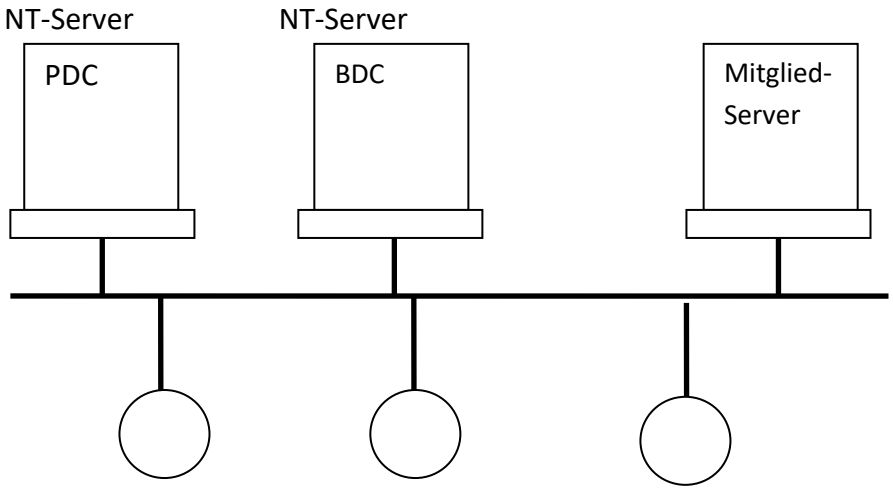
Windows

In der aktuellen Industrietechnik sind Microsoft-Systeme die dominierende Technik. Deshalb müssen Sie mit Netzen auf dieser Basis ein wenig umgehen können.

Windows NT war die erste wirklich stabile, industrietaugliche Systembasis von Microsoft. Damals wurde der Wechsel zum präemptiven Multuitasking vollzogen, Sie wissen was das bedeutet. Das Netz war „serverbasiert".

Mit Windows 2000 verlies Microsoft den proprietären Ansatz, und ging mit Active Directory in Richtung offener, „verzeichnisbasierter" Standards.

Serverbasiertes Konzept (Windows NT) :



In Windows NT war die Administration nur auf dem PDC (primary domain controller) möglich. Ein BDC (backup domain controller) trug eine „read-only" - Kopie, um bei Ausfall des PDC den Netzbetrieb aufrecht halten zu können.

Damit können nur Microsoft-Systeme verwaltet werden, als nur Clientrechner mit Windows als Betriebssystem !

Was ist ein „Server“ ?

Hier muß man ein wenig präziser mit den Begriffen umgehen.
Eigentlich (das hatten wir schon) ist ein Server ein Programm, das auf irgendeinem Rechner (oder Handy oder so) läuft, und irgendwelche nützlichen Dinge tut, die man nutzen kann.

Dazu schicken sie ihm eine „Dienstanforderung“ (Request), und er tut das, was Sie wollen (Response).

Ein Fileserver zum Beispiel ist ein Programm, das auf einem Rechner läuft, und besonders gut besonders viele Daten speichern und bereitstellen kann.

Das Problem ist : umgangssprachlich (und falsch !) wird meist nicht der eigentliche „Server“, also die Software, sondern der Rechner, auf dem sie läuft, als „Server“ bezeichnet.

Präzise betrachtet, ist das Gerät, also der PC, nur die Hardware (incl. Betriebssystem) auf dem die Serversoftware läuft.

Wenn von „Servermaschinen“ geredet wird, ist das nur eine Hardware, die sich wegen ihrer Zuverlässigkeit und Leistung besonders gut für den Betrieb von Serversoftware eignet.

Wozu braucht man einen „Server“ ?

Betrachten wir das Netz einer Zahnarztpraxis.
Die beiden Sprechstundenhilfen am Empfang haben je einen PC. Einer steht im Laborraum, einer im Behandlungsraum.
In der Praxis arbeiten der Zahnarzt und die beiden Sprechstundenhilfen.

Der Arzt will jetzt im Behandlungsraum auf die Röntgenbilder zugreifen, die im Laborraum-PC gespeichert sind. Auf die Rechner der Sprechstundenhilfen sollen Zugriff haben, und jeder an jedem Rechner arbeiten können.
Weil sie nicht mit USB-Sticks hantieren wollen, vernetzen sie die Rechner (natürlich Ethernet), und greifen über das Freigabeprotokoll von Windows auf die anderen Rechner zu.
Dazu müssen sie jetzt auf jedem der 4 Rechner Kennungen und Passwörter für die 3 Mitarbeiter anlegen. Einen neuen Mitarbeiter legen Sie dann wieder auf jedem der 4 Rechner an.

