Zone konfiguriert ist. Die Zone selbst enthält auf dem W2K Server keinerlei Einträge, da diese diese ja sofort an den WINS Server weiterleiten muß. Die (W2K-) Clients werden in den `erweiterten TCP/IP-Einstellungen` so konfiguriert, daß sie den Namen dieser Zone (=Subdomain) automatisch anhängen. Falls der Client jetzt eine Anfrage zur Namensauflösung an den primären DNS-Serve richtet und eine negative Antwort bekommt, wiederholt er seine Anfrage indem er bei der die oben konfiguriert Subdomain zwischen Hostname und Domainname einfügt und die Anfrage dann an den hierfür zuständigen WINS-Server stellt.

10.2 Die WINS Datenbank

Komprimierung

Die Namenszuordnungen des WINS-Servers werden mit erweiterten Angaben in der WINS-Datenbank in einem File im `mdb` Format gespeichert. Die Records enthalten neben den Angaben über Rechnernamen und IP-Adressen noch Einträge über Diensttype, Status, Eigentümer, eine bei jeder änderung inkrementierte Versionsnummer und das Ablaufdatum. Die einzelnen Tupel können mit Hilfe der MMC manuell bearbeitet werden. Falls die Datenbank zu groß wird, wird sie vom System automatisch komprimiert. Dieses kann auch manuell mit Hilfe des Tools `jetpack` durchgeführt werden. Hierfür muß der WINS dienst beendet und nach der Komprimierung wieder manuell neu gestartet werden.

Verifizierung

Neben der Komprimierung sollte die Datenbank regelmäßig auf ihre Konsistenz überprüft werden. Die Zeitintervalle hierfür werden in den Eingenschaften für den WINS-Server festgelegt. Zur Verifizierung überprüft der WINS-Server unter anderem die Clients. Dieses bewirkt einen nicht zu vernachlässigenden Traffic auf dem Netzwerk, so daß die Zeitintervalle nicht zu klein gewählt werden sollten.

10.2.1 Backup der WINS-Datenbank

In regelmäßigen Abständen sollte ein Backup der WINS-Datenbank durchgeführt werden. Bei einem manuellen Backup wird der WINS-Dienst zuerst

gestoppt. Dann wird im Fenster für WINS per Menüeintrag ausgewählt werden daß ein Backup der Datenbank durchgeführt werden soll und wohin die Daten gespeichert werden. Das Backup kann auch so konfiguriert werden, daß es automatisch in bestimmten Intervallen durchgeführt wird. In diesem Fall muß allerdings darauf geachtet werden, daß die Backup-Datei *lokal* auf dem Rechner gespeichert wird, da das Backup sonst fehlschlägt. Das Restore erfolgt durch Auswählen des entsprechenden Menüpunktes und Auswahl des Pfades zu den Backupdateien.

10.2.2 Replizierung von WINS Datenbanken

In größeren gerouteten Netzwerken bietet es sich an, mehrere WINS-Server in verschiedenen Segmenten anzuordnen. Um die WINS-Datenbanken konsistent zu halten werden die WINS-Server so konfiguriert, daß sie sich untereinander abgleichen. Nach grundlegendem Abgleich werden nur noch die Änderungen an den WINS-Datenbanken ausgetauscht. Die Partner, mit denen sich die WINS-Server abgleichen werden in der Regel manuell konfiguriert. Falls sich die WINS Server im gleichen IP-Subnetz befinden, finden sie sich automatisch. Bei einem größeren Netzwerk mit mehreren IP-Subnetzen ist dieses nur möglich, wenn die Router Multicast unterstützen und alle WINS Server entsprechend konfiguriert werden. Die Server gehören per Default der Mulitcastgruppe `224.0.1.24` an.

Für den Abgleich der WINS-Datenbanken sind verschiedenen Szenarien möglich:

Pull Ein WINS Server kan zum Abgleich als *PULL* Partner konfiguriert werden. Hier spricht dieser Server den oder die Partner in festgesetzten Zeitintervallen an, um eine Replizierung durchzuführen. Diese Vorgehensweise wird vor allem bei langsamen Verbindungen empfohlen.

PUSH Bei der *PUSH* Einstellung wird eine Replikation nach einer festegelegten Zahl von Änderungen in der Datenbank angestoßen. Diese Änderungen erfolgen in erster Linie durch das An- und Abmelden von Clients. Die PULL Replikation wird empfohlen, falls der aktuelle Stand der WINS Einträge im Netz auf beiden WINS Servern notwendig ist. Der Nachteil liegt hier im größeren Traffic zum Abgleich der Datenbanken.

PUSH/PULL Die einzelnen WINS-Server können auch auf einen kombinierten PUSH/PULL Abgleich eingestellt werden. Hier werden eine Replikationsschwelle und ein Zeitintervall parallel definiet. Eine Replikation findet entweder nach dem festgelegten Intervall statt oder wenn die Anzahl der Änderungen überschritten wurde.

Im Netz müssen sich in der Defaulteinstellung *immer* PUSH und PULL Partner befinden. Daher muß bei zwei WINS Servern weinigstens einer auf

PUSH und der andere auf PULL eingestellt werden, bzw. beide werden für die PUSH/PULL Replikation konfiguriert.

10.2.3 Burstbehandlung von Anfragen

Falls der WINS-Server zeitweilig eine hohe Zahl von Clientregistrierungen vornehmen muß, wie dieses z.B. zu Dienstbeginn auftreten kann, kann er die jeweiligen Einträge nicht schnell genug in seinen Datenbank eintragen, um die Anfragen vor Ablaufen der Timeouts zu behandeln. Für diesen Fall kann das *Burst Handling* für den Server eingestellt werden. Falls einen gewisse Anzahl von Registrierungsanfragen in einem bestimmten Zeitraum an den Server gerichtet wird, beantwortet er die Anfragen ohne sie in seiner Datenbank abzulegen. Um mögliche Inkonsistenzen zu vermeiden wird für diese Registrierungen eine kurze Leasezeit festgelegt, so daß die Clients die Lease nach kurzer Zeit wiederholen müssen.

Kapitel 11

Internet Connection Sharing und NAT

Um in einem Netzwerk mit mehreren Clients per Dial-Up-Verbindung auf das Internet zugreifen zu können, wird an dem Rechner mit dem Internetzugang das Internet Connection Sharing eingestellt. Der Rechner mit der Dial-Up Internetverbindung fungiert jetzt automatisch als DHCP-Server, der den Clients private IP-Adressen und die Einstellungen für das Default-Gateway zuweist.Die Client-Maschinen werden so konfiguriert, daß sie die IP-Adressen automatisch erhalten. Eingehende Verbindungen werden ins Internet geroutet, wobei die Absenderadresse der ausgehenden Pakete auf die eigene vom ISP (Internet Service Provider) zugewiesene umgesetzt wird. Eingehende Pakete werden umadressiert und an den jeweiligen Empfänger im lokalen Netz weitergeleitet.

11.1 Network Address Translation

Falls sich im Netzwerk schon DNS-Server, Gateways oder DHCP-Server befinden, sollte *kein* Internet Connection Sharing genutzt werden, sondern NAT (Network Address Translation). Hier fungiert der Rechner mit der Internetverbindung als ein (transparenter) Proxy, der TCP/IP-Adressen der Clients intern auf Portnummern abbildet und dann mit die Adressen im Internet kontakt aufnimmt. Die zurückkommenden Pakete werden dann an die jeweiligen Ports weitergeleitet.

Kapitel 12

Routing und Remote Access Service (RRAS)

Der *Routing und Reomote Access Service* unter W2K bietet verschiedene Möglichkeiten der Netzwerkkonfiguration hinsichtlich Routing und Remote Access, also den Zugriff auf die Maschine bzw. das Netzwerk über Telefon- oder ISDN-Leitungen. Bei RAS werden die Netzwerkprotokolle in ein PPP-Protokoll gekapselt, also quasi durch die Punkt-zu-Punkt Verbindung getunnelt. Alle auf dem jeweiligem Rechner installierten Netzwerkprotokolle können automatisch ohne weitere Konfiguration für den Betrieb über eine Punkt-zu-Punkt Verbindung genutzt werden. Dieses ist daher möglich, da das PPP-Protokolll unterhalb der IP-Schicht ansetzt und im System ein Netzwerkdevice zur Verfügung stellt, daß auf dieser Abstraktionsebene wie eine beliebige Netzwerkkarte angesprochen werden kann. Auf der Maschine die als RRAS-Server fungiert, kann eingestellt für jedes werden ob es von dieser Maschine auch in das angeschlossene Netzwerk bzw. über die PPP-Verbindung geroutet wird.

Beim Start des RRAS Services wird für jedes an das System angeschlossene Modem und für jede parallele Schnittstelle ein sogenannter Port erstellt. Die Ports stellen ein Netzwerkgerät im System dar, über das die Kommunikation abgewickelt werden kann. Für Modems kann optional die Telefonnummer des jeweiligen Anschlusses angegeben werden. Neben den Ports für die physikalischen PPP-fähigen Netzwerkschnittstellen werden automatisch jeweils 5 L2TP (s.a. 27.0.36) und 5 PPTP (s.a. 27.0.48) Ports erstellt.

Die Konfiguration von Einwahlmöglichkeiten wird unterschiedlich durchgeführt. Ist die Maschine ein Server, der ein Mitglied einer Domäne ist, wird RRAS für die Konfiguration der Einwahlports genutzt. Hier können VPNs und die Nutzung von Modem-Pools eingestellt werden. Eine Workstation oder eine Server, der keiner Domäne angehört wird mit Hilfe des Internet Connection Wizards konfiguriert.

12.1 IP-Adressvergabe bei RRAS

Die Remote-Clients, die das Netzwerk per Modem nutzen wollen benötigen eine für dieses Netzwerk gültige IP-Adresse. Diese kann in den Clients fest verdrahtet werden, also dem Modemdevice für jeden einzelnen Remote-Partner, zu dem einen Verbindung aufgebaut werden soll, fest eingestellt werden. Diese Möglichkeit sollte allerdings nicht genutzt werden. Die Pflege der Clientadressen ist sehr aufwendig und extrem Fehleranfällig.

Der RRAS Server kann so konfiguriert werden, daß er den Clients, die sich einwählen eine IP-Adresse zuweist. Hierdurch werden die IP-Adressen im Netzwerk selbst verwaltet. Diese Möglichkeit hält den Aufwand und die Gefahr einer doppelten Vergabe von IP-Adressen gering. Die Verwaltung der IP-Adressen auf Seiten des RRAS Servers kann auf zwei Arten erfolgen:

RRAS mit eigenem Adresspool Hier wird dem RRAS Server ein eigener Adresspool zugewiesen, den er an die Clients bei der Einwahl vergibt. Dieser Adresspool wird *direkt auf dem RRAS* Server verwaltet. Zu beachten ist, daß dieser Adressbereich nicht mit den schon im Netzwerk vergebenen Adressen in Konflikt gerät.

RRAS und DHCP Falls sich schon ein DHCP Server im Netzwerk befindet, kann der RRAS Server so konfiguriert werden, daß er diesen nutzt, um gültige Adressen für die Einwahlclients zu erhalten. Der RRAS Server fordert beim Start 10 IP-Adressen vom DHCP Server an. Die erste Adresse nimmt er für sich. Die anderen werden an die Clients vergeben. Falls alle Adressen vergeben sind, fordert er einen neuen Pool von 10 Adressen vom DHCP Server an.

Falls die Nutzung des DHCP Servers konfiguriert wurde, dieser aber beim Start des RRAS Servers nicht erreichbar ist, wechselt der RRAS Server zum *Automatic Private IP Addressing* über. Hier vergibt er an sich und die Clients Adressen aus dem Bereich *169.254.0.1 - 169.254.255.254*.

12.2 RRAS Policies

Die Berechtigungseinstellungen für den RRAS-Zugriff auf das lokale Netzwerk erfolgen in zwei Ebenen.

- *Remote Access Policies*
- Einwahlberechtigungen des jeweiligen User Accounts

Die erste Ebene bildet die *Remote Access Policy*, über die die grundlegenden Einstellungen zur Einwahl auf dem jeweiligen RRAS Server konfiguriert werden. An dieser Stelle läßt sich eine Einwahl in den RRAS Server und

somit auch in das Netzwerk zentral unterbinden. Wird diese Richline z.B. entfernt ist keine Einwahl in den RRAS mehr möglich. Diese Richtlinie wird *direkt* auf dem RRAS Server gespeichert und *nicht* im Active Directory, so daß die Einstellungen verschiedener RRAS Server im Netzwerk durchaus voneinander abweichen können. Die RAS-Richtlinie setzt sich aus drei Komponenten zusammen:

Bedingungen (conditions) stellen Eingenschaften hinsichtlich der Verbindung dar, die vom Client bzw. der Verbindung erfüllt werden müssen, *damit diese Richtlinie überhaupt angewandt wird.* Bespiele hierfür sind:

- Zeit der Einwahl,
- IP-Adresse des Clients (bei fester vergebenen IP-Adressen),
- Gruppe der der Client angehören muß,
- User ID des Clients

Berechtigungen (permissions) Hier werden die globalen Einwahlberechtigungen festgelegt, wie z.B. einer Gruppe von Usern die Einwahl zu erlauben. So kann z.B. der Gruppe der Administratoren die Einwahl jederzeit erlaubt werden, einer Benutzergruppe wird die Erlaubnis nur zu den Geschäftszeiten erlaubt.

Profil (profile) Im Profil werden Einstellungen hinsichtlich der Verbindung festgelegt. Eine Verbindung kann z.B. auf ein bestimmtes Verschlüsselungs- oder Authentifikationsprotokoll festgelegt werden. Die Begrenzung einer Verbindung auf eine maximale Verbindungsdauer wird auch hier festgelegt.

Mit der zweiten Ebene werden die Einstellungen für den jeweiligen User festgelegt. Diese erfolgen bei den Einstellungen für den Useraccount unter `Einwahlberechtigungen` und werden daher im Active Directory gespeichert.

12.2.1 Anwendung der RRAS Policies

Erfolgt jetzt ein Einwahlversuch, so werden vom System die verschiedenen Berechtigungen in einer festgelegten Reihenfolge überprüft.

1. Prüfung der *Routing- und Remotezugriffsrichtlinie*
   Sie wird auf zutreffende Bedingungen (z.B. Tageszeit) überprüft. Falls hier keine Bedingungen zutrifft (s.o.) wird der Zugang schon hier abgeblockt. Auch eine nicht vorhandene Richtlinie untersagt den Zugriff. Falls eine Bedingung zutrifft werden die nächsten Punkte überprüft.

2. Überprüfung der Einwahlberechtigungen des jeweiligen Useraccounts
   Die Einwahlberechtigungen können so eingestellt werden, daß der Zugriff erlaubt oder verboten wird, oder daß Eingestellten Berechtigungen, die in der *Remote Access Policy* eingestellt sind, über den Zugriff entscheiden.

12.3 Authentifizierungsprotokolle

Für die Authentifizierung über PPP-Verbindungen wurden verschiedene Protokolle entwickelt und teilweise in RFCs veröffentlicht. Die Art der Authentifizierung für eine Einwahlverbindung wird auf dem Feld *Security* in den Eigenschaften für den RRAS Server eingestellt. Die Einstellungen können nur für den gesamten Server erfolgen, nicht für einzelne Einwahlports. (?) Bei Einwahl in einen RRAS Server unter W2K kann mit Hilfe der folgenden Protokolle eine Authentifizierung erfolgen:

PAP Das *Password Authentication Protocol* bietet ein reines Name-Passwort basiertes Login. Der gravierende Nachteil hier ist, daß die Passwörter im Klartext übertragen werden. Des weiterten besteht natürlich die Möglichkeit von Brute-Force Angriffen, wobei die Sicherheit hier natürlich durch eine geschickte Passwortwahl erheblich vergrößer werden kann.

PAP ist in der Regel immer verfügbar. Aufgrund der Nachteile hinsichtlich der Klartext-Passwortübertragung sollte es nur dann eingesetzt werden, wenn einer der Kommunikationspartner kein anderes Authentifizierungsprotokoll unterstützt. Beim Einsatz der unverschlüsselten Passwortübermittlung ist auf jeden Fall darauf zu achten, daß die Übertragungskanäle relativ sicher sein sollten.

SPAP Das *Shiva Password Authentication Protocol* arbeitet mit reversibel verschlüsselten Passwörtern, so daß eine gewisse Sicherheit hinsichtlich des Logins gegeben ist.

SPAP ist nicht allzu weit verbreitet, bzw. wird nicht bei allen Systemen direkt mitgeliefert und wird daher eher selten eingesetzt.

CHAP Das *Challenge Handshake Authentication Protocol* oder Message Digest 5 (MD-5)- CHAP arbeitet mit MD5 Verschlüsselung. Der hier eingesetzte Algorithmus bietet eine sehr sichere Einwegverschlüsselung und somit eine große Sicherheit gegen Angriffe.

Das CHAP- Protokoll ist sehr weit verbreitet und wird bei den gängigsten Systemen mitgeliefert. Aufgrund der verschlüsselten Passwortübertragung und seiner Verbreitung sollte dieses Authentifizierungsprotokoll bevorzugt eingesetzt werden.

Der Login-Vorgang läuft bei CHAP 3-Stufig ab:

1. Einer der beiden Partner (bei RRAS unter W2K immer der RRAS-Server) sendet dem anderen eine Anforderung zur Authentifikation. Das Anforderungs-Paket enthält einen für diese Sitzung eindeutigen Sitzungsschlüssel und einen willkürlich erzeugten String (der sogenannte *Challenge* String).
2. Die Gegenseite empfängt dieses Paket und erzeugt ein Antwortpaket, indem der Username und mit die mit einer Einwegverschlüsselung verknüpften Elemente Passwort, Sitzungsschlüssel und Challenge-String enthalten sind.
3. Wenn die anfordernde Seite (idR der Server, s.o.) das Paket erhält vergleicht extrahiert er hieraus den Usernamen. Er erzeugt aus den in seiner lokalen Authentifizierungsdatenbank hinterlegten Daten von Username und Passwort auf die gleiche Weise ein Paket und vergleicht die beiden miteinander. Sind die verschlüsselten Daten gleich, ist die Authentifizierung erfolgreich. CHAP bietet daneben noch Optionen an, um diesen Vorgang während der Sitzung in regelmäßigen Abständen zu wiederholen. Hierdurch läßt sich erkennen, wenn eine Sitzung "entführt" wurde, der Gegenpart sich inzwischen geändert hat.

MS-CHAP ist ein propritäres Authentifizierungsprotokoll, daß ähnlich wie CHAP arbeitet. Es ist außerhalb der Microsoft-Welt kaum verbreitet. Die Passwortverschlüsselung arbeitet hier wie auch bei Standard-CHAP mit einem Algorithmus zur Einwegverschlüsselung. MS-CHAP ermöglicht eine Punkt-zu-Punkt Verschlüsselung der übertragenen Daten, wobei natürlich beide Seiten der Verbindung MS-CHAP unterstützen müssen. Ein W2K arbeitet in der Defaulteinstellung mit MS-CHAP zur Authentifizierung.

MS-CHAP kann nur dann eingesetzt werden, wenn alle beteiligten Systeme dieses Protokoll unterstützen. Daher sollte wenn möglich mit offenen Standards wie CHAP gearbeitet werden.

MS-CHAP v2 ist eine Weiterentwicklung des proprietären MS-CHAP Protokolls. Es bietet gegenüber von MS-CHAP eine wechselseitige Authentifizierung, eine stärkere Verschlüsselung der übertragenen Daten und unterschiedliche Schlüssel für den Versand und den Empfang von Daten. W2K bietet bei der Installation eines VPN vorrangig die Authentifizierung mit MS-CHAP v2 an. Das MS-CHAP v2 Protokoll kann nur von W2K Clients und nur bei VPN-Verbindungen genutzt werden. NT4 und Windows 98 Maschinen können MS-CHAP v2 nur für die Authentifikation bei Eröffnung einer VPN Verbindung einsetzen.

MS-CHAP v2 wird nur von Windows 2000 unterstützt, kann daher nur in einer streng homogenen Umgebung eingesetzt werden. Beim prak-

tischen Einsatz ist abzuwägen, ob die Anforderungen den Einsatz von MS-CHAP v2 unbedingt erforderlich machen und somit die zukünftige Richtung der Lösung festgeschrieben wird, oder ob sich das gegebene Ziel nicht auch mit einer flexibeleren Lösung erreichen läßt.

EAP Das *Extensible Authentifikation Protocol* stellt eine API (Application Programming Interface, Programmierschnittstelle) für andere Authentifikationsprotokolle zur Verfügung. EAP ist in den RFCs 2284 und 2716 definiert. Mit Hilfe von EAP können die Kommunikationspartner vor der eigentlichen Authentifizierung aushandeln, welche Authentifizierungsmethode verwandt wird. Aufgrund der Ausführung als API können auch in Zukunft entwickelte Protokolle auf EAP aufsetzen und dieses Nutzen. Zur Zeit bietet EAP die Möglichkeit die folgenden Protokolle zu nutzen:

MD5-CHAP Verschlüsselung von Usernamen und Passwörtern mit MD5 (s.o.)

