

Ausarbeitung

Windows 2003 Server

Benutzerprofile & Skripte



```
GA Anmeldescript - (c) by daniel baier
#####
# Hallo b.benutzer!
# Willkommen in der Domäne DUDDITSLAB.LOCAL am PC DUDDITS-LAP!!!
# Es ist
16:31
# am
30.03.2006
# Viel spass!
#####

Z: wurde erfolgreich gelöscht.

Der Befehl wurde erfolgreich ausgeführt.

Beachten Sie, dass Ihre Sitzung protokolliert wird!
```



Daniel Baier

Vorwort:

Dieses Dokument befasst sich mit der Thematik der Benutzerprofile und das Verwenden von Scripten unter Windows 2003 Server. Dennoch sind die meisten hier gezeigten Techniken auch auf Windows 2000 Server/Professionell übertragbar.

Dieses Dokument versteht sich keines Wegs als Fachliteratur in die Welt der Benutzerprofile und Scripte unter Windows, sondern viel mehr als Einstieg in die wirre Welt der Scripte und Benutzerprofile unter Windows.

Voraussetzung:

Als Voraussetzung für dieses Dokument gelten Grundkenntnisse der Administration von Windows XP Professionell sowie von Windows 2003 Server.

Über den Autor:

Daniel Baier ist Schüler mit Schwerpunkt Informatik und beschäftigt sich seit nun mehr als 3 Jahren mit Windows. Weitere Spezialisierungen sind Linux/Unix sowie Computersicherheit.

Ausgangssituation:

Dieses Dokument geht von der Ausgangssituation aus, das ein Windows 2003 Server System, welches hier immer als Server bezeichnet wird und die IP Adresse *192.168.0.1* hat, vorhanden ist. Auf diesem Server sind die Server-Dienste DNS, DHCP und eine Domäne im Active Directory bereitgestellt.

Der Client bekommt bezieht seine IP-Adresse sowie seine DNS Serveradresse dynamisch vom Server.

Auf dem Client läuft Windows XP Professionell unter Umständen auch Windows 2000 Professionell, welcher Mitglied der Domäne ist.

Weitere Voraussetzungen werden in Kapitel 1 - *Vorkonfiguration des Servers* -behandelt.

Kapitel 1 - Vorkonfiguration des Servers

1.1 Ändern der Kennwortrichtlinien

Damit es beim Einrichten der Benutzer zu keinen Schwierigkeiten kommt, stellt man in den Gruppenrichtlinien zunächst einmal die Kennwortkomplexitätsvoraussetzungen aus sowie die minimale Kennwortlänge setzen wir auf Null.

Achtung:

Es ist normalerweise davon abzuraten diese Funktionen zu deaktivieren, da dies das Verwenden von schwachen Kennwörtern erlaubt. Dies ist ein hohes Sicherheitsrisiko und sollte nur bei den Beispielen dieses Dokumentes eingesetzt werden.

Dazu klickt man auf Start und wählt nun Ausführen (alternativ über die Tastenkombination Windowstaste + R). Nun ruft man das Snap-In *Active Directory Benutzer und Gruppen* mit den Befehl `dsa.msc` auf.

Dort wählt man mit der Rechten Maustaste die Eigenschaften der Domäne.

Im anschließenden erscheinenden Fenster wählt man den Abschnitt Gruppenrichtlinien und markiert das Gruppenrichtlinien Objekt *Default Domain Policy*. Hier wählt man anschließend den Button *Bearbeiten*.

Nun wechselt man in den Pfad Computerkonfiguration/Windows

Einstellungen/Sicherheitseinstellungen/Kontorichtlinien/Kennwortrichtlinien und ändert wie in Abbildung 1 die Werte.