Und damit wird klar, wozu man einen „Server“ braucht :
Stellen Sie sich einfach eine Software-Firma mit 200 PC und 200 Mitarbeitern vor, die alle beliebige Zugriffe brauchen !

Der „Server“ verwaltet zentral die „Resourcen“, also Benutzer und Rechner.

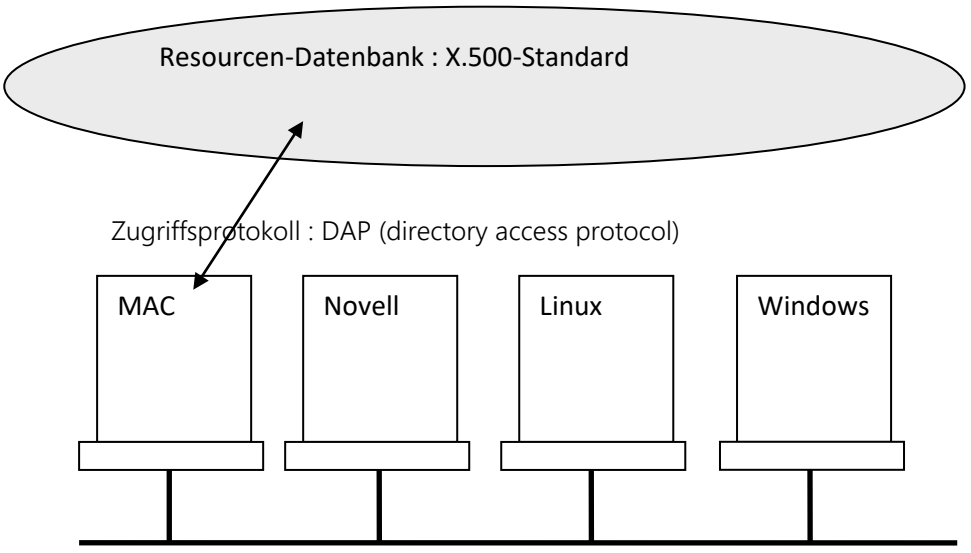
Sie legen z.b. einen neuen Mitarbeiter einmal auf dem Server an, dann kann er sich auf allen 200 PC einloggen !

Was ist ein „Verzeichnisdienst“ ?

In der Praxis sind die Netze aber „bunter“, neben Windows sind noch viele andere Systeme am laufen. UNIX, Android, I-Phones, Novell, irgendwelche MACs, SPS-en, usw. usw ….

Deshalb haben amerikanische Universitäten um 1990 ein Datenbanksystem entwickelt, das zur „plattformübergreifenden“ Verwaltung der Netzresourcen dienen soll. (Mit Plattform ist hier Betriebssystem gemeint)

Also eine Datenbank, die „über“ den ganzen Betriebssstemen steht, und für alle gemeinsam user und PC verwaltet :

