Windows 2000 Professional

Prüfungsvorbereitung für MCSE 70-210.

Christian Zahler

Verweise beziehen sich auf die MCSE-Prüfungsvorbereitung 70-210 (Professional) bzw. 70-215 (Server) (grüner Einband).

1 Einführung in Windows 2000

Windows 2000-Produktpalette

- MS Windows 2000 *Professional*
- MS Windows 2000 *Server*
- MS Windows 2000 *Advanced Server*
- MS Windows 2000 *Datacenter Server* (64 Bit-System)

Zusätzlich zur bestehenden Produktpalette wird geplant:

- MS Windows 2000 *Application Center*: für Objekte bei Geschäftsvorgänge (COM, DCOM) – Lastverteilung über mehrere Rechner möglich (Beispiel: Webserver mit mehreren IP-Adressen) Der *Application Server* ist ein gesondertes Server-Produkt.

  COM = *Component Object Model*: fertige Komponenten; neue Software besteht oft nur mehr aus Visual Basic-Scripts, die auf fertige Komponenten zugreifen. Das ganze Betriebssystem Windows 2000 ist sehr stark komponentenorientiert ausgeführt.

  Achtung: Lastverteilung ist nicht gleich *Clustering*!

  Clustering = mehrere physische Rechner als einen logischen ansprechen

  Windows Server: Active Directory, Domainen, ...

  Es handelt sich immer um dasselbe System, das allerdings unterschiedlich konfiguriert ist.

Neuigkeiten

- leichtere Installation von Produkten auf Workstations über das *Active Directory* und zentrale Profilverfaltung (*IntelliMirror*)
- weniger Verwaltungsaufwand: bessere Verwaltungstools (*Microsoft Management Console* MMC)
- Skalierbarkeit: Windows 2000 *Professional* kann 2 Prozessoren verwalten, Windows 2000 *Server* unterstützt 4 CPU's und 4 GB Hauptspeicher, *Advanced Server* 8 CPU's und 8 GB Hauptspeicher und der *Datacenter Server* bis zu 32 CPU's und 64GB Hauptspeicher.
- Klonen von Maschinen von NT 4: Sehr problematisch!
- SID (*Security ID*) Changer notwendig! (Public Domain)
- HAL = *Hardware Abstraction Layer* („Treiber" fürs Motherboard, eine DLL, die die gesamte Funktionalität des Motherboards umfasst).
- Bei Windows 2000 ist mit dem *Remote Installation Service* (RIS) ein Werkzeug zur Installation von Clients enthalten. Ein Clone-Prozess durch Kopieren von Festplatten ist damit nicht mehr notwendig.

Hardwareunterstützung

- Plug & Play
- USB-Unterstützung (erst ab NT 4 SP 6a)
- WDM (*Windows Driver Model*)-Treiber-Unterstützung
- Notebooks
- symmetrisches Multiprocessing (Praxis: 2 CPUs auf einer Workstation)
- symmetrisches Multiprocessing: 2 Prozessoren teilen sich die Aufgaben und den RAM
- asymmetrisches Multiprocessing: Prozessoren für Spezialaufgaben zuständig (eine CPU verwaltet DB-Server, eine andere Massenspeichergeräte usw)

Dateisysteme

- FAT16
- FAT32 (seit Win95B)
- NTFS (verbessert – dynamische Erweiterung von Partitionen möglich)

Datenträger-Bereitstellungspunkte: Ein scheinbares Unterverzeichnis wird einer physischen Festplatte zugeordnet.

Sicherheitsfunktionen von Windows 2000

- **Kerberos 5**: am MIT entwickelt, inzwischen exportfähig, bei UNIX seit vielen Jahren als Standard etabliert.
- **EFS** (*Encrypting File System*): verschlüsseltes Dateisystem
- **IPSec** (*Internet Protocol Security*): Verschlüsselung von IP-Paketen

Netzwerktechnologien

- **Windows 2000-Arbeitsgruppen:** Benutzer muss auf jedem Rechner, auf den er zugreifen will, ein Benutzerkonto besitzen. Funktioniert mit Windows 2000 Professional oder besser.
- **Windows 2000-Domänen:** Benutzeranmeldung von Domänencontroller. Funktioniert mit Windows 2000 Server oder besser.

  Bisher (NT 4): PDC, BDC (wird auch von Win 2000 im Standardmodus = Kompatibilitätsmodus zu Windows NT 4 unterstützt, notwendig, wenn NT4 und W2000 gemischt im Netz eingesetzt werden)

  Neu (W2000): lauter gleichberechtigte DC (Domänencontroller)

2 Windows 2000-Installation

Hardware-Anforderungen

- Pentium CPU
- 32 MB Minimum, 128 MB realistisch
- Festplattenkapazität: 650 MB mindestens, realistisch für eine Systempartition als absolutes Minimum 2 GB (allein die Auslagerungsdatei hat mehrere 100 MB)
- Netzwerkkarte (es geht auch ohne)
- Grafikkarte: VGA minimal, 800 x 600 pixel empfohlen
- CD-ROM-Laufwerk empfohlen, 12fach oder schneller (alte CD-ROM-Laufwerke abhängen!)
- Diskettenlaufwerk für die Installation eines Minimal-Betriebssystem (DOS etc)
- Tastatur, Maus

  HCL = *Hardware Compatibility List* (was wird an Hardware unterstützt)

  Beschränkung für Erstpartition (4 GB – Win NT) ist gefallen.

  Empfehlenswert: eigene Systempartition, Datenpartition

Auswahl des Dateisystems für die Systempartition

- NTFS (empfohlen wegen Sicherheitseinstellung)
- FAT16 (2 GB max. Partitionsgröße, Vorteil: mit DOS-Diskette kann auf diese Partition zugegriffen werden)
- FAT32 (mehr als 2 GB Partitionsgröße, mit DOS-Diskette ist kein Zugriff möglich, mit Win98-Diskette schon)

Lizenzierung für Windows 2000-Netzwerk

- Windows 2000 Professional (oder anderes Client-Betriebssystem wie Windows 98)
- CAL = *Client Access License* für Zugriff auf W2000-Server (Achtung: Extra-Produkt!)

Lizenzierung

- pro Server: mit dem Server werden z.B. 25 CALs miterworben (für kleinere Unternehmen günstiger)
- pro Arbeitsplatz: pro Client wird eine CAL mitgekauft (mit diesen Lizenzen kann ein Arbeitsplatz auf beliebig viele Server zugegriffen werden; für größere Unternehmen mit mehr als drei Servern empfehlenswert)

  Bei der Installation kann eine Maschine zu einer bestehenden W2K-Domäne hinzugefügt werden. (Hier würde der Domänen-Administrator automatisch Administratorrechte auf dieser Maschine erhalten.)

Installation von CD-ROM

PC mit eingelegter Windows 2000-Professional-CD starten; falls noch keine Partition angelegt ist, startet das Setup-Programm, falls nicht, wird gefragt, ob von CD oder von Festplatte gebootet werden soll.

Motherboards mit El Torito-System unterstützen bootfähige CD-ROMs.

ACPI (*Advanced Configuration and Power Interface*)

BX-Chipsatz (steht unten auf dem Startmonitor)

1. Teil: Textbasierte Installation
Zunächst werden Hardwarekomponenten durchsucht und eine Minimalversion von Windows 2000 geladen.

R-Taste ... Reparaturinstallation

Enter-Taste ... Installieren

Lizenzvertrag bestätigen

Systempartition erstellen, formatieren mit NTFS/FAT

Dateien werden in einen temporären Installationsordner kopiert, dann wird der PC neu gestartet.

2. Teil: Setup-Assistent startet im Grafikmodus
Minimalkonfiguration des grafischen Teils des Betriebssystems wird geladen.

Gebietsschema wird festgelegt (für System und Benutzer getrennt möglich!)

Betriebssysteminstern wird mit dem 16 bit-UTF8-Zeichensatz („UNICODE“) gearbeitet, während Applikationen oft noch mit 8 bit-ISO-Zeichensätzen arbeiten.

Tastaturlayout

- Deutsch – DIN – Dauerumschalttaste (alle Zeichen mit Zweitbelegung)
- Deutsch (IBM) – CapsLock-Taste (alle Buchstaben groß, Zahlen normal)

Computernamen (NetBIOS-Name) angeben

Administratorkennwort vergeben

Namensdienste

- WINS (LMHOSTS) – Auflösung der Windows-NetBIOS-Namens durch Broadcasts (für ältere Maschinen nötig)
- DNS – Auflösung der Namen internetmäßig

Netzwerkkonfiguration

TCP/IP-Protokoll
Standardmäßig wird versucht, dem PC eine gültige IP-Adresse zuzuweisen (problematisch!!!) – entweder von einem DHCP-Server bezogen oder aus einem gültigen Bereich für lokale IP-Adressen.

Nachher muss angegeben werden, ob der PC nicht im Netzwerk/in einer Arbeitsgruppe oder Mitglied einer Domäne werden soll.