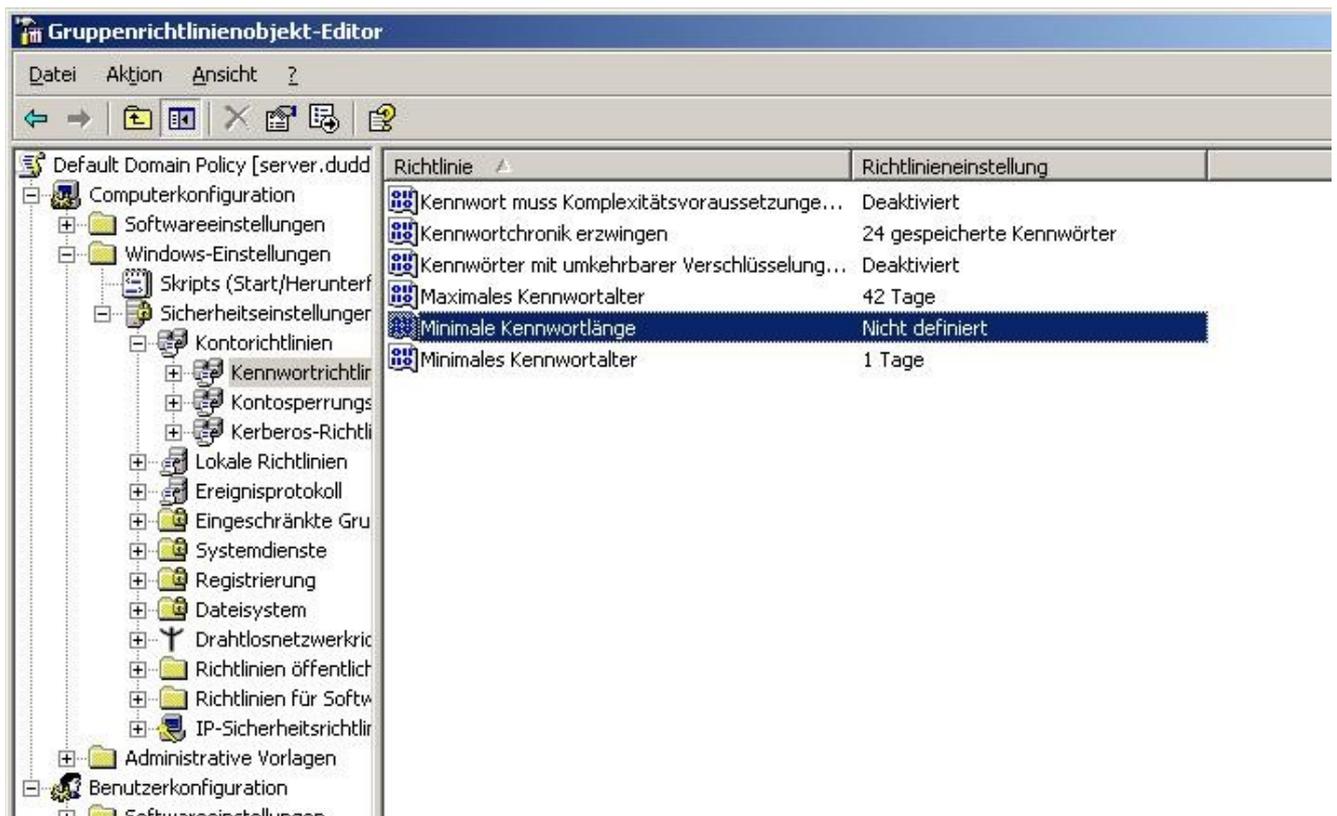


Abb. 1: Ändern der Kennwortrichtlinien

Nachdem alle Werte entsprechend geändert und übernommen wurden, können die Gruppenrichtlinien nun geschlossen werden. Jetzt müssen nur noch die Gruppenrichtlinien aktualisiert werden. Standardmäßig aktualisieren sich die Richtlinien nach 90 Min. bei Domänenmitgliedern und 5 Min. bei Domänencontrollern. Damit die Änderungen sofort

wirksam werden, öffnet man wieder die Befehlseingabeaufforderung unter Start -> Ausführen und gibt das Kommando `gpupdate /force` ein und bestätigt dies mit dem Ok-Button (siehe auch Abbildung 2). Standardmäßig werden nur geänderte Richtlinien angewendet mit dem Parameter `/force` werden nochmals alle Richtlinien angewendet.

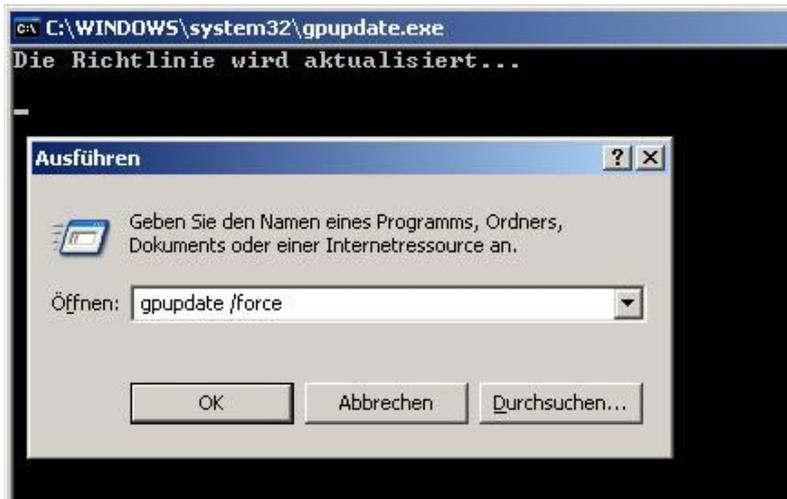


Abb. 2: Aktualisierung der Gruppenrichtlinien

1.2 Das Vorkonfigurations-Script

Um sich ein wenig Arbeit zu ersparen, schreibt man sich z.B. dieses kleine Batch-Script, welches einen Benutzer sowie eine Organisationseinheit für die Beispiele des Dokumentes erstellt.

```
vorkonfiguration - Editor
Datei Bearbeiten Format Ansicht ?
@echo off
rem (c) by daniel baier
rem GNU Public License
rem for more infos mail at dudditslab@googlemail.com

cls
title vorkonfiguration fuer Ausarbeitung Benutzerprofile und Scripte
echo Organisationseinheit >>Projekt<< wird erstellt....
dsadd ou "OU=Projekt,DC=dudditslab,DC=local"
echo;
echo Benutzer >>Schueler<< wird erstellt....
dsadd user "CN=Schueler,OU=Projekt,DC=dudditslab,DC=local" -samid schueler -upn
schueler@dudditslab.local -pwd * -disabled no -acctexpires never -pwdneverexpires yes
-canchpwd no -mustchpwd no
echo;
cd C:\
mkdir shares
cd shares
mkdir schueler
mkdir profil-2e46
net share schueler$=C:\Shares\schueler /GRANT:schueler,change
net share 2e41$=C:\Shares\profil-2e46 /GRANT:jeder,change
net share
pause
```

Abb. 3: vorkonfiguration.bat

Wie man vielleicht sieht, steht in der ersten Zeile der Stapelverarbeitungsdatei (Batchdatei; .bat bzw. .cmd) `@echo off`. Diese Anweisung ist normalerweise üblich am Beginn einer Stapelverarbeitungsdatei und sorgt dafür, dass keine Befehle beim Ausführen der Batchdatei angezeigt werden, sondern nur deren Resultate.