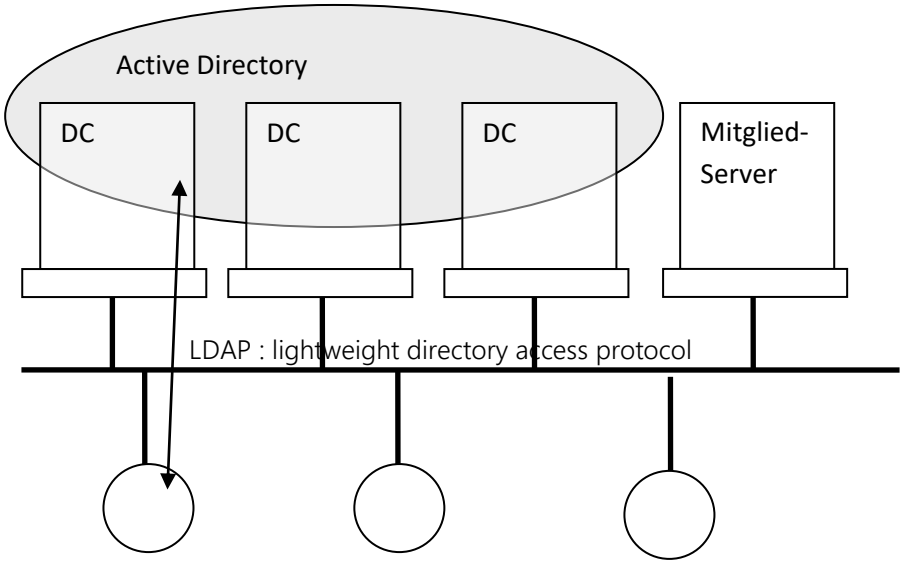


Diese Idee hat schwer eingeschlagen.

Novell (damals Marktführer für Fileserversysteme) hat ein eigenes Protokoll entwickelt, das kompatibel zu X.500 ist : NDS (novell directory service)

Microsoft hat Windows NT in die Tonne getreten, und ist ebenfalls mit einem X.500 – kompatiblen System auf den Markt : Active Directory.

Active Directory ist, wie NDS, wesentlich „kleiner" als X.500 (das war ursprünglich so gedacht, daß man am Ende weltweite alle Rechensysteme zentral verwalten kann). Die Datenbank läuft repliziert auf den sogenannten „Domänencontrollern"



Verzeichnisdienst Active Directory

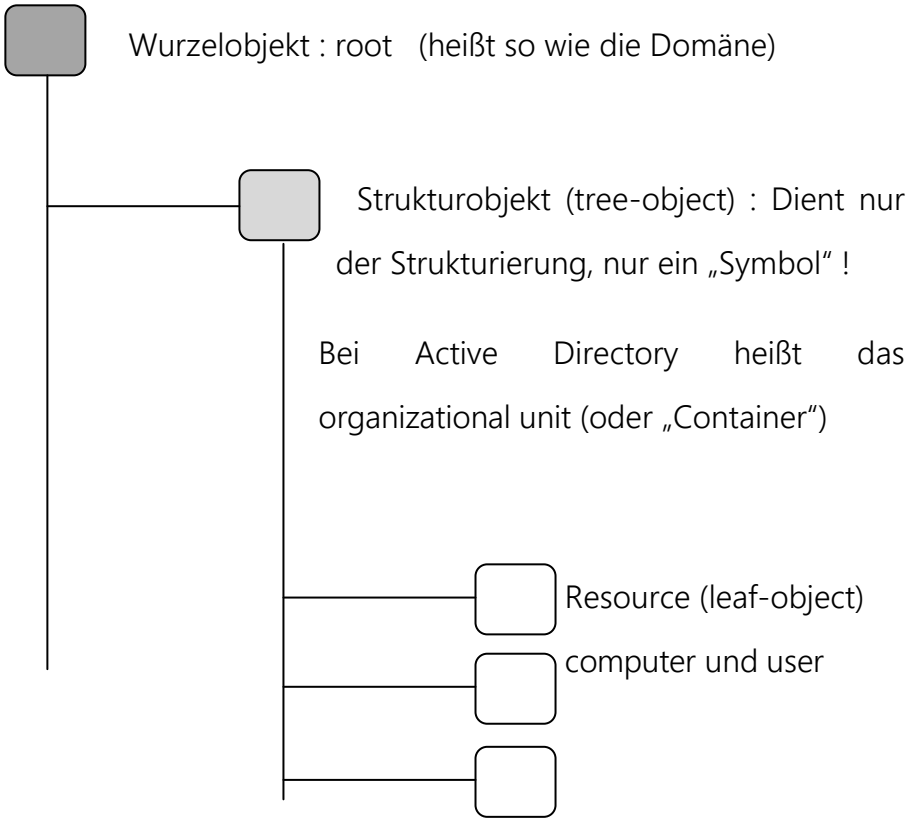
Ab Windows 2000 mit Active Directory ist die Administration der Netzresourcen auf allen DC möglich, jeder trägt eine beschreibbare Kopie der Datenbank, die in zyklischen Abständen von allen DC repliziert wird. Hierzu werden Zeitstempel auf die Einträge benutzt, die sogenannten „update sequence numbers". Diese sorgen dafür, daß immer die neuste Änderung netzweit auf allen DC aktualisiert wird. Weitere DC erhöhen die Betriebs-sicherheit des Netzes.