Unbeaufsichtigte Installation (*Unattended Setup*)

- Antwort-Datei (Textdatei) **`UNATTEND.TXT`**
- UDF
- DOS-Diskette mit FDISK

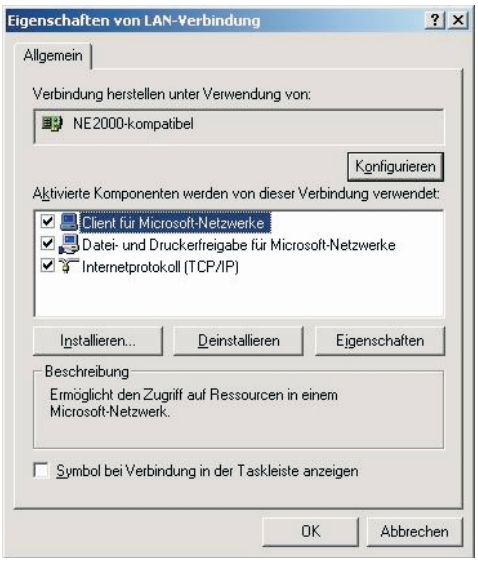
Viele *Real Mode* DOS-Treiber funktionieren nur mit einer Windows 95-Bootdiskette (d.h. DOS 7.0).

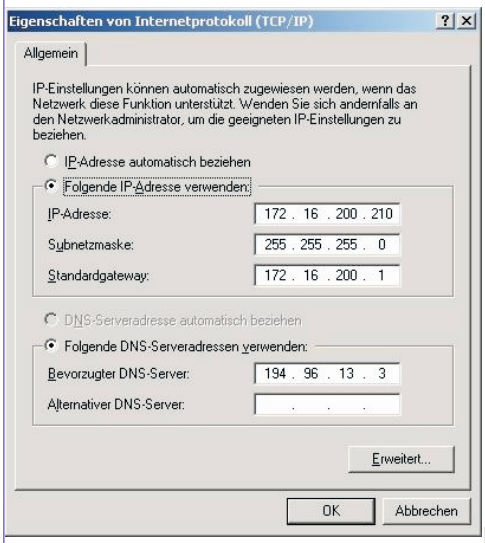
Installation/Update von einem bestehenden Betriebssystem aus
`WINNT.EXE` (Installation von Win 95 aus)

`WINNT32.EXE` (Installation von Win NT 4.0/2000 aus)

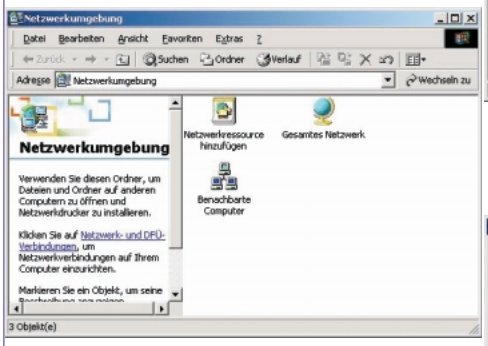
Verknüpfung anlegen, eingeben als Parameter **`/?`**

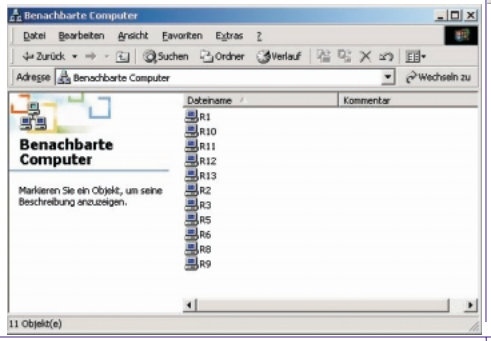
Konfiguration der Windows 2000-Professional Maschine





Eigenschaften von TCP/IP
Mit einem Doppelklick auf die Netzwerkumgebung können “***Benachbarte Computer***” (d.h. die Arbeitsgruppe) angezeigt. Ein Doppelklick auf “***Gesamtes Netzwerk***” bringt auch andere Domänen und Netware-Server zum Vorschein.





3 Microsoft Management Konsole (MMC)

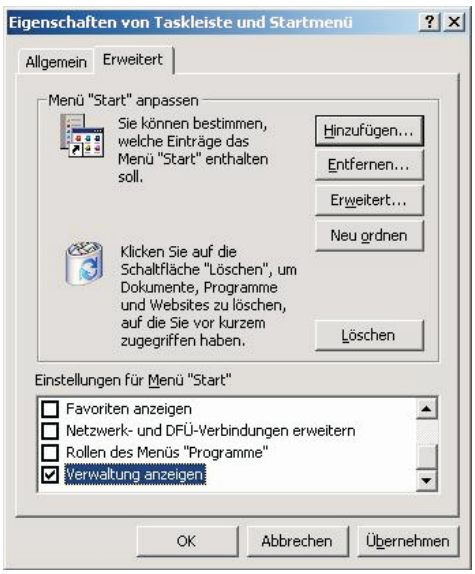
Das wesentliche Werkzeug zur Verwaltung des eigenen, aber auch von entfernten Rechnern, ist die MMC.

Früher: viele Tools (Festplatten-Manager, Benutzerverwaltung, ...)

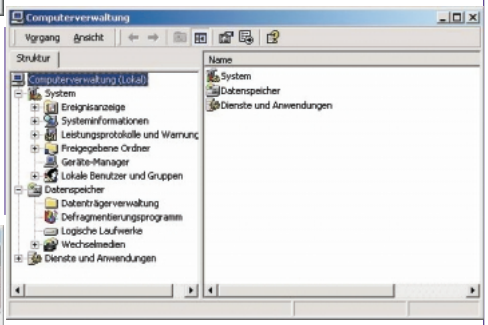
Heute: MMC als Rahmenprogramm, Snap-Ins für spezielle Funktionen.

Konfigurieren der MMC
Wenn einmal eine Konsole gespeichert wurde, wird im Menü “Start”- Programme die Verwaltungsprogrammgruppe aktiviert.

Man kann diese Gruppe auch händisch aktivieren, indem man die Eigenschaften der Taskleiste öffnet:

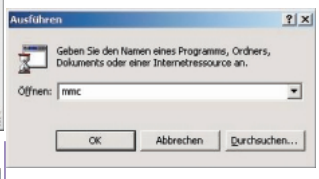


Es gibt eine Reihe vordefinierter Konsolen, etwa die Computerverwaltung:



Man kann allerdings auch selbst Konsolen definieren; das funktioniert so:

Start - Ausführen



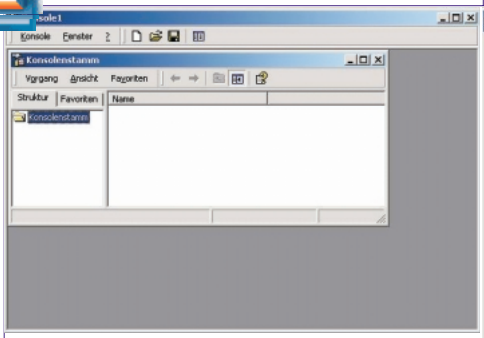
Die Microsoft Management Konsole startet im Autorenmodus:

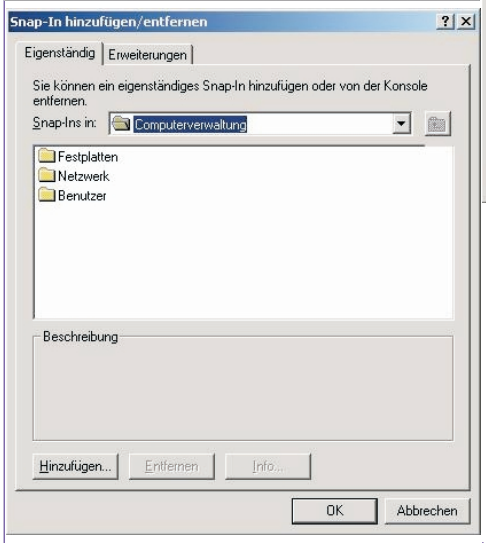
Durch “***Speichern unter***” kann der Konsole ein Name gegeben werden, etwa “Testkonsole”.

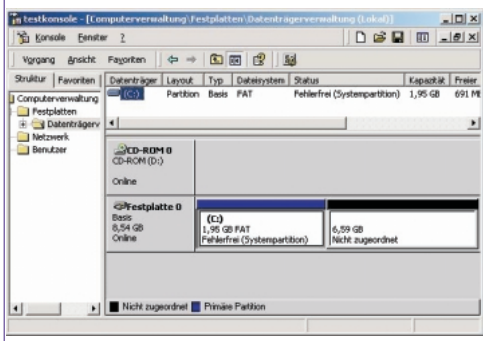
Umbenennen des Konsolenstamms.