Somit erscheinen nur noch mittels der Anweisung `echo`, Meldungen auf den Prompt(Konsole) oder halt Fehlermeldungen beim Ausführen der Batchdatei sowie die Ergebnisse der einzelnen Befehle/Kommandos.

Durch die Anweisung *rem* werden Kommentare im Script realisiert. Nun wird durch den Befehl *cls*(steht für clear screen) der Inhalt der Befehlszeile gelöscht und mit dem Befehl *title* der Titel der Befehlszeile festgelegt. Anschließend wird mit dem Kommando *dsadd ou* die Organisationseinheit erstellt. Dabei muss man den Distinguished Name angeben, dieser wird in Anführungszeichen(“) angegeben. Nach dem die Organisationseinheit erstellt wurde wird über den Befehl *dsadd user* der Benutzer Schueler erstellt. Dieser darf sein Kennwort niemals ändern und sein Kennwort sowie sein Benutzerkonto verfällt niemals. Weiterhin wird mit dem Parameter *-pwd ** das Kennwort festgelegt. Dabei spielt aber das *** eine Sonderrolle, da dies zur Passworteingabe auffordert, anstelle dessen könnte man auch das Kennwort in Klartext eintragen. Jetzt wechselt das Script mittels *cd* nach *C:* und erstellt den Ordner Shares. In diesem werden dann 2 weitere Ordner erstellt. Nun werden diese beiden Verzeichnisse über das Kommando *net share* im Netzwerk Freigegeben, wobei die Berechtigungen auf die Freigabe direkt gesetzt sind. Abschließend wird mit der Anweisung die Stapelverarbeitungsdatei angehalten.

1.3 Client in die Domäne einbinden

Um den Client in die Domäne einzubinden ruft man das Kontextmenü des Arbeitsplatzes auf und wählt die Eigenschaften(schneller: Windowstaste + Pausetaste). Dort wählt man die Registerkarte Computernamen und klickt auf *Ändern...* .Nun ist der Name der Domäne einzutragen sowie sich an dieser anzumelden (am besten als Administrator, siehe Abbildung 4).