Transport Layer Security wird bei Smart-Cards und anderen Sicherheitsmechanismen gentutzt, die verschiedene Medien zur Authentifizierung einsetzen.

Dritthersteller bieten u.U. Systeme an, die auf EAP aufsetzen können.

Die EAP Authentifizierung in den Eigenschaften auf der `Security` Karte eingestellt.

12.4 RAS-Protokolle

W2K unterstützt verschiedene RAS Protokolle:

PPP ist das am weitesten verbreitete RAS-Protokoll. PPP ist ein offener Standard und kann relaiv einfach implementiert werden.

SLIP Das *Serial Line Internet Protocol* ist ein offenes Protokoll zur Punkt-zu-Punkt Verbindung. Es kann als das Vorläuferprotokoll von PPP angesehen werden, bietet allerdings erheblich weniger Möglichkeiten und wird daher kaum noch eingesetzt. W2K unterstützt PPP nur noch als SLIP-Client; die Verbindung zu einem W2K RAS-Server mittels SLIP ist nicht möglich.

Microsoft RAS ist ein proprietäres Punkt-zu-Punkt Protokoll von Microsoft, daß in den Vorläufer-Versionen zu W2K eingesetzt wurde. Es íst außerhalb der MS-Welt kaum verbreitet. Es wird benötigt, falls sich ein W2K-Client mit einem RAS-Server verbinden muß, der unter WfW, WinNT 3.1, MSDos oder mit LAN Manager läuft.

ARAP Das *AppleTalk Remote Access Protocol* wird für PPP-Verbindungen in AppleTalk-Netzen eingesetzt und ist auch nur hier verbreitet. W2K unterstützt ARAP auf der Serverseite, so daß sich Clients die dieses Protokoll nutzen auf dem W2K Server einwählen können.

12.5 Verschlüsselte Kommunikation unter RRAS

Eine verschlüsselte Kommunikation über die PP-Verbindung ist zum einen Möglich, wenn ein verschlüsselter Kanal über die Verbindung aufgebaut wird, oder wenn die beiden Endpunkte der PP-Verbindung, der RAS-Server und der Client die Daten verschlüsseln wenn sie diese an die Verbindung senden. Die Verschlüsselung wird mit Hilfe einer Policy aktiviert, wobei zwischen mehrenen Optionen gewählt werden kann, die unterschiedliche Arten der Verschlüsselung ermöglichen. Jede dieser Optionen kann einzeln eingestellt werden, so daß auch eine Kombination möglich ist:

keine Verschlüsselung Diese Gruppe darf auch unverschlüsselte Verbindungen aufbauen.

Standardverschlüsselung (Basic) Die Mitglieder dieser Gruppe können mit einer 56-Bit DES Verschlüsselung auf IPSec oder mit einer 40-Bit MPPE[1] Verschlüsselung der Verbindung gearbeitet.

Starke Verschlüsselung Hier die IPSec 56-Bit DES oder die MPPE 56-Bit Datenverschlüsselung aktiviert.

Stärkste Verschlüsselung Bei Wahl der starken Verschlüsselung dürfen die Gruppenmitglieder eine Verbindung aufbauen, die mit IPSec und Triple DES (3DES) oder mit MPPE 128-Bit verschlüsselt wird. Zur Nutzung der 128-Bit Verschlüsselung muß allerdings das W2K Pakte für die starke Verschlüsselung vom MS-Update-Webserver geladen werden!

12.6 Weitere Konfigurationsoptionen von RRAS

Callback Mit Hilfe der *Callback* Funktion kan für spezifische Benutzer festgelegt werden, daß die Verbindung nach erfolgreicher Authentifizierung unterbrochen wird. Der RRAS Server baut dann selbstständig eine Verbindung zu einer vorkonfigurierten Telefonnummer oder zur Nummer des Anrufers auf. Aus Sicherheitsgründen sollte möglichst ein Rückruf zu einer vorkonfigurierten Nummer erfolgen.

[1] MPPE wird zur Verschlüsselung der Daten eingesetzt, die bei einer PPTP- VPN Verbindung zwischen dem Client und dem Server übertragen werden. MPPE bietet 3 Sicherheitsstufen: 40, 56 und 128 Bit.

DHCP-Relay-Agent In RRAS ist ein *DHCP-Relay-Agent* implementiert, der die Broadcasts eines DHCP-Clients zur Ermittlung seiner IP-Adresse an einen DHCP-Server in einem anderen Netzwerksegment weiterleiten kann (s.a. 27.0.25). Hierbei wird die Anfrage gezielt an den jeweiligen Server weitergeleitet. Dieser erkennt aufgrund des Formates, daß die Anfrage über einen Forwarder gekommen ist, und sendet seine Antwort entsprechend direkt an diesen zurück.

Dial-in Konfiguration Die Möglichkeit der Einwahl wird je nach Typ der RRAS-Maschine unterschiedlich konfiguriert. Auf einem *Standalone*-Server erfolgen die Einstellungen im `Dial-In` Feld der Eigenschaften-Box für den jeweiligen User-Accounts. Hier ist nur einen Einstellung zwischen grundsätzlicher Erlaubnis oder grundsätzlichem Verbot der Einwahl möglich.

Ein Server, der in das *Active-Directory* eingebunden ist wird in den Eigenschaften für `Active Directory Benutzer und Computer` konfiguriert. Hier wird der RRAS-Server global so eingestellt, daß die Einwahl grundsätzlich erlaubt oder verboten ist. Ist die Einwahl erlaubt werden für bestimmte Profile oder direkt für einzelne Useraccounts die Feineinstellungen mit Hife von Policies festgelegt. Diese überschreiben auch die globalen Einstellungen für RRAS. Mit Hilfe der *RAS-Richlinien* läßt sich unter W2K genau einstellen welcher RAS-Client bzw. User sich wann in das Netzwerk einwählen darf. Hierfür muß sich die Domäne jedoch im einheitlichen Modus befinden. Neben diesen Optionen ist auch eine Überprüfung der Telefonnummer des Anrufers möglich, so daß die Einwahl nur bestimmten Anrufern gestattet wird. Zu beachten ist bei dieser Lösung jedoch, daß die gesamte Kommunikationsstrecke die Übermittlung von Telefonnummern unterstützen muß.

Die Einwahloptionen für das System kann nur für Benutzer oder Gruppen angepaßt werden. Eine Einstellung für ein spezifisches Gerät (z.B. Modem x) ist nicht möglich. (?) Für die Nutzung der RAS-Richtlinien ist allerdings der Einheitliche Modus der Domäne voraussetzung. Bei Servern im gemischten Modus besteht nur die Möglichkeit dem einzelnen User die grundsätzliche Berechtigungen zur Einwahl zu erteilen oder zu verweigern.

Bei nach der Authentifizierung des Clients wird zuerst die *Default Remote Access Policy* überprüft, die die allgemeinen Einstellungen für jeden sich einwählendne Client festlegt. Danach werden die Einstellungen der Policies des einzelnen Benutzers übernommen, die die Default Remote Access Policy überschreiben können. Falls die Default Remote Access Policy entfernt wurde, kann sich niemand mehr über diesen RRAS Server einwählen.

Dial on Demand Ein für *Dial on Demand* konfigurierter WAN-Router baut bei Bedarf eine Verbindung zu einem anderen Rechner per Wählleitung auf. Der WAN-Router ist so konfiguriert, daß seine Routingtabellen für die Dial on Demand Einträge auf das Device zeigen, über das der Datenverkehr für die Wählverbindung abgewickelt wird. Treffen bei diesem Device nun IP-Pakte ein, wird eine Verbindung aufgebaut. Weiterhin kan eingestellt werden, daß nach erfolgreichem Verbindungsaufbau ein- oder mehrere statische Routen über dieses Device erstellt werden.

Multilink und BAP RRAS ermöglicht es eine Verbindung parallel über mehrere Kanäle (Modems, ISDN-Kanalbündelung) aufzubauen um die Bandbreite zu vergrößern. Diese Kanalbündelung wird durch eine Erweiterung des PPP Protokolls erreicht. Hierfür stehen die Protokolle PPP-Multilink (RFC 1990) oder das *BAP (Bandwith Allocation Protocol, RFC 2125)* zur Verfügung. BAP bietet gegenüber PPP Multilink den Vorteil, daß hier dynamisch weitere Kanäle hinzuzuschalten bzw. geschlossen werden können.

Multiprotokoll Routing Die Routingfunktionalität ermöglicht das Routing der Protokolle *IP* und *IPX*.

NAT RRAS bietet *Network Address Translation (NAT), s.a. 27.0.43*, bei der eine IP-Adresse auf mehreren anderen IP-Adressen abgebildet werden kann. Dieses wird z.B. bei der Verbindung eines privaten Netzes (Intranet) mit dem Internet genutzt.

RAS Einwahl von Außerhalb Es kann eine Einwahl in den Rechner bzw. das angeschlossene Netzwerk von außerhalb per Modem- oder ISDN-Leitung stattfinden. Hierbei können Verbindungen mit den Protokollen *IP*, *IPX* und *Appletalk* aufgebaut werden.

RIP und OSPF Mit Hilfe von RRAS werden für IP-Netze die Routing Protokolle *RIP* (Routing Information Protocol, s.a. 27.0.54) und *OSPF* (Open Shortest Path First, s.a. 27.0.47) unterstützt.

Paktetfilterung Die RRAS Implementierung ermöglicht eine einfache Paketfilterfuntionalität. Hier kann z.B. eingestellt werden, daß IP-Pakete, die von außerhalb kommend an eine bestimmte Adresse oder einen bestimmten Port gehen, nicht weitergeleitet werden.

RAS Kontosperrung RRAS läßt sich konfigurieren, daß ein Konto deaktiviert wird, wenn hier wiederholt eine Einwahl aufgrund eines falschen Passwortes fehlgeschlagen ist. Diese Möglichkeit ist in der Defaulteinstellung allerdings deaktiviert. Sie läßt sich nur direkt in der Registry einstellen.

RADIUS-Authentifizierung RRAS bietet die Möglichkeit, daß zur Authentifizierung eines Bentzers ein *RADUIS* Server kontaktiert wird. Der W2K Server arbeitet in diesem Fall als RADIUS-Client. Die Nutzung eines RADIUS-Servers wird bei den RRAS Optionen konfiguriert.

EAP Mit Hilfe der *EAP (Extensible Authentifikation Protocol)* Schnittstelle lassen sich verschiedene andere Authentifizierungsmöglichkeiten verwenden.

VPN Ein W2K Server läßt sich mit Hilfe von RRAS als VPN (Virtual Private Network) Server einsetzen. VPN Clients können hiermit einen gesicherten Kanal über das Internet zum privaten Netzwerk aufbauen (s.a. 27.0.68). Die VPN-Verbindungen laufen über sogenannte VPN-Ports ab, die bein unter den Einstelloptionen für RRAS konfiguriert werden können.

Kapitel 13

DHCP Konfiguration

Mit Hilfe eines DHCP-Servers wird die Zuweisung der IP-Adressen an die Clients automatisiert. Die Servermaschinen sollten feste IP-Adressen erhalten. Bei der Konfiguration des DHCP-Servers werden genügend IP-Adressen für die sich gleichzeitig am Netz angemeldeten Clientmaschinen "reserviert", es wird ein sogenannter Scope gebildet. Diese Adressen müssen fortlaufend in einem zusammenhängenden Bereich gewählt werden.

Bei AD integrierten DCHP-Servern muß der DHCP-Server authorisiert werden, um IP-Adressen an die Clients zu vergeben. Falls dieses nicht der Fall ist, wird der Client eine Fehlermeldung wie *"DCHP unavailable"* ausgeben.(?)

Aus Redundanzgründen werden in einem Subnetz manchmal zwei DHCP-Server betrieben. Wenn ein Client einen Broadcast zur Adressabfrage sendet wird die Adresse von dem DCHP-Server vergeben, der zuerst antwortet. Die Scopes auf den Servern werden hier so eingestellt, daß auf beide Maschinen der gesamte Adressbereich als Scope definiert wird, wobei zwei sich aneinander anschließende Bereiche definiert werden, die von der Adressvergabe ausgeschlossen sind. Dieser Bereich umfaßt auf der einen Maschine ca. 20% des gesamten Adressbereichs, während er auf der anderen Maschine 80% aller Adressen einschließt.

Wird ein Adressbereich erweitert, oder sollen andere Änderungen am Scope vorgenommen werden, sollten alle Clients ihre IP-Adressen erneuern. Hier müssen dann alle Clients gleichzeitig vom Netz genommen werden bevor die Änderungen am Scope durchgeführt werden können. Soll ein "gleitender" Übergang erfolgen, oder kann der Bereich der zu vergebenden Adressen aus irgendeinem Grund nicht zusammenhängend gewählt werden kann, so müssen die einzelnen Bereiche zu einem sogenannten *Superscope* zusammengefaßt werden.

Wird bei laufendem DHCP-Server ein Scope neu erstellt, muß dieser nach Abschluß der Konfiguration aktiviert werden.

13.1 Superscopes

Der *Superscope* ist eine übergeordnete logische Einheit, die mehrere Scopes enthalten kann. Der Superscope kann verwaltungstechnisch als eine Einheit angesprochen werden wie jeder andere Scope auch.

Die Bildung von Superscopes bietet sich an, falls der gesamte zu nutzende Adressbereich nicht kontinuierlich verläuft, oder wenn er erweitert werden soll. Die einzelnene Adressbereiche bilden dann den Superscope. Mit dieser Maßnahme wird eine Umstellung oder Erweiterung des Netzwerkes im laufenden Betrieb ermöglicht, da der ursprüngliche Scopt nicht extra gelöscht werden muß und die Client nicht zu einer Erneuerung ihrer Adressen aufgefordert werden müssen. Sich neu anmeldenden Rechner erhalten jetzt automatisch Adressen aus dem neuen Superscope, der beide ursprünglichen Adressbereiche umfaßt.

Auch wenn ein Subnetz in mehrere logische Segmente unterteilt werden soll (Multinet), wird hierfür ein Superscope eingerichtet. Dieser enthält dann die einzelnen Scopes für die Adressbereiche der logischen Subnetze.

Ein Superscope kann im Verwaltungstool für den DHCP Server erstellt werden.

Eine feste Zuordnung von IP-Adressen zu Clientmaschinen ist möglich, indem der IP-Adresse eine MAC-Adresse der NIC zugeordnet wird. Diese Adressen werden bei einer Anfrage nach Überprüfung der MAC-Adresse vergeben. Ansonsten verläuft die Adressvergabe wie bei allen anderen Anfragen auch. Aus diesem Grunde dürfen sich reservierte Adressen nicht außerhalb des Scopes befinden. Auch die Zuordnung zu einem von der Vergabe ausgenommenen Berereich (*Exclusion-Range*) ist nicht sinnvoll, da dann keine Vergabe stattfindet.

Es ist in keinem Fall möglich, einigen Maschinen Adressen aus einem bestimmten Bereich zuzuordnen, also eine Zuordnung einer Menge von MAC-Adressen zu einer Menge von IP-Adressen.

13.2 User-Classes

Falls für eine Gruppe von Usern/Maschinen eine spezielle Konfiguration gelten sollt, erfolgt dieses über die Definition einer Benutzerklasse (*User-Class*). Die Benutzerklasse wird in den Eigenschaften des DHCP-Servers deklariert. Nach Vergabe eines Namens und einer eideutigen Class-ID werden die Eigenschaften für diese spezielle Gruppe eingestellt. Dieses kann z.B. eine kürzere Leasedauer für mobile Rechner sein, oder ein anderer anzusprechender DNS-Server. Auf den Clientmaschinen, die dieser Benutzerklasse angehören sollen, wird die Klassen ID dem Befehl `ipconfig /setclassid` zugeordnet.

13.3 DHCP und DDNS (dynamisches DNS)

DHCP Clients, die mit Windows 2000 oder Windows 98 laufen können ihre IP-Adresse automatisch bei einem DNS-Server registrieren, der den `RFC 2136` unterstützt. Im Falle der Adressverwaltung mittels DHCP kann dieses auch vom DCHP-Server vorgenommen werden. Dieses wird in den Eigenschaften für den DHCP-Server oder für einen Scope des DHCP-Servers eingestellt. An den (primären) DNS-Server werden in einem solchen Falle DNS-Updates gesandt. Falls im Logfile eines DNS- Servers solche Nachrichten in regelmäßigen Abständen auftauchen und abgewiesen werden, sollte nach einem falsch konfigurierten DHCP-Server im Netzwerk Ausschau gehalten werden.

13.4 DHCP Relay Agent

Die Client-Anfragen für DHCP erfolgen mittels Broadcasts, so daß sie im Regelfall nicht geroutet werden. Um einen Anfrage an einen DCHP-Server weiterzuleiten, der sich in einem anderen Subnetz befindet besteht zum einen die Möglichkeit einen kompatiblen Router einzusetzen. Die andere Möglichkeit ist die Nutzung eines *DCHP Relay Agent*. Dieses ist ein speziell konfigurierter Server, auf dem im Falle von W2K das RRAS-Protokoll installiert sein muß (s.a. **??**). Der DCHP Relay Agent erkennt die Anfrage eines Clients und leitet sie direkt an den in seiner Konfuration eingestellten DHCP-Server weiter. Dieser erkennt, daß die Anfrage über eine Relay Agent erfolgte und sendet die gewünschten Informationen an diesen zurück, der sie dann an den Client weiterleitet. Der DCHP Relay Agent muß so konfiguriert werden, daß dieser Service für die Interfaces eingerichtet wird, aus dessen Subnetzen Anfragen erwartet werden. Dieses kann z.B. auch ein ISDN-Interface eines RRAS Einwahlservers sein.

Kapitel 14

Das DNS System

Windows 9x und Windows NT 4.0 unterstützen selbst kein dynamisches DNS. Die Unterstützung erfolgt hier über einen (Windows 2000) DHCP-Server. Falls kein W2K DHCP-Server im Netz läuft, können diese Maschinen manuell eingetragen werden.

14.1 Zonen

Ein DNS Server verwaltet eine logische Einheit, eine sogenannte *Zone*. Hier werden Gruppen von Rechnern zusammengefaßt, die auf irgendeine Art und Weise logisch zusammengehören. Eine Zone *im Sinne von DNS* kann sich über mehrere Domänen erstrecken oder auch ein Teil einer Domäne sein.

Innerhalb einer Zone wird ein DNS-Server zum *primären* (autorisierenden) DNS Server erklärt. Dieser hat das alleinige Verwaltungsrecht (also das Recht Einträge zu ändern) an der DNS-Zone. Diese Hierarchie wurde aus Gründen der Konsistenz eingeführt. Die nicht autorisierenden DNS Server in der Zone dienen daher nur dazu die Rechenlast zu verteilen. Sie besitzen Kopien der zentralen DNS Datenbank des authorisierenden DNS-Servers. Der Vorgang des Kopierens wird als Zonentransfer oder Replikation bezeichnet. Zur Verringerung der Netzlast wurde ein Verfahren entwickelt, mit dem beim Zonentransfer nicht mehr die gesamte Datenbank übertragen wird, sondern nur kann der Zonentransfer auch *inkrementell* erfolgen. Das heißt, daß nur noch die Änderungen an der Datenbank übertragen werden. Dieses Verfahren ist in *RFC 1995* festgelegt.

Der Zonentransfer kann entweder im *Pull-* bzw. *Polling-* Verfahren oder im push Verfahren erfolgen. Beim Pull-Verfahren fragen die sekundären Server in regelmäßigen Abständen beim primären Zonenserver an, ob sich in der Zonendatenbank Änderungen ergeben haben.
Beim Transfer im *Push-* Verfahren initiert der primäre Server die Zonentransfers. Er sendet den sekundären Servern eine Benachrichtigung, falls sich Änderungen an seiner Datenbank ergeben haben. Der Sekundäre Ser-

ver fragt beim Master dann die Änderungen ab. Die Konfiguration für diese Verfahren erfolgt direkt in der Registry.

14.2 Form eines DNS-Eintrags

Ein DNS- Eintrag wird als *Ressorce Record* (RR) bezeichnet. Neben der Zuordnung von Hostnamen zu IP-Adresse wird hier auch der Typ des Eintrags festgelegt, der bestimmt für welchen Einsatzzweck dieser DNS-Name vorgesehen ist. So wird ein `MX`-Record z.B. die IP-Adresse für einen Mail Server festlegen, an den die Mail für diesen DNS-Namen gesandt wird. Für einen NS-Record können u.a. die folgenden Typen festgelegt werden:

SOA Definiert allgemeine Parameter.