Man kann nun eigenständige Snap-Ins hinzufügen: ***[Datei]-[Snap-In hinzufügen]***

Um eine Gliederung zu erhalten, kann das “Ordner”-Snap-In verwenden werden:



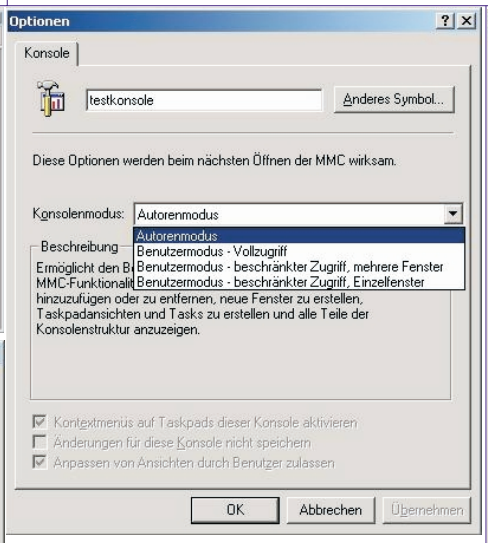




Um die fertig definierte Konsole vor Änderungen zu schützen, muss *[Konsole]-[Optionen]* aufgerufen werden und der Konsolenmodus geändert werden:

Die Konsoleneinstellungen werden standardmäßig im eigenen Profil gespeichert.

Achtung: Die Profile werden nicht mehr unter `\WINNT\Profiles` gespeichert, sondern unter `C:\Dokumente und Einstellungen\` !!!



Taskplaner

Anwendungsprogramm, das bestimmte Visual-Basic Scripts, Programme ... zu bestimmten Zeiten ausführt. (WINNT 4: `ATT`, `WINATT`)

Hardware-Profile

Ziel: Einzelne Hardwarekomponenten können gezielt aktiviert und deaktiviert werden.

In Wirklichkeit nur sinnvoll bei Notebooks: Docking-Station, fremdes Netzwerk, ohne Netzwerk

rechte Maustaste - Eigenschaften von Arbeitsplatz

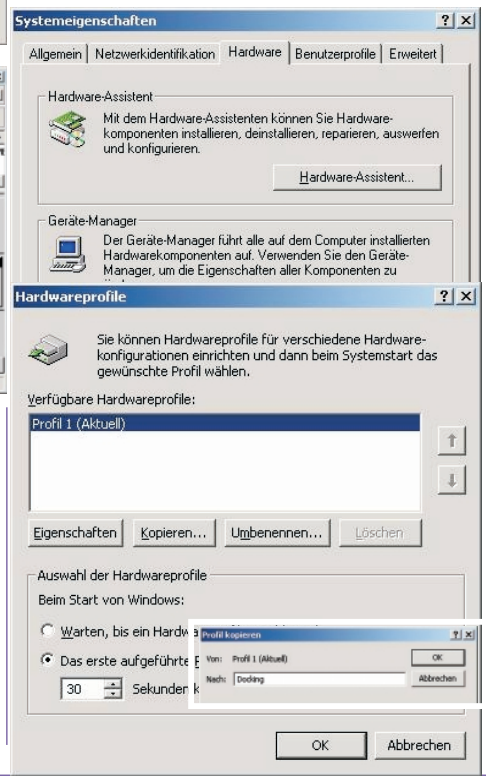
Beim Starten kann zwischen den einzelnen Profilen ausgewählt werden.

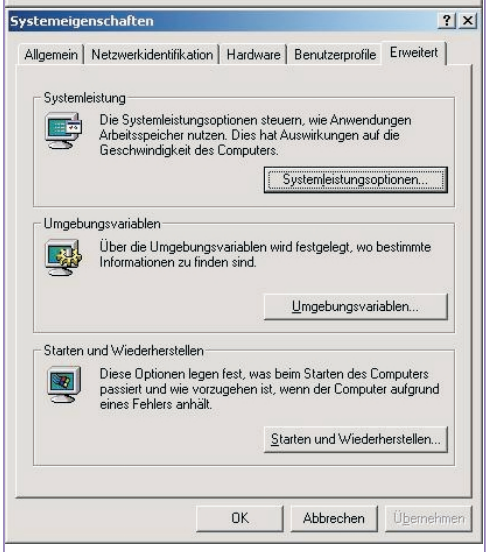
Man kann durch Kopieren Profile anlegen.

4 Die Windows-Systemsteuerung

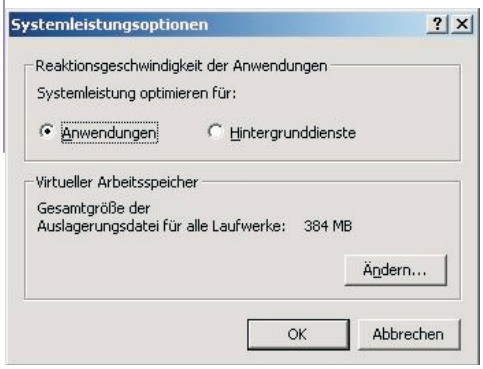
Systemeinstellungen

Rechte Maustaste auf ***Arbeitsplatz - Eigenschaften*** - Karteikarte ***"Erweitert"***, Schaltfläche ***"Systemleistungsoptionen"***



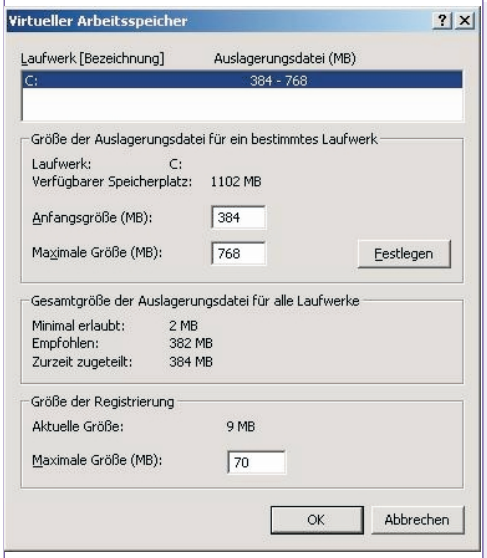


1. Systemleistungsoptionen
Durch Klick auf "Ändern" kann der virtuelle Arbeitsspeicher (d.h. Größe der Auslagerungsdatei, engl. *Swap*-Datei) geändert werden.



Empfohlene Größe der Auslagerungsdatei: etwa 1,5 x des installierten Hauptspeichers (mehr hat keinen Sinn, da sonst Performance-Verluste auftreten!).
Braucht man mehr, so ist es sinnvoller, physischen Speicherplatz zu ergänzen.

Windows NT unterstützt einen 32 Bit Adressraum, das bedeutet einen virtuellen Adressbereich von 4 GB. Jedem Programm wird ein solcher virtueller 4 GB-Adressraum zugeordnet. (Hätte man diesen Speicher auch physikalisch, so könnte das Programm diesen Speicher auch nutzen!)

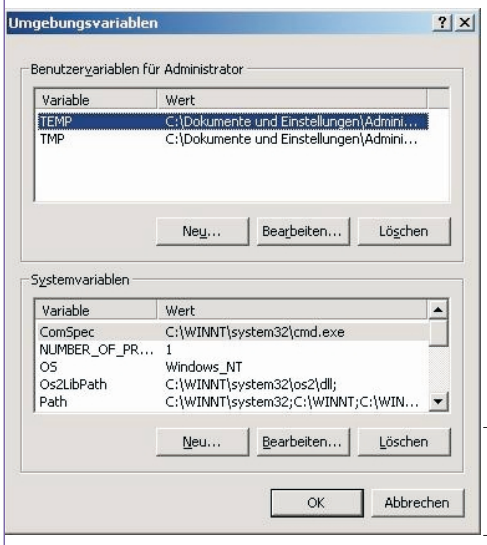


Die Zuordnung zwischen tatsächlich vorhandenem Speicher und virtuellem Speicher wird vom VMM = *Virtual Memory Manager* durchgeführt.

Ist für mehrere Programme eine Zuweisung von tatsächlichem RAM nicht mehr möglich (*Page Fault* = Seitenzuordnungsfehler), so muss ein Teilbereich aus dem RAM auf die Festplatte ausgelagert werden. Damit werden diese Daten auf die "Swap-Datei" (Auslagerungsdatei) auf die Festplatte ausgelagert. Die Auslagerung erfolgt generell in 4 kB-Blöcken.

2. Umgebungsvariablen

Altes Konzept, mit dem Programme (älteren Datums) gesteuert werden können.