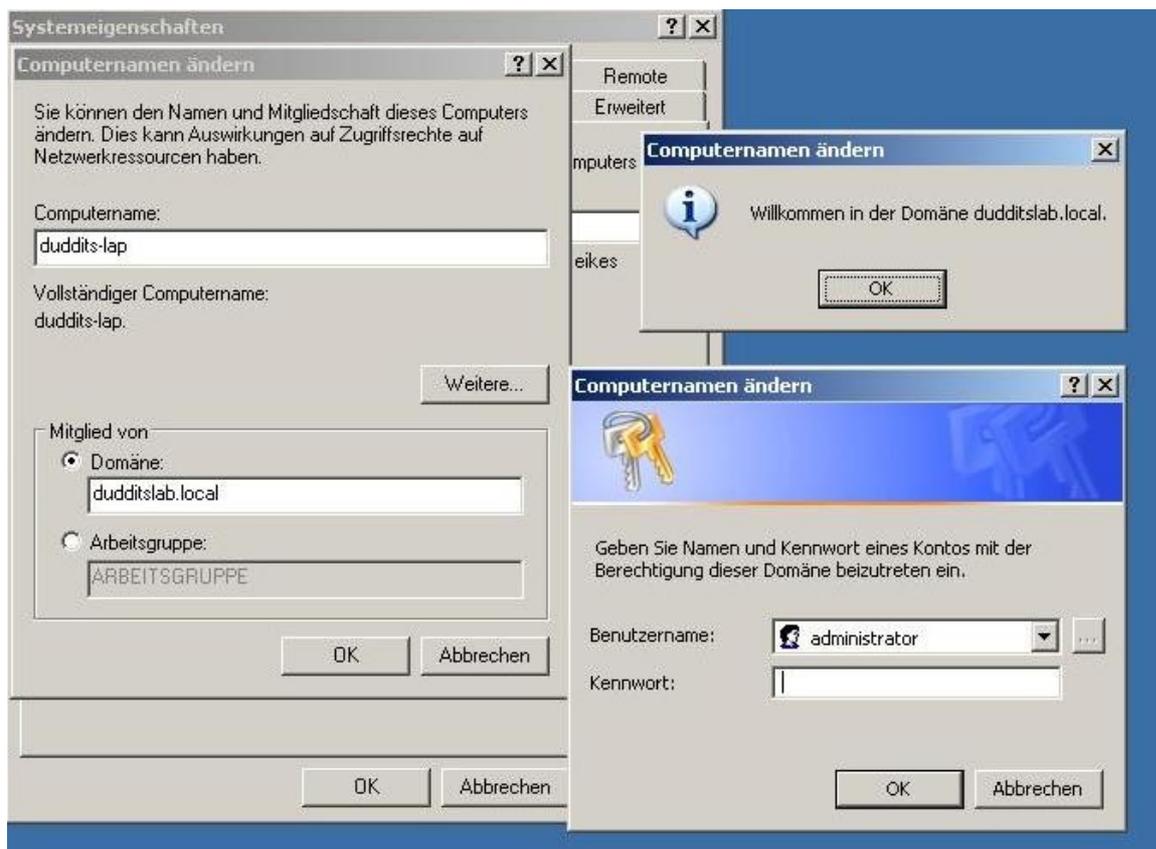


Abb. 4: vorkonfiguration.bat

Herzlichen Glückwunsch jetzt haben Sie die Vorkonfiguration des Servers abgeschlossen und können mit dem eigentlichen Thema den Benutzerprofilen beginnen.

Kapitel 2 – Benutzerprofile

2.1 Benutzerprofile Allgemein

In einem Profil ist alles hinterlegt, was ein Benutzer an Desktopeinstellungen an seiner Arbeitsumgebung einstellen und verändern kann. Zum Beispiel Dinge, wie die Position der Icons auf dem Desktop oder die Hintergrundfarbe, Eigene Dateien, Favoriten, usw.

Ein solches Benutzerprofil bekommt jeder Benutzer, der sich das erste Mal an einem Windows-PC anmeldet, dabei wird automatisch ein eigenes Profil des Benutzer erstellt. Als Vorlage dient dafür das "Default User"- Profil, welches vom Windows einfach kopiert wird. Diese Profile werden seit Windows 2000 unter dem Pfad C:\Domumente und Einstellungen\%username% abgelegt. Wobei %username% durch den Benutzernamen des jeweiligen Windowsbenutzers zu ersetzen ist.

Zusätzlich bindet Windows beim Anmelden bei jedem Benutzer noch zum eigenen Profil das "All Users"- Profile mit ein.

Hinweis:

%username% ist eine Umgebungsvariable, welche den Wert des gerade angemeldeten Benutzers beinhaltet. Man kann sich alle Umgebungsvariablen unter Windows mit dem Befehl *set* in der Konsole anzeigen lassen sowie deren Inhalt. Mit *echo %username%* erhält man den Wert von %username%. Weiterhin kann bei den Systemeigenschaften, Registerkarte Erweitert und dann unter Umgebungsvariablen ebenfalls sich diese anzeigen-lassen bzw. bearbeiten.

Bei Windows wird zwischen drei verschiedenen Profiltypen unterschieden:

lokales Benutzerprofil (local profile):

Das lokale Profil wird beim ersten Anmelden an einem Computer erstellt. Es wird auf der lokalen Festplatte dieses Computers gespeichert. Einstellungen und Änderungen am lokalen Benutzerprofil wirken sich lediglich auf den Computer aus, an dem diese Änderungen vorgenommen worden sind.

servergespeichertes Benutzerprofil: roaming profile

Das servergespeicherte Profil wird vom Administrator erstellt und auf einem Server in einer Freigabe abgelegt. Über das AD wird dem Benutzerkonto mitgegeben, wo das Profil "zu finden" ist. Dieses Profil steht jeweils beim Anmelden an einem Computer im LAN zur Verfügung, wobei bei der Anmeldung eine Kopie des servergespeicherten Profils auf den Client kopiert wird. Meldet sich der User wieder vom PC ab, wird das Profil auf den Server zurück geschrieben, damit die Änderungen die der Benutzer u.U. vorgenommen hat, gesichert sind.

verbindliches Benutzerprofil: mandatory profile

Das verbindliche Profil ist auch ein servergespeichertes Profil, mit dem Unterschied, dass dieses Profil einmalig vom Systemadministrator erstellt wird und dann auch nur von ihm verändert werden kann. Wenn sich ein Benutzer nach getaner Arbeit vom Client abmeldet, werden alle Veränderungen verworfen, die er an dem Profil vorgenommen hat.

"Default User"- Profile

Wenn sich ein Benutzer zum ersten Mal am Client anmeldet, prüft Windows zunächst, ob der Benutzer ein lokales oder ein serverbasiertes Profil besitzt. Wenn kein Benutzerprofil existiert, wird das lokale Standard-Benutzerprofil "DEFAULT USERS" in ein Profilverzeichnis unter C:\Dokumente und Einstellungen mit dem Namen des Benutzers kopiert. Danach wird es als "normales" Benutzerprofil verwendet. Je nach Umgebung bleibt es ein lokales Profil oder wird ein servergespeichertes.

"All users"- Profile

Dieses Profil ist im Prinzip wie ein normales Profil, aber mit einem Unterschied: Wie der Name schon aussagt, gelten Einstellungen aus diesem Profil für alle Benutzer. Wenn sich ein Benutzer anmeldet, wird zum eigenen Profil immer das All Users "dazu addiert".