NS Nameserver

A Host

CNAME Aliasname für einen Host

MX Mail Exchange, Mail-Server

HINFO liefert Informationene über einen Host

WINS Host ist ein WINS-Server

PTR Pointer (Zeiger) Einträge

14.2.1 Reverse Lookup Zone

Zur rückwärtigen Zuordnung einer IP-Addresse auf einen DNS-Namen speichert ein DNS-Server zusätzliche Einträge in der speziellen *Reverse-Lookup-Zone* in der Zonendatei für die Domain *in-addr.arpa* . Falls ein Rechner den Hostnamen sucht, der einer speziellen IP-Adresse (a.b.c.d) zugeordnet ist, sucht der DNS-Server in der Reverse-Lookup-Zonendatei nach dem PTR Eintrag `d.c.b.a.in-add.arpa`. Dieser enthält den gewünschten Hostnamen sowie die zugehörige IP-Addresse.

14.2.2 Formen der DNS Abfrage

Ein Client, der einen anderen Rechner adressieren will, stellt eine Anfrage an den DNS-Sever, der in seiner Konfiguration eingetragen ist. Dieser DNS Server sieht zuerst in seinem lokalen Cache und dann in seiner Datenbank nach, ob er diesen DNS-Namen zuordnen kann. Falls nicht, leitet er die Anfrage an einen in der Hirarchie über ihm stehenden Server weiter. Dieses geht so lange, bis schließlich ein Eintrag aufgelöst werden kann, oder ein Root-Server gefragt werden muß. Diese Art der Abfrage wird als *iterative*

Abfrage bezeichnet.
Eine andere Form der Abfrage ist die *rekursive* Abfrage. Falls der Nameserver den Namen nicht auflösen kann, sendet er dem Client die Adresse des hierarchisch über ihm stehenden DNS-Servers, der dann vom Client direkt gefragt wird.
Die inverse Abfrage schließlich ist eine Anfrage, bei der zu einer gegebenen IP-Adresse ein Hostname geliefert wird.

Das DNS-Caching läßt sich für jeden DNS Server hinsichtlich der Zeitdauer, wie lange ein Abfrageergebnis gecached wird, individuell einstellen. Seit Windows 2000 Workstation (W2K Professional) läßt sich das Caching auch auf den Clients einstellen.

Neben dem DNS-Cache auf den Workstations und dem dynamischen DNS ist bei W2K auch das *Round-Robin-DNS* eingeführt worden. Hier sind in der Zonendatei für einen FQDN (Fully Qualified Domain Name) mehrere IP-Adressen angegeben. Mit dieser Konfiguration besteht die Möglichkeit eine Lastverteilung durchzuführen. Das DNS-System liefert jeder Anfrage für einen so konfigurierten Hostnamen eine andere IP-Adresse zurück. Hiermit ist für den Client völlig transparent, daß die Ressourcen parallel von verschiedenen Servern geliefert werden.

14.3 Active Directory Integration

Unter W2K kann die Speicherung der DNS auch im Active Directory erfolgen. Falls jetzt das System der primären und sekundären DNS- Server eingehalten wird, so daß Änderungen nur von einem Rechner aus erfolgen können, wird man beim Zonentransfer von einer *Single-Master-Replikation* sprechen. Windows 2000 bietet die zusätzlich die Möglichkeit, daß bei einem AD basierten DNS-System Änderungen an der DNS-Tabelle von jedem beliebigen DNS-Server durchgeführt werden können. Dieses wird auch als *Multi-Master-Replikation* bezeichnet. Wenn der DNS-Server in das Active Directory integriert wurde besteht die Möglichkeit ACL-Listen von Benutzeraccounts zu führen, die diese Zonen updaten dürfen (*Allow only secure updates*).

Unter NT oder Un*x erfolgt immer eine vollständige Replikation der Zonendatei, wohingegen ein Active Directory basiertes DNS-System unter W2K nur die Änderungen repliziert.

In gemischten Umgebungen können sowohl das herkömmliche (NT4) DNS als auch das Active Directory basierte DNS – auf verschiedenen DNS Servern – parallel eingesetzt werden. Wird ein Domänencontroller mit Active Directory installiert, so wird diese Maschine zusätzlich *automatisch* als DNS Server konfiguriert.

14.3.1 Dynamisches DNS per DHCP

Um dem W2K- DHCP-Server zu ermöglichen die DNS-Einträge dynamisch zu aktualisieren, die Datenbank des DNS-Servers also bei der Vergabe einer Adresse an einen Host und bei Ablauf der Leasezeit zu ändern, muß das System auf Active Directory aufsetzten. Die DNS- Einträge enthalten jetzt eine Liste mit Eigenschaften, in der auch der Eigentümer eingetragen ist, der diesen Eintrag in die Datenbank eingefügt hat. Im Falle eines dynamischen Eintrags vom DHCP-Server können die Einträge auch nur von diesem gelöscht werden, was in der Praxis Probleme mit sich bringen könnte. Aus diesem Grunde wurde die Sicherheitsgruppe *DnsUpdateProxy* eingeführt. Alle Rechner die dieser Gruppe angehören fügen Einträge in das DNS System ein, ohne sich als Eigentümer für diesen Wert in die Datenbank einzutragen. Diese Einträge können dann später von anderen Rechnern problemlos wieder gelöscht werden.

Kapitel 15

Netzwerksicherheit

W2K bietet verschiedene Möglichkeiten und Hierarchieen um die Sicherheit und Vertrauchlichkeit der Daten im Netzwerk zu gewährleisten.

15.1 Windows 2000 PKI

W2K erlaubt es einer Organisation als ihre eigene *CA* aufzutreten, und somit digitale Zertifikate zu erzeugen und zu verteilen. Hier wird zwischen zwei Typen von *CA*'s unterschieden:

Enterprise CA Die Form der *Enterprise CA* wird gewählt, falls die Zertifizierung und Authentifizierung nur *innerhalb* des logischen Netzes der Organisation gültig werden soll. Um ein verteiltes System zu implementieren, kann eine Hierarchie mit *Root-* und *Subordinate CA's* aufgebaut werden. Die Zertifikate der Subordinate CA's werden dann von der eigenen Root CA signiert. Die Enterprise CA stützt sich auf das Active Directory und ist somit auf auf W2K-Systeme beschränkt. Alle Benutzer und Computer müssen einen Account im AD besitzen um die Zertifikate dieser CA nutzen zu können. In heterogenen Netzwerken (Internet) kann diese Form daher nicht verwandt werden.

Für die Implementierung einer Enterprise CA werden neben den administrativen Rechten am CA-Server selbst auch noch Rechte zur Konfiguration des Active Directory und des DNS benötigt. Falls weitere Zertifikate im Active veröffentlicht werden sollen, muß der veröffentlichende Mitglied der Gruppe der *Zertifikationsdistributoren (?) (Cert Publisher)* sein.

Stand-alone CA Die *Stand-alone CA* wird in einem heterogenen Netzwerk gewählt, da sie kein Active Directory für die Funktion benötigt. Die Zertifikate können jetzt auch ausserhalb der eigenen Organisation verteilt und eingesetzt werden. Falls die Zertifikate der CA auch

von dritten anerkannt werden sollen, muß eine *Stand-alone Subordinate CA* installiert werden, die sich wiederum von einer (externen) *Root CA* signieren läßt.

Innerhalb der Organsiation können die Zertifikate mit Hilfe des Active Directory repliziert. Die PKI ist allerdings nicht in jedem Fall auf Active Directory angewiesen. Zertifikate können auch mit Hilfe von Webseiten oder in anderer Form verteilt werden. Die PKI wird von Windows 2000 in Verbindung mit *SSL (Secure Socket Layer)* oder *IPSec (IP Security)* genutzt. Mit Hilfe von Zertifikaten können sich die einzelnen an der Kommunikation beteiligten Partner gegeneinander authentifizieren. Die Kommunikation erfolgt dann verschlüsselt über SSL oder IPSec.

15.1.1 Installation und Nutzung von Zertifikaten

Ein Zertifikat erlaubt die Authentifizierung eines Users oder eines Computers. Um dieses zu nutzen, muß es auf dem Computer oder für den Benutzeraccount installiert werden. Auf dem Computer wird ein Zertifikat installiert, indem sich der Administrator mit dem Administratoraccount anmeldet, die Zertifizierungsdienste installiert und dann ein Zertifikat im Namen des Computers für diesen anfordert. Der Computer hat dann ein Zertifikat, mit dem er sich gegenüber anderen Stellen authentifizieren kann. Um diesen Vorgang zu automatisieren wird eine *Gruppenrichtlinie für öffentliche Schlüssel (Public Key Group Policy)* für die Domäne erstellt. Hier wird allen gewünschten Rechnern das Recht zur Eintragung eines Zertifikates (Enroll permission) gegeben.

Der User kann das Zertifikat von der CA anfordern. Wie dieses geschieht ist abhängig vom Typ der CA. Bei einer Enterprise-CA kann das Zertifikat aufgrund der Bindung an das Active Direktory mit Hilfe eines Wizards angefordert werden. Bei den Stand-alone CA's erfolgt dieses über eine Webseite.

15.1.2 Templates für Zertifikate

Ein Enterprise CA kann Zertifikate für verschiedene Aufgaben basierend auf Systemrichtlinien (Policies) ausstellen. Folgende Typen von Zertifikaten sind vordefiniert:

Administrator Das Zertifikat darf für die Signierung von Dateien, Vertrauenslisten, EFS (Encrypted File System), Email-Verschlüsselung und für die Client-Authentifizierung genutzt werden.

Domain Controller Hiermit wird ein Zertifikat für die Authentifizierung von Client- und Servermaschinen erstellt.

Computer Hiermit wird ein Zertifikat für die Authentifizierung von Client- und Servermaschinen erstellt.

Basic EFS Das Zertifikat ist nur für die Benutzung von EFS gültig.

EFS Recovery Agent Zertifikat zur Wiederherstellung von Dateien auf dem Encrypted File System

User Gebrauch des Zertifikates für EFS, Authentifikation des Clients und die Verschlüsselung von Email

Web Server Zertifikat für die Authentifizierung eines Servers gegenüber einem Client

15.2 Zertifizierung

Nachdem die Zertifizierungsdienste in einer Domäne installiert wurden, kann kein Computer nur aus dieser Domäne umbenannt, hinzugefügt oder herausgenommen werden, nachdem die Zertifizierungsdienste von diesem Rechner entfernt wurden.

Teil IV

Domänenstrukturen

Kapitel 16

Organisation in Domänen

Die *Domäne* ist die zentrale Organisationsform eines Windows NT Netzwerks. Mit Hilfe der Domäne werden logisch zusammengehörige Objekte wie Benutzer, Gruppen und Computer zusammengefaßt. Die enthaltenen Objekte werden in administrativer wie auch in sicherheitstechnischer Sicht zusammengefaßt. Administrative Berechtigungen oder Sicherheitsrichtlinien, die in einer Domäne gelten wirken sich nicht auf andere Domänen aus. Die Informationen über Securityprincipals werden in der Verzeichnisdatenbank *Active Directory* abgelegt. Bei Erstellung von Objekten im Active Directory ist zu beachten, daß der Name *jedes* Objektes innerhalb vom AD eindeutig sein muß. Ein Computerobjekt darf also z.B. nicht den gleichen Namen besitzen wie ein Benutzerobjekt.

Die Erstellung der Domäne erfolgt automatisch mit Installation des darin enthaltenen Domänencontrollers. Sie steht für einen gemeinsamen DNS-Namespace, der über einen DNS-Namen eindeutig identifiziert wird. Innerhalb einer Domäne sind alle Domänencontroller gleichberechtigt. Das heißt daß die Verwaltung der Domänen an jedem beliebigen Domänencontroller durchgeführt werden kann. Hiermit entfällt das aus NT4 bekannte Schema der Domänencontroller mit untergeordneten Backup- Domänencontrollern.

16.1 Vertrauensstellungen

Falls im Netzwerk mehrere Domänen existieren, die hierin erhaltenen User oder Ressourcen aber gemeinsam verwaltet werden sollen, lassen sich die Domänen miteinander verbinden. Dieses erfolgt über die Vertrauensstellungen . Alle Domänen in diesem Verbund vertrauen einander und lassen sich daher auch gemeinsam verwalten. Die Vertrauensstellungen sind bidirektional und transitiv. Das heißt, das das Vertrauen nicht gerichtet ist (bidirektional). Jede Domäne traut zudem jeder anderen im Verbund (transitiv), so daß auch einer Domäne vertraut wird, die zwar im Verbund steht, aber zu der keine direkten Beziehungen bestehen. Bei Bedarf kann jedoch auch

eine unidirektionale oder nicht vererbbare Vertrauensstellung eingerichtet werden.

Die Vertrauensstellungen können unter

```
Verwaltung - Active Directory Domänen und Vertrauensstellungen
```

konfiguriert werden. Die Einrichtung von manuellen (auch verknüpfte Vertrauensstellungen genannt) Vertrauensstellungen ist auch möglich, so daß eine Domäne einer anderen im Forest *direkt* vertraut. Hierfür ist allerdings notwendig, daß eine *physische* Verbindung zwischen den beiden Domänen besteht. Diese Art der Vertrauensstellung ist wie in der Domänenstruktur unter NT4 unidirektional und *nicht* transitiv.

16.2 Dömanenstruktur (Tree) und Gesamtstruktur (Forest)

In einer Gruppen von Domänen wird die erste Domäne, die erstellt wurde als Stammdomäne (*Root Domain*) bezeichnet. Die Stammdomäne legt sozusagen den kürzesten DNS-Namen im Namensraum fest. Alle weiteren Domänen, die dieser zugeordnet werden, bezeichnet man auch als untergeordnete Domänen. Der DNS-Name der untergeordneten Domänen setzt sich aus dem DNS-Namen untergordneten Domäne und dem mit einem Punkt abgetrennten Namen der der Stammdomäne zusammen (z.B. marketing.oreilly.com).

Da die einzelnen Domänen hinsichtlich der Verwaltung administrative Grenzen ziehen lassen sich mit Hilfe einer Domänenstruktur administrative Bereiche wie z.B. Abteilungen einfach im Netzwerk abbilden. Ein Administrator einer übergeordneten Domäne kann die untergeordneten Domänen per default nicht verwalten.

Zur Zusammenfassung von mehreren Domänenstrukturen mit jeweils einem eigenen Namensraum wird eine *Gesamtstruktur* (Forest) gebildet. Die Root-Domains der der einzelnen Domänenstrukturen werden hier miteinander verbunden. Die einzelnen Strukturen der Gesamtstruktur besitzen *keinen* gemeinsamen Namespace.

Bei Installation enthält die Stammdomäne der Gesamtstruktur zwei die gesamte Struktur umfassende vordefinierte Gruppen, die nur in der Stammdomäne dieser Gesamtstruktur vorhanden sind.

Organisations-Admins Mitglieder dieser Gruppe dürfen Änderungen an der gesamten Struktur vornehmen, wie z.B. Domänen hinzufügen und entfernen. Per default wird hier nur das Administratorenkonto des Administrators für die Stammdomäne der Gesamtstruktur eingefügt.

Schema-Admins Diese Gruppe ermöglicht es ihren Mitgliedern, änderungen am Schema des Active Directory durchzuführen. In der Standardeinstellung ist hier auch nur das Administratorenkonto der Stammdomäne der Gesamtstruktur eingetragen.

Im einheitlichen Modus werden diese Gruppen in universelle Gruppen gewandelt.

16.2.1 Installation einer neuen Gesamtstruktur

Die Erstellung einer Gesamtstruktur erfolgt mit Hilfe des Tools `dcpromo.exe`, das auch zur Installation von AD verwendet wird. Hier können per Wizard Strukturen und Gesamtstrukturen erstellt werden, einer vorhandenen Struktur beigetreten, oder mehrere Strukturen miteinander verbunden werden.

16.3 Rollen von Servern in Domänen

Ein W2K-Server kann verschiedene Rollen einnehmen. Wird er als *Domänen-Controller* eingesetzt, verwaltete er die Verzeichnisdienste (Active Directory) und somit die gemeinsamen Ressourcen der Domäne. Hierzu gehören auch die Benutzerkonten, die im AD abgelegt sind so daß die Anmeldung an der Domäne mit Hilfe des Domänen-Controllers abgewickelt wird. Jede Domäne im AD muß mindestens einen Domänen-Controller enthalten. Es können jedoch auch mehrere Domänen-Controller in der Domäne stehen, wobei diese als gleichrangig angesehen werden. Sie können alle lesen und schreibend auf das AD zugreifen.

Wird ein W2K-Server in die Domäne eingebunden, so muß er allerdings nicht als Domänen-Controller fungieren. In diesem Fall wird er als Mitglieds-Server (*Member-Server*) eingestuft. Ein Member-Server hat keinerlei Verwaltungsfunktionen am AD woraus folgt, daß er den Zugriff auf Domänenressourcen nicht steuern kann. Beispielsweise muß die Anmeldung an der Domäne immer über einen Domänencontroller erfolgen. Der Member-Server führt, obwohl er in die Domäne eingebunden ist jedoch eine zusätzliche lokale Benutzerkonten-Datenbank.

Um einen Member-Server zum Domänencontroller hochzustufen, bzw. einen Domänen-Controller zum Member-Server herabzustufen kann das Programm `dcpromo` genutzt werden.

Falls ein W2K-Server nicht in eine Domäne eingebunden werden soll und auch nicht als DC fungieren soll, kann er als eigenständiger Server (Standalone Server) genutzt werden. In diesem Falle besitzt er keinen Verzeichnisdienst, so daß die Ressourcenverwaltung mittels Freigaben gesteuert wird. Er verfügt über eine vollkommen eigene lokale Userdatenbank.

16.4 Organisatorische Einheiten

Die einzelne Domäne kann mit Hilfe von *Organisatorischen Einheiten* (OU), die im Active Directory angesiedelt sind, weiter strukturiert werden. Die OUs sind Containerobjekte, die andere OUs und Blattobjekte wie

- Benutzer
- Gruppen
- Computer
- freigegebene Verzeichnisse
- Drucker
- Kontakte

enthalten können.

Die Gruppierung in Organisationseinheiten erfolgt primär aus administrativen Erwägungen wie z.B. die Delegation von Verwaltungsaufgaben (Passwort-Vergabe) an einen User oder für die Verknüpfung von Gruppenrichtlinien.

Eine Organisationseinheit können allerdings keine Berechtigungen zugewiesen werden!

16.5 Verknüpfungen von OUs mit Gruppenrichtlinien

Kapitel 17

Benutzerkonten

Für den Zugriff auf Lokale- und Domänenressourcen werden Benutzerkonten benötigt. Es werden drei Typen von Benutzerkonten unterschieden:

Lokales Benutzerkonto Ermöglicht einem Benutzer die Anmeldung an einem Rechner um Zugriff auf diesen zu erhalten. Für den Zugriff auf die Ressourcen eines anderen Rechners muß der User auch auf diesem Rechner über ein Konto verfügen. *Die lokalen Benutzerkonten befinden sich im SAM* Security Accounts Manager *des Rechners.* Auf einem Rechner, der Teil einer Domäne ist sollte *kein* lokales Benutzerkonto erstellt werden, da die Domäne keine lokalen Benutzerkonten erkennt, und dieses Konto daher nur Zugriff auf die lokalen Ressourcen erhalten würde.

Auf einem Domänencontroller können keine lokalen Benutzer angelegt werden.

Domänenbenutzerkonto Das Domänenbenutzerkonto ermöglicht einem Benutzer die Anmeldung an einer Domäne. Hierdurch kann er mit Hilfe eines einzigen Benutzerkonots Zugriff auf Netzwerkressourcen erhalten. *Die Domänenbenutzerkonten befinden sich im Active Directory.*

Der Domänenuser kann auf Ressourcen in anderen Domänen zugreifen, wenn zwischen den Domänen eine Vertrauensstellung besteht.

Vordefiniertes Benutzerkonto Es werden bei der Installation automatisch zwei vordefinierte Benutzerkonten eingerichtet. Dieses sind die Konten *Administrator* und *Gast*. Sie ermöglichen die Ausführung von Managementaufgaben bzw. sind für den temporären Zugriff erstellt worden. Lokale Benutzerkonten befinden sich wieder im *SAM*, bzw. im Active Directory.

Das lokale Administratorenkonto ist für eine lokale Anmeldung notwendig, falls kein Zugang zum Domänencontroller besteht (TCP/IP-Stack defekt).

Ein User darf sich nicht lokal an einem Domänencontroller anmelden. Um dieses einzustellen muß der User (bzw. die Gruppe aller User für die lokale Anmeldung freigegeben werden).

17.1 Lokale Benutzerkonten

Ein lokales Benutzerkonto wird nur auf alleinstehenden Workstations oder in Arbeitsgruppen verwandt. Es kann auch nur auf Maschinen unter W2K Professional (Workstation) oder auf alleinstehenden Servern oder Mitgliedsservern erstellt werden.

Die Erstellung des Kontos wird in der `Computerverwaltung` unter der Erweiterung `Lokale Benutzer und Gruppen` durchgeführt.

17.2 Domänenbenutzerkonten

Der Anmeldename eines Benutzers muß im gesamten Active Directory eindeutig sein. Hierbei ist zu beachten, daß die ersten 20 Zeichen des Anmeldenamens ausgewertet werden, so daß der Anmeldename in diesem Bereich AD-weit eindeutig ist. Der *vollständige Name* für das Domänenbenutzerkonto muß dagegen nur *innerhalb der Domäne* eindeutig sein.