Besondere Funktionen des ersten installierten DC :
Der erste installierte Domänencontroller agiert als Betriebsmaster. Seine Spezial-Funktionen („FSMO" flexible single master operations) werden nicht repliziert, das heißt bei Ausfall muß ein anderer Server manuell zum Betriebsmaster hochgestuft werden . Zu diesen Aufgaben gehört die Verwaltung der numerischen ID der Objekte (user, computer usw.), des Active-Dir Schemas (welche Funktionen möglich sind) und noch eine Reihe von weiteren Verwaltungsaufgaben.

Aufbau eines Verzeichnisdienstes

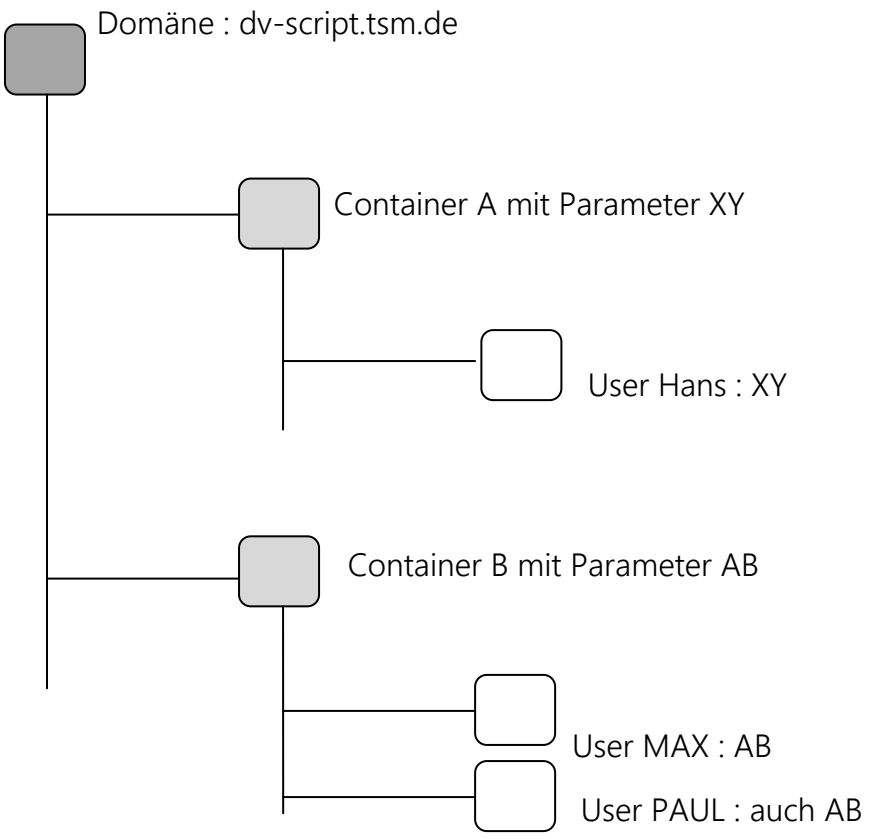
In X.500 heißt der Protokollstandard DAP (directory access protokoll). LDAP ist eine Untermenge davon, das lightweight directory access protocol. (Die Bezeichnung „OpenLDAP“ für einen LINUX-basierten open source- Verzeichnisdienst ist unkorrekt, weil LDAP ja ein Protokoll ist, kein Dienst)

Die Datenbankstruktur eines Directory Service läßt sich gut graphisch darstellen, das sieht aus wie ein Baum (heißt auch tree), aber auf dem Kopf stehend (die Wurzel ist oben) :



In Active Directory gibt es nach Installation eine Reihe von vorgegebenen Objekten und Containern. (Bei Novell z.b. ist das anders, da ist der Baum erstmal leer).
Die wesentlichste Eigenschaft des directory tree ist, daß er ein hierarchisches System beschreibt : Für einen Container definierte Einstellungen übertragen sich nach unten an alle im Ast liegende Objekte, auch in weiteren Containern.

Man nennt dies Vererbung oder inheritation :



Objekte in Active Directory :

Administriert werden im wesentlichen Computer und User. Im objektorientierten Sinn sind dies Klassen, also „Vorlagen" für die zu erzeugenden Objekte.