Ein Beispiel:

Legt ein Administrator in dem "Desktop-Verzeichnis des All Users eine Verknüpfung zu einem Programm ab, bekommt jeder User, der sich an dem PC anmeldet, dieses Icon auf dem Desktop angezeigt (dieser kann es natürlich auch nicht löschen).

2.2 Aufbau des Benutzerprofils:

Im Prinzip besteht das Profil nur aus Ordnern (mit Unterordnern) und Dateien. Schauen wir uns das mal ein bisschen genauer an:

Anwendungsdaten:	In diesem Ordner legen installierte Programme benutzerspezifische Dateien ab
Cookies:	Die eingesammelten Cookies der letzten Internetbesuche.
Desktop:	Was auf dem Desktop zu sehen ist, liegt in diesem Ordner
Druckerumgebung:	Verknüpfungen zu Elementen im Druckerordner
Eigene Dateien:	Speicherort der Eigenen Dateien
Favoriten:	Hier legt der Internet Explorer die Inhaltsverzeichnisse (Bookmarks) des Benutzers ab.
Lokale Einstellungen:	benutzerspezifische Konfigurationen und Dateien (z.B. temporary Internetfiles)
Netzwerkumgebung:	Verknüpfungen zur Netzwerkumgebung
Recent:	Verknüpfungen zu "zuletzt verwendete Dateien"
SendTo:	Elemente des Rechte-Maus-Menüs "Senden an..."
Startmenü:	Benutzerspezifische Elemente der Startmenüs
UserData:	keine Informationen....
Vorlagen:	Vorlagen für Office (nur ältere Versionen)

NTUSER.DAT: Diese Datei enthält die benutzerspezifische Registrierungsstruktur des Users.

Hinweis:

NTUSER.DAT wird bei der Anmeldung nach HKey_Current_Users (HKCU) importiert. Durch umbenennen der Endung „.dat“ in „.man“ wird das Benutzerprofil verbindlich. Siehe auch Kapitel 2.1 verbindliches Benutzerprofil.

ntuser.dat.log: Diese Transaktionsdatei enthält die aktuellen Änderungen eines Benutzerprofils und dient der Fehlertoleranz.

ntuser.ini: Hier werden Initialisierungseinstellungen für Terminaldienste abgelegt.

2.3 Einrichten und Erstellen des servergespeicherten Profils

Um ein servergespeichertes Profils zu erstellen, entscheidet man sich hier zu aller erst dazu, für jeden Raum/Standort in dem man Rechner administriert eine entsprechende Umgebungsvariable zu erstellen, somit unterscheiden sich die Profile durch Anpassung an den entsprechenden Rechnern der entsprechenden Räume.

Zur Umsetzung meldet man sich als lokaler Administrator am Client an und öffnet wieder die Systemeigenschaften(Windowstaste + Pause) auf. Wählt dort auf der Registerkarte *Erweitert* den Button Umgebungsvariable (siehe Abbildung 5). Im nun erscheinenden Fenster wählt man *Neu* und erstellt eine neue Systemvariable/Umgebungsvariable.

Dabei spielen Name und Wert keine Rolle, doch es macht Sinn als Bezeichnung z.B. orte bzw. location zu nehmen und als Wert den Raumnamen zu nehmen, somit sind die Bezeichnungen für jeden verständlich und schlüssig.