Bei Vergabe der Anmeldenamen sollte darauf geachtet werden, daß nach einer einheitlichen Vergabekonvention vorgegangen wird (z.B. Vorname + 1. Buchstabe des Nachnamens).

Jedes Benutzerkonto sollte mit einem Kennwort geschützt werden. Dieses sollte mindestens 8 Zeichen lang sein und möglichst aus Sonderzeichen, Zahlen und Groß- und Kleinbuchstaben bestehen um einen Brute-Force[1] Angriff auf die Password-Datenbank zu erschweren. *Auf keinen Fall sollten Daten, Initialien etc aus dem persönlichen Bereich genommen werden, da diese leicht zu erraten sind (sog. social engineering).*

Ein Domänenbenutzerkonto befindet sich auf dem Domänencontroller (im Active Directory) und wird automatisch auf alle anderen Domänencontroller repliziert.

Zum Benutzerkonto können die Eigenschaften dieses Kontos eingestellt werden. Hierzu gehören:

Allgemein Name des Benutzers, allgemeine Beschreibung des Arbeitsplatzes, Telefonnummer, Email-Alias und Homepageadresse.

Adresse Erweiterte Adressangaben wie: Straße, Postfach, Stadt, Bundesland, PLZ und Land.

[1] auch Wörterbuchangriff genannt, Versuch das Password durch (automatisiertes) ausprobieren zu erraten. Wird oft mit Hilfe eines Wörterbuches durchgeführt, indem die am häufigsten für Passwörter genutzten Wörter zuerst getestet werden.

Konto Auf das Konto bezogene Einstellungen wie: *Anmeldename*, Kontooptionen wie Anmeldezeiten und Ablaufdatum des Kontos. Hier kann unter `Anmelden` eingerichtet werden, von welchen Computern aus sich ein User an der Domäne anmelden kann.

Profil Einstellung von Profilpfad und Basisverzeichnis (Homeverzeichnis) des Users,

Rufnummern Weitere (private) Rufnummern des Users, IP-Adresse und Anmerkungen.

Organisation Anrede, Abteilung, Vorgesetzte(r) und direkte Mitarbeiter.

Mitglied von Gruppen, denen der Benutzer angehört,

Umgebung Einstellung von Anmeldescripten und Verbindungen zu Netzwerkgeräten bei Anmeldung.

Sitzungen Einstellungen für die Terminaldienste.

Remoteüberwachung Remoteüberwachungseinstellungen für Terminaldienste.

Terminaldienstprofile Legt das Terminaldienstprofil des Users fest.

17.3 Erstellen von Domänenbenutzerkonten

Ein Domänenbenutzerkonto kann unter `Verwaltung - Active Directory Benutzer und Computer` erstellt werden. Hier muß dann die Domäne ausgewählt werden in der der Benutzer erstellt werden soll. Mit `RM - Neu - User` kann der User dann im passenden Unterverzeichnis erstellt werden. In der Regel wird das Konto im Standardverzeichnis "Users" oder in einem anderen extra hierfür vorgesehenem Verzeichnis erstellt. Auch hier gelten die Konventionen für Anmeldenamen (s. Kap. 17.2).

Zur Vereinfachung bei der Erstellung eines neuen Users kann einfach ein schon bestehendes Konto kopiert werden[2]. Hierbei werden einige Informationen aus dem schon bestehenden Konto in das neue übernommen. Die Rechte und Berechtigungen, die einem *einzelnen* Benutzerkonto zugeteilt wurden, werden *nicht* übernommen.

Zur Definition einer Benutzerkontenvorlage sollte ein Dummy-Konto erstellt werden, daß als Kopiervorlage dient. Dieses Konto sollte dann in den Kennwortanforderungen deaktiviert werden , da es nur als Vorlage dienen soll. Es sollte jeweils eine Vorlage für bestimmte Benutzergruppen erstellt werden wie z.B. Vertriebsmitarbeiter, Buchhalter etc. Für Mitarbeiter, die das Netzwerk nur temporär oder nur Kurz benutzen sollte eine Vorlage mit entsprechendne voreingestellten Beschränkungen erstellt werden.

[2]Diese kann allerdings nur auf Domänencontrollern erfolgen.

17.3.1 Übernahme von Einträgen beim Kopieren

Allgemein kein Eintrag wird übernommen.

Adresse Alle Einträge außer Straße.

Konto Alle außer Anmeldename.

Profil Hier werden der Profilpfad und der Basisordner geändert.

Rufnummern keine

Organisation Alle außer Anrede.

Miglied von Übernahme aller Einträge.

Einwählen Keine Übernahme. Das neue Konto erhält Standardeinstellungen.

Umgebung Keine Übernahme. Das neue Konto erhält Standardeinstellungen.

Sitzungen Keine Übernahme. Das neue Konto erhält Standardeinstellungen.

Remoteüberwachung Keine Übernahme. Das neue Konto erhält Standardeinstellungen.

Terminaldienstprofile Keine Übernahme. Das neue Konto erhält Standardeinstellungen.

17.4 Standard- Benutzergruppen

Die Benutzer können beliebigen (Benutzer-) Gruppen angehören, für die Sicherheitsrichtlinien definiert wurden. Auf einem neu installierten System sind schon einige Standardsicherheisteinstellungen für spezielle Gruppen definert.

- Administratoren
- Hauptbenutzer (Poweruser)
- Sicherungsoperatoren (Backup Operators)
- Benutzer
- Sondergruppen
  - Interaktive Gruppe

- Netzwerk
- Terminal-Server Benutzer

Den Sondergruppen wird ein Benutzer automatisch hinzugefügt, sobald er sich am System anmeldet oder auf dieses zugreift. Ein manueller Eingriff in diese Gruppen ist nicht unbedingt möglich.

17.4.1 Administratoren

Ein Mitglied der (lokalen) Gruppe der Administratoren ist in der Lage den (lokalen) Rechner komplett zu verwalten. Innerhalb einer Domänenstruktur ist die globale Gruppe der *Domänen- Admins* in der Standardeinstellung Mitglied der lokalen Gruppe der Administratoren, so daß ein Mitglied dieser globalen Gruppe auf jeder Maschine in der Domäne Administratorrechte besitzt. Die Domänen- Admins besitzen also die volle Kontrolle über alle Objekte dieser Domäne. Zu beachten ist allerdings, daß die Domänen Admins natürlich aus diese Gruppe entfernt werden können und somit auf den lokalen Maschinen keine Administratorrechte mehr besitzen.

17.4.2 Hauptbenutzer

Der Hauptbenutzer (Poweruser) hat gegenüber dem normalen User erweiterte Rechte. Er darf z.B.

alle Anwendungen ausführen Neben für Windows 2000 zertifizierten Anwendungen darf er auch Anwendungen ür frühere Betriebssysteme ausführen.

Programme einrichten Er darf Programme einrichten. Diese dürfen aber *keine* Systemdienste einrichten und auch *keine* Betriebssytemdateien modifizieren.

Ressourcen verwalten Anpassung von systemweiten Ressourcen wie Datum/Uhrzeit, Energieoptionen und andere Ressourcen der Systemsteuerung.

Drucker einrichten Einrichtung von lokalen Druckern.

lokale Benutzerkonten verwalten Erstellung und Verwaltung von *lokalen* Benutzerkonten und Gruppen.

manuell Dienste aktivieren Aktivierung von Diensten, die manuell gestartet und beendet werden können.

17.4.3 Sicherungsoperatoren

Die Gruppe Sicherungsoperatoren (Backupoperators) verfügt über Berechtigungen, Dateien auf dem Rechner zu sichern und wiederherzustellen. Dieses wird unabhängig von den sonstigen Berechtigungen zum Schutz der Dateien gehandhabt. Daneben sind die Sicherungsoperatoren dazu berechtigt, den Computer *herunterzufahren*.

Da die Mitglieder dieser Gruppe über die Berechtigungen verfügen, Dateien zu lesen und zu schreiben stellt dieses eine eventuelle Sicherheitslücke dar. Um dieses weitergehend abzusichern, kann eine lokale Sicherheitsrichtlinie erstellt werden, die den Desktop der Sicherungsoperatoren so einschränkt, daß sie nur die für ihre Arbeit benötigten Programme aufrufen dürfen.

17.4.4 Benutzer

Ein Benutzer gehört bei Erstellung automatisch zur Gruppe der Benutzer. Die Standardberechtigungen dieser Gruppe ermöglichen das Ausführen von Programmen, das Erstellen von Dateien und Verzeichnissen und das Nutzen von Druckern. Die Installation von kleineren Applikationen die nicht tiefer ins System eingreift ist diesr Gruppe von Usern auch möglich. Ein Benutzer der dieser Gruppe angehört, darf die lokalen Einstellungen für *Offline-Folder* so setzen, daß diese Offline verfügbar sind (vorausgesetzt diese Möglichkeit ist auch auf dem Server aktiviert).

17.4.5 Interaktive Gruppe

Ein am System angemeldeter Benutzer ist automatisch Mitglied in dieser Gruppe. Wird ein NT 4 System auf W2K aktualisiert, werden die Benutzer dieser Gruppe auf dem NT 4 System zudem automatisch der Gruppe Hauptbenutzer hinzugefügt, so daß auch nicht für W2K speziell berechtigte Anwendungen wie vorher funktionieren.

17.4.6 Netzwerk

Diese Gruppe umfaßt alle User, die zur Zeit über das Netzwerk auf das lokale System zugreifen.

Kapitel 18

Gruppen

18.1 Gruppentypen

Eine Gruppe kann je nach ihrer Typzugehörigkeit zur Verwaltung von Rechten dienen oder nur als Gruppierungseinheit unabhängig von der Rechteverwaltung.

Verteilergruppen Eine Verteilergruppe kann *nur* als Gruppierungseinheit ohne Rechte verwandt werden. Hiermit kann z.B. eine Gruppe für die Mailverteilung an eine Gruppe von Usern implementiert werden.

Verteilergruppen können *nicht* zur Verteilung (Weitergabe) von Rechten genutzt werden.

Sicherheitsgruppen Eine Sicherheitsgruppe kann sowohl zur Verteilung von Rechten als auch als Mailverteilerliste verwandt werden.

18.2 Gruppenbereiche

Die Verwaltung der Domäne(n) sollte aus Gründen der Übersichtlichkeit und der Vereinfachung von Rechtezuweisungen generell mit Hilfe von Gruppen erfolgen. Aufgrund der Einschränkung, daß an Organisatorische Einheiten keine Rechte vergeben werden können, dienen die Gruppen auch als Hilfskonstrukte zur Rechtevergabe. Einzelne User, Computer oder andere Gruppen können zu Gruppen zusammengefaßt werden.

In erster Linie werden die globalen Gruppen und lokalen Gruppen zur Verwaltung der Berechtigungen genutzt. Die Begriffe *lokal* und *global* beziehen sich hier auf lokalisation der Ressourcen, die mit Hilfe einer Gruppe dieses Bereichs verwaltet werden. Die Ressourcen der *lokalen* Domäne werden mit einer Gruppe verwaltet, die in diser Domäne erstellt wurde und zum lokalen Gruppenbereich gehört. Gruppen des globalen Bereichs dienen dagegen zur domänenübergreifenden Verwaltung mit Hilfe von Gruppen.

18.2.1 Globale Gruppen

Die globale Gruppe kann Domänengrenzen überschreiten. Sie dienen dazu, Benutzer mit ähnlichen Anforderungen an den Netzwerkzugriff zusammenzufassen. Einer globalen Gruppe können Berechtigungen an Ressourcen zugewiesen werden, die sich in einer beliebigen (global) Domäne befinden. Globale Gruppen weisen die folgenden Eigenschaften auf:

- Globale Gruppen können in andere globale Gruppen *der gleichen Domäne*, zu universellen Gruppen oder zu Gruppen der lokalen Domäne in anderen Domänen hinzugefügt werden.
- Einer globalen Gruppe können *nur* Benutzerkonten und andere globalen Gruppen hinzugefügt werden, die in der gleichen Domäne erstellt wurden.

Globale Gruppen dienen also zur Verschachtelung von Gruppen um die Weitergabe von Berechtigungen steuern zu können. Die Mitgliedschaft an globalen Gruppen ist allerdings auf Objekte beschränkt, die sich in der gleichen Domäne befinden.

18.2.2 Lokale Gruppe oder Domänenlokalegruppe

Dieser Gruppenbereich wird zur Vergabe von Berechtigungen an Domänenressourcen (*innerhalb* der Domäne) genutzt, die sich in *der gleichen Domäne befinden*.[1] Die jeweilige Ressource, an der diese Berechtigungen erteilt werden, muß sich nicht auf einem Domänencontroller befinden, kann sich also z.B. auf einem Memberserver befinden, der als Fileserver dient. Für domänenlokale Gruppen gelten die folgenden Eigenschaften:

- Gruppen der lokalen Domäne können nicht in andere Gruppen eingefügt werden. Eine Gruppe der lokalen Domäne kann zu *keiner* anderen Gruppe hinzugefügt werden.
- Einer domänenlokalen Gruppe können Benutzerkonten, universelle Gruppen und globale Gruppen *jeder beliebigen Domäne* hinzugefügt werden.

Die Domänenlokale Gruppe wird auf allen Domänencontrollern (der Domäne zu der sie gehört) repliziert.

[1] Nicht zu verwechseln mit der lokalen Gruppe, die nur auf einem einzelnen Rechner erstellt werden und zur Verwaltung dieses einzelnen Systems dient. Eine lokale Gruppe kann nicht auf einem Domänencontroller erstellt werden.

18.2.3 universelle Gruppe

[2]

Die universellen Gruppen werden genutzt um ähnlichen Ressourcen Treeübergreifend Berechtigungen zu erteilen. Zu beachten ist jedoch, daß die universellen Gruppen im globalen Katalog geführt werden und dieser daher durch intensive Nutzung der universellen Gruppen stark anwachsen kann.

Die universellen Gruppen sind mit folgenden Eigenschaften ausgestattet:

- Universelle Gruppen können beliebig in andere universelle Gruppen einer beliebigen Domäne und in domänenlokalen Gruppen der lokalen Domäne eingefügt werden
- Den universellen Gruppen können Benutzerkonten und Gruppen der lokalen Domäne hinzugefügt werden (Achtung: Keine domänenlokalen Gruppen).

18.3 Integrierte und vordefinierte Gruppen

Die integrierten Gruppen der lokalen Domäne erteilen den Benutzern vordefinierte Rechte und Berechtigungen, damit diese spezielle Aufgaben durchführen können.

Der erste Administrator, der in der Domäne erstellt wird, wird automatisch Mitglied in allen Gruppen, die für die vollständige Administration wichtig sind.

18.3.1 vordefinierte Gruppen

Jeder Jeder, der Zugriff auf die Domäne hat.

Besitzer/Ersteller der jeweilige Besitzer/Ersteller des Objektes.

Netzwerk Mitglieder dieser Gruppe sind die User, die sich über das Netzwerk angemeldet haben. (?),

Interaktiv jeder, der sich interaktiv am System angemeldet *hat*, gehört automatisch zu dieser Gruppe.

System die Gruppe System braucht nicht konfiguriert zu werden. In der Gruppe System ist z.B. das System vertreten.

Ein User wird einer “besonderen” Gruppe automatisch zugewiesen. Zu dieser Gruppe kann niemand manuell hinzugefügt bzw. entfernt werden.

[2] Universelle Gruppen können nur dann als Sicherheitsgruppen erstellt werden, wenn sich die Domäne im einheitlichen (nur W2k-) Modus befindet.

18.4 Strategien zur Erstellung von Gruppen

Die Hierarchische Ordnung der Gruppen und die Zuweisung an User sollte nach der sogenannten *AGDLP*-Strategie erfolgen.

AG User (Accounts) mit gemeinsamen Verantwortungen (und somit Rechten) werden mit Hilfe einer globalen Gruppe zusammengefaßt.

DL Die globalen Gruppen mit gleichen Anforderungen an ein Zugriffsprofil werden in Gruppen der *lokalen Domäne* zusammengefaßt. So lassen sich die Zugriffsberechtigungen für alle untergeordneten Gruppen und User mit Hilfe diese Gruppe einstellen.

P Die einzelnen Berechtigungen (Permissions) werden schließlich an die Gruppen der lokalen Domäne auf dem Domänencontroller vergeben.

Kapitel 19

Berechtigungen

Berechtigungen können für alle Objekte im Windows 2000 System eingestellt werden. Der Begriff Objekt umfaßt hier alle Einträge im Actvive Diretory sowie auch Verzeichnisse und Dateien im NTFS Filesystem. Die Berechtigungen sind nicht mit den *Benutzerrechten* einer lokalen Richtlinie zu verwechseln. Die Berechtigungen beziehen sich auf eine Domäne oder das NT-Filesystem, während Benutzerrechte den lokalen Rechner selbst betreffen. Mit Hilfe der Berechtigungen wird der Zugriff *auf das Objekt selbst* und der Zugriff *auf die Attribute des Objekts* gesteuert.

19.1 Hierarchie der Berechtigungen

Berechtigungen werden innerhalb des Filesystems vom Rootdirectory zu allen darunterliegenden Verzeichnissen und Dateien vererbt. Eine Vererbungshierarchie läßt sich auf Ebene eines Verzeichnisses blockieren. Allerdings läßt sich für jedes Recht einzeln wiederum einstellen, daß die Vererbung erzwungen wird. Diese Einstellung erfolgt mit dem Feld:

> Berechtigungen in allen untergeordneten Objekten zurücksetzen und die Verbreitung vererbbarer Berechtigungen aktivieren.

Nachdem der Vorgang bestätigt wurde, werden in den untergeordneten Verzeichnissen die Berechtigungseinträge der Vererbungshierarchie neu gesetzt. Die "alten" Berechtigungseinträge werden dann u.U. gelöscht. Jedes Objekt erbt standardmäßig die Berechtigungen des darüberliegenden Objektes. Auch neu hinzugefügte Objekte übernehmen diese Berechtigungshierarchie.

Tritt der Fall ein, daß sich die (ererbten) Berechtigungen an einem Objekt wiedersprechen, so besitzen die einer Datei oder einem Verzeichnis direkt(er) zugewiesenen Berechtigungen eine höhere Priorität als Berechtigungen, die in der Hierarchie weiter entfernt vom Objekt zugewiesen wurden. Das heißt, daß dem Objekt direkt zugewiesene Berechtigungen immer die

höchste Priorität besitzen. In der Praxis sollte die direkte Zuweisung von Berechtigungen an ein Objekt jedoch vermieden werden, da die Struktur des Gesamten Berechtigungssystems hierdurch sehr schnell extrem kompliziert wird. Bei in der gleicher Ebene zugewiesenen Rechten besitzt eine verweigerte Berechtigung eine höhere Priorität als eine erlaubende Berechtigung.

19.2 Einstellungen für Berechtigungen

Die Einstellung von Berechtigungen sowie der Vererbungsmöglichkeiten erfolgt mit Hilfe des *ACL-Editors*, der über die Registerkarte `Sicherheit` im Eigenschaftsfeld eines Objektes zu erreichen ist. Im oberen Fenster des ACL-Editors werden die User und Gruppen angezeigt, für die Berechtigungen an diesem Objekt gelten. Der untere Teil zeigt die Berechtigungen des jeweiligen Users bzw. der Gruppe am jeweiligen Objekt. Hier können die insgesamt 6 *Verzeichnisberechtigungen* bzw. *Dateiberechtigungen* zugelassen oder verweigert werden. *Das Recht die Attribute und Berechtigungen einer Datei zu ändern erhält nur der, der die Rechte für Vollzugriff besitzt.*

Ein grau hinterlegtes Kästchen zeigt an, daß die jeweiligen Berechtigungen von darüberliegenden Objekten geerbt wurden. Wenn keines der Kästchen markiert oder grau hinterlegt ist heißt dieses allerdings nicht, daß das im oberen Fenster markierte Objekt keinerlei Berechtigungen besitzt. Die Dateiberechtigungen dieses Fensters stellen eine vorgefertigte Zusammenfassung der sogenannten *beschränkten Berechtigungen* eines Objektes dar. Mit Markieren eines dieser Kästchen werden mehrere der über die Schaltfläche `Erweitert` zu erreichenden beschränkten Berechtigungen gesetzt.

19.2.1 beschränkte Berechtigungen

- Ordner durchsuchen / Datei ausführen
- Ordner auflisten / Daten lesen
- Attribute lesen
- Erweiterte Attribute lesen
- Dateien erstellen / Dateien schreiben
- Ordner erstellen / Daten anhängen
- Attribute schreiben
- Erweiterte Attribute schreiben
- Unterordner und Dateien löschen

- Löschen
- Berechtigungen lesen
- Berechtigungen ändern
- Besitzrechte übernehmen

Die im Eigenschaftsfenster eines Objektes angezeigten Datei- oder Verzeichisberechtigungen werden auf den beschränkten Berechtigungen abgebildet. Sie stellen immer eine Zusammenfassung von mehreren beschränkten Berechtigungen dar:

Vollzugriff Alle Rechte, daß Objekt oder untergeordnete Objekte zu lesen, schreiben, löschen, modifizieren oder zu löschen. Auch die *Übernahme des Besitzes* ist erlaubt.