Wie es sich für Objekte gehört, haben diese eine Reihe von Eigenschaften (Attribute : mehrere Namen, Telefonnummern, usw…). Ein Teil davon sind „lebenswichtige" Attribute, ohne die ein Objekt nicht existieren kann : mandatory attributes. Die übrigen, nicht lebenswichtigen, heißen optional attributes.

Objekte in Active Directory haben neben den internen numerischen Kennungen (SID) für den Menschen lesbare Namen :

distinguished name (DN) :

cn = HANS, ou = B, ou = A, dc = dv-script, dc = tsm, dc = de

common name organizational unit domain component

Eine vereinfachte Form ist der "kontextfreie" Anmeldename (der Kontext, die Stelle im Baum, wird dann automatisch gesucht) :
user prinzipal name (UPN) : HANS@dv-script.tsm.de

Administration mit Active Directory :

Administrieren in Active Dir bedeutet zum Einen, daß die zu verwaltenden Objekte, also die Computer im Netz und die daran arbeitenden User in einen sinnvoll strukturierten Verzeichnissbaum eingegeben (oder mit einem Programm importiert) werden müssen. Dann können Sie mit Parametern zurechtgestutzt werden. Aus geschichtlichen Gründen heißen diese Parameter bei Microsoft Gruppenrichtlinien (group policies).

Gruppenrichtlinien werden an Container vergeben. Sie vererben sich dann wie beschrieben nach unten. Wenn der Baum geschickt aufgebaut ist, kommt man mit wenigen Richtlinien aus.

Es gibt enorm viele einstellbare Parameter, sie sind aber streng in zwei Familien eingeteilt

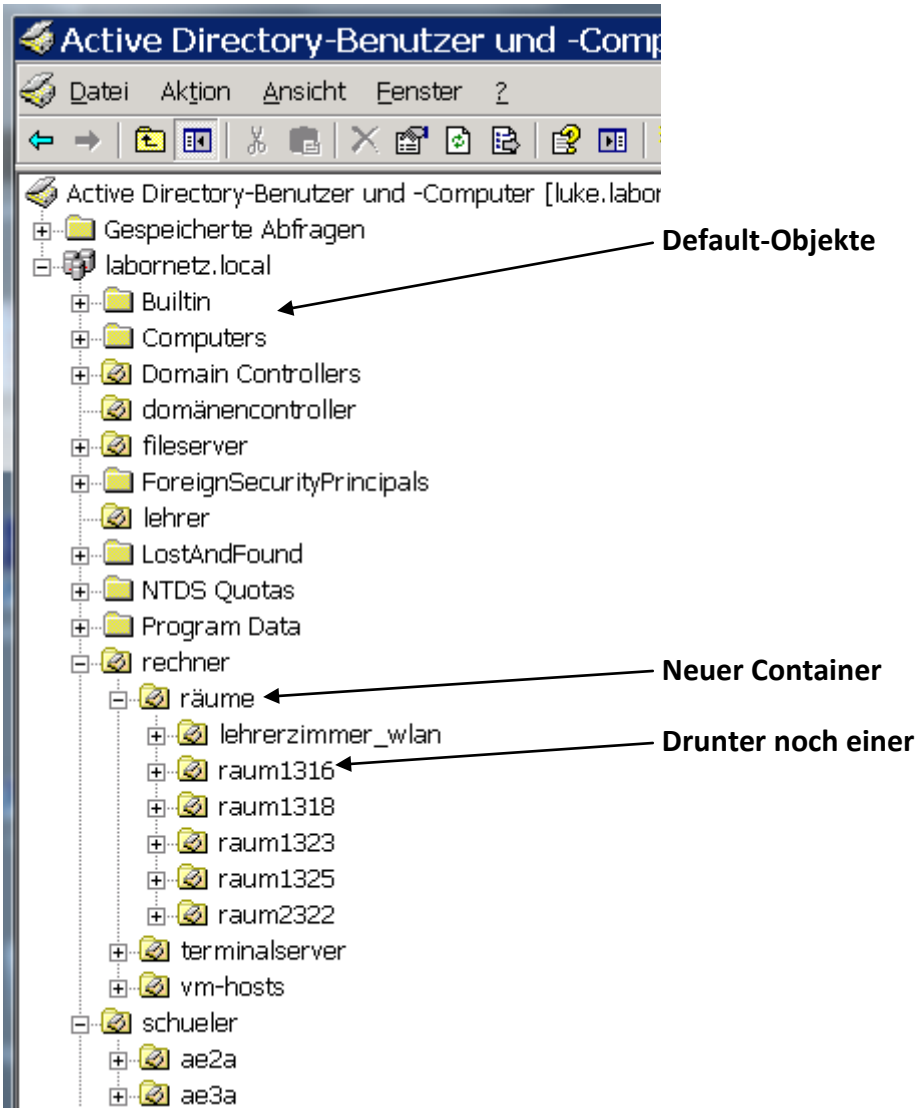
Computerrichtlinien wirken nur auf den Objekttyp Computer