Die Umgebungsvariablen können in der Kommandozeile abgefragt werden:

```
echo %ComSpec%
```

Diese Variablen können auch gesetzt werden:

```
set werbinich=Kaliba
echo %werbinich%
```

Mit

```
set
```

können alle Umgebungsvariablen ausgelesen werden:

```
C:\>set
ALLUSERSPROFILE=C:\Dokumente und
Einstellungen\All Users
APPDATA=C:\Dokumente und
Einstellungen\Administrator\Anwendungsdaten
CommonProgramFiles=C:\Programme\Gemeinsame
Dateien
COMPUTERNAME=R10
ComSpec=C:\WINNT\system32\cmd.exe
HOMEDRIVE=C:
HOMEPATH=\
LOGONSERVER=\\R10
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=C:\WINNT\system32\os2\dll;
Path=C:\WINNT\system32;C:\WINNT;C:\WINNT\sys
tem32\WBEM
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.J
SE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 7
Stepping 2, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0702
ProgramFiles=C:\Programme
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINNT
TEMP=C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp
TMP=C:\DOKUME~1\ADMINI~1\LOKALE~1\Temp
USERDOMAIN=R10
USERNAME=Administrator
USERPROFILE=C:\Dokumente und
Einstellungen\Administrator
windir=C:\WINNT
```

Mit **CMD.EXE** kann ein neuer Kommandoprozessor gestartet werden. (Entspricht dem Aufruf von **COMMAND.COM** im DOS bzw. Windows).

USB-Geräte

Wenn Windows 98-kompatible WDM-Treiber (*Windows Driver Model*) vorhanden sind, ist die Installation von USB-Geräten problemlos.

Registry

NTDETECT

- schreibt Geräteausstattung in Registry
- Konfiguration von Anwendungsprogrammen
- Favorisierte Einstellungen der Benutzer
- etc.

Auto-IP-Konfiguration verhindern mit Registry-Einstellungen: Buch S. 181

Windows 2000 kann IP-Adressen auf drei Arten erhalten:

- manuelle Konfiguration
- DCHP
- Auto-Konfiguration (Win 2000 sucht sich selbst Adressen)

5 Die Registrierung

Buch S. 127 – 144

6 Datenträgerverwaltung

Buch S. 145 – 170

7 Netzwerkprotokolle installieren und konfigurieren

ISO/OSI-7 Schicht-Modell

Schicht 1 physikalische Netzwerkkonfiguration:

- Normen von Kupfer-, Glasfaserkabeln: Kategorie 3, 5

Schicht 2

Ethernet = Übertragung von Daten-Frames, Codierung in elektrische Signale

Alternativen: ATM (*Asynchronous Transfer Mode*), FDDI (*Fiber Distributed Data Interface*), *Token Ring*, ...

MAC-Adressen (*Media Access Control*): Jede Netzwerkkarte benötigt eine eindeutige MAC-Adresse, je nach verwendetem Netzwerktyp unterscheidet man:

- Ethernet-Adressen sind 24 bit-Adressen, die weltweit eindeutig vergeben werden.
- Bei *Token Ring* und FDDI können MAC-Adressen manuell eingestellt werden (d.h. man ist selbst verantwortlich, dass diese Adressen nicht doppelt auftreten!)

Zwischen Schicht 2 und 3: ARP (*Address Resolution Protocol*) zur Auflösung von IP-Adressen in MAC-Adressen.

Schicht 3: IP (*Internet Protocol*)

- organisiert 1/2 Million Netzwerke
- nur wenige Router enthalten wirklich alle Informationen über alle Netzwerke
- Datenversand zunächst ans Ziel-Netzwerk, dann an den Einzelrechner
- IANA verteilt IP-Adressen

Class A, B, C-Netze: Für Internet

Class D-Netze:

Paketbildung an einen Empfänger: Unicast

Gruppenbildung: Multicast (z.B. *Videoconferencing*) - nicht für Internet verwendet

IP adressiert normalerweise so, dass die Anzahl der Hops (Sprünge von Router zu Router) minimal ist. Dazu wird im IP-Header eine sogenannte "Metrik" mitgeliefert, die üblicherweise der Anzahl der Hops entspricht.

Standard-Gateway: Muss im selben Netz sein!

ICMP (*Internet Control Message Protocol*): spezielle Form des IP-Protocols speziell für die Übertragung von Fehlermeldungen (z.B. "Kein Weg zum angegebenen Ziel-IP-Adresse". Dieses Protokoll kann auch "*Redirect*"-Anweisungen zurückschicken, damit ein korrigierter Routing-Eintrag in der lokalen Routing-Tabelle durchgeführt werden kann.

IGMP: Verwaltung von Multicast-Gruppen

Schicht 4: TCP (*Transfer Control Protocol*)

Beispiel für TCP: Webserver, *Real Video Server* (Quicktime verwendet das RTP = *Real Time Protocol*)

Alternatives Protokoll zu TCP: UDP (keine Zustellungsbestätigungen)

Beispiel für UDP: Freigabe von Ordnern und Dateien im LAN, DNS)

Internet I: kommerzielles Netzwerk, verwendet IPv4-Protokoll (32 bit)

Internet II: neues Netzwerk für Universitäten, verwendet IPv6-Protokoll (64 bit)

Schicht 5

- WinSock: eine Socket-Schnittstelle, die von fast allen Internet-Programmen verwendet wird. z.B. Webbrowser, Webserver, Mailserver, ...

- NetBT: NetBIOS-Dienste; z.B. *Named Pipes* für Datenbankzugriff (SQL Server) - typische Windows-Programme

Schicht 6 und 7

Anwendungen selbst (Webbrowser etc.)

Dienstprogramme zur TCP/IP-Fehlerbehandlung auf DOS-Ebene siehe eigenen Artikel.

Automatische private IP-Adressierung

- TCP/IP versucht bei der Installation, einen DHCP-Server zu finden.
- Wenn kein DHCP-Server auffindbar, dann wird eine IP-Adresse des Netzwerks 169.254.x.y mit der Subnetzmaske 255.255.0.0 zugewiesen.

Andere Protokolle

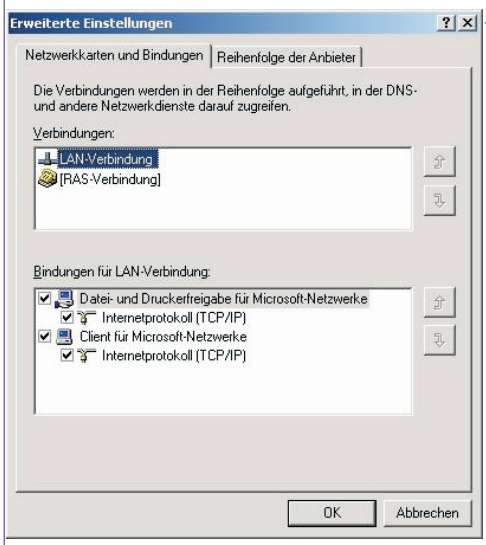
- **NetBEUI**: nicht routingfähig, kennt nur eigene Adresse
- **NWLink** (=Microsoft-Name für IPX/SPX) routingfähig, für Weitverkehrsnetze eher ungeeignet, bei Novell Netware-Anbindungen oft verwendet. "Schwester-Protokoll" von IP.

Es wird nur ein Frametyp automatisch erkannt!

Achtung: Ethernet-Frame von Novell 3.11 ist 802.3, ab 3.12 wird 802.2 verwendet! (Wenn mehrere Rahmentypen, dann müssen diese extra konfiguriert werden!)

Netzwerkbindungen

ermöglichen die Kommunikation zwischen Treibern für Netzwerkkarten, Protokollen und Diensten. "Stack" - Verbindung eines Netzwerk-Protokolls zu einem darunterliegenden Protokoll. Datei- und Druckfreigaben: funktionieren über das SMB-Protokoll (*Server Message Block*).



8 Der DNS-Dienst

www.domainforum.at

Auflösung:

- . = *Root-Domain* der obersten Ebene kennt Name-Server der Top-Level-Domänen
- Name-Server sind hierarchisch angeordner
- Zunächst wird Name Server oberster Ebene gefragt: welche IP hat **www.xyz.at**?
- Antwort: Weiß ich nicht, aber ich kenne den Name-Server für .at
- Nächste Anfrage an .at-Name Server: welche IP hat **www.xyz.at**?
- Antwort: Weiß ich nicht, aber ich kenne den Name-Server für **xyz.at**
- Dritte Anfrage an .**xyz.at**-Name Server: welche IP hat **www.xyz.at**?
- 193.122.32.27

wird zurückgeliefert, damit kann die Verbindung aufgebaut werden. Weitere Bedingungen für Domain Namen:

- In Domain Namen dürfen Groß- und Kleinbuchstaben sowie Bindestriche verwendet werden, nicht aber Sonderzeichen!
- Windows 2000 unterstützt auch UNICODE-Zeichen!
- Maximallänge von Domänennamen: 63 Zeichen
- Gesamtlänge eines *Fully Qualified Domain Name* (FQDN): 255 Zeichen

Unter Umständen kann es sinnvoll sein, mehrere *Name Server* einzurichten:

- Redundanz
- Lastverteilung

Reverse Lookup: Herausfinden des DNS-Namens zu einer IP-Adresse

Kommandozeilenprogramm **nslookup** siehe eigenen Artikel.

9 Active Directory

Verzeichnisdienst: dient zur eindeutigen Identifikation von Benutzern und Ressourcen im Netz.

Domänen: werden gesteuert von Domänencontrollern (DC)

In einer Domäne kann es mehrere gleichberechtigte DCs geben. (In der Standardinstallation wird der "NT 4-Kompatibilitätsmodus" installiert, bei dem es genau einen Primären Domänencontroller (PDC) geben darf, alle anderen werden als *Backup Domain Controller* (BDC) konfiguriert).