Ändern Am Objekt selbst dürfen Änderungen einschließlich der Löschung desselben vorgenommen werden. Die Übernahme des Besitzes oder das *Ändern von Berechtigungen* ist nicht erlaubt. Des Weiteren dürfen keine untergordneten Objekte gelöscht werden. Alle Optionen an den Objekten dürfen gelesen werden.

Lesen, Ausführen Änderungen am Objekt oder untergeordneten Objekten sind nicht erlaubt. Leseberechtigungen bestehen für alle Attribute und Inhalte.

Ordnerinhalt auflisten Gleiche Berechtigungen wie Lesen und Ausführen, allerdings auf Verzeichnisse bezogen. Das Verzeichnis und Unterverzeichnisse dürfen gelesen und durchsucht werden. Auch die Attribute dürfen für alle Objekte gelesen werden.

Lesen Nur Leserechte. Das *Ausführen* von Dateien oder das *Durchsuchen* von Verzeichnissen ist nicht erlaubt.

Schreiben Es darf nur schreibend zugegriffen werden. Das Durchsuchen von Verzeichnissen und das Ausführen von Dateien ist nicht erlaubt. Die Attribute einer Datei oder eines Verzeichnisses dürfen gesetzt werden. Die *Berechtigungen* von Dateien oder Verzeichnissen dürfen allerdings *nur gelesen* werden.

Neben den Einstellungen für die Berechtigungen eines Objektes können hier weitere Eigenschaften wie die Überwachung (s.a. unter 6) von Zugriffen auf das Objekt und die Besitzeinstellungen konfiguriert werden.

19.3 Vorgänge beim Zugriff auf ein Objekt

Wenn ein Benuter einen beliebigen Zugriff auf ein Objekt durchführen möchte, untersucht das System die *Sicherheitsbeschreibung* (Security Descriptor) für dieses Objekt um festzustellen ob der Zugreifende berechtigt ist, in der gewünschten Art und Weise auf das Objekt zuzugreifen. Die Sicherheitsbeschreibung des einzelnen Objektes umfaßt dabei zwei Zugriffslisten, die *DACL* (Discretional Access Controll List, die ACL für diskrete (einzelne) Zugriffe) und die die *SACL* (System Access Control List).

DACL Die DACL gibt an,

- wer der Besitzer des Objektes ist und daher über die Besitzrechte verfügt,
- welchen Usern oder Gruppen Berechtigungen zum Zugriff auf das Objekt erteilt wurden und welchen sie verwehrt wurden,
- Wie die innerhalb eines Containers enthaltenen Objekte Berechtigungen des Containers erben dürfen.

Die Einstellungen an der DACL werden mit den Einstellungen unter den Menüpunkten *Berechtigungen* vorgenommen.

SACL In der SACL ist hingegen festgehalten welche Zugriffsereignisse von welchen Benutzern oder Gruppen auf dieses Objekt überwacht werden sollen.

Die Einstellungen für die Systemzugriffe werden unter den Menüpunkten für die Überwachung vorgenommen.

Kapitel 20

Freigaben

Eine W2K Maschine kann Ressourcen wie Drucker oder Dateien Netzwerkweit freigeben. Freigaben können für Verzeichnisse und Drucker auf einem Rechner installiert werden. Zusätzlich besteht die Möglichkeit eine Freigabe im AD zu installieren. Hierfür muß das entsprechende freigegebene Objekt nicht unbedingt bzw. nur temporär existieren.

Die Netzwerkfreigabe an einem Verzeichnis wird entfernt, falls dieses verschoben oder unbenannt wird. Das System gibt in diesem Fall eine Warung aus. Nach dem Vorgang muß das Verzeichnis wieder neu freigegeben werden.

Die Berechtigungen sind im System Üblicherweise so organisiert, daß die Rechte kummuliert (addiert) werden. Beim Zugriff auf eine Freigabe über das Netz gilt dagegen, daß nur das *am meisten einschränkende* Recht (the most restricive right) wirksam wird (s.a. 4.1).

Defaultberechtigungen einer Freigabe

Neu erstellte Freigaben erhalten als Defaulteinstellung die Berechtigung *Vollzugriff für die Gruppe* Jeder *(Everyone)*. Wie oben erwähnt gelten zusätzlich die Filesytemberechtigungen an den Dateien der Freigabe.

Std-Berechtigungen an neu erstellten Verzeichnissen. freigegebene Verzeichnisse: Std: Vollzugriff für *Everyone*, bei Verschieben auf einen anderen Datenträger erhält es die Standardfreigabe, Wenn er umbenannt oder (lokal) verschoben wird, wird die Freigabe entfernt, d.h. es ist ein “normales” Verzeichnis.

20.1 Lokale Zwischenspeicherung mit Offline-Dateien

Um mit Freigaben auch ohne Netzzugang arbeiten zu können (z.B. bei Laptops), müssen die Daten lokal auf der Maschine zur Verfügung stehen. Der Zugriff auf die Daten erfolgt für den Benutzer vollkommen transparent. Aus seiner Sicht stellt sich der Zugriff auf einen Zugriff auf eine Freigabe im Netzwerk dar.

Für ein im Netz freigegebenens Verzeichnis wird per *Defaulteinstellung* die Option zum Offline-Zwischenspeichern der Datei aktiviert. Die Konfiguration dieser Optionen erfolgt auf der Karte mit den Einstellungen für die Freigabe unter dem Punkt Zwischenspeichern.

Die grundlegende Aktivierung für die Nutzung der Offlinedateien erfolgt in der Systemsteuerung unter dem Icon `Ordneroptionen`. Die Unterschiede zwischen der Workstation-Version und der Serververision von W2K ist hier, daß die Nutzung von Offlinedateien in der Workstation-Version (W2K Professional) standardmäßig *aktiviert* ist, während sie auf der Serverversion per default *deaktiviert* ist. Weiter Optionen für die lokale Zwischenspeicherung ist .z.B. die maximale Größe von Dateien, die noch lokal zwischengespeichert werden und die Angabe des maximalen Speicherplatzes, der für Offline-Dateien zur Verfügung gestellt werden soll. Ein Server, der als Terminalserver fungiert ist die Zurverfügungstellung von Offlinedateien nicht möglich.

Das Zwischenspeichern (Caching) von freigegebenen Dateien kann nur auf Verzeichnisebene gesteuert werden. Die *Defaulteinstellung* ist das manuelle Zwischenspeichern der Dateien, bei der die Benutzer für jede Datei einzeln angeben müssen, ob diese lokal Zwischengespeichert werden soll. Die automatisierte Auswahl sieht zwei mögliche Einstellungen vor:

Automatisches Zwischenspeichern für Programme Hier werden Dateien, die vom Client auf dem Server geöffnet werden zum Client übertragen und hier zwischengespeichert. Danach wird die Datei auf dem Server wieder geschlossen. Weiter Zugriffe des Clients erfolgen nur auf lokal zwischengespeciherte Datei. Einem anderen Nutzer ist es möglich ist die Datei auf dem Server mit einer geänderten Version zu überschreiben. Daher ist diese Einstellung nur für Dateien in einer schreibgeschützten Freigabe zu empfehlen. Als Nebeneffekt vermindert diese Einstellung die Netzwerklast.

Automatisches Zwischenspeichern für Dokumente Hier wird die auf dem Server geöffnete Datei zum Client übertragen, aber auf dem Server weiterhin offen gehalten so daß andere User diese nicht verändern können. Die Datei auf dem Server wird geschlossen, wenn sich der Client (z.B. ein Notebook) vom Server abmeldet.(?) Das Problem der Versionsverwaltung ist hiermit allerdings auch nicht zufriedenstellend gelöst, da die Datei jetzt von einem Dritten mit einer geänderten Version überschrieben werden kann.

Bei Abmelden des Users werden Server und Client beidseitig synchronisiert, so daß auf beiden Maschinen der gleiche Stand der Dateien vorliegt. Bei der nächsten Anmeldung des Users wird der Server einseitig mit der Usermaschine synchronisiert, indem die geänderten Dateien der Usermaschine

auf den Server kopiert werden. Die Einstellungen für die Synchronisierung erfolgen unter `Zubehör - Synchronisieren`.

Kapitel 21

Benutzerprofile und Gruppenrichtlinien

Die Arbeitsumgebung eines Benutzers läßt sich mit Hilfe von Gruppenrichtlinien und Benutzerprofilen konfigurieren. Diese Konstrukte können so eingestellt werden, daß sie ein sogenanntes *Roaming Profile* bilden, das dem User bei Anmeldung an jedem beliebigen Computer in der Domäne zur Verfügung steht. Voraussetzung für die Nutzung von Gruppenrichtlinien ist ein Domänen-Controller, auf dem Active Directory installiert ist.

21.1 Benutzerprofile

Unter W2K ist neben der Einrichtung von Gruppenrichtlinien auch noch die Konfiguration der aus NT 4 bekannten Benutzerprofile möglich. Für jeden Benuter wird spätestens bei der ersten lokalen Anmeldung an einer Workstation ein Benutzerprofil erstellt. Der Administrator kann die Einstellungen des Benutzerprofils zentral im *MMC-Snap-In* `Active Directory-Benutzer und -Computer` auf der Registerkarte `Profile` verwalten. Hier erfolgt auch die Einstellung des (UNC-) Pfades zum Profil, das eingentlich nur aus einer Verzeichnisstruktur mit einigen notwendigen Dateien besteht.[1] Die Einstellungen, die ein Benutzerprofil beinhaltet sind also komplett im Dateisystem hinterlegt. Einige Einstellungen sind in einem Teilzweig der Registry gespeichert, die im Profil in der Datei `ntuser.dat` abgelegt sind. Aus diesem Grunde kann ein Profil auch nicht einfach mit Hilfe des Filemanagers kopiert werden, wie es zur Vereinfachung der Verwaltung notwendig ist. Das Kopieren muß daher in der `Systemsteuerung` unter `System - Benutzerprofile` erfolgen.

Ein Benutzer ist in der Lage sein Benutzerprofil zu ändern falls es sich nicht um ein servergespeichertes Profil handelt, daß auf dem Server read

[1] Bei Pfadangaben ist hier die Nutzung der Umgebungsvariable %username% sehr zu empfehlen.

only abgelegt ist. In dieser Hinsicht unterscheidet sich das Benutzerprofil von der Gruppenrichtlinie, die in der Verzeichnisdatenbank hinterlegt wird.

21.2 Gruppenrichtlinien

Alle Konfigurationseinstellungen des Benutzerprofils, wie z.B. die Verwaltung der Favoriten können auch mit Hilfe einer Gruppenrichtlinie durchgeführt werden. Die hier gemachten Einstellungen überschreiben dabei immer anderslautende Einstellungen in Benutzerprofilen, so daß letztendlich immer die Gruppenrichtlinie zum Tragen kommt. Der Benutzer kann an den ihm zugewiesenen Einstellungen nichts ändern.

Mit Hilfe der Gruppenrichlinen erfolgt die Verwaltung der kompletten Umgebung der Benutzer. Die Profile sind jetzt vor allem für das zentrale Speichern von benutzerspezifischen Verzeichnissen wie z.B. `Dokumente und Einstellungen` notwendig.

Kapitel 22

Systemrichtlinien (Policies)

Mit Hilfe von Systemrichtlinien (Policies) lassen sich alle Bereiche im System einstellen. Eine Policy hat einen genau definierten Geltungsbereich.

- lokale Richtlinie
- Domäne
- Organisationseinheit (OU)
- Userrichtlinie
- Computerrichtlinie

Die Konfiguration der Policies erfolgt in den Eigenschaften der einzelnen Komponente. Die Kontorichlinien, also die Policies, die die Benutzerkonten (User Accounts) betreffen, werden nur wirksam, wenn sie auf Domänenebene definiert werden. Dieses Verhalten dient zur Verhinderung von unterschiedlichen Kontorichtlinien für ein und dasselbe Benutzerkonto auf verschiedenen Rechnern. Dieses würde die Administration extrem unübersichlich werden lassen. Policies für Benutzerkonten die auf anderen Ebenen definiert werden, werden vom System immer ignoriert ((?)oder nur wenn einen Richtlinie auf Domänenebene definiert wurde?(?)).

22.0.1 Refresh der Richtlinieneinstellungen

Das System liest die Systemrichtlinien beim Start des Systems ein, wobei die Computerspezifischen Einstellungen beim Booten, die userspezifischen Einstellungen beim Anmelden des Users geladen werden. Wenn die Einstellung *Hintergrundaktualisierung der Gruppenrichtlinie deaktivieren* (Disable background refresh of group policy) *nicht* aktiviert ist (default), werden die User- und Computerspezifischen Einstellungen in einem zufällig gewählten Zeitraum im Invervall von 90 bis 120 Minuten neu eingelesen. Hier kann die Fixzeit (hier 90 min) eingestellt werden und die variable zufällige Totzeit

(default 30 min) deaktiviert werden. Diese Einstellung sollte beibehalten werden, um eine gleichzeitige Aktualisierung aller Rechner im Netzwerk zu vermeiden.

22.1 Vererbung von Policies

Innerhalb der AD Hierarchie werden die Policies von übergeordneten Containern in die darunterliegenden vererbt. Um dieses zu verhindern kann die Option *Block Policy inheritance* gesetzt werden. Zum Erzwingen der Vererbung kann am Gruppenrichtlinienobjekt die Option `No Override` gesetzt werden.

22.2 Policies für NT4 Clients

Die sich im Netzwerk befindlichen NT4 Clients unterstützen keine W2K Policies. Mit Hilfe des *System Policy Editors* können auf administrativen Schablonen basierende NT4 Policies erstellt werden. Die hiermit erstellte Systemrichtlinie sollte im Verzeichnis `%systemroot%SYSVOL\sysvol\`*Domänenname*`\scripts` gespeichert unter dem Namen `NTConfig.pol` werden. Diese Datei wird dann im Zuge der Replikationsvorgänge auf alle anderen Domänencontroller verteilt.

Kapitel 23

Sicherheitsrichtlinien

Zur Implementierung der Sicherheit wird auf einer nicht zu einer Domäne gehörenden Maschine eine lokale Sicherheitsrichtlinie konfiguriert. Diese wird im Menü `Verwaltung` unter `Lokale Sicherheitsrichtlinie` konfiguriert. Alternativ ist auf der Aufruf des Befehls `gpedit.msc` möglich. In AD Netzwerken können zur Vereinfachung der Administration Gruppenrichtlinien in der `Computerconfiguration` oder der `Benutzerkonfiguration` eingerichtet.

Zuerst wird die lokale Sicherheitsrichtlinie abgearbeitet. Die folgenden Gruppensicherheitsrichlinien werden in der folgenden Reihenfolge berücksichtigt:

1. Standort
2. Domäne
3. Organisatorische Einheit (OU)

Bei sich wiedersprechenden Einstellungen überschreibt die jeweils nachfolgende Richtlinie die vorhergehenden Einstellungen. Eine "näher" am Objekt definierte Richtlinie hat wiederum Vorrang vor einer in der Hierarchie entferntere Einstellung.

23.1 Vordefinierte Sicherheitsrichtlinien

W2K hat verschiedene Sicherheitsrichtlinienpakete vordefiniert. Diese können aus dem Verzeichnis `%SystemRoot%/security/templates` importiert werden. Die jeweiligen Vorlagen sind mit folgenden Dateien assoziiert. Dabei setzt sich der Name aus Sicherheitsstufe (BASIC, COMPATibel, SECURE, HISECure) und der Art des Systems (WorKstation, StandardserVer, DomänenController) zusammen.

Basis In der Datei basic??.inf sind die Standardeinstellungen der Sicherheitsrichtlinien von Windows 2000 z.B. hinsichtlich der Rechte des Hauptbenuters, Administratoren etc. hinterlegt. Sie können von hier aus einfach installiert werden. Diese Schablone sollte auf Rechnern genutzt werden, die von NT4 auf W2K upgegraded werden.

- Basicwk.inf
- Basicsv.inf
- Basicdc.inf

Kompatibel Die Compatws.inf Richtiline ermöglicht ein erfolgreiches Ausführen der meisten Anwendungen im Benutzerkontext, indem die Sicherheitsstufen bei bestimmten Dateien, Verzeichnissen und Registrierungsschlüsseln herabgesetzt wird.

Sicher Die Anwendung von *secure??.inf* Policies setzt viele Registry-Einstellungen auf höhere Sicherheitsstufen.

- Securews.inf
- Securedc.inf

Sehr Sicher Bei Anwendung der *hisec??.inf* Policies findet jegliche Netzwerkkommunikation verschlüsselt über *IPSec* statt. Mit dieser Maßnahme ist keinerlei Kommunikation mehr mit Microsoft-Rechnern mehr möglich, die nicht mindestens mit Windows 2000 laufen, da alle vorherigen MS-Betriebssyteme noch kein IPSec unterstützen.

- Hisecws.inf
- Hisecdc.inf

Das Tool `secedit` ermöglicht die automatisierte Konfiguration von Sicherheitsrichtlinien mittels der Console. Hiermit lassen sich aus dem GUI-Tool exportierte Sicherheitsrichtlinien automatisch anlegen.

23.1.1 Anmeldeversuch und Anmeldeereignis

Eine Amneldung wird dort aufgezeichnet wo sie stattfindet (Domäne oder Lokal). Die Anmeldung eines Users kann an der Domäne erfolgen, obwohl sich dieser gemäß einer lokalen Richtlinie an der lokalen Maschine nicht anmelden kann.

Hinsichtlich der zu überwachenden Ereignisse unterscheidet MS unter Anmeldeversuchen und Anmeldeereignissen. Im oben beschriebenen Fall wird der *Anmeldeversuch* auf dem Domänecontroller protokolliert, das *Anmeldeereignis* auf der lokalen Maschine.

Das Anmeldeereignis ist ein erfolgreich oder nicht erfolgreich zuendegeführter Anmeldeversuch.

23.2 Hierarchie der Sicherheitsrichtlinien

Die Sicherheitsrichtlininen unterliegen einer Vererbungshierarchie mit der Möglichkeit die Vererbung zu blocken. Eine Ausnahme unter den User-Account Einstellungen bilden hier allerdings die für die Passwort-Eigenschaften, die nicht blockiert werden können.

Teil V

Active Directory

Das sogenannte *Active Directory* ist die Verzeichnisdatenbank von Windows 2000. Hier werden Informationen zu allen Objekten im Netzwerk gespeichert. Active Directory Objekte sind:

- Benutzer
- Gruppen
- Computer
- Drucker
- Server
- Domänen
- Standorte

Das Directory ist als verteilte Datenbank aufgebaut, so daß die Administration an den Objekten dezentral erfolgen kann.

Kapitel 24

Aufbau des Active Directory

Der Aufbau des Verzeichnisses wird zuerst durch das *Schema* vorgegeben. Dieses enthält Definitionen aller Objekttypen, wie z.B. Benutzer oder Computer, die im Active Directory angelegt und verwaltet werden können. Im Schema können grundsätzlich zwei verschiedene Eintragstypen definiert werden.

Objektklassen beschreiben die möglichen Verzeichnisobjekte, die erstellt werden können.

Attribute werden den einzelenen Objektklassen zugeordnet und beschreiben das einzelne Objekt genau. Attribute werden hier nur einmal definiert. Die Zuordnung von Attributen zu Objektklassen erfolgt über eine Art Pointer, so daß eine Änderung an einem Attribut sich auf alle Attribute dieses Typs in allen Objektklassen auswirkt.

Das Schema ist zentral für alle Objekte gültig und kann dynamisch geändert werden. Die Änderungen wirken sich nach einer gewissen Replikationsdauer auf alle Objekte im Verzeichnis aus.

Der Zugriff auf das Gesamtschema des Verzeichnisses wird über die *DACL* (Discretionaly Access Control List) gesteuert, so daß nur bestimmte Accounts Änderungen am Schema vornehmen können.

24.1 Objekthierarchie

Die Hierarchie der Objekte in Active Directory ist wie ein Verzeichnisbaum aufgebaut. Hierarchisch besteht hier folgende Reihenfolge:

1. Forest (Gesamtstruktur)
2. Tree (Struktur)
3. Domäne

4. Organisationseinheit (OU)

Die einzelnene, strukturbestimmenden Objekte habe die folgenden Funktionen:

Forest (auch: Gesamtstruktur) Wenn zwischen mehreren Strukturen Vertrauensstellungen aufgebaut werden, bilden diese die sogenannte *Gesamtstruktur* oder *Forest*. Die Gesamtstruktur wird also gebildet, in dem zwischen den einzelnen Trees Vertrauensstellungen aufgebaut werden. Diese sind automatisch bidirektional und transitiv. Dieses Konstrukt ist dadurch gekennzeichnet, daß es keinen gemeinsamen Namensraum nutzt. Allerdings wird ein gemeinsames Verzeichnis*Schema* und ein gemeinsamer *globaler Katalog* genutzt. Wie oben angedeutet, wird die zuerst erstellte Domäne der Gesamtstruktur auch die *Stammdomäne der Gesamtstruktur*.