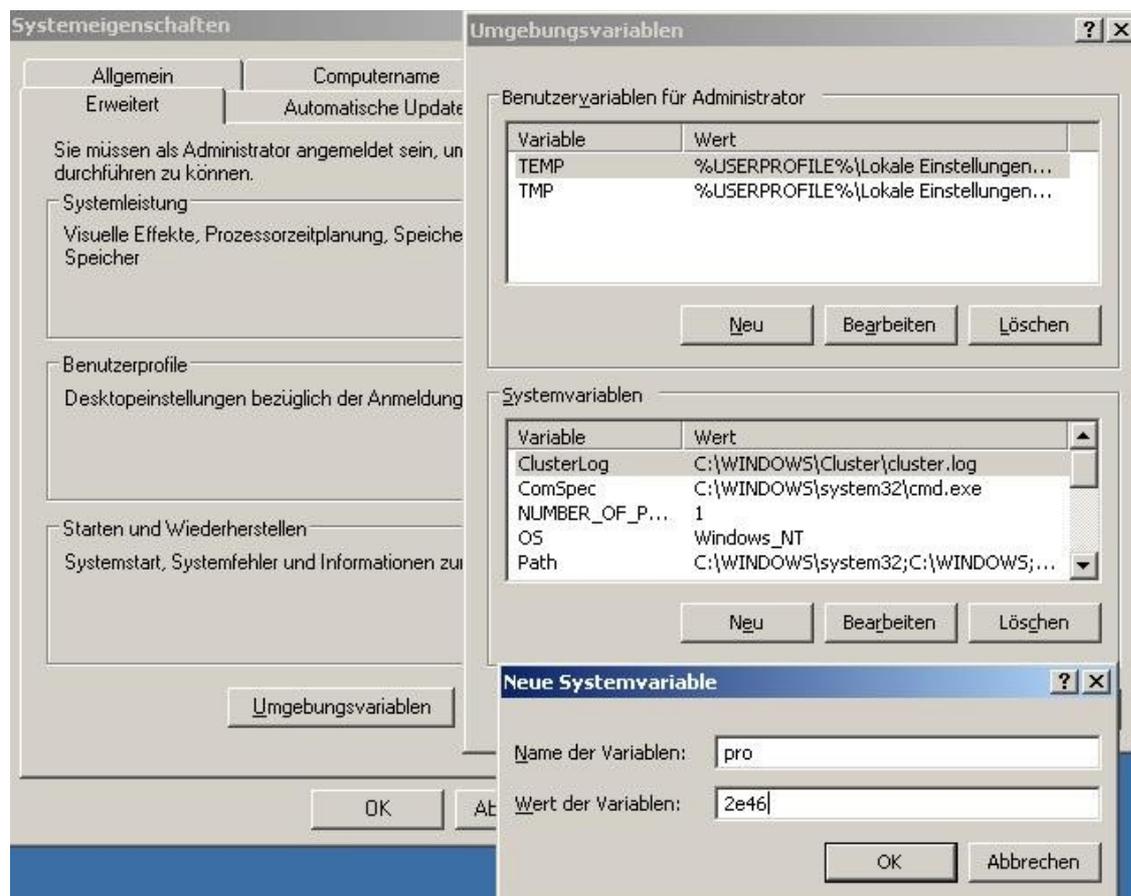
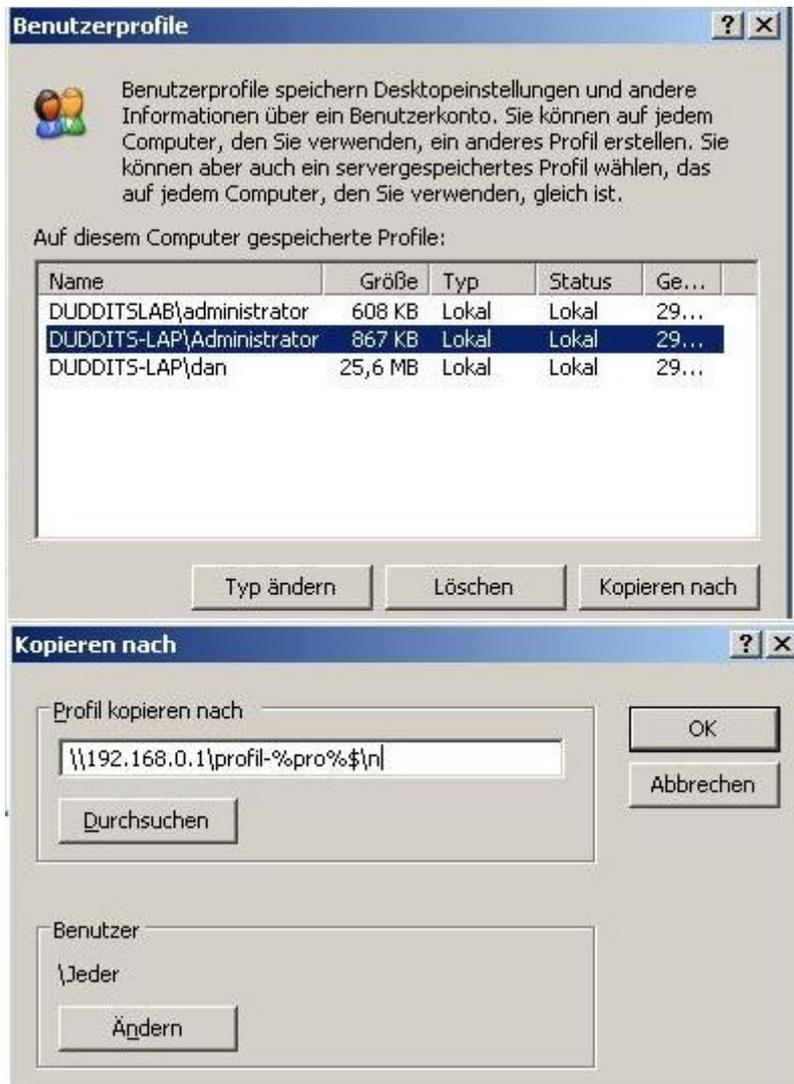


Abb. 5: Erstellen einer neuen Systemvariable bzw. Umgebungsvariable

Nach dem man die Umgebungsvariable erfolgreich erstellt hat meldet man sich ab. Nun will man, das lokale gespeicherte Administrator-Profil als Server gespeichertes anbieten. Dies hat den Vorteil, das man in der Domäne eingeschränkte Benutzer hat, die dennoch die Möglichkeit haben, Anwendungen zu benutzen, die Administrator Rechte brauchen. Ein weiterer Vorteil daran ist, dass der Benutzer von alledem nichts mitbekommt. Hierzu muss man sich als Domänenadministrator anmelden oder einen anderen Benutzer der über genügend Rechte verfügt. Nachdem man sich jetzt angemeldet hat, öffnet man wieder die Registerkarte Erweitert unter dem Systemeigenschaften auf und wählt dies mal Benutzerprofile. In dem nun erscheinenden Fenster selektiert man das lokale Administrator-Konto und wählt *Kopieren nach*.