Die *Active Directory*-Verzeichnisdienste verwenden DNS als Namenssystem.

Active Directory arbeitet mit allen Anwendungen und Verzeichnissen zusammen, die das LDAP = *Lightweight Directory Access Protocol* unterstützen.

Folgende Standards für das Ansprechen von Benutzern und Ressourcen sind zulässig:

- UNC (NT-4-Standard): **\\server.noe.wifi.at\Projekte**
- RFC 822-kompatible Namen, *User Principal Name*: e-mail-artige Namen, z.B. **PKaliba@noe.wifi.at**
- HTTP: **http://ldap.noe.wifi.at/Users/PKaliba/**
- LDAP: **ldap://ldap.noe.wifi.at/CD=PKaliba,OU=trainer,DC=EDV**
- derzeitige Anwendung von LDAP im Internet: Abfragen von E-Mail-Adressen von Benutzern (etwa bei **www.yahoo.com** o.ä.)

Gliederung

- *Forests*, bestehen aus mehreren
- *Trees*, bestehen aus mehreren
- *Domains*, bestehen aus mehreren
- *Organisational Units* (Organisationseinheiten)
- *Scheme*: enthält formale Definition des Inhalts und der Struktur von Active Directory-Verzeichnisdiensten

Entstehung des Active Directory-Konzepts

X.500-Verzeichnisdienst (ISO-Norm)

Viele kommerzielle Anbieter versuchen sich an diese Norm anzulehnen (Win2000: *Active Directory*, Novell: *Novell Directory System* etc.)

Zusätzlich *Directory Access Protocol* (DAP)

wird auch grundlegend verwendet für den X.400-Mail-Transport (Exchange Server)

Für Win2000 wurde dieses Konzept abgespeckt: Statt X.500 wird eben Active Directory verwendet, statt des DAP ein LDAP.

Da X.400 Mail sehr umfangreiche Funktionalität bietet, wird es oft in großen Unternehmen als "Backbone E-Mail System" verwendet, da keine Spezialfeatures von E-Mail-Systemen verlorengehen (Lotus, Outlook etc.).

Active Directory-Namenskonventionen

/DC=com /DC=microsoft /ON=div /CN=benutzer /CN=Josef Maier
bedeutet:

In der Domäne **microsoft.com**, die sich u.a. aus der Organisationseinheit "**div**" zusammensetzt. In dieser **OU** ist eine Benutzergruppe "**benutzer**" angelegt, einer davon ist "**Josef Maier**". Ich kann daraus aber NICHT den Anmeldenamen oder die E-Mail-Adresse von "**Josef Maier**" feststellen.

Hinweis: LDAP- und X.400-Namen ist genauso aufgebaut wie Active Directory-Namen, allerdings verwendet LDAP Kommas statt den Schrägstrichen, X.400 verwendet Strichpunkte statt Schrägstrich.

Problematik bei Active Directory-Strukturen

- Die erste Planung muss im Wesentlichen stimmen, da eine Umorganisation praktisch nicht möglich ist.

Ansprechen von NetWare-Servern

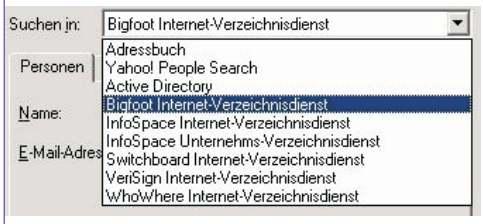
1. Installation des NWLink-Protokolls

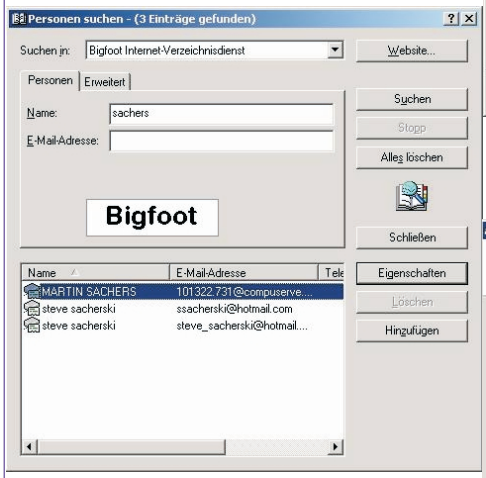
2. Installation des Client Service für NetWare

Dann ist im WIFI der WIFI-Server sichtbar:

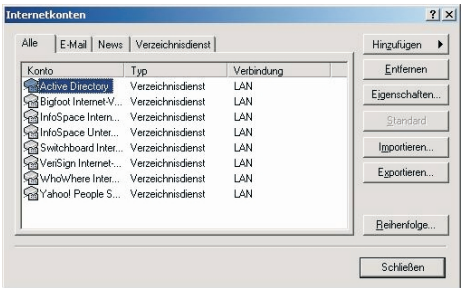
Verwendung von LDAP-Diensten über Outlook Express

[Bearbeiten]-[Suchen]-[Personen]





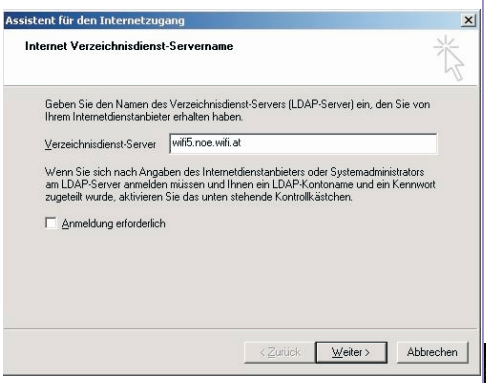
Man kann auch neue LDAP-Verbindungen zu z.B. Exchange-Servern herstellen, z.B.: ***[Extras]-[Konten]***

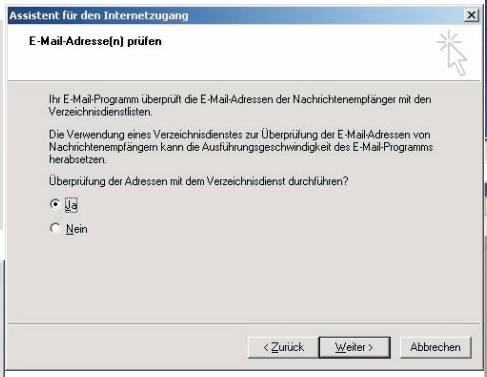


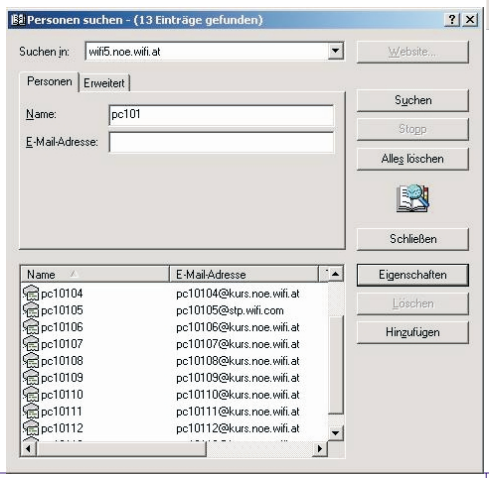
Klick auf ***Hinzufügen- [Verzeichnisdienst...]***

Der WIFI-Exchange-Server heißt **wifi5.noe.wifi.at**:

Sofort kann der hinzugefügte Verzeichnisdienst benutzt werden:







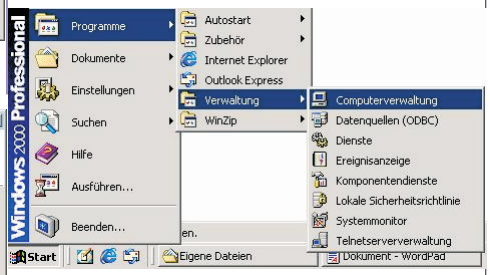
10 Benutzerkonten

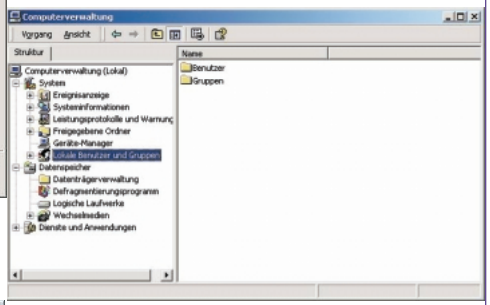
- **lokale Benutzerkonten**: liegt auf dem lokalen PC
- **Domänen-Benutzerkonten**: liegt auf DC, ist in der Domäne und allen vertrauten Domänen verfügbar

  Für jede dieser beiden Gruppen gibt es vordefinierte Konten:
- **Administrator**: kann nicht gelöscht werden, aber umbenannt
- **Gast**

Jeder DC repliziert die Benutzerinformationen auf alle anderen DC auf der Domäne.Man kann den zeitlichen Ablauf einstellen, wie die Synchronisierung erfolgen soll (etwa beim Deaktivieren von Benutzerkonten sofort, beim Neuanlegen nach 10 Minuten etc.).