Eine einzelne standalone Struktur, stellt automatisch eine Gesamtstruktur dar, die aus einer einzigen Struktur besteht. Jede Stammdomäne einer Struktur besitzt daher eine transitive Vertrauensstellung mit der Stammdomäne der Gesamtstruktur. Das Konstrukt der Gesamtstrukturen bietet also die Möglichkeit, einer bestehenden Domänenhierarchie eine Domäne hinzuzufügen, ohne daß diese in den Namensraum der vorhandenen Domänenstruktur aufgenommen werden muß. Da die der Gesamtstruktur hinzugefügte Domäne(nstruktur) automatisch bidirektionale und transitve Vertrauensstellungen zur Stammdomäne der Gesamtstruktur besitzt, werden die Vertrauensstellungen innerhalb der Gesamtstruktur über die Namensräume hinweg vererbt.

Tree Als Tree (Struktur) wird eine hierarchische Anordnung von W2K Domänen bezeichnet, die einen zusammenhängenden (DNS-) Namensraum verwenden. Die erste Domäne, die erstellt wird ist automatisch die *Stammdomäne des Forest*.

Die Struktur eines Active Directory ist direkt auf dem DNS-Namensraum abgebildet. Ein AD-Baum entspricht dem DNS-Baum, so daß für jede (Sub-) Domain ein einzelner Baum entsteht. Wird einer vorhandenen Struktur eine neue Domäne hinzugefügt, wird diese der Stammdomäne der Struktur untergeordnet. Der Domänenname setzt sich jetzt aus dem eigentlichen Namen der Domäne und dem DNS Namen der Struktur zusammen. Hierbei wird rechts an den Namen der neuen Domäne der Name der Gesamtstruktur angehängt, so daß sich die neue Domäne eindeutig im DNS Namensraum zuordnen läßt.

Die untergeordneten Domänen besitzen bidirektionale und transitive Vertrauensstellungen zur übergreifenden Domäne. Aufgrund der transitiven Vertrauensstellungen vertrauen alle Domänen der Struktur ein-

ander direkt oder indirekt, da eine Vererbung der Vertrauensstellungen innerhalb der Domäne stattfindet.

Domänen Eine Domäne ist eine Sammlung von Computern, die durch die Administration festgelegt wird. Die Domäne muß einen netzwerkweiten, eindeutigen Namen besitzen, damit die Zuordnung der Ressourcen der Domäne im gesamten Netzwerk eindeutig ist. Sie stellt den Zugriff auf die zentralisierten Benuter- und Gruppenkonten zur Verfügung. Die Verwaltung der Domäne obliegt dem *Domänenadministrator.* Somit stellt die Domänen auch eine *Sicherheitsgrenze* zu anderen Domänen dar. Der Domänenadministrator besitzt nur Rechte innerhalb dieser einen Domäne, wenn ihm nicht explizit auch Rechte an anderen Domänen zugewiesen wurden.

Alle Mitglieder einer Domäne verwenden gemeinsam eine Verzeichnisdatenbank. Diese wird auf allen Domänencontrollern dieser Domäne replieziert, so daß sie vollständig auf allen Domänencontrollern vorliegt.

Organisationseinheit (OU) Eine Organisationseinheit ist ein Containerobjekt, daß zum Gruppieren anderer Objekte im AD dient. Eine Organisationseinheit kann neben Objekten auch andere Organisationseinheiten enthalten. Die Hierarchie der Organisationseinheiten kann innerhalb einer Domäne frei gewählt werden. In der Regel richtet sie sich nach den Netzwerkstrukturen (Netzwerkverwaltungsmodell) oder nach der Organisationsstruktur des Unternehmens.

Verwaltungsaufgaben an Objekten einer OU können an bestimmte Bentzer deligiert werden. Hierzu werden diesen Accounts die Berechtigungenen für die Organisationseinheit und den enthaltenen Objekten zugewiesen. Hierbei kann sowohl die volle Kontrolle über die Objekte eingestellt werden, wie auch nur eingeschränkte Verwaltungsmöglichkeiten.

24.2 Globaler Katalog

Die Gesamtstruktur stützt sich auf den *globalen Katalog.* Hier werden die Objektattribute gespeichert, die am häufigsten bei Abfragen benötigt werden. Hierunter fallen z.B. Namen und Anmeldenamen von Accounts. Im globalen Katalog sind außerdem alle Angaben gespeichert, die nötig sind, den Speicherort eines bestimmten Objektes zu ermitteln. Der globale Katalog wird also genutzt, um Abfragen und den Anmeldevorgang zu beschleunigen und um die Speicherorte der einzelnen Objekte ermitteln zu können. Des weiteren sind hier die Zugriffsberechtigungen für jedes Objekt und Attribut

des globalen Katalogs gespeichert, um bestimmen zu können ob und wie ein bestimmter Account Zugriff auf diese Information haben darf.

Zur weiteren Beschleunigung wurde der globale Katalogserver eingeführt, der eine Kopie der Abfragen speichert und diese an den globalen Katalog zur Abfrage weiterleitet. Der erste in AD erstellte Domänencontroller wird automatisch der globale Katalogsever. Zum Lastenausgleich können mehrere Katalogserver aufgesetzt werden.

24.3 Physische Struktur

Die logische Struktur von AD, die in Strukturen, Domänen und OUs aufgeteilt ist, wird von der physischen Struktur des Netzwerks getrennt. Die logische Struktur dient dazu, die Verwaltung der Netzwerkressourchen zu organisieren, während die physische Struktur sich auf den Netzwerkverkehr auswirkt. Die physische Struktur des AD Netzwerks wird durch die beiden Komponenten

- Domänencontroller und
- Standorte

abgebildet. Die physische Struktur legt fest, wie der Datenverkehr für die Anmeldung verläuft und über welche Verbindungen die Replikationen erfolgen.

24.3.1 Sites (Standorte)

Als Standort der phyische Teilbereich eines Netzwerks bezeichnet, dessen einzelne Teilnetze mit Hochgeschwindigkeitsleitungen verbunden sind. In der Regel sind sieses LAN-Netze, können jedoch auch über hochgeschwindigkeits WAN Verbindungen laufen. Mit Hilfe dieses Konstrukts kann das Netzwerk so aufgebaut werden, daß die Replikationen über Verbindungen mit genügend Bandbreite abgewickelt werden. Falls im Standort ein Domänencontroller installiert ist, verbleibt der Anmeldeverkehr innerhalb eines Standortes, so daß die Anmeldung auch komplett über schnelle Verbindungen abgewickelt wird und die Verzögerungen somit gering gehalten werden. In jeder Site *sollte* aus Gründen des schnellen Zugriffs zumindest ein globaler Katalogserver und ein Domänencontroller installiert werden.

Die Konfiguration der Sites erfolgt mit Hilfe des MMC-Snap-In `Active Directory Standorte und -Dienste`. Hier werden die einzelnen Domänen und die Netzwerkverbindungen zu einem Standort hinzugefügt. Die Verbindung zwischen den Standorten werden über die sogenannten *Site Links* festgelegt. Dieses sind zumeist Verbindungen mit niedrigerer Bandbreite.

Hierbei läßt sich auch einstellen, wann und wie der Datenverkehr zur Replizierung über diese Verbindungen abgewickelt wird. Die Replizierung innerhalb eines Standorts wird als *Intra-Site* (standortintern) bezeichnet. Diese findet wesentlich häufiger statt als eine standortübergreifende (*Inter-Site*) Replizierung.

Per Default erfolgt die Replizierung über *RPC* (Remote Procedure Call). *Inter-Site* Replikationen können aus Gründen der Bandbreitenbeschränkung so konfiguriert werden, daß sie über SMTP (Simple Mail Transfer Protocol) abgewickelt werden. Hierbei werden Emails verschickt (SMTP), die komprimierte verschlüsselte Replikationsinformationen enthalten. Die Email muß zudem von einer Zertifizierungsautorität signiert werden. Daher ist die Installation einer Zertifizierungsautorität (CA) zur notwendig. Diese Option ist allerdings nur für die Replikation zwischen *verschiedenen* Domänen möglich. Standortübergreifende Replikationen innerhalb einer Domän erfolgt immer direkt über IP.

24.4 Backup des Active Directory

In einer Domänenstruktur mit mehreren Domänencontrollern ist ein ist ein Komplettausfall aufgrund der verteilten Datenbankstruktur des AD eher unwarscheinlich. Die Informationen werden in mehr oder weniger regelmäßigen Abständen auf die anderen Domänencontroller repliziert, so daß die Datenbank nach einiger Zeit redundant vorliegt. Aus Sicherheitsgründen[1] sollte aber auf jeden Fall auch ein Backup des Active Directory erfolgen.

Ein Restore der Daten wird in der Regel vor allem dann benötigt, falls versehentlich Daten innerhalb der AD Struktur gelöscht wurden. Hier wird kein Vollrestore benötigt, sondern nur ein eine Teilwiederherstellung. Bei der Wiederherstellung kann zwischen einer *autoritativen*[2] Wiederherstellung des AD und einer nicht *authoritativen* gewählt werden. Die Daten, die bei der autoritative Wiederherstellung eingespielt werden werden an die anderen Domänencontroller repliziert und überschreiben dort andere Einstellungen. Die nicht autoritativ wiederhergestellten Daten werden nur auf einem Domänencontroller gehalten und beim nächsten Replizierungsvorgang wieder überschrieben.

24.4.1 Durchführung eines Restore des Active Directoy

Zur Durchführung des *autoritativen* Restores muß der Rechner im *Modus für die Wiederherstellung der Verzeichnisdienste* gestartet werden. An-

[1] Das System kann nicht nur durch Fehler in der Soft- oder Hardware beeinträchtigt werden, sondern auch durch äußere Umstände wie z.B. ein Wassereinbruck oder Feuer im Gebäude. Aus diesem Grunde sollte ein Teil der Sicherungsmedien auch immer außerhalb des Gebäudes aufbewahrt werden.

[2] autoritativ: maßgebend, maßgeblich

schließend kann das Verzeichnis `SYSVOL` und das Active Directory wiederhergestellt werden. Falls eine *authoritative* Wiederherstellung erfolgen soll, wird jetzt das Konsolenprogramm `ntdsutil` gestartet. Hiermit können AD-Objekte für die maßgebende Wiederherstellung markiert werden, indem die Sequenzunummer der Objekte für die Replizierung soweit inkrementiert wird, daß sie größer ist als die der anderen Aktualisierungsnummern. Das Objekt wird dann bei der Replizierung nicht von anderen überschrieben, sondern überschreibt selbst die Einstellungen auf den anderen Domänen Controllern.

Anschließend muß der Rechner auf neu gestartet werden um wieder im normalen Modus zu laufen. Die Wiederherstellung der Systemstatusdaten kann nur am lokalen Computer erfolgen. Eine Remote-Wiederherstellung ist nicht möglich.

Kapitel 25

Operations Master

Die Replizierung der Verzeichnisdatenbank arbeitet im *Mulitmaster*- Betrieb. Bei verschiedenen Aufgabenstellungen könnte diese Betriebsart jedoch zu Konflikten führen, so daß der Betrieb empfindlich gestört werden würde. Hierfür wurden verschiedene Aufgabenbereiche aus dem Multimasterbetrieb ausgekoppelt und dürfen nur im Einzelmasterbetrieb durchgeführt werden. Diese Rolle übernimmt ein Domänencontroller, der als einziger im gesamten Forest oder Tree diese Rolle ausführen darf. Dieser Domänencontroller wird dann *Operations Master* (deutsch: Betriebsmaster) genannt. Die folgenden Aufgabenbereiche dürfen nur im Einzelmasterbetrieb ausgeführt werden:

Schemamaster Der Schemamaster überwacht die Änderungen am AD-Schema. Es darf zum selben Zeitpunkt nur ein Schemamaster im Forest existieren.
Um das Schema des Forest zu ändern, benötigt der Administrator Zugriff zu dem Schemamaster DC und muß Mitglied der Gruppe Schema Admins sein.

Domain Naming Master (deutsch: DNS- Master) Der Domain Naming Master ist für das Hinzufügen und Entfernen von Domänen aus dem Forest verantwortlich. Diese Rolle sollte eine Maschine übernehmen, auf der auch der Globale Katalog lokalisiert ist. Auch diese Rolle darf zur gleichen Zeit nur einmal im Forest vorhanden sein.

PDC-Emulator Der PDC-Emulator zeichnet für die pre W2K Clients verantwortlich. Er ist der Einzelmaster für die eventuell noch vorhandenen BDCs in der Domäne. Mit Hilfe des PDC- Emulators können z.B. Clients, die kein AD unterstützen, z.B. ihre Passwortänderungen vornehmen. Die Rolle des PDC- Emulators muß *domänenweit* einmalig definiert werden.

RID-Master Der RID-Master weist den Domänencontrollern *einer Domäne* Seqenzen von relativen IDs (RIDs) zu. Die Domänencontroller fordern

beim RID-Master einen Pool von RIDs an, die sie zur Generierung von Security-IDs (SIDs) benötigen. Ein Objekt wird über die SID eindeutig gekennzeichnet. Diese besteht unter anderem aus der Domänen-SID und der RID. Die Domänen SID ist innerhalb des Forests, die RID innerhalb der Domäne eindeutig, so daß jedes Objekt im Forest eindeutig identifiziert werden kann. Da der RID Master eine domäneneindeutige ID erzeugt darf er nur einmal in der Domäne vorkommen. Der RID Master wird auch benötigt, falls ein Objekt von einer Domäne zu einer anderen mit Hilfe des Befehls `movetree` verschoben wird.

Infrastrukturmaster Der Infrastrukturmaster ist für den akutellen Stand der domänenübergreifenden Zuordnungen verantwortlich. Er paßt beispielsweise die Zuordnungen der Userobjekte zu den Gruppenobjekten an, wenn diese sich ändern. Die Rolle des Infrastrukturmasters ist domänenweit eindeutig. Die von ihm durchgeführten Änderungen werden dann mit Hilfe der normalen Replikationsvorgänge auf die anderen Domänencontroller übertragen.

Teil VI

Anhang

Kapitel 26

sonstiges

26.1 16 Bit Applikationen

Zur Ausführung von 16 Bit Applikationen emuliert W2K eine Umgebung mit Hilfe des Prozesses `NTVDM` (NT Virtual Device Manager (?)). Alle gestarteten 16 Bit Applikationen laufen als Threads dieses Prozesses und teilen sich einen gemeinsamen Adressraum. Auf diese Weise können sie, falls vorgesehen miteinader kommunizieren. Falls eines der 16 Bit Programme ausfällt oder "hängt", blockiert dieses auch die anderen 16 Bit Programme. Im Task-Manager können die einzelnen Prozesse nicht mehr einzeln identifiziert werden, da nur der NTVDM Task sichtbar ist. Soll ein Prozeß in einem separaten Adressraum starten, kann dieses auf der Registerkarte `Eigenschaften` unter dem Punkt *Im separaten Adressraum starten* eingestellt werden. Eine andere Möglichkeit ist den Prozeß per Konsole oder Batchdatei mit dem Befehl `start /separate` aufzurufen.

26.2 Installationsdateien

Windows 2000 kennt neben den .exe Dateien verschiedene ausführbare Dateitypen, die die Softwareverteilung und -Installation erleichtern.

.msi Diese Dateiendung kennzeichnet die sogenannten Windows Installer Pakte. Sie werden vom Softwarehersteller zur Erleichterung der Installation einer Anwendung zur Verfügung gestellt. Die Datei muß im gleichen Verzeichnis wie die anderen Installationsdateien liegen.

Die Dateiendung .msi ist mit dem Programm *msiexec.exe* verknüpft, das eine .msi Datei läd und die Installation entsprechend startet.

.mst Dateien mit der Endung .mst werden auch Transformationsdateien genannt. Mit Hilfe dieser Dateien wird die Installation eines Windows-Installer Paketes (.msi) zum Zeitpunkt der Zuweisung oder Veröffent-

lichung angepaßt, so daß z.B. nur ein Teil einer Anwendung oder bestimmte Optionen installiert werden. Der Administrator kann dem User also eine für seine Zwecke angepaßte Installation zur Verfügung stellen.

.msp Zum Einspielen kleinerer Patche in Form von Dateien, die installiert werden müssen werden die .msp-Dateien verwendet. Diese Patches sollten nur für Bugfixes und Service Packs zur Anwendung kommen, da mit Hilfe der .msp-Dateien das Entfernen oder Ändern im Produktcode nicht möglich ist. Es können hiermit also *keine* Dateien gepatcht werden, sondern nur Dateien eingespielt werden. Auch das Ändern von Dateinamen oder Registryeinstellungen ist hiermit nicht erlaubt.

.zap Zap-Dateien sind reine ASCII-Dateien, die mit einem Editor erzeugt und bearbeitet werden können. In einer .zap- Datei wird ein Executable angegeben, daß unter dem Punkt *Software* in der Systemsteuerung angezeigt wird. Der Systemadministrator kann eine .zap-Datei für eine Applikation erzeugen, wenn hierfür z.B. keine .msi- Datei vorliegt.

.aas Scripte für die Zuweisung von Anwendungen z.B. an Dateiendungen werden in Form von .aas- Dateien veröffentlicht.

26.3 boot.ini

Beim Systemstart wird aus der Datei `boot.ini`, die im Rootverzeichnis der aktiven Partition liegt, ermittelt von wo das System gestartet wird[1]. Hier legt der sogenannte ARC-Pfad (Advanced Risc Computing) fest, wie welches System gestartet wird.

Die Angaben unterscheiden sich je nach dem Bussystem.

26.3.1 AT-Bus

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT=''W2K'' /param
```

multi(0) Angabe des Controllers und der Controllernummer. Bei AT-Bus immer multi(0).

disk(0) *Bei AT-Bus (multi) immer 0.*

rdisk(0) Nummer der Platte am Controller (0 oder 1)

partition(1) Partitionsnummer. Beginnt bei 1, da 0 für den MBR vorgesehen ist.

\WINNT Subdirectory in dem die Systemdateien liegen (s.a. 3.3).

[1] Die Angaben gelten auch für NT4

="W2K" Eintrag, der im Bootmenue angezeigt wird.

/param Parameter, die beim Programmstart gesetzt werden können.

26.3.2 SCSI-Bus

```
scsi(0)disk(0)rdisk(0)partition(1)\WINNT=''W2K'' /param
```

scsi(0) Angabe des Controllers und der Controllernummer.

disk(0) SCSI-ID der Platte.

rdisk(0) *Bei SCSI immer 0.* (ältere Angabe: LUN des Devices?)

partition(1) Partitionsnummer. Beginnt bei 1, da 0 für den MBR vorgesehen ist.

\WINNT Subdirectory in dem die Systemdateien liegen (s.a. 3.3).

="W2K" Eintrag, der im Bootmenue angezeigt wird.

/param Parameter, die beim Programmstart gesetzt werden können.

26.3.3 Parameter in der boot.ini

Unter anderm können folgende Parameter in der `boot.ini` eingestellt werden:

/basevideo W2K wird mit dem Standard-VGA Treiber geladen.

fastdetect=comX comY Die serielle Mauserkennung wird deaktiviert. Ohne Festlegung einer Schnittstelle wird die Mauserkennung generell deaktiviert.

/maxmem Maximaler Speicher, der genutzt wird, z.B. bei der Suche nach defekten Speicherchips.

/noguiboot Beim Systemstart wird der Bildschirm mit dem Ladestatus nicht angezeigt.

/sos Die Namen der Gerätetreiber werden beim Laden angzeigt, um den fehlgeschlagenen Start eines Treibers festzustellen.

26.4 compatws.inf

Die Datei %SYSTEMROOT%\security\templates\compatws.inf ist ein Template für die Sicherheitseinstellungen für die einzelnen (vordefinierten) Benutzeraccounts wie z.B. Hauptbenutzer.

26.5 sysdiff

Das Tool `sysdiff` sollte genutzt werden, falls Applikationen installiert werden, die nicht über eine spezielle Installationsprozedur verfügen. Mit Hilfe dieses Tools wird ein Schnappschuß vom System vor und nach der Installation einer Applikation gemacht. Die Applikation soll sich dann später komplett aus dem System entfernen lassen.

Der Schalter `/q` weist das Tool an im *unattended mode* zu laufen.

26.6 Programme der Recovery Console

Die Recoveryconsole bietet einige der aus DOS bekannten Befehle sowie als Erweiterung die folgenden Befehle:

batch führt Befehle aus einer Datei aus.

disable Deaktiviert einen Systemdienst oder einen Gerätetreiber.

diskpart Tool zur Verwaltung von Festplattenpartitionen.

enable Startet oder aktiviert einen Systemdiens oder einen Gerätetreiber.

exit Beenden und Computer neu starten.

expand Extrahiert komprimierte Dateien der W2k-CD.

fixboot Schreibt einen neuen Partitionsbootsektor auf die Systempartition.

fixmbr Repariert den MBR des Partitionsbootsektors.

logon Ermöglicht die Anmeldung an einer W2K Installation.

listsvc Zeigt alle Dienste und Treiber an.

map Zeigt die Zuordnung der Laufwerksbuchstaben an.

more Zeigt Dateiinhalte an.

systemroot Legt das aktuelle Verzeichnis als Stammverzeichnis (root) des Systems fest, an dem man zur Zeit angemeldet ist.

type Zeigt Dateiinhalte an.

systemroot Setzt das aktuelle Verzeichnis auf %SystemRoot%.

26.7 Beispiel einer Unattended- Antwortdatei

```
;file: unattend.txt
;SetupMgrTag

[Data]
    AutoPartition=1
    MsDosInitiated="0"              ; muß immer auf 0 (falls Setup von CDROM)
    UnattendedInstall="Yes"

[Unattended]
    UnattendMode=FullUnattended

    OemSkipEula=Yes           ; Nachfrage n. Lizenzzustimmung?