Dort gibt man den Pfad zur Serverfreigabe an, in dem das Profil nachher gespeichert werden soll. Damit das Profil später von allen Benutzern der Domäne genutzt werden kann, wird als Benutzer „Jeder“ festgelegt. Da dies aber ein nicht unerhebliches Sicherheitsrisiko ist, sollte man anstelle dessen den Benutzer „Authentifizierte Benutzer“ festlegen. Somit sind nur Benutzer die sich an der Domäne authentifizieren dazu berechtigt. Weiterhin muss man ein weiteres Verzeichnis in der Freigabe angeben, da es sonst zu Fehlermeldungen kommt. Nun ist noch mit *Ok* zu bestätigen und schon ist das Profil auf dem Server.

Abb. 6: Benutzerprofile

Anschließend wechselt man wieder zum Server und schneidet alle Dateien(auch versteckte) aus und kopiert diese in das übergeordnete Verzeichnis – hier wäre es *profil%pro%\$* , wobei *%pro%* den Inhalt der zuvor erstellten Systemvariable hat. Jetzt will man natürlich das Profil noch verbindlich machen und ändert die Endung der Datei *Ntuser.dat* in *Ntuser.man* um.

Kapitel 3 - Anmelde Script

Hier im letzten Kapitel wird man sich mit dem Start-Script und der abschließenden Konfiguration befassen.

3.1 Anmelde Script

Um den Benutzer der Domäne auf dem Server Speicherplatz zu bieten, richtet man für diesen ein Netzlaufwerk ein. Darüber hinaus sollen diese ihrer Systemzeit mit dem des Servers synchronisieren. Weiterhin sollen die Benutzer auf die Protokollierung ihres Sitzung hingewiesen werden.

Um diese Aufgaben komfortabel zu bewältigen bedient man sich den Möglichkeiten eines Anmeldescripts.

Hierzu erstellt man zunächst einmal so genannte Kontingenten Einträge für die entsprechenden Benutzer auf dem Laufwerk, wo sich später die Netzlaufwerke befinden soll. Dazu öffnet man das Kontextmenü auf dem das Netzlaufwerk später liegen soll und wählt die *Eigenschaften*. Anschließend selektiert man die Registerkarte *Kontingent*(siehe Abbildung 7).

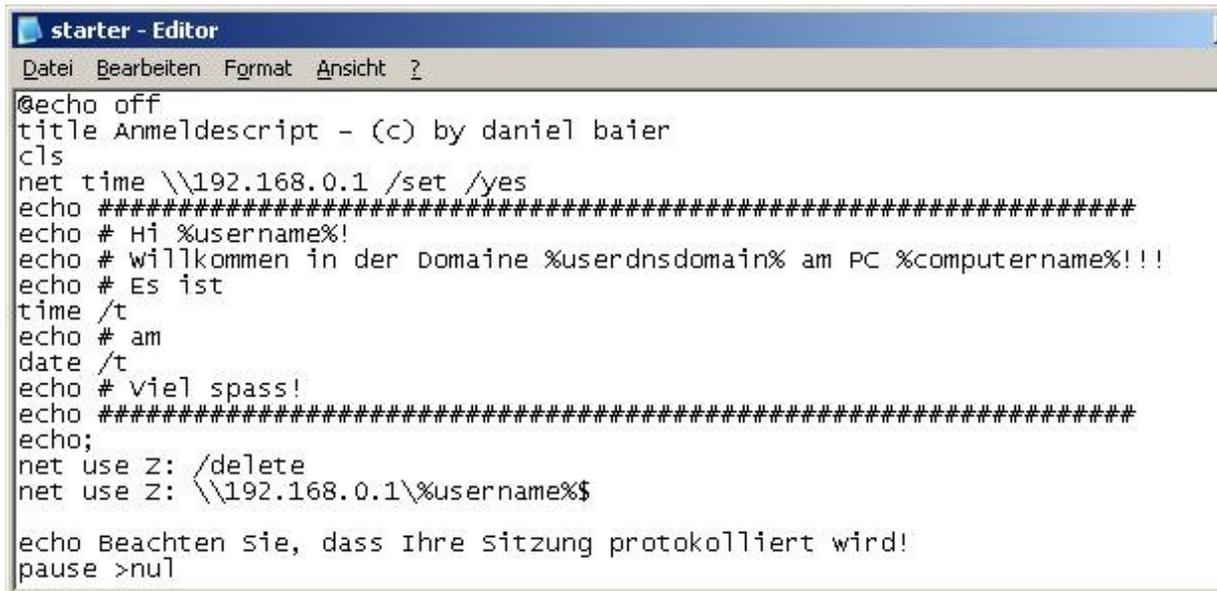
Dort legt man die Warnstufe und die maximal erlaubte Festplattenkapazität für jeden Benutzer fest. Danach wird das Kontingent aktiviert. Wenn man unterschiedlichen Benutzern unterschiedlich viel Platz anbieten möchte so muss man den Button *Kontingenteinträge...* wählen.



Abb. 7: Kontingent verwalten/einrichten

Nach abschließen dieser Konfiguration sind nun alle Voraussetzungen für das Anmeldescript gegeben und man macht sich nun daran eins zu entwerfen.

Da der Benutzer nichts von den Befehlen zum sehen bekommen soll, beginnt man das Script wieder mit @echo off.



```
@echo off
title Anmeldescript - (c) by daniel baier
cls
net time \\192.168.0.1 /set /yes
echo #####
echo # Hi %username%!
echo # willkommen in der Domaine %userdnsdomain% am PC %computername%!!!
echo # Es ist
time /t
echo # am
date /t
echo # Viel spass!
echo #####
echo;
net use Z: </delete
net use Z: \\192.168.0.1\%username%$

echo Beachten sie, dass Ihre Sitzung protokolliert wird!
pause >nul
```

Abb. 7: Anmeldescript starter.bat

Neu sind dieses Mal die Befehle *time /t* sowie *date /t*, diese geben einmal die aktuelle Uhrzeit an und das Datum.

Zuvor wird mit dem Befehl *net time* die Zeit des Clients mit der des Server synchronisiert, sofern auf diesen ein Zeit-Server läuft. Damit der Benutzer das Recht hat die Zeit zu ändern muss in dem Gruppenrichtlinien-Objekt *Default Domain Policy* das Recht dazu eingestellt werden.

Des Weiteren wird mit dem Kommando *net use* der Client mit seinem Netzlaufwerk verbunden. Das Dollar Zeichen bei der Freigabe sorgt dafür, dass die Freigaben versteckt sind- man nennt diese Art der Freigabe auch Administrative Freigaben.

3.2 Script und Profil zuweisen

Damit der Client später weiß wo sich das Anmeldescript befindet, kopiert man es in das dafür vorgesehene Verzeichnis auf dem Server. Nach *C:\Windows\Sysvol\sysvol\%userdnsdomain%\scripts*.



Abb. 8: Verzeichnis für Anmelde Script(die Freigabe Netlogon bezieht sich darauf)

Nach dem man nun das Script fertig an seinen Platz kopiert hat und ein servergespeichertes Benutzerprofil auf dem Server hat, muss man nun zuletzt dem sich anmeldenden Benutzer irgendwie kenntlich machen, wo er danach zu suchen hat.

Dies löst man über das Snap-In *Active Directory Benutzer und Gruppen* welches man mit den Befehl *dsa.msc* aufruft.

Dort selektiert man bei dem entsprechenden Benutzer die *Eigenschaften* im Kontextmenü und wählt anschließend die Registerkarte *Profile* (siehe Abbildung 9).

Nun gibt man einfach unter „Pfad zum Script“ den Namen des Scripts ein, dabei reicht es auch nur z.B. *starter* einzugeben anstelle von *starter.bat*. Des Weiteren ist noch der Pfad der Freigabe zum Profil anzugeben [\\ServerIP\PfadZumProfil](#) unter Profilpfad einzutragen. Dabei kann man die Server-IP durch den Domainnamen ersetzen.

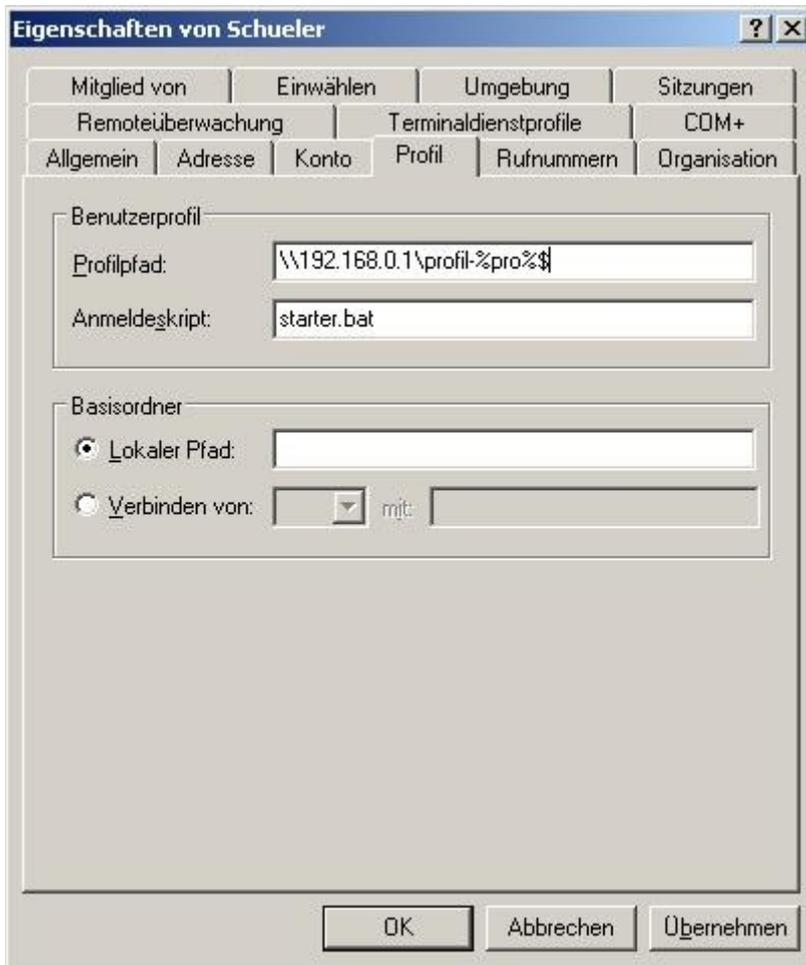


Abb. 9: Registerkarte Profil