Anlegen von Benutzern





Vermeiden Sie Sonderzeichen für den Benutzernamen.

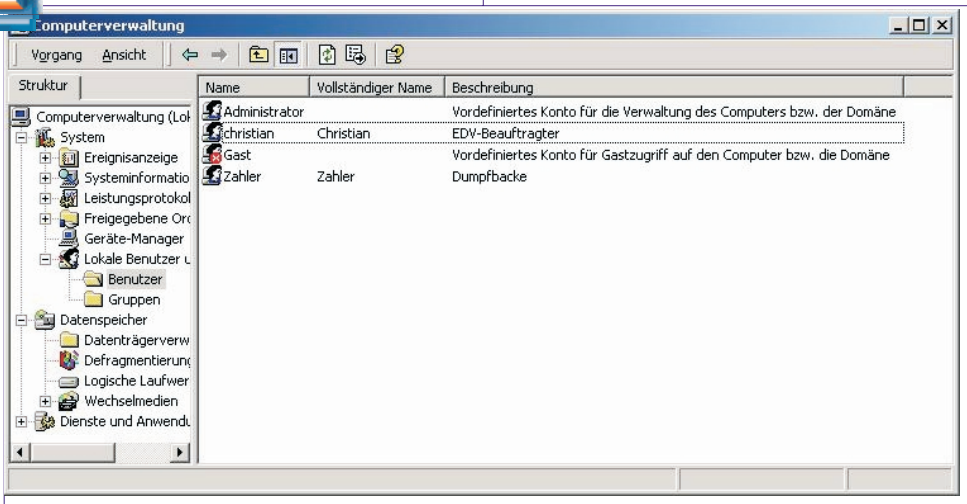
Verboten sind:

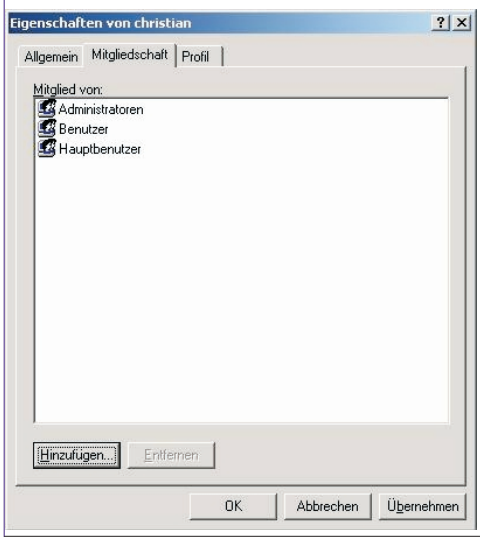
" / | \ < > ? * = [ ] : ;

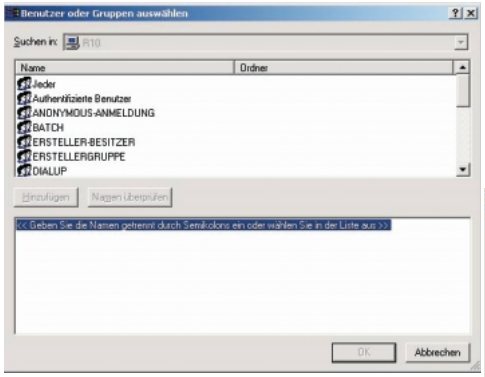
Windows 2000 verwendet nur die ersten 20 Zeichen des Benutzernamens.

Der Benutzername ist nicht case-sensitiv, beim Passwort wird allerdings Groß- und Kleinschreibung unterschieden.

Kennwörter können bis zu 128 Zeichen lang sein.







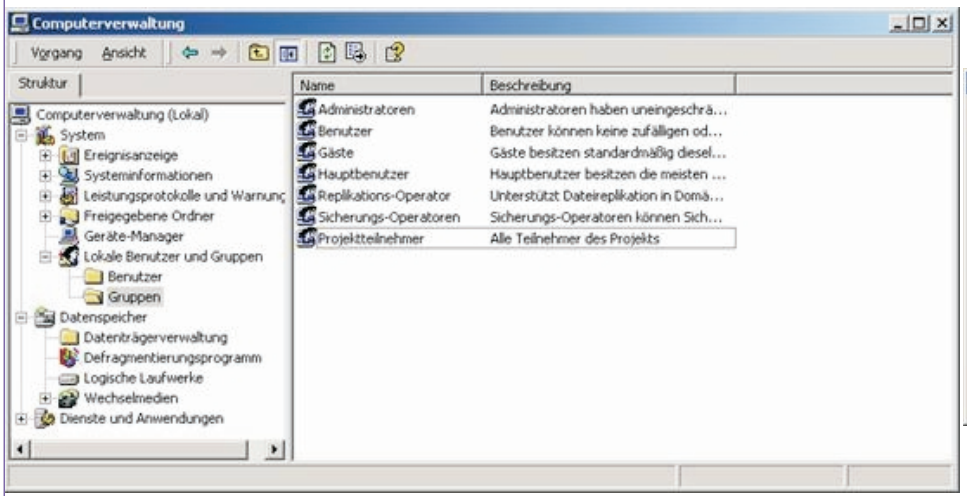
11 Gruppen

- **lokale Gruppen**: werden für den Zugriff auf lokale Ressourcen verwendet. Eine lokale Gruppe kann lokale Benutzer, Domänenbenutzer oder auch Benutzer einer fremden Domäne enthalten. Zweite Verwendung: PC, der zu keiner Domäne gehört, administrieren. Lokale Gruppen können keine Gruppen, sondern nur Benutzer aufnehmen.
- **globale Gruppen**

  Wieder gibt es vordefinierte Gruppen.
- **Jeder**

Anlegen von lokalen Gruppen

Wieder im MMC-Snap-In "Computerverwaltung". Rechtsklick auf "***Gruppen***" - ***[Neue Gruppe]***



14 Ressourcen sichern mit NTFS-Berechtigungen

Windows 2000 übernimmt ein Feature von Novell Netware:

Rechte können jetzt an Unterordner und die darin befindlichen Dateien vererbt werden.

- Zugriffsberechtigung für die Gruppe ...

  Ordner Projekte: **`Administratoren`**
- Ordner A: **`Administratoren, Mitglieder der Projektgruppe A`**
- Ordner B: **`Administratoren, Mitglieder der Projektgruppe B`**
- Ordner C: **`Administratoren, Mitglieder der Projektgruppe C`**

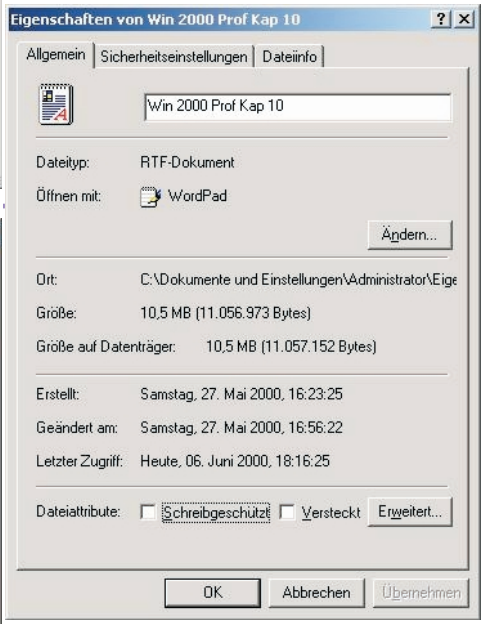
  Wenn die Gruppe "**`Geschäftsführung`**" auf die Ordner A, B und C zugreifen will, dann verliere ich die ursprünglichen Rechte der Ordner!

  Ausweg unter NT 4: Kommandozeile (Anweisung **`chgacl`**)

  Jetzt neu: Rechte vererben sich automatisch auf die Unterordner!

  Man kann allerdings diese Vererbung blockieren und die Rechte neu festlegen.

  Eigenschaften NTFS-Dateien (Kontextmenü - [***Eigenschaften***]).



Die Attribute dienen u. a. der DOS-Kompatibilität, wobei allerdings das Systemattribut nicht mehr verwendet wird. Stattdessen wurden erweiterte Attribute eingeführt, mit denen man etwa die Datei komprimieren **Oder** verschlüsseln kann.

Der Inhalt kann komprimiert werden.