    OemPreinstall=No          ; OemPreinstall=Yes: erst Kopie von
                              ; Inststallationsdateien auf lokale
                                    ; Platte. I.d.r No

    TargetPath=\WINNT

[GuiUnattended]
    AdminPassword=passwd
    OEMSkipRegional=1         ; Überspringt regionale Einstellungen
    TimeZone=110              ; W.Europa=110, GMT=090
    OemSkipWelcome=1          ; Begrüßungsnachricht wird übersprungen

[UserData]
    FullName="Martin Werthmoeller"
    ComputerName=singapore
    ProductID=MBK9M-JR62W-793WW-B3QHR-TY4D6

[Display]
    BitsPerPel=32             ; Bit pro Pixel (8,16,32)
    Xresolution=1024
    YResolution=768
    Vrefresh=85

[LicenseFilePrintData]        ; Lizenzmodell
    AutoMode=PerServer
    AutoUsers=50

[TapiLocation]
    CountryCode=49
```

```
    AreaCode=0251

[RegionalSettings]
    LanguageGroup=1
    Language=00000407

[Identification]
    JoinDomain=werthmoeller  ; In Domäne werthmoeller aufnehmen
;   JoinWorkgroup=wgroup     ; In Arbeitsgr. aufnehmen (eins von beiden)

[Networking]
    InstallDefaultComponents=No

; NetAdapters
; Frei definierbarer Adaptername(n) als Key mit frei definierbarem
; Wert. Der Wert beschreibt den Namen einer neuen Sektion, in der
; weitere Key-Value-Paare eine Bezeichnung für die Karte festlegen

[NetAdapters]
    Adapter1=params.Adapter1

[params.Adapter1]
    INFID="3com b"

[NetClients]
    MS_MSClient=params.MS_MSClient

[NetServices]
    MS_SERVER=params.MS_SERVER

[NetProtocols]
    MS_TCPIP=params.MS_TCPIP

[params.MS_TCPIP]
    DNS=Yes
    UseDomainNameDevolution=No
    EnableLMHosts=Yes
    AdapterSections=params.MS_TCPIP.Adapter1

[params.MS_TCPIP.Adapter1]
    SpecificTo=Adapter1
    DHCP=Yes
    WINS=No
    NetBIOSOptions=0
```

26.8 Das Setupprogramm winnt

Winnt32 dient zur Einrichtung oder Aktualisierung von Windows 2000 Server oder Windows 2000 Professional. Der Befeh `winnt32` läßt sich an der Konsole von Windows 95, Windows 98 oder Windows NT nutzen. Auf 16-Bit Systemen (z.B. über DOS-Bootdiskette gestartet) wird der Befehl `winnt` genutzt. *Achtung! Die Kommandozeilenparameter der beiden Befehle unterscheiden sich.*

26.8.1 winnt

```
winnt /u:<Antwortdatei> /s:<Quellpfad> /t:<Ziellaufwerk>
```

Antwortdatei Dateiname (ev. mit Pfad) der Antwortdatei

Quellpfad Pfad zu den Quelldateien

Ziellaufwerk Ziellaufwerk auf das W2K installiert werden soll (optional)

26.8.2 Parameter von winnt32

```
winnt32 [/s:Quellpfad] [/tempdrive:Laufwerk] [/unattend[Sekunden]:[Antwortdatei]]
[/copydir:Verzeichnisname] [/copysource:Verzeichnisname] [/cmd:Befehlszeile]
[/debug[Ebene]:[Dateiname]] [/udf:ID[,UDF-Datei]] [/syspart:Laufwerk]
[/checkupgradeonly] [/cmdcons] [/m:Verzeichnisname] [makelocalsource]
[/noreboot]
```

/s:Quellpfad Gibt den Quellort der Windows 2000-Dateien an. Um gleichzeitig Dateien von mehreren Servern zu kopieren, geben Sie mehrere /s-Quellen an. Wenn Sie mehrere /s-Optionen verwenden, muss der erste angegebene Server verfügbar sein. Andernfalls schlägt Setup fehl.

/tempdrive:Laufwerk Weist Setup an, temporäre Dateien auf der angegebenen Partition zu speichern und Windows 2000 auf dieser Partition zu installieren.

/unattend Aktualisiert frühere Versionen von Windows 2000, Windows NT 4.0, Windows 3.51, Windows 95 oder Windows 98 im Setupmodus ohne Beaufsichtigung. Sämtliche Benutzereinstellungen werden von der vorherigen Installation übernommen, so dass Setup ohne Benutzereingriff ausgeführt werden kann.

Mit der Option /unattend zur Automatisierung von Setup bestätigen Sie, dass Sie den Microsoft-Lizenzvertrag für Windows 2000 gelesen haben und sich mit diesem einverstanden erklären. Bevor Sie Windows

2000 mit dieser Option für eine andere Organisation als Ihre eigene installieren, müssen Sie sicherstellen, dass der Endbenutzer (entweder eine Einzelperson oder eine juristische Person) die im Microsoft-Lizenzvertrag für Windows 2000 festgelegten Bedingungen erhalten, gelesen und akzeptiert hat. OEMs dürfen diesen Schlüssel nicht auf Computern angeben, die an Endbenutzer verkauft werden.

/unattend[Sekunden :[Antwortdatei]] Führt eine Neuinstallation im Setupmodus ohne Beaufsichtigung durch. Die Antwortdatei übergibt Ihre Spezifikationen an das Installationsprogramm.

Sekunden ist die Anzahl der Sekunden zwischen dem Zeitpunkt, zu dem Setup das Kopieren der Dateien beendet hat, und dem Neustart des Computers. Sie können Sekunden auf jedem Computer verwenden, der Windows NT oder Windows 2000 ausführt.

Antwortdatei ist der Name der Antwortdatei.

/copydir:Verzeichnisname Erstellt eine zusätzlichen Verzeichnis innerhalb des Verzeichnisses, in dem die Windows 2000-Dateien installiert werden. Wenn z. B. der Quellverzeichis ein Verzeichnis namens Eigene_Treiber enthält, der Änderungen nur für Ihren Standort umfasst, können Sie /copydir Eigene_Treiber eingeben, damit Setup diesen Verzeichnis in Ihren Windows 2000-Installationsverzeichnis kopiert, wobei das neue Verzeichnis C:/Winnt/Eigene_Treiber lautet. Sie können /copydir zum Erstellen beliebig vieler zusätzlicher Verzeichnisse verwenden.

/copysource:Ordnername Erstellt einen zusätzlichen temporären Ordner innerhalb des Ordners, in dem die Windows 2000-Dateien installiert sind. Wenn z. B. der Quellordner einen Ordner namens Eigene_Treiber enthält, der Änderungen nur für Ihren Standort umfasst, können Sie /copysource Eigene_Treiber eingeben, damit Setup diesen Ordner in Ihren Windows 2000-Installationsordner kopiert und die darin enthaltenen Dateien beim Setup verwendet, wobei das temporäre Ordnerverzeichnis C:/Winnt/Eigene_Treiber lautet. Im Gegensatz zu den von /copydir erstellten Ordnern werden /copysource-Ordner nach Abschluss von Setup gelöscht.

/cmd:Befehlszeile Weist Setup an, vor der Schlussphase von Setup einen bestimmten Befehl auszuführen. Dieser Zeitpunkt liegt nach dem zweimaligen Neustarten des Computers und nachdem Setup die erforderlichen Konfigurationsdaten gesammelt hat, jedoch vor Abschluss von Setup. Anstelle eines einzelnen Befehls kann hier auch der Pfad zur Datei `cmdlines.txt` angegeben werden, in der die auszuführenden Befehle aufgelistet sind.

/debug[Ebene :[Dateiname]] Erstellt ein Fehlersuchprotokoll auf der angegebenen Ebene, z. B. /debug4:C:/Win2000.log. Die Standardprotokolldatei ist C:/%Windir%/Winnt32.log mit der Debugebene 2. Die Protokollebenen sind wie folgt definiert: 0: Schwere Fehler; 1: Fehler; 2: Warnungen; 3: Informationen; 4: Detaillierte Informationen zur Fehlersuche. Jede Ebene beinhaltet jeweils die darunter befindlichen Ebenen.

/udf:ID[,UDB-Datei] Gibt einen Bezeichner (ID) an, den Setup verwendet, um anzugeben, wie eine Uniqueness Database (UDB)-Datei eine Antwortdatei ändert (siehe unter /unattend). Der Parameter /udf überschreibt Werte in der Antwortdatei, und der Bezeichner bestimmt, welche Werte in der UDB-Datei verwendet werden. So überschreibt z. B. /udf:RAS_Benutzer,Unsere_Firma.udb Einstellungen, die für den Bezeichner RAS_Benutzer in der Datei Unsere_Firma.udb angegeben sind. Ohne Angabe von UDB-Datei fordert Setup den Benutzer auf, eine Diskette einzulegen, die die Datei $Unique$.udb enthält.

/syspart:Laufwerk Gibt an, dass Sie Setup-Startdateien auf eine Festplatte kopieren, die Festplatte als aktiv kennzeichnen und sie dann in einen anderen Computer einbauen können. Wenn Sie diesen Computer booten, startet er automatisch mit der nächsten Phase von Setup. Sie müssen den Parameter /tempdrive immer zusammen mit dem Parameter /syspart verwenden.

/checkupgradeonly Überprüft, ob der Computer für die Aktualisierung auf Windows 2000 kompatibel ist. Für die Aktualisierung von Windows 95 oder Windows 98 erstellt Setup im Windows-Installationsordner eine Berichtdatei mit dem Namen Upgrade.txt. Für die Aktualisierung von Windows NT 3.51 oder 4.0 speichert Setup diesen Bericht in Winnt32.log im Installationsordner.

/cmdcons Fügt dem Bildschirm für die Betriebssystemauswahl die Option Wiederherstellungskonsole zum Reparieren einer fehlgeschlagenen Installation hinzu. Diese wird nur im Anschluss an Setup verwendet.

/m:Ordnername Gibt an, dass Setup Ersatzdateien von einer alternativen Quelle kopiert. Weist Setup an, zuerst an der alternativen Quelle zu suchen. Wenn dort Dateien vorhanden sind, werden diese anstelle der Dateien auf dem Standardpfad verwendet.

/makelocalsource Weist Setup an, alle Installationsquelldateien auf Ihre lokale Festplatte zu kopieren. Verwenden Sie /makelocalsource beim Installieren von einer CD, um Installationsdateien auch dann zur Verfügung zu haben, wenn die CD im weiteren Installationsverlauf nicht mehr verfügbar ist.

/noreboot Weist Setup an, den Computer nicht neu zu starten, nachdem winnt32 die Dateikopierphase abgeschlossen hat, damit Sie einen anderen Befehl ausführen können.

26.9 Konvertieren in NTFS

Falls ein Laufwerk mit dem FAT Filesystem formatiert wurde kann es nachträglich auf NTFS konvertiert werden. Hierzu wird der Befehl `convert` genutzt. Falls das Systemlaufwerk konvertiert werden soll, muß der Rechner noch einmal neu gestartet werden. Die Syntax des Befehls lautet:

```
CONVERT Datenträger /FS:NTFS [/V]

Datenträger  Gibt den Laufwerkbuchstaben (gefolgt von einem Doppelpunkt), den
             Bereitstellungspunkt oder den Datenträgernamen an.
/FS:NTFS     Gibt den Datenträger an, der in das NTFS-Format konvertiert
             werden soll.
/V           Ausführliches Anzeigeformat bei der Ausführung von CONVERT.
```

Die Konvertierung des Laufwerks erfolgt z.B. mit:
`convert c: /FS:NTFS`

26.10 Bootdiskette mit Netzwerkzugriff

Eine rudimentäre bootfähige Diskette kann mit den Befehlen `format` oder `sys` erstellt werden:

- `format a: /s /u`
- `sys a:`

Eine Bootdiskette für den Netzwerkzugriff kann unter Novell oder NT4 erfolgen. Hier wird das Zusammenstellen der Treiber durch Installation der *Netzwerk Clientsoftware* erfolgen. Hier werden die protokollspezifischen Treiber auf die Diskette kopiert. Die Treiber für die Netzwerkkarte werden dann manuell auf die Diskette kopiert, und die Bootdiskette entsprechend angepaßt.

datei.dos Kartenspezifischer Treiber, der auf die Diskette kopiert wird.

protocol.ini Muß systemspezifisch angepaßt werden. Die Beschreibung hierfür findet sich in der Regel im Verzeichnis für den DOS NIC-Treiber.

system.ini Wird zum Laden des Treibers angepaßt.

26.11 format (Parameter)