Benutzerrichtlinien wirken nur auf den Objekttyp User

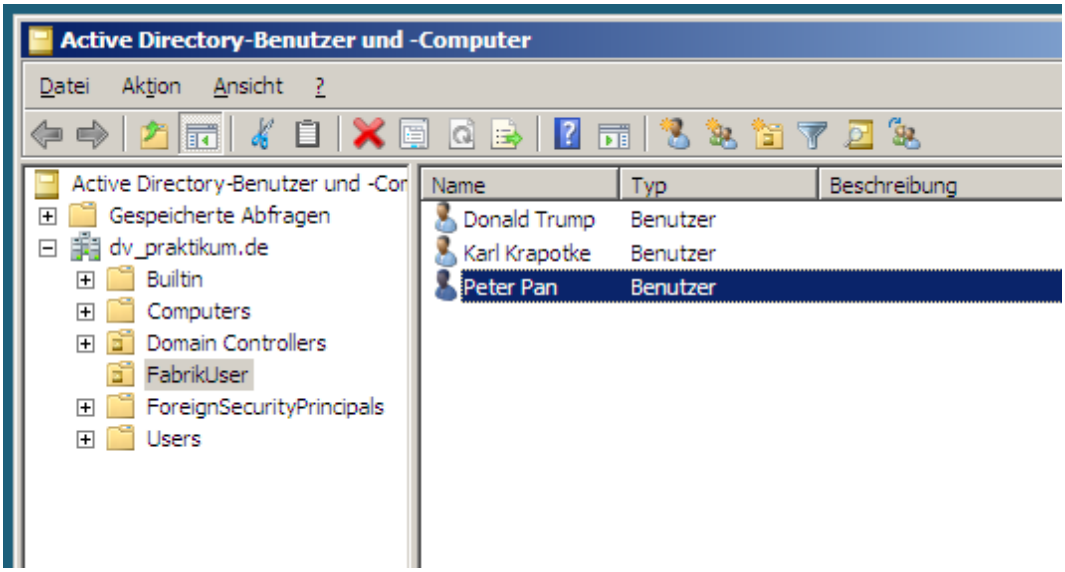
Das kann Probleme bereiten, wenn man unsauber arbeitet. Wenn in Containern die Objekttypen gemischt sind, ist die Wirkung der Richtlinien nicht sehr übersichtlich …

Active Directory in der Praxis :

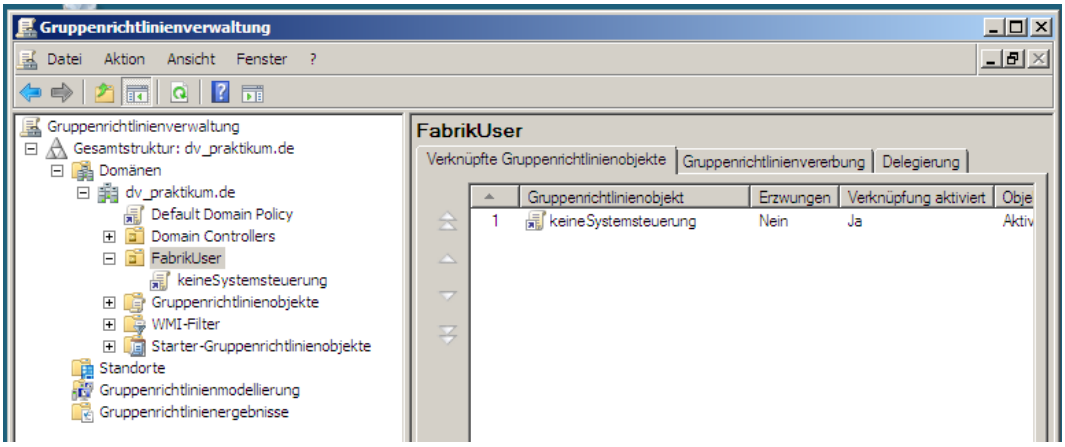
Hier ein Ausschnitt der Labornetzverwaltung der Technikerschule :