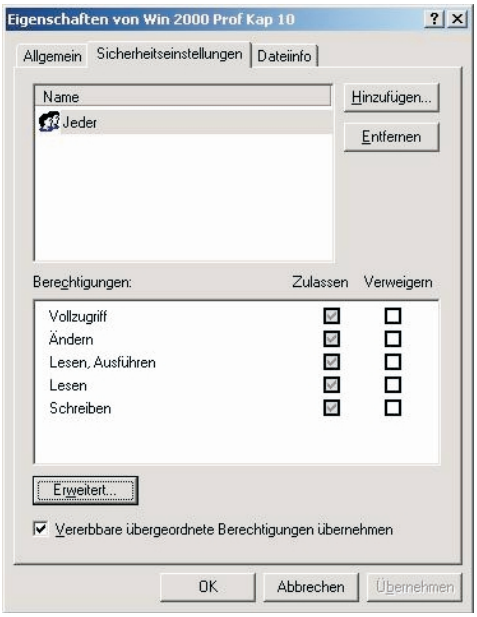
Typische Clustergrößen für 2 GB-Festplatte und darüber: 2 KB

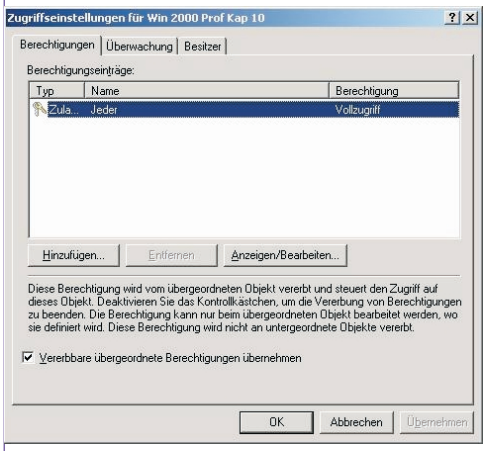
Sicherheitseinstellungen

Hier sieht man, welche Rechte vom übergeordneten Verzeichnis ererbt worden sind:

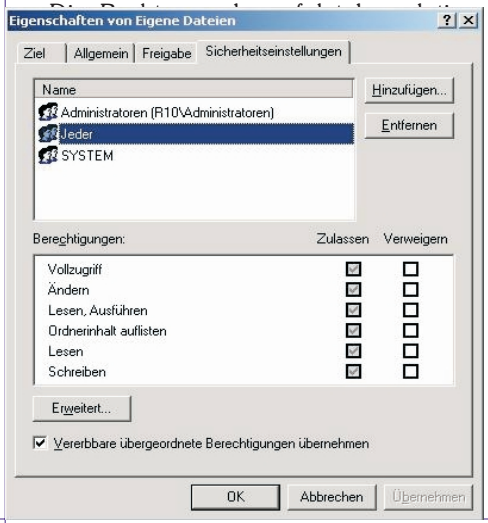
☑ Diese Rechte wurden vom übergeordneten Verzeichnis ererbt!

☑ Diese Rechte wurden im aktuellen Verzeichnis gesetzt





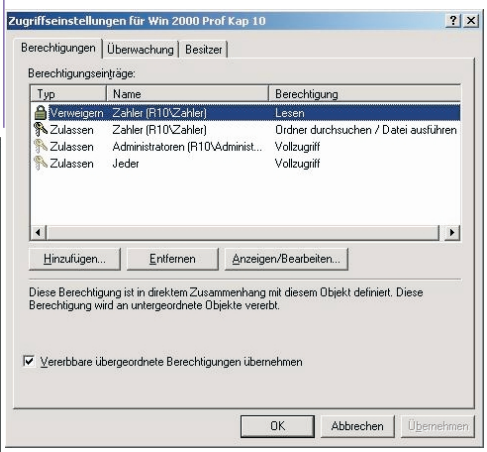
Durch Deaktivieren des Kontrollkästchens "***Vererbbare übergeordnete Berechtigungen übernehmen***" wird die Vererbungskette genau an dieser Stelle unterbrochen.



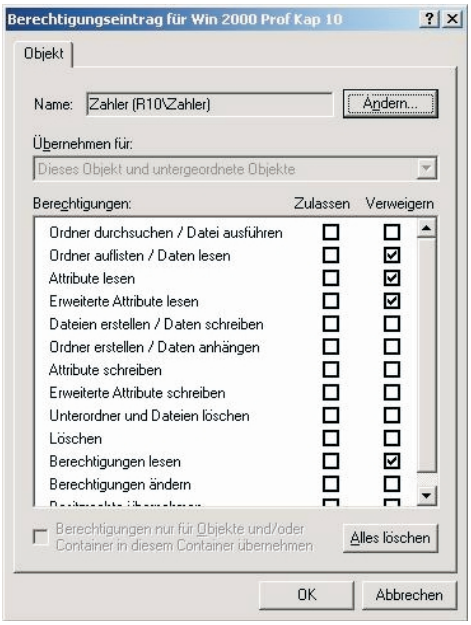
- Sicherungsoperatoren: (negatives Recht "Lesen")

Herr Meier gehört zu beiden Gruppen. Darf er auf diese Datei lesend zugreifen?

Antwort: Nein, weil das negative Recht Vorrang hat!



Mit der Schaltfläche "***Anzeigen***" können die wirklichen Rechte detailliert eingesehen werden:



Rechte kann man in Grundkategorien einteilen:

Voneinander unabhängig sind

- Lesen
- Schreiben

Voneinander abhängig sind:

- Lesen und Ausführen: beinhaltet das Leserecht
- Ändern = Lesen + Ausführen + Schreiben
- Vollzugriff = alles (inkl. Besitzrechte übernehmen, Berechtigungen ändern)

Das Recht "Besitz übernehmen" ist das "oberste Recht", da es geeignet ist, alle anderen Rechte beliebig festzulegen.

Der Besitzer hat immer das Recht, Besitz zu übernehmen.

Es ist günstig, Dateien mit gleichen Sicherheitseigenschaften im selben Ordner zu speichern!

Für die Rechtevergabe gibt es zwei stark unterschiedliche Strategien:

- Ich entziehe den Benutzern nur die Rechte, die dem System Schaden zufügen können - sehr liberale Strategie.
- Ich gebe den Benutzern nur die Rechte, die sie unbedingt benötigen - sehr strenge Strategie.

Im Wurzelverzeichnis `C:\` hat jeder Benutzer Vollzugriff! Allerdings werden die Rechte im WINNT-Verzeichnis nicht weitervererbt (d.h. die Vererbungskette ist standardmäßig unterbrochen).

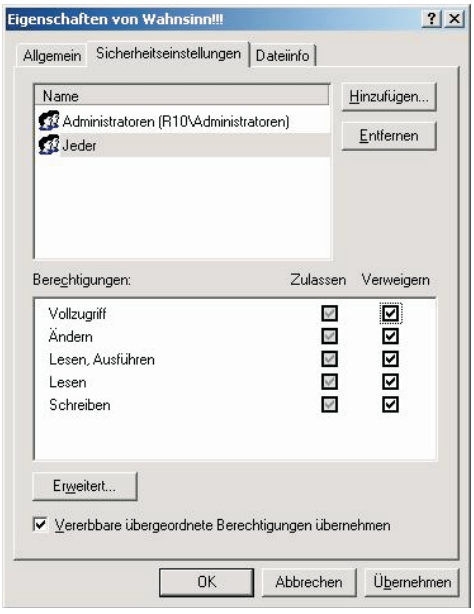
In einer neuen NTFS-Partition hat ebenfalls standardmäßig jeder Benutzer Vollzugriff!

Wenn ein Ordner auf demselben Laufwerk verschoben wird, werden die Berechtigungen "mitgenommen".

Wenn ein Ordner in ein anderes Laufwerk verschoben wird, werden die Berechtigungen nicht mitgenommen!

Beim Kopieren werden die Berechtigungen nicht mitübernommen! (Kopieren = Neuerstellen + Lesen im alten Ordner) Man erhält als vererbte Berechtigungen nur die im Zielordner.

Problem



Wenn man "**Jeder**" alle Rechte entzieht, könnte theoretisch niemand mehr (auch der Administrator nicht) keine Änderungen mehr durchführen!

Abhilfe: Der **Administrator** und die Gruppe der **Sicherungsoperatoren** haben das **Recht**, **bestehende Zugriffsrechte zu ignorieren (dies wird aber mitprotokolliert!)!**

Mit dem Recht "Ordner durchsuchen" kann man den Ordner nicht öffnen, aber eine Verknüpfung zu einer im Ordner befindlichen Datei erstellen und auf diese Datei zugreifen. Mit dem Recht "Ordner auflisten" kann der Ordnerinhalt angezeigt werden:

Beispiel: Rechte für Ordner entsprechen

(ähnlich wie bei Linux) Rechten für Dateien

Ordner durchsuchen / Datei ausführen	☑	☐
Ordner auflisten / Daten lesen	☑	☐
Attribute lesen	☑	☐
Erweiterte Attribute lesen	☑	☐
Dateien erstellen / Daten schreiben	☑	☐
Ordner erstellen / Daten anhängen	☑	☐
Attribute schreiben	☑	☐
Erweiterte Attribute schreiben	☑	☐
Unterordner und Dateien löschen	☑	☐
Löschen	☑	☐
Berechtigungen lesen	☑	☐

Also: Attribute werden für Dateien anders interpretiert wie für Ordner!

15 Freigegebene Ordner verwalten

Um Ordner, Drucker und Dateien im Netzwerk gemeinsam verwenden zu können, ist die Einrichtung von Freigaben nötig.