```
format
/s      Systemdateien mitkopieren (wie sys a:)
/u
/q      Quickformat
```

26.12 Dienste

26.12.1 Serverdienst

Der Serverdienst ist für Datei- und Druckeranfragen aus dem Netz zuständig. Der Arbietsstationsdienst ist für die lokalen Datei- und Druckeranfragen zuständig.

Kapitel 27

Begriffsbestimmungen und Abkürzungen

27.0.2 Account/Logon Event

Ein *Logon Event* ist ein Ereignis, daß auftritt, wenn über das Netzwerk auf freigegebene Ressourcen zugegriffen wird. Dieses Ereignis kann mitprotokolliert werden. Ein *Account Event* ist dagegen ein Ereignis, daß auftritt wenn sich jemand an einem Benutzeraccount anmeldet.

27.0.3 Acitve Directory

Das Active Directory ist auf jedem Domänencontroller lokal in einer Datei abgespeichert `(ntds/ntds.dit)`. Änderungen am Directory werden zuerst lokal gespeichert und dann auf die anderen Rechner verteilt. Jede Domäne hat ein eigenes AD (Active Directory).

27.0.4 ACE

Ein *Access Control Entry* (deutsch Berechtigungseintrag) ist ein Eintrag in der Systemdatenbank, in dem Informationen gespeichert werden, für welchen Sicherheitsprincipal (z.B. einen Benutzer) Zugriffsrechte gewährt oder verweigert werden, oder welche Zugriffsereignisse überwacht werden sollen. Die ACEs eines Objektes werden zu einer geordneten Liste – der ACL – zusammengefaßt.
Siehe auch 27.0.5

27.0.5 ACL

Die *Access Control List* (deusch Zugriffkontrolliste) legt die Berechtigugnen für jedes Objekt fest. Die Sicherheitsbeschreibung eines Objektes besteht genau genommen aus einer ACL für die Benutzer und Gruppen denen ein Zugriff gewährt wird (DACL 27.0.16), sowie aus einer ACL in der vermerkt ist,

welche Zugriffe auf das zugehörige Objekt überwacht werden sollen (SACL 27.0.56).
Siehe auch 27.0.4

27.0.6 ACPI

Advanced Configuration and Power Interface
Von Microsoft, Intel und Toshiba erstellte Spezifikation zur Beschreibung definierter Schnittstellen zur Hardware um die Steuerung von Plug-and-Play und Powermanagement zu vereinheitlichen. Das Betriebsystem und die Hardware können hierüber systemnahe Konfigurationsinformationen austauschen.

27.0.7 ADSI

Active Directory Services Interface

27.0.8 AGLP

Access Global Group Local Group Permissions

27.0.9 ALP

Accounts Access Local Group Permissions

27.0.10 ARC

Advanced Risc Computing (s.a. 26.3)

27.0.11 APM

Advanced Power Management

27.0.12 Dialogbox `Ausführen` (Run)

Im Startmenü befindet sich die Dialogbox `Ausführen` (`Run`) mit der ein Programm, insbesondere ein Konsolenprogramm direkt aufgerufen werden kann. Allerdings ist hier zu beachten, daß `interne` Befehle des Kommandozeileninterpreters (`cmd.exe`) nicht direkt aufgerufen werden können, sondern nur indem dieser explizit mit dem Schalter `/c` und dem internen Befehl gestartet wird, wie z.B.: `cmd /c start /low httpd.exe`.

27.0.13 Backup Domänencontroller (BDC)

Der Backup Domänencontroller ist ein Konstrukt der NT 3.x/4 Domänenstruktur. Er dient dazu, eine Kopie der Verzeichnisdatenbank mit allen Domäneneinstellungen zu halten. An dieser Maschiene können keine Eistellungen hinsichtlich der Domäne vorgenommen werden. Dieses darf nur auf dem primären Domänencontroller durchgeführt werden. Der BDC gleicht sich in regelmäßigen Abständen automatisch mit dem primären Domänencontroler ab. Um einen BDC zu einem PDC hochzustufen, muß der PDC entfernt werden und der BDC dann hochgestuft werden. Ein einfacher Memberserver kann nur durch Neuinstallation mit entsprechender Konfiguration bei der Installation zu einem BDC/PDC hochgestuft werden.

27.0.14 Benutzerprofile

Die Benutzerprofile sind in der Datei `ntuser.dat` unter `Dokumente und Einstellungen` je nach User abgelegt. Das Profil wird erst geschrieben nachdem sich der User an- und wieder abgemeldet hat. Falls diese Datei in `ntuser.man` umbenannt wird, kann der User sein Profil nicht mehr ändern.

27.0.15 CN

Der CN ist der Name für ein Objekt, das keine Organsiationseinheit (OU) und auch keine Domänenkomponente (DC) ist. Letztendlich kennzeichnet er das Objekt innerhalb der OU eindeutig.

27.0.16 DACL

Die *Discretional Access Control List* gibt die Benutzer und Gruppen an, denen der Zugriff auf das gehörige Objekt gewährt oder verweigert wird.
Siehe auch ACL 27.0.5

27.0.17 Daemon

Unter Un*x-System Bezeichnung für Programm, welches im Hintergrund laufend als Severdienst fungiert.

27.0.18 DC

Eine DC ist einen Komponente eines FQDM wie z.B. *com* oder *de*.

27.0.19 DDF

Data Decryption Field
Feld im Vorspann einer Datei im NT-Filesystem, in dem die Schlüssel hinterlegt werden (s.a. 4.2.2).

27.0.20 displayName

Der *displayName* ist der Name, der in das Feld "vollständiger Name" auf dem Blatt `Neues Objekt - User` eingegeben wurde, bzw. unter der Eigenschaft "Anzeigename" für ein Objekt angezeigt wird.

27.0.21 DRF

Data Recovery Field
Feld im Vorspann einer Datei im NT-Filesystem, in dem die Schlüssel für die Datenwiederherstellung hinterlegt werden (s.a. 4.2.2).

27.0.22 DN

Der Distinguished Name gibt den Pfad zum Benutzerkonto im Verzeichnis an.

27.0.23 DNS

Domain Name System, Achtung! Ein DNS-Name darf keinen Unterstrich enthalten.

27.0.24 DNS

Desoxiribonukleinsäure, auch DNA (Desoxyribonucleinacid)

27.0.25 DHCP

Dynamic Host Configuration Protocol

Mit Hilfe eines DHCP-Servers werden IP Adressen automatisch im Netzwerk verteilt. Ein Client, der eine Adresse anfordert schickt beim Systemstart ein Paktet mit der Absenderadresse `0.0.0.0` an die Adresse `255.255.255.255`. Die Adresse `255.255.255.255` ist in jedem Netzwerksegment eine Broadcastadresse, die von jeder Maschine im IP-Netz empfangen wird. Ein DHCP-Server der eine solche Anfrage empfängt, teilt diesem Client eine IP-Adresse zu. Daneben werden dem Client noch die Adresse des *Defaultgateway* und eventuell die WINS-Serveradresse (bei Windows-DHCP-Servern) mitgeteilt.

Falls die automatische Adresszuweisung in einem grouteten Netz erfolgen soll, stellt sich das Problem, daß die Router Broadcasts nicht in eine anderes Netzwerksegment übermitteln. Um die per Broadcast erfolgenden DHCP-Anfragen an einen Router in einem anderen Subnetz weiterzuleiten, müssen die zwischengeschalteten Router so konfiguriert werden können, daß sie die Anfragen der DHCP-Clients routen (*RFC 1542*). In einem größeren Netzwerk mit vielen Segmenten würde diese Lösung allerdings einen erhebliche Netzlast in jedem Segment erzeugen. Aus diesem Grunde wird hier

oft ein *DHCP Relay Agent* eingesetzt. Dieser ist in jedem Subnetz installiert, in dem sich DCHP-Clients befinden. Er nimmt einen Broadcast eines Clients entgegen und sendet ihn per *Unicast* direkt an den DHCP-Server. Dieser erkennt, daß die Anfrage über einen *Relay Agent* erfolgte und sendet die Antwort wiederum direkt an den Agent, der sie an den DHCP-Client weiterleitet.

DHCP-Optionen

Das DHCP Protokoll bietet die Möglichkeit verschiedenste Informationen an den Client zu übermitteln. Die zu übermittelndne Optionen können auf dem DHCP-Server global oder für einen Adressbereich zugewiesen werden. Auch hier besitzen letztendlich die für eine Adresse oder einen Adressbereich festgelegten Optionen Vorrang vor denen, die global definiert wurden. Die Standard- Optionen sind im *RFC 2132* aufgeführt. Sie können noch durch Herstellerspezifische Optionen ergänzt werden. In Windows Systemen werden häufig genutzt:

Subnet-Mask Subnetzmaske des DHCP-Clients,

Router IP-Adresse von einem oder mehreren Routern, die als Gateway für den Client fungieren,

DNS-Server IP-Adressen der zu benutzendne DNS-Server,

Domain-Name Domain-Name des DHCP-Clients,

WINS/NBNS-Server IP-Adressen von zu nutzenden WINS/NetBIOS-Nameservern,

WINS/NetBT-Knotentyp NetBIOS-Knotentyp für NetBIOS over TCP/IP,

NetBIOS Scope ID NetBIOS over TCP/IP Scope-ID

27.0.26 EAP

Das Extended Authentification Protocol ist eine Erweiterung des Point-to-Point Protokolls (PPP). Es erlaubt Clients mit RAS-Verbindungen eine (verschlüsselte) Authentifikation. Das Protokoll ist in RFC 2284 definiert.

27.0.27 einheitlicher Modus

Eine Domäne, die sich im *einheitlichen* Modus (native mode) befindet, kann nur W2K Domänencontroler enthalten. Falls sich in der Domäne noch NT4 (Backup-)Domänencontroller befinden, muß die Domäne im gemischten Modus (mixed-mode) betrieben werden. Eine Domäne kann jeder Zeit in den einheitlichen Modus überführt werden, allerdings ist ein zurückführen in den gemischten Modus dann nicht mehr möglich.

27.0.28 EFS

Encrypted File System (s.a. 4.2.2)

27.0.29 Gatewayservices

Die Gatewayservices (GSNW Gateway (and Client) Services for NetWare) ermöglichen es einen W2K Server so zu konfigurieren, daß er als Gateway zwischen den NetWare Servern und den Windows Clients fungiert. Mit dieser Konfiguration benötigen die Clients keinen *NW Client* für den Zugriff auf die NetWare Ressourcen. Der Zugriff läuft immer über den W2K Server. Allerdings müssen die User, die mit Hilfe der Gatewayservices auf den NW-Server zugreifen sollen, zur Gruppe *NTGATEWAY* gehören. Dieses beinhaltet den Nachteil, daß keine differenzierte Rechteverwaltung der Novell-Seite möglich ist. Falls die *Netware* Server noch mit SPX/IPX kommunizieren, muß auf dem W2K Server zusätzlich noch *NWLink*, die MS Implementierung des SPX/IPX Protokollstacks, installiert werden. Zusätzlich wird noch die Installation von *NetBIOS over NWLink* empfohlen, um die Server direkt mit ihren Computername ansprechen zu können.

Die Gateway-Services für Novell benötigen auf jeden Fall das NWLink Protokoll, auch wenn der NetWare Server mit Hilfe von TCP/IP kommuniziert.

27.0.30 globaler Katalog

Im globalen Katalog sind alle Ressourcen und User des gesamten Forrest mit ihrer Domänenzugehörigkeit aufgeführt. Zugleich enthält er die Zugriffsberechtigungen der Objekte. Er stellt so etwas wie eine Index-Relation der Datenbank dar. Er ist in erster Linie dafür zuständig ein bestimmtes Objekt eindeutig lokalisieren zu können. Der erste installierte Domänencontroller ist der per Standard der Katalogserver. Es können jedoch noch weitere Domänencontroller zu Katalogservern erklärt werden.

27.0.31 GPO

Group Policy Object, Gruppenrichtlinienobjekt

27.0.32 HCL

Hardware Compatibility List

27.0.33 Hot Swap

W2K ist in der Lage mit externen, *Hot Swap* fähigen Geräten zu arbeiten. Dieses sind in der Regel externe Geräte, die dem System im laufenden

Betrieb hinzugefügt oder entfernt werden können. Werden Hot Swap Festplattenlaufwerke genutzt, sollten diese im Hot Swap Betrieb neu eingelesen werden, um sicherzustellen, daß die internen Puffer auf dem aktuellen Stand sind. Dieses erfolgt mit dem Menüpunkt `Festplatten neu einlesen` (`Rescan Disks`) in der Computerverwaltungskonsole.

27.0.34 IIS

Internet Information Server, MS- Webserver, vergleichbar mit dem *Apache* httpd Server.

27.0.35 Internet Connection Sharing (ICS)

Als *Internet Connection Sharing* wird die Möglichkeit bezeichnet, ein an einem lokalen Rechner angeschlossenes Modem (oder ISDN-Karte) im Netzwerk anderen Rechnern zur Verfügung zu stellen.

27.0.36 IP-Adresszuweisung

Falls der Rechner keine IP-Adresse zugewiesen bekommen hat, stellt er selbstständig eine Adresse im Adressraum `169.254.xxx.xxx` ein.

27.0.37 IPSec

Zur Sicherung der Datenauthentizität (Erkennen von Änderungen, Verhindern von Änderungen) auf dem Transportweg, sowie zur Verschlüsselung von Daten auf dem Transportweg bietet sich die Nutzung von IPSec an. IPSec sitzt auf der IP-Schicht des Protokollstapels und arbeitet für die darüberliegenden Protokollschichten vollkommen transparent. Zur Nutzung von IPSec müssen die darüberliegenden Anwendungen also nicht speziell angepaßt werden (wie dieses z.B. bei SSL notwendig ist).

Mit Hilfe von IPSec kann ein gesicherter Tunnel zwischen zwei Rechnern aufgebaut werden. Hier können sich die an der Übertragung beteiligten Partner gegenseitig authentifizieren (AH Authentication Header). Die Verbindung kann darüber hinaus die Authentizität der übermittelten Datenpakete gewährleisten, und bietet eine Verschlüsselung der Daten auf dem Übertragungsweg an (EPS Encapsulating Security Payloads).

Die Konfiguration eines sicheren Tunnels kann auf zwei verschiedene Arten durchgeführt werden.

L2TP/IPSec

Das *Layer Two Tunneling Protocol* ist wie der Name schon sagt auf der zweiten Netzwerkschicht ansetzendes Protokoll zum Aufbau einer Punkt-zu-Punkt Verbindung über ein Netzwerk. L2TP ist in RFC 2661 beschrieben

und geht auf letztendlich auf ein Protokoll der Firma Cisco zurück. Die Verschlüsselung der Daten erfolgt hier mittels IPSec.

Liegt auf der Verbindungsschicht und kann daher unterhalb beliebiger Transportprotokollen wie IP oder Frame Relay genutzt werden. Die einzige Voraussetzung für den Einsatz von L2TP ist daß die in den Schichten unterhalb von L2TP liegenden Protokolle paketorientierten Punkt-zu-Punkt-Netzwerkverkehr ermöglichen. Hierfür müssen entweder spezielle Router eingesetzt werden, die zu L2TP kompatibel sind, oder es muß eine Einwahlverbindung aufgebaut werden.(?) L2TP bietet selbst eine optionale Header-Komprimierung an.

Beim Aufbau eines VPN mit L2TP/IPSec wird der Tunnel direkt zwischen den beiden Endpunkten der Kommunikation aufgebaut, so daß an dieser Stelle auch eine Benutzerauthentifizierung erfolgen kann.

IPSec Tunnelmodus

Im IPSec Tunnelmodus wird eine Punkt-zu-Punkt Verbindung auf IP-Ebene aufgebaut. Hier werden die Daten mit Hilfe von ESP (Encapsulated Security Payloads) verschlüsselt. Ein IPSec- Tunnel kann zwischen zwei beliebigen Servermaschinen aufgebaut werden und hier an bestimmte TCP- Ports gebunden werden. Somit läßt sich ein transparenter VPN Tunnel über ein unsicheres Netzwerk aufbauen.

Der IPSec Tunnelmodus ermöglicht eine Authentifizierung der beiden an der Kommunikation beteiligten Rechner an. Eine gegenseitige Authentifizierung der Benutzer ist hier nicht möglich.

27.0.38 Kerberos

Von Windows 2000 per default genutztes Authentifizierungsprotokoll im Netzwerk. Der Kerberos Authentifizierungsmechanismus arbeitet mit *verschlüsselten* Sitztungsschlüsseln, mit deren Hilfe sich der jeweilige Client gegenüber dem einzelnen Serverdienst authentifiziert. Zwischen Client und Server wird ein sogenanntes Schlüsselverteilungscenter (Key Distribution Center KDC) installiert, welches einen *verschlüsselten* Schlüssel für die jeweilige Sitzung erstellt und dem Client und Server gleichermaßen vertrauen.

27.0.39 KDC (Key Distribution Center)

Ein *KDC* ist ein Schlüsselverteilungscenter für die Kerberos-Authentifizierung. Von diesem wird das Sitzungsticket ausgestellt. Unter W2K dient der Domänencontroller als KDC.

27.0.40 LDAP

Lightweight Directory Access Protocol

27.0.41 LPD

Line Printer Daemon
Druckservice auf UN*X Systemen.

27.0.42 MTBF

Mean Time Between Failure, durchschnittliche Betriebszeit (in h) bis ein Gerät ausfällt.

27.0.43 NAT

Die Technik des *Network Address Translation (NAT)* bietet die Möglichkeit, die IP-Adressen eines Teilnetzes auf einer einzigen anderen IP-Adresse abzubilden. Hiermit läßt sich z.B. ein privates Netzwerk an das Internet anschließen, wobei die Rechner im privaten Netzwerk mit IP-Adressen aus den privaten Adressbereichen arbeiten können. NAT funktioniert so, daß die Kombinationen interne IP-Adresse / Sendeport auf einem Port des NAT-Rechners abgebildet werden, der dann eine Verbindung mit dem entfernten Host aufnimmt. Ein NAT-Rechner wird auch als transparenter Proxy bezeichnet. (?)

NAT kann als *Dynamic NAT* arbeiten, bei der eine *n:1* Zuordnung zwischen den privaten IP-Adressen (n) und der offizell zugeteilten IP-Adresse (1) erfolgt. Gleichfalls kann eine *n:m* Zuordnung erfolgen (*Static NAT*), bei der die Adressen des internen Netzes auf mehreren offiziellen Adressen abgebildet werden.

27.0.44 NWLink

NWLink muß auf den Clients für die Nutzung von Novell-Diensten in MS-Netzwerken installiert werden. Nwlink unterstützt Schnittstellen zu Socket und zu NetBIOS. Hier werden die Systemaufrufe von Windows in entsprechende Aufrufe der Novell Netzwerk API umgesetzt.

Für die Nutzung in IPX-Netzwerken muß noch das IPX-Protokoll installiert werden und an die Netzwerkkarte gebunden werden.

27.0.45 organisatorische Einheiten

Die Domänenstruktur kann zusätzlich mit Hilfe von organisatorischen Einheiten unterteilt werden. Die Strukturierung sollte möglichst die Firmenstruktur abbilden. Hierdurch wird die Domänenstruktur für den User vollkommen transparent.

Innerhalb der einzelnen OU können die Ressourcen abgebildet werden.

27.0.46 OS

Operating System (Betriebsystem)

27.0.47 OSPF

Das *Open Shortest Path First (OSPF)* Protokoll ist eines der Protokolle, die das dynamische Routing unter IP ermöglichen (s.a. 27.0.54). Hier tauscht der jeweilige Router mit benachbarten Routern Informationen über den Status seiner Verbindungen zu anderen Netzen aus. Sobald sich die Routen eines Routers ändern, werden diese Informationen an die benachbarten Router weitergegeben. Dieses Protokoll ist also gut geeignet, wenn die Routingtabellen in kleineren Netzen mit möglichst geringer Verzögerung aktualisert werden sollen, wie es z.B. bei einem Router mit einer Dial-up Verbindung notwendig ist. Für Dial-on-Demand Verbindungen wird das OSPF Protokoll unter W2K allerdings nur unterstützt, wenn diese Verbindungen persistent gehalten werden, also immer nur eine Verbindung zum gleichen Subnetz aufgebaut wird. Das OSFP-Protokoll ist im *RFC 2328* beschrieben. Es ist vor allem zum Einsatz in großen Netzwerken geeignet.

27.0.48 PPTP

Das *Point-to-Point Tunneling Protocol* bietet die Möglichkeit der Verschlüsselung einer Verbindung auf der PPP-Ebene. Es setzt im Gegensatz zu L2TP (siehe auch 27.0.36) IP als Netzwerkprotkoll voraus und bietet keinerlei Möglichkeit der gegenseitigen Authentifizierung. PPTP bietet die Möglichkeit, einen Tunnel zu Maschinen aufzubauen, die temporär per NAT an das Netz angeschlossen sind.

Falls eine VPN- Verbindung (s. 27.0.68) Router passieren soll, die kein *L2TP* unterstützen, oder ein verschlüsselter Kanal zu Rechnern mit Windows NT 4.0 oder Windows 98 aufgebaut werden soll ist die Nutzung von PPTP zwingend erforderlich. Die älteren Microsoft Betriebssysteme unterstützen kein IPSec.

27.0.49 Principalname

Der *Pricipalname* (Prinzipalname) ist volle Name eines Users in Form einer SMTP Adresse, wie z.B. `adminstrator@bog.local`.

27.0.50 PXE

Pre Boot Execution Environment z. Booten über das Netzwerk

27.0.51 PWS

Peer Web Server, Webserver für kleiner Intranets

27.0.52 Quotas

Mit Hilfe der Disk-Quotas läßt sich die maximal zu speichernde Datenmenge *pro Benutzer* und *pro Volume(?)/Partition* einstellen. Zu beachten ist hier, daß zur Berechnung der Quotas die *unkomprimierte* Größe einer Datei herangezogen wird. Eine Komprimierung auf Filesystemebene ermöglicht also keine größere zu speichernde Datenmenge (s.a. 4.2.1). Ebenso werden die Dateien des Benutzers im "Papierkorb" (Recycle Bin) mit zur Berechnung herangezogen, so daß bei Überschreiten der Quotas zuerst einmal der Papierkorb geleert werden sollte.

27.0.53 RDP

Remote Desktop Protocol

27.0.54 RIP

Das *Routing Information Protocol (RIP)* ist ein Protokoll um das dynamische Routing zu ermöglichen. Hier sendet jeder RIP- Router in regelmäßigen Abständen (30 Sekunden, eventuell auch wenn eine Änderung vorliegt), Informationen darüber welche Netzwerke über ihn erreichbar sind, an andere Router. Mit Hilfe dieser Technik wird ein relaiv zuverlässiges Routing ermöglicht, da die Informationen vor allen in kleinen Netzen ziemlich schnell im ganzen Netz aktualisiert werden. RIP liegt in zwei Versionen vor, die sich u.a. in der Technik des Informationsaustausches unterscheiden. RIPv1 arbeitet zur Weitergabe seiner Routing-Informationen mit Broadcasts, was in größeren Netzen eine nicht unerhebliche Netzlast erzeugt, hier also nicht unbedingt geeignet ist. RIPv2 dagegen spricht die anderen Router direkt per Mulitcast an. Allerdings wird bei größeren Netzen auch hier eine gewisse Netzlast erzeugt, da eine größere Anzahl von Routern erreicht werden muß.

Die RIP Protokolle sind vor allem in kleineren Netzen und für nicht persistente Dial-Up Verbindungen gut geeignet, da die Informationen gezielt ausgetauscht werden. RIP sollte nicht eingesetzt werden, wenn die Routingeinträge möglichst zeitnah aktuell gehalten werden müssen, da die Informationen eine gewisse Zeit benötigen, bis sie repliziert werden.

27.0.55 RPC

Remote Procedure Call

27.0.56 SACL

Die *System Access Control List* gibt an, welche Zugriffe auf das zugehörige Objekt überwacht werden sollen.
Sihe auch ACL 27.0.5

27.0.57 samAccountName

Der *samAccountName* ist der Benuzteranmeldename, wie er unter Windows NT 3.5x/4.0 genutzt wurde. Es ist also der UPN (s.a. 27.0.64) *ohne* das Suffix nach dem "@"

27.0.58 SID

Security Identifier
Ein Security Identifier ist eine interne Kennung für ein Objket (z.B. Benutzer, Gruppe, ...). Er kennzeichnet ein Objekt eindeutig. Wird das zuehörige Objekt gelöscht, wird auch der SID unwiederruflich entfernt.

27.0.59 SMB

Server Message Block

27.0.60 SMS

System Management Server

27.0.61 start (interner Befehl)

Der interne Befehl `start` startet ein Programm in einem neuen Fenster. Für dieses Programm kann z.B. der Titel oder die Prozeßpriorität (z.B.: /NORMAL, /HIGH, /REALTIME) eingestellt werden. Der Befehl wird häufig in Batch-Scripten benutzt, um ein Programm im Hintergrund auszführen, so daß nicht auf die Beendigung des Programmes gewartet werden soll.

27.0.62 UNC

Universal Naming Convention

27.0.63 URL

Uniform Ressource Locator (z.B. http://www.servername.com)

27.0.64 UPN (userPrincipalName)

Der *User Principal Name* (UPN) ist der Anmeldename, der für die Anmeldung am Windows 2000 Netzwerk verwendet werden kann. Ein UPN besteht aus einem Präfix und einem Suffix, die durch das @ Symbol getrennt werden. Das Präfix ist der Benutzername während das Suffix die Stammdomäne dieses Benutzers ist (Bsp.: foo@bar.baz.com). Die Anmeldung kann nun erfolgen, ohne daß im entsprechenden Feld eine Domäne angegeben wird. Bei Eingabe eines "@" im Feld "Benutzername" des Anmeldefensters wird das

Feld “Domäne” automatisch abgeblendet und für Eingaben gesperrt. Der UPN ist im gesamten AD eindeutig; er ändert sich nicht wenn ein Benutzerkonto in eine andere Domäne verschoben wird. Aufgrund des speziellen Formates kann sich ein User mit seiner Email-Adresse am Netzwerk anmelden.

27.0.65 userAccountControl

Mitm dem userAccountControl werden die Eigenschaften eines Benutzerkontos eingestellt. Für den Import einer ASCII-Datei mit Einstellungen wird hier z.B. der Wert *512* für ein aktiviertes Konto, *514* für ein deaktiviertes Konto eingestellt.

27.0.66 Verwaltungsprogramme

Um auf einer W2K Workstation die Verwaltung der Domäne durchführen zu können werden hier die Verwaltungsprogramme (Start/Programme/Verwaltung) benötigt. Diese Programme werden von der Installations-CD von `I386/Adminpak.msi` installiert.

27.0.67 Vertrauensstellungen!transitive

Die Domänenstruktur unter W2K sieht `transitive` Vertrauensstellungen vor. Transitive Vertrauensstellungen gelten implizit (oder indirekt) zwischen einzelnen Domäenen, so daß alle Domänen in einer Struktur einander vertrauen, ohne daß explizit für jedes Paar eine Vertrauensstellung eingerichtet werden muß.

27.0.68 Virtual Private Network (VPN)

Ein *Virtal Private Network* ist eine verschlüsselte Verbindung zwischen zwei Hosts oder Netzwerken über einen unsicheren Kanal, wie z.B. das Internet. Unter W2K wird der verschlüsselte Tunnel mit den Protokoll PPTP (Point to Point Tunnelin Protocol) oder mit L2TP (Layer Two Tunneling Protocol) aufgebaut. Diese Protokolle werden automatisch installiert, falls bei der Installation von RRAS VPN-Ports erstellt werden sollen.

27.0.69 Windows Update

Mit Hilfe der Website von *Windows Update* kann das System dahingehend überprüft werden, ob Treiber, aktuelle Patches oder andere Komponenten aktualisiert werden sollten.

27.0.70 WINS

Windows Internet Naming Service
Wins ordnet IP-Adressen NetBIOS Namen zu.

27.0.71 WINS-Proxy

Ein Wins-Proxy wird für Clients benötigt, die ihre Namensauflösung nicht über einen Wins-Server durchführen können. Dieses sind Clients, die die Namensauflösung *nur* über einen Broadcast durchführen können.