Hier die Ansicht des Verzeichnisbaums :

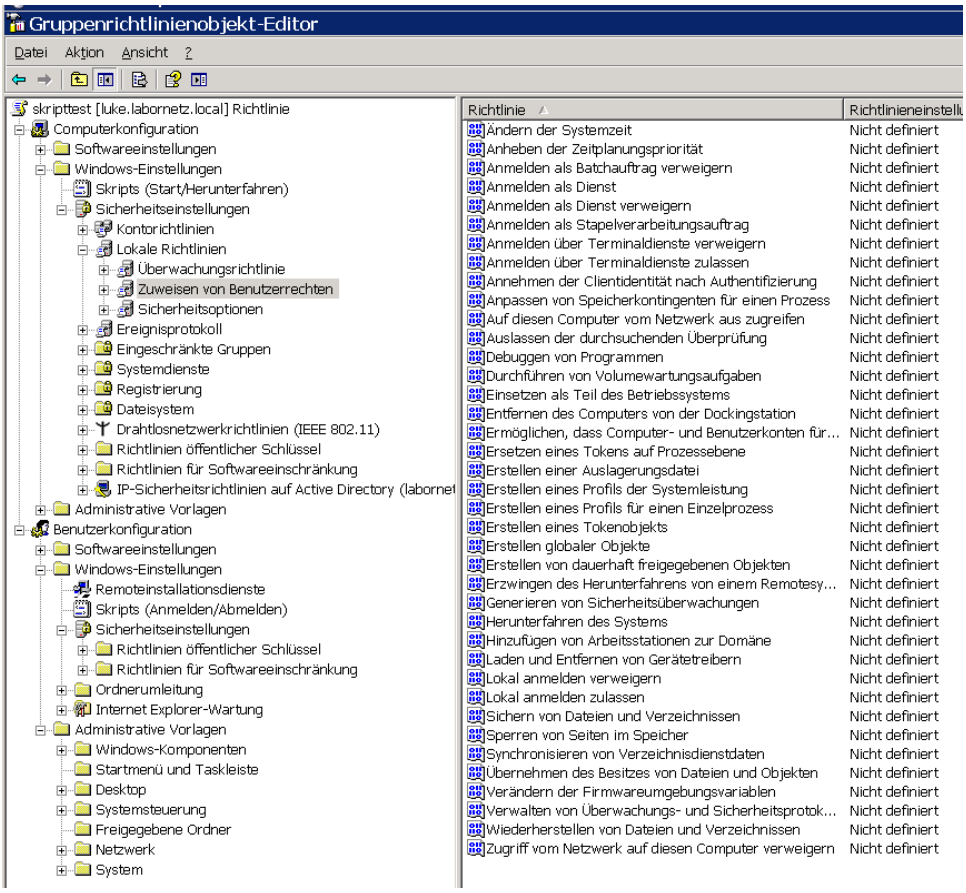


Und hier die dazugehörige Gruppenrichtlinienansicht :



Eine solche Gruppenrichlinie kann beliebig viele Parameter-einstellungen enthalten. Es ist aber eine gute Idee, pro Richlinien nur eine einzige Parameteränderung durchzuführen, und die Richtlinie entsprechend zu benennen, um das System übersichtlich zu gestalten.

Mit einem RechtsKlick auf ein AD-Objekt kann eine neue Gruppenrichtlinie hinzugefügt werden. Dann kann nach einem RechtsKlick auf die neue Richtlinie mit BEARBEITEN der Gruppenrichtlinien-Editor geöffnet werden :



Man erkennt die wichtige Unterscheidung in Computerkonfiguration und Benutzerkonfiguration. Wenn in diesem Beispiel in Benutzerkonfiguration eine passende Richtlinie gefunden und aktiviert wird, bewirkt das dann NICHTS, weil das Objekt, an dem wir arbeiten, der Container räume, keine Benutzer, sondern nur Computer enthält !