Berechtigungen ändern	☑	☐
Besitzrechte übernehmen	☑	☐

Freigaben dürfen von Administratoren und Hauptbenutzern durchgeführt werden (beim Server auch Server-Operatoren).

Berechtigungen für die Freigabe gelten auch für alle Unterordner und alle Dateien in der Freigabe.

Zweck der Freigaben

- Auch unter einem FAT16/FAT32-Dateisystem kann der Zugriff auf eine Ressource über das Netzwerk grob geregelt werden.
- Unter NTFS ist das Arbeiten mit Freigaben meist nicht üblich.

Freigaben wirken wie eine Art "Filter"; zunächst gelten die Freigabe-Berechtigungen, da die Datei-Sicherheitseinstellungen.

Freigabenamen mit einem $-Zeichen am Ende sind "unsichtbar". (Verknüpfungen zu diesen Freigaben können nur dann eingerichtet werden, wenn der Freigabename bekannt ist)

Vordefinierte Freigaben

ADMIN$ .... zeigt auf \WINNT - für administrative Zugriffe

PRINT$ .... für Druckeradministration; Print-Operatoren, Administratoren haben Vollzugriff

C$**, **D$, **E$** ..... Systemfreigabe für jeden Laufwerksbuchstaben

Die Freigabe ist in der Netzwerkumgebung als verbundener Ordner sichtbar:

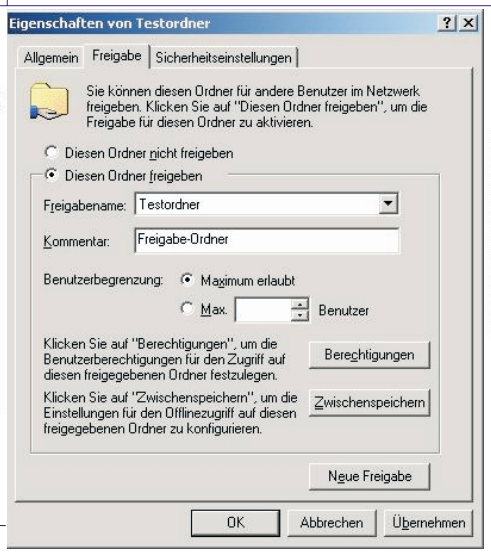
Jeder Freigabe kann ein Laufwerksbuchstabe zugeordnet werden:

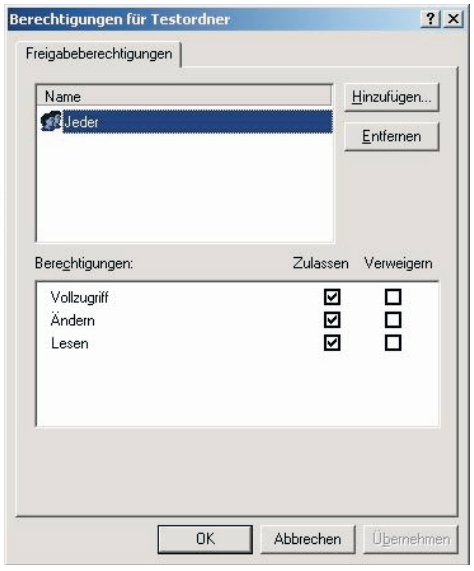
Freigabe anlegen in der Kommandozeile: mit der Anweisung net use Laufwerksbuchstabe UNC-Pfad

Beispiel:

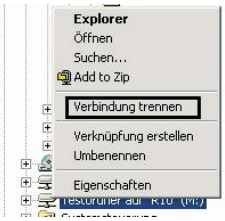
```
C:\>net use M: \\r10\Testordner
```

Der Befehl wurde erfolgreich ausgeführt.





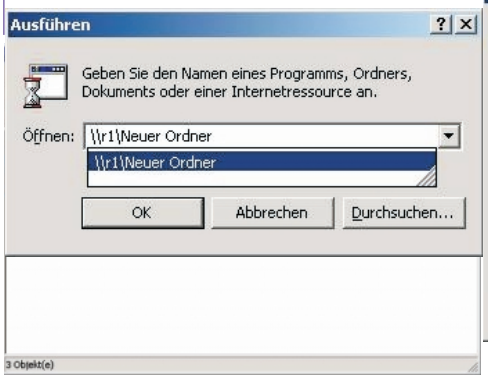
Werden zugeordnete Laufwerksbuchstaben nicht mehr benötigt, so kann die Freigabe wieder getrennt werden:

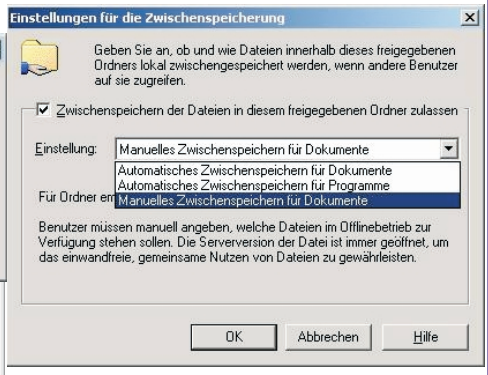


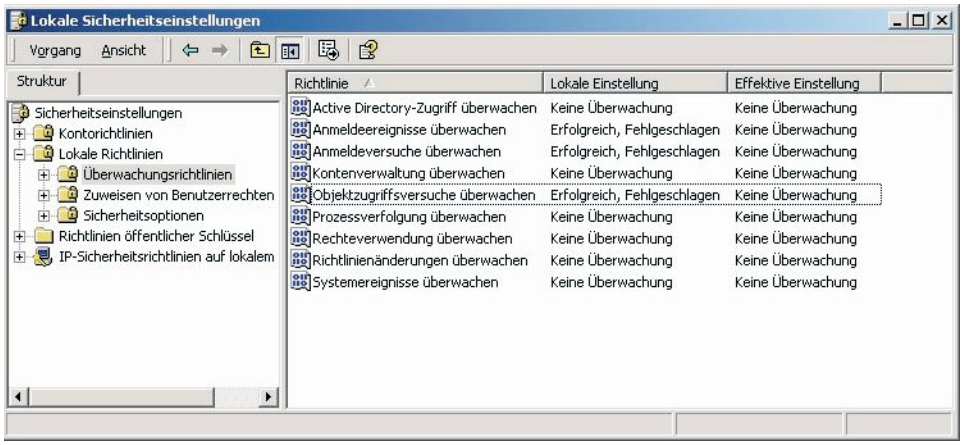
Wichtig für die **Offline-Ordner**:

Verbesserte Version des "Aktenkoffers": Hier kann auf eine Netzwerkressource zugegriffen werden, obwohl sie nicht mehr verfügbar ist. Standardmäßig wird für das Zwischenspeichern 10 % der Festplatte verwendet; kann geändert werden.

Weitere Möglichkeit: ***Start - Ausführen***







16 Ressourcen und Ereignisse überwachen

Überwacht werden können:

- Art der Zugriffe auf Ressourcen (schreibend, lesend, Änderungen)
- Datei- und Objektzugriffe
- An- und Abmeldungen
- Prozesse

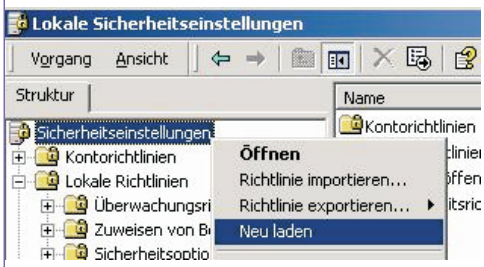
Dafür muss eine Sicherheitsrichtlinie eingerichtet werden:

Start - Programme - Verwaltung - Lokale Sicherheitsrichtlinie

Um tatsächlich die Zugriffe auf Dateien mitzuprotokollieren, muss diese Option auf Dateiebene erst eingeschaltet werden!

Die Protokolle sind unter ***Verwaltung - Ereignisanzeige*** auszulesen: Dort können unter "***Sicherheitsprotokoll***" die protokollierten Vorgänge beobachtet werden.

Um die eingestellten Rechte auch tatsächlich zu sehen, können die Sicherheitseinstellungen neu geladen werden:



Die eingestellten Rechte werden übernommen und auch in der Spalte "Effektive Rechte" dargestellt.

Möchte man etwa den Zugriff auf eine Textdatei überwachen, so setzt man in den ***Eigenschaften - Sicherheitseinstellungen*** in der Karteikarte "***Überwachung***" einen Überwachungseintrag:

Wird auf diese Datei zugegriffen, dann entstehen in der Ereignisanzeige Einträge wie dieser:

Protokolldateien können in verschiedenen Formaten gespeichert werden:

- ***.EVT** - internes Format
- ***.TXT** - Textdatei
- ***.CSV** (*comma separated value*) - in Excel weiterverarbeitet

Beispiel für CSV-Datei
Mit Filterfunktionen können die Ereignisse nach Gruppen etc. gefiltert werden: