

**Benutzerhandbuch  
für die  
Domäne ADS.MWN.DE**  
Ver. 0.8.1

Version: 0.8.1  
Erstellt am: 12.10.07  
Zuletzt geändert am: 09.03.10  
Erstellt von: Thomas Niedermeier  
Zuletzt geändert von: Thomas Niedermeier

## **Inhaltsverzeichnis**

<b>1</b>	<b>Einleitung und Übersicht</b>	<b>5</b>
1.1	Häufig verwendete Begriffe und Abkürzungen	5
1.2	Support	6
1.3	Sprache	6
<b>2</b>	<b>Allgemeine Beschreibung der Domäne ADS.MWN.de und deren Möglichkeiten</b>	<b>7</b>
2.1	Teiladmin	7
2.2	Namenskonzept	7
2.3	Benutzerverwaltung	8
2.4	Verwaltungswerkzeuge	8
2.4.1	Management-Server	8
2.4.2	Admin-Pak:	8
2.5	Definition der Teilbereiche im AD	9
2.5.1	Gruppenverwaltung (momentan offen)	11
2.5.2	Gruppenrichtlinien	11
2.5.3	Systemmanagement	12
2.5.4	Benutzer	12
2.5.4.1	Passwortänderung	12
2.5.4.2	Belegte Benutzerattribute	12
2.5.5	Anbindung des Storage NAS.ads.mwn.de	12
2.5.5.1	Persönliches Verzeichnis	13
2.5.5.2	Projektverzeichnis	13
2.5.5.3	Temporäres Ablageverzeichnis	13
2.5.5.4	Backup-Snapshots	13
2.5.5.5	Erreichbarkeit	13
2.5.6	Laufwerksbuchstaben Konzept für Windows	13
2.5.7	Benutzerprofile	14
2.5.7.1	Keine servergespeicherten Profile	14
2.5.7.2	Mandatory Profile	14
2.5.7.3	Roaming Profile	14
<b>3</b>	<b>Howtos</b>	<b>15</b>
3.1	Aufnahme von Windows Rechnern in die Domäne ads.mwn.de	15
3.1.1	Nutzung der grafischen Oberfläche:	16
3.1.2	Kommandozeile/Skript	19
3.1.3	Notebooks mit zentraler Nutzerverwaltung der Domäne ads.mwn.de	19
3.2	Hinzufügen von Teiladmins zur lokalen Gruppe der Administratoren	20
3.3	Gruppenrichtlinien	21
3.3.1	Win 2000, XP und 2003	21
3.3.2	Änderungen ab Vista	24
3.3.3	Besonderheiten in der Domäne ads.mwn.de	25
3.3.3.1	Loopbackverarbeitungsmodus	25
3.3.3.2	Rechte auf Gruppenrichtlinien	26
3.3.3.3	Fehlende Rechte auf Gruppenrichtlinien für Teiladmins	27
3.4	Loginskripte in der Domäne ads.mwn.de	27
3.5	Verwendung von Mandatory Profiles in der Domäne ads.mwn.de	29
3.6	Vergaben von Rechten auf Ressourcen in der Domäne ads.mwn.de	35

3.6.1	Anlegen einer Gruppe: _____	35
3.6.2	Vergeben von Rechten auf Dateiebene auf nas.ads.mwn.de _____	38
3.6.3	Vergeben von Rechten auf Drucker in der Domäne _____	40
3.6.4	Beschränken der Anmeldung an einem Rechner _____	41
<b>3.7</b>	<b>Anbinden des Storages nas.ads.mwn.de für nicht Domänenrechner _____</b>	<b>43</b>
3.7.1	Einmaliges Anbinden des Storages _____	43
3.7.2	Netzlaufwerk – dauerhaftes Anbinden des Storage nas.ads.mwn.de _____	45
<b>3.8</b>	<b>Wiederherstellung von Dateien auf nas.ads.mwn.de über Snapshots _____</b>	<b>46</b>
<b>4</b>	<b>FAQ _____</b>	<b>48</b>
<b>4.1</b>	<b>Benutzerverwaltung _____</b>	<b>48</b>
4.1.1	Frage: Wo sind meine Nutzer? _____	48
4.1.2	Frage: Darf ich selber Nutzer hinzufügen? _____	48
4.1.3	Frage: Woher bekomme ich meine LRZ-Kennung? _____	48
4.1.4	Frage: Was ist mit meinen alten Projektkennungen vom LRZ? _____	48
4.1.5	Frage: Kann ich an meinem Benutzerobjekt im Active Directory Einstellungen vornehmen? _____	48
4.1.6	Frage: Wie ändere ich oder setze ich mein Passwort zurück? _____	48
4.1.7	Frage: Wer ist mein IO an der TUM? _____	48
4.1.8	Frage: Meine Einrichtung fehlt noch im Active Directory, an wen kann ich mich wenden? _____	48
<b>4.2</b>	<b>Berechtigungen _____</b>	<b>49</b>
4.2.1	Frage: Ich habe einen Nutzer zu einer Gruppe hinzugefügt, aber er hat keine weiteren Berechtigungen erhalten? _____	49
4.2.2	Frage: Wieso bekomme ich den Fehler „Dieser Netzwerkordner ist zurzeit unter Verwendung eines anderen Namens und Kennwortes verbunden“? _____	49
<b>4.3</b>	<b>Gruppenrichtlinien _____</b>	<b>49</b>
4.3.1	Frage: Warum wird meine Gruppenrichtlinie immer ausgefiltert wenn ich mir gresult anzeigen lasse? _____	49
4.3.2	Frage: Warum kann ich als Teiladmin eine Gruppenrichtlinie nicht bearbeiten, die von einem anderen Teiladmin der Einheit erstellt wurde? _____	49
<b>4.4</b>	<b>Woher krieg ich Hilfe zu verschiedenen Themen? _____</b>	<b>49</b>

## **Abbildungsverzeichnis**

2.5.1	Übersicht über die Domäne ads.mwn.de.....	9
3.1.1	Teilstruktur im Active Directory .....	16
3.1.2	Anlegen eines Computerkontos .....	16
3.1.3	Vergeben eines Computernamens .....	17
3.1.4	Ändern eines Rechnernamens .....	17
3.1.5	Aufnahme in die Domäne ads.mwn.de .....	18
3.1.6	Authentifizierung gegenüber der Domäne ads.mwn.de .....	18
3.1.7	Bestätigung der erfolgreichen Aufnahme in die Domäne .....	18
3.1.8	Sicherheitsoption für interaktive Anmeldung .....	19
3.2.1	Benutzer und Gruppen in Computerverwaltung .....	20
3.2.2	Mitglieder der lokalen Gruppe Administratoren .....	20
3.2.3	Suchen von Nutzern und hinzufügen zur Gruppe der Administratoren.....	21
3.3.1	Ansicht des Teilbaums im Active Directory zur Verwaltung von Computern .....	22
3.3.2	Maske für die Verwaltung von Gruppenrichtlinien .....	22
3.3.3	Struktur einer Gruppenrichtlinie .....	23
3.3.4	Einstellungen und Erklärung einer Gruppenrichtlinie .....	23
3.3.5	Gruppenrichtlinienverwaltung ab Windows Vista.....	24

3.3.6	Erweiterte Gruppenrichtlinien mit zusätzlichen Einstellungen.....	25
3.3.7	Wichtige Gruppenrichtlinie: Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien .....	26
3.3.8	Eigenschaften einer Gruppenrichtlinie.....	26
3.3.9	Sicherheitskonfiguration einer Gruppenrichtlinie.....	27
3.4.1	Skripte in den Gruppenrichtlinien .....	28
3.4.2	Verwalten von Skripten für eine Gruppenrichtlinie.....	28
3.5.1	Wichtige Gruppenrichtlinie: Nur lokale Benutzerprofile zulassen.....	30
3.5.2	Wichtige Gruppenrichtlinie: Eigentümer von servergespeicherten Profilen nicht prüfen .....	30
3.5.3	Wichtige Gruppenrichtlinie: Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien .....	31
3.5.4	Hinzufügen einer Umgebungsvariable.....	31
3.5.5	Systemeigenschaften aus der Systemsteuerung .....	32
3.5.6	Übersicht über die lokalen Benutzerprofile am Rechner .....	32
3.5.7	Verallgemeinern und kopieren des Profils in einen freien Ordner.....	33
3.5.8	Übersicht über ein Nutzerprofil für Windows XP .....	33
3.5.9	Ergebnis einer Abfrage mit gpresult .....	34
3.6.1	Hinzufügen von Objekten .....	37
3.6.2	Erweiterte Suche von Objekten im Active Directory.....	37
3.6.3	Der Nutzernamen wird aufgelöst .....	37
3.6.4	Übersicht der aktuellen Mitglieder in der Gruppe .....	38
3.6.5	Verwalten von Berechtigungen für einen Dateiordner .....	38
3.6.6	Leserecht für einen Nutzer oder Gruppe .....	39
3.6.7	Schreibrecht für einen Nutzer oder Gruppe .....	39
3.6.8	Vollzugriff für einen Nutzer oder Gruppe.....	39
3.6.9	Erweiterte Dateirechte für komplexere Dateirechte.....	40
3.6.10	Vollzugriff für die Gruppe Administratoren .....	41
3.6.11	Dokumente Verwalten für die Gruppe Ersteller-Besitzer .....	41
3.6.12	Lokale Benutzerverwaltung in der Computerverwaltung .....	42
3.6.13	Mitglieder der lokalen Gruppe Benutzer mit der vordefinierten Gruppe ads\Domänen- Benutzer .....	42
3.6.14	Mitglieder der lokalen Gruppe Benutzer mit einer explizit hinzugefügten Gruppe.....	43
3.7.1	Verbinden mit nas.ads.mwn.de über Start - Ausführen .....	43
3.7.2	Anmeldedialog .....	44
3.7.3	Sichtbare Freigaben auf nas.ads.mwn.de .....	44
3.7.4	Netzlaufwerk verbinden .....	45
3.7.5	Hinterlegen der Zugangsdaten für den Zugriff auf die Ablage.....	46
3.7.6	Windows-Anmeldedialog.....	46
3.8.1	Verfügbare Snapshots für einen Ordner.....	47
3.8.2	Inhalt eines Snapshots im Explorer angezeigt.....	47

# 1 Einleitung und Übersicht

Das LRZ betreibt für das MWN ein Active Directory (AD) auf Basis von Windows Server 2008. Das Active Directory stellt Benutzerauthentifizierung und Autorisierung für verschiedene an das Active Directory angeschlossene Dienste bereit. Dies umfasst momentan in erster Linie den Fileservice „Storage für die Wissenschaft“, Exchange als Groupware und Clientmanagement für Windows Betriebssysteme.

Dabei wurde das Active Directory so strukturiert um eine delegierte Verwaltung von einzelnen Einheiten, meist auf Lehrstuhlbasis, zu ermöglichen. Benannte sog. Teiladmins haben dabei die Möglichkeit für ihre Teilbereiche Arbeiten des täglichen Administrationsbedarfes zu erledigen. Dies umfasst das Verwalten des Storage, wie das Anlegen einer Dateistruktur und die Vergabe von Rechten auf diese, das Anlegen von Gruppen um Berechtigungsmodelle auf Ressourcen anzuwenden oder Rechner in das Active Directory aufzunehmen und über Gruppenrichtlinien oder Loginskripte zu verwalten.

Dabei wurde darauf geachtet den Teiladmins einen möglichst hohen Grad an Rechten zu gewähren und die Einschränkungen durch die fehlende herstellerseitige Mandantenfähigkeit des Active Directory möglichst gering zu halten. Es soll die Möglichkeit geschaffen werden auch kleineren Einheiten im MWN eine zentrale Administration ihrer Ressourcen zu ermöglichen ohne den Overhead selbst ein Active Directory zu betreiben. Dadurch kann bei den Teileinheiten Geld und Arbeitszeit eingespart werden und ein höherwertiger Service in Verbindung mit einer höheren Verfügbarkeit erbracht werden.

Ziel dieses Handbuches ist es den Teiladmins eine Übersicht über die Möglichkeiten in der Domäne ads.mwn.de zu geben, mit einfachen Howto-Anleitungen bei den alltäglichen Tätigkeiten zu unterstützen und Hinweise auf Best Practice Methoden zu vermitteln. Abschließend finden sich noch häufig gestellte Fragen, die sich aus dem Pilotbetrieb mit mehreren Teiladmins der letzten Monate ergaben.

## 1.1 Häufig verwendete Begriffe und Abkürzungen

AD – Active Directory	Als Active Directory wird der Verzeichnisdienst von Microsoft bezeichnet. Er dient dazu das Netzwerk zu gliedern und verschiedene Objekte wie Rechner, Benutzer, Gruppen, Ressourcen zu verwalten. Dabei kann der Zugriff über Rechte gesteuert werden
OU – Organisationseinheit	Ein Einheit um ein Active Directory zu strukturieren und Objekte wie Computer zu gruppieren. Durch diese Gruppierung können gezielt Rechte vergeben werden.
GPO – Gruppenrichtlinien	Ein Bündel aus Regeln das auf einzelne Nutzer oder Computer angewandt werden kann um bestimmte Einstellungen am Rechner oder für einen Nutzer vorzunehmen. Darin können enthalten sein Loginskripte,

	Desktopeinstellungen, SW-Verteilung, Registry-Einstellungen und Sicherheits-Einstellungen
Ads.mwn.de	DNS-Name der Active Directory Domäne am LRZ
Nas.ads.mwn.de	DNS-Name des Online-Speichers
LRZ-Kennung	Eine 7-stellige, alphanumerische Benutzerkennung, die vom LRZ verwaltet und von TUMonline vergeben wird. Diese Kennung bleibt lebenslang erhalten. Die eigene LRZ-Kennung können TUM-Benutzer im MyTUM-Portal unter „persönliche Einstellungen“ nachschauen. Für den Zugriff auf die Dateidienste können (derzeit) keine bestehenden Kennungen aus separat beantragten LRZ-Projekten verwendet werden: es ist stets die im MyTUM-Portal bzw. TUMonline hinterlegte LRZ-Kennung nötig.
Münchner Wissenschaftsnetz (MWN)	Das MWN bezeichnet das gesamte vom LRZ betriebene Netz an der TUM, der LMU sowie weiteren Hochschul- und Forschungseinrichtungen.
CIO - Chief Information Officer	Leiter für Informationstechnologie an der TUM
IO - Information Officer	Verantwortliche für Information und Kommunikation aus den einzelnen Einrichtungen/Fakultäten der TUM
ADUC	Kurzbezeichnung für das Verwaltungstool Active Directory-Benutzer und –Computer um Objekte im Active Directory zu verwalten. Dieses Tool ist auf den Managementservern vorinstalliert.
TUMonline	TUMonline ( <a href="http://campus.tum.de">http://campus.tum.de</a> ) ist das Campus Management System der TUM. Es dient unter anderem auch Identitymanagement System. Dort können die Benutzer ihre Passwörter setzen. Außerdem gibt TUMonline die AD-Namen vorgegeben.

## 1.2 Support

Bei Fragen und Problemen kann der IT-Service Desk der TU München kontaktiert werden.

E-Mail: [it-support@tum.de](mailto:it-support@tum.de)

Telefon: 089-28917123

WWW: <http://portal.mytum.de/iuk/service/servicedesk/support/>

## 1.3 Sprache

In diesem Handbuch haben wir uns generell um geschlechtsneutrale Formulierungen bemüht. An Stellen, an denen aus Gründen besserer Lesbarkeit das generische Maskulinum zu finden ist, sind selbstverständlich stets Frauen und Männer gleichermaßen gemeint.

## 2 Allgemeine Beschreibung der Domäne ADS.MWN.de und deren Möglichkeiten

Das Active Directory ADS.MWN.DE für das MWN wurde für mehrere voneinander unabhängige Mandanten angelegt. Um diese voneinander zu trennen und einzelne Managementaufgaben an Teiladmins zu delegieren, mussten einige grundlegende Anpassungen am Active Directory vorgenommen werden. Daraus ergaben sich ein paar Einschränkungen, die man als vollwertiger Domänen-Admin nicht gewohnt ist. Auf den nächsten Seiten soll auf die Einschränkungen, aber auch auf die Möglichkeiten bei der Administration eingegangen werden.

### 2.1 Teiladmin

Als Teiladmin werden Kennungen bezeichnet, die für die Verwaltung einer Teilstruktur im Active Directory verantwortlich sind. Es gibt Teiladmins für einzelne Einrichtungen/Lehrstühle/Fachgebiete und Teiladmins auf Fakultätsebene, sog. Fakultätsadmins. Letztere können in den untergeordneten Einrichtungen/Lehrstühlen/Fachgebieten der Fakultät alle Teilaufgaben erledigen. Ein Teiladmin für eine Struktur wird vom jeweiligen IO (Information Officer) der Fakultät bestimmt. Um Teiladmin zu werden richtet man eine Anfrage an den IT-Support ([it-support@tum.de](mailto:it-support@tum.de)) der TUM mit folgenden Daten:

- Vorname, Nachname
- email-Adresse
- Telefonnummer
- zu verwaltende Einheit
- LRZ-Kennung

Der IT-Support leitet die Anfrage an den IO der Fakultät weiter, der dann den Antrag genehmigen muss. Danach erhalten Sie eine Bestätigungsmail vom LRZ mit den Zugangsdaten.

### 2.2 Namenskonzept

Im Active Directory müssen Objekte wie Rechner, Gruppen oder Nutzer eindeutige Namen haben. Um dies zu gewährleisten wurde ein Namenskonzept erarbeitet, welches für alle Einrichtungen, die das Active Directory nutzen wollen, bindend ist. Bei nicht Einhaltung des Namenskonzept, kann es zu zwangsweisen Umebenennungen von Seiten des LRZ kommen.

Eine ausführliche Dokumentation findet man in der Beschreibung AD-Namenskonzept unter [http://portal.mytum.de/iuk/service/dokumentation/index\\_html](http://portal.mytum.de/iuk/service/dokumentation/index_html).

Ein paar Kurzbeispiele für die Einheit TU (Mandant TUM), AR (Fakultät Architektur), L01 (Lehrstuhl 1):

Computerkonto	TUARL01-Computer1
Gruppe	TUARL01GF-Mitarb
Service-Kennung	TUARL01L0-SRV
Gruppenrichtlinie	TUARL01P0-Pool

## 2.3 Benutzerverwaltung

Jeder Mitarbeiter, Student oder Gast der TUM hat eine LRZ-Kennung und kann mit dieser die Dienste im Active Directory nutzen. Die LRZ-Kennungen werden über TUMonline verwaltet. Das Active Directory ist nur ein Endsystem und ist über Connectoren an die zentrale Benutzerverwaltung angebunden. Sämtliche Änderungen an den Nutzerobjekten wie Passwörter, Vornamen, Nachnamen, Email-Adressen erfolgen ausschließlich durch das übergeordnete Directory. Die Teiladmins können an den LRZ-Kennungen der Nutzer keine Änderungen wie Profilpfade oder Passwortänderungen vornehmen.

## 2.4 Verwaltungswerkzeuge

### 2.4.1 Management-Server

Für die Administration von Gruppen und das Setzen von Rechten gibt es in der Domäne zwei Terminalserver (Win 2003 und Win 2008). Auf diesen Maschinen sind die entsprechenden Tools für die AD-Verwaltung vorhanden, sodass Sie unabhängig von Ihrem Betriebssystem oder Standort jederzeit Zugriff auf eine funktionierende Verwaltungsumgebung haben.

Sie können sich auf den Maschinen mit einer Teiladmin-Kennung (z.B. TUARFARL0-Admin0) und einem RDP-Client anmelden.

Namen der Managementserver:

Badwlrz-swmgmt1.ads.mwn.de (Win 2003)

Badwlrz-swmgmt2.ads.mwn.de (Win 2008)

RDP-Clients gibt es auch für andere Plattformen:

Linux: <http://www.rdesktop.org/>

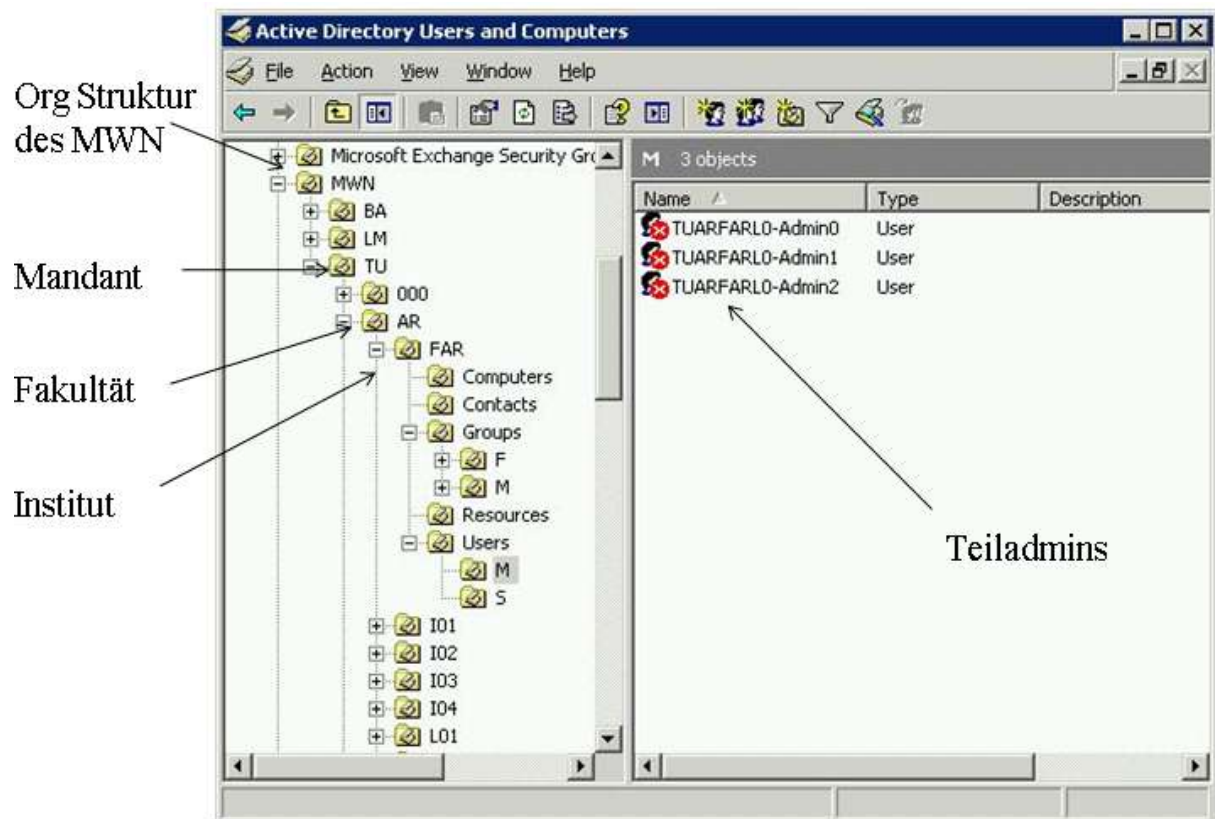
Apple: <http://www.microsoft.com/mac/products/remote-desktop/default.msp>

### 2.4.2 Admin-Pak:

Es gibt auch die Möglichkeit selbst die nötigen Verwaltungswerkzeuge auf einem Windowsclient im MWN zu installieren. Für Windows XP und Windows 2003 verwendet man das Windows Server 2003 Administration Tools Pack. Die Microsoft Remoteserver-Verwaltungstools sind für Windows Vista nötig. Die aktuellen Tools können von der Microsoft Homepage runtergeladen werden oder vom Verzeichnis \\ads.mwn.de\NETLOGON\Tools\Verwaltungstools kopiert werden.

## 2.5 Definition der Teilbereiche im AD

Die Struktur aus Fakultäten und Lehrstühlen der TUM ist im Active Directory nachgebildet. Es gibt die zwei Verwaltungsebenen Fakultät und Institut/Lehrstuhl.



2.5.1 Übersicht über die Domäne ads.mwn.de

### Fakultät:

Jede Fakultät hat eine Fakultäts OU mit dem Kürzel F und dem Fakultätskürzel (z.B. FEI für die Elektrotechnik). Vom jeweiligen IO der Fakultät werden sogenannte Fakultätsadmins festgelegt. Diese haben unterhalb der Fakultät Berechtigungen, um die darunter liegenden Lehrstuhl OUs und den entsprechenden Ablagebereich auf dem NAS-Filer zu verwalten. Über eine Webschnittstelle können auch die Quotas der einzelnen Lehrstühle von den Fakultätsadmins angepaßt werden.

### Institut/Lehrstuhl:

In der Lehrstuhlebene sind integriert Dekanate, Department, Fachschaften und Institute. Der Name der jeweiligen OU ergibt sich aus dem Namenskonzept. Die Namen der einzelnen Lehrstuhl OU sowie der beschreibende Name werden vom jeweiligen IO der Fakultäten in Abstimmung mit den Lehrstühlen festgelegt (siehe auch Namenskonzept). Kurzfristig wird eine Einheit der im Organisationsbaum von TUMonline verwendeten OU Namen und den Namen im Active Directory angestrebt. Die Definition von Organisationseinheiten innerhalb von TUMonline erfolgt zentral.

Die Verwaltung der AD-Struktur wird an die Lehrstühle delegiert. Für jeden Lehrstuhl gibt es eine festgelegte Admin-Gruppe, die die notwendigen Aufgaben innerhalb des Active Directory und zur Verwaltung von in die Domäne integrierten Clients erfüllen kann. Es ist

aber auch möglich und erwünscht, dass ein Lehrstuhl diese Aufgaben nach oben an die Fakultät abtritt oder an einen anderen Lehrstuhl aus der Fakultät übergibt.

Unterhalb jeder Lehrstuhl OU wird eine OU-Struktur zentral vorgegeben, die teilweise von den jeweiligen Teiladmins (Fakultäts- und Lehrstuhladmins) erweitert werden kann.

#### -OU=Lehrstuhl

##### -OU=Computers

OU dient zur Verwaltung der Computerkonten des Lehrstuhls oder der Fakultät. Die Namen der Computer müssen dem Namenskonzept entsprechen. Für die OU können Gruppenrichtlinien definiert werden, die dann für die Computer unterhalb dieser OU gelten.

Zur Strukturierung von Computeraccounts können weitere OUs unterhalb von „Computers“ angelegt werden. Die Struktur ist möglichst flach zu halten (<= 3 Ebenen).

Rechte der Teiladmins:

- Hinzufügen von Computern z.Bsp: TUARL01-WAP01
- Erstellen von OUs
- Erstellen von Gruppenrichtlinien z. Bsp TUARL01PO-WAP

#### -OU=Contacts

OU dient als Speicher für die Kontakte, die für Exchange benötigt werden.

Rechte der Teiladmins:

- keine

#### -OU=Groups

OU für die Gruppen

Gruppen werden verwendet um Rechte auf Ressourcen zu vergeben.

Gruppen können auch als Mailverteiler verwendet werden.

Es gibt vorgegebene und freie Gruppen, entsprechend dem Namenskonzept.

Unterhalb von Groups gibt es zwei weitere OUs:

##### -OU=F (free, frei)

ADS-interne Systemgruppen, individuell

Rechte der Teiladmins:

- Anlegen und löschen von Gruppen z.Bsp: TUARFARGF-HIWI
- Ändern von Gruppenmitgliedschaften

##### -OU=M (mandatory, verpflichtend)

ADS-interne Systemgruppen, vorgegeben

Rechte der Teiladmins:

- keine

-OU=Ressources

OU für Ressourcen von Exchange wie z.B. Räume

Rechte der Teiladmins:

-keine

-OU=Users

OU für Benutzer

Teiladmin kann eigene Benutzer anlegen nach dem Namenskonzept.

Diese Benutzer dienen nur der lokalen Verwaltung von Objekten.

**Reguläre Benutzer sind über die zentrale Benutzerverwaltung zu erzeugen. Keine eigene Gästeverwaltung!**

-OU=S (Services)

Benutzerobjekte für Systemdienste z. Bsp: TUARL22L0-MSSQL

Rechte der Teiladmins:

-Anlegen und löschen von Serviceaccounts

z. Bsp: TUARL22L0-MYSQL

-OU=M (Mandatory, verpflichtend)

Benutzerobjekte für Managementaufgaben

Rechte der Teiladmins:

-keine

### 2.5.1 Gruppenverwaltung (momentan offen)

Eine Gruppenverwaltung (in TUMonline) ist in Planung. Bis dahin müssen die Teiladmins ihre Gruppen selbst in ADUC anlegen und dann befüllen. Wie sie Gruppen anlegen und Rechte auf Ressourcen vergeben, finden sie im Kapitel 3.6 Vergaben von Rechten auf Ressourcen in der Domäne ads.mwn.de.

### 2.5.2 Gruppenrichtlinien

Die Teiladmingruppe kann innerhalb der OU Computers Gruppenrichtlinien anlegen und verwalten. Die Richtlinien dienen der Verwaltung von Computern und an den Rechnern angemeldeten Usern. Es können Start- und Loginskripte oder eigene administrative Vorlagen hinterlegt werden.

Aufgrund des AD-Designs liegen alle Benutzer in einer OU und somit können Gruppenrichtlinien nicht direkt auf das Benutzerobjekt angewendet werden. Um trotzdem die Rechte von Benutzern zu steuern ist die Benutzung der Loopback-Gruppenrichtlinie notwendig. Mit dieser Richtlinie ist es möglich, Gruppenrichtlinien auch auf Benutzerobjekte

anzuwenden, die nicht in der gleichen OU liegen wie die Gruppenrichtlinie. Sehen sie hierzu auch die Anmerkungen im Kapitel 3.3.3 Besonderheiten in der Domäne ads.mwn.de.

### **2.5.3 Systemmanagement**

Momentan unterstützte OS-Versionen:

Windows: Win 2000, XP Prof, 2003, 2008, Vista Business, Enterprise, Ultimate, Windows 7

MAC: OS X

Linux: auf Anfrage

Der Rechnername im Active Directory ist eindeutig. Um Namenskonflikte zu vermeiden muss der Rechnername gemäß dem Namenskonzept gewählt werden (Beispiel: TUARL01-Pool1). Eine sprechende Beschreibung des Computerobjekts im Active Directory wird empfohlen.

Eine Anleitung zur Integration von Rechnern in die Domäne finden sie im Kapitel 3.1 Aufnahme von Windows Rechnern in die Domäne ads.mwn.de.

### **2.5.4 Benutzer**

Die Anmeldung an einem Rechner erfolgt über die siebenstellige LRZ-Kennung. Die Anmeldedomäne ist ADS.

#### **2.5.4.1 Passwortänderung**

Die Änderung des Passwortes eines einzelnen Benutzerobjektes erfolgt über TUMonline und wird dann über IntegraTUM in das Active Directory synchronisiert. Kennungen, die von den Teiladministratoren angelegt werden und zur Verwaltung des Active Directory dienen, müssen über die Windowstools verwaltet werden.

#### **2.5.4.2 Belegte Benutzerattribute**

Am Benutzerobjekt werden momentan die folgenden Attribute über Synchronisation mit dem IntegraTUM gesetzt und können von jedem Benutzer des jeweiligen Mandanten ausgelesen werden:

1. LRZ-Kennung
2. Vorname
3. Nachname
4. email-Adresse
5. Org-Zugehörigkeiten

### **2.5.5 Anbindung des Storage NAS.ads.mwn.de**

Das LRZ bietet den Nutzern und Einrichtungen des ADS.MWN.DE die Nutzung eines zentralen hochverfügbaren Speichersystems. Das Speichersystem verwendet das CIFS-Protokoll und unterstützt die Betriebssysteme Windows, Linux/Unix sowie Mac OS X.

### **2.5.5.1 Persönliches Verzeichnis**

Alle im Active Directory eingerichteten Studierenden, Mitarbeiter und Gäste verfügen über einen persönlichen Speicherplatz für die Ablage von Dokumenten. Diese Ablage umfasst pro Benutzer momentan eine Kapazität von derzeit 10 GB in maximal 30.000 Dateien. Auf diesen persönlichen Bereich können nur die Besitzer selbst zugreifen. Der Zugriff erfolgt über den UNC-Pfad <\\nas.ads.mwn.de\<LRZ-Kennung>>, also z.B. <\\nas.ads.mwn.de\zi99>zuv.

### **2.5.5.2 Projektverzeichnis**

Fakultäten, Lehrstühle sowie andere Einrichtungen können gemeinsame Dateiablagen in Abstimmung mit den IOs einrichten lassen. Hier sind größere Speicherkapazitäten möglich und die Zugriffsrechte können feingranular vergeben werden. Die Einzelquotas für die Einrichtungen unterhalb einer Fakultät haben eine Startquota von 50 GB und werden vom jeweiligen Fakultätsadmin nach Genehmigung durch den IO der Fakultät verwaltet. Bei Änderungswünschen wenden sie sich bitte an den IT-Service-Desk. Der UNC-Pfad für die Ablage lautet <\\nas.ads.mwn.de\<EinrichtungsPräfix>>\$, also z.B. <\\nas.ads.mwn.de\tuarfar>\$.

### **2.5.5.3 Temporäres Ablageverzeichnis**

Für einen schnellen und unkomplizierten Datenaustausch mit anderen Teilnehmern im MWN-AD kann ein temporärer Ablagebereich genutzt werden. Dateien in dieser Ablage werden über eine Gleitlöschung nach zwei Tagen ohne Zugriff gelöscht. Die temporäre Ablage kann über den UNC-Pfad <\\nas.ads.mwn.de\mwntemp> angesprochen werden.

### **2.5.5.4 Backup-Snapshots**

Als eine besondere Funktion des Speichers ist die Snapshotfunktion zu sehen. Diese Snapshots fungieren als Backups des Ablagesystems und ermöglichen es dem Nutzer selbstständig ohne zu tun des Administrators Dateien wiederherzustellen. Die Snapshots reichen maximal vier Wochen zurück. Eine Anleitung findet sich im Kapitel 3.8 Wiederherstellung von Dateien auf nas.ads.mwn.de über Snapshots.

Weiterführende Informationen zum Speicher für die Wissenschaft finden Sie im Benutzerhandbuch zentraler Speicher unter [http://portal.mytum.de/iuk/service/dokumentation/index\\_html](http://portal.mytum.de/iuk/service/dokumentation/index_html)

### **2.5.5.5 Erreichbarkeit**

Auf den zentralen Speicher kann innerhalb des MWN über das SMB-Protokoll zugegriffen werden. Außerhalb des MWN ist dafür der Aufbau einer VPN-Verbindung notwendig. Zusätzlich gibt für den Zugriff ohne VPN-Verbindung die Möglichkeit über Web zu zugreifen. Dafür wird vom LRZ eine Weboberfläche zur Verfügung gestellt die unter der URL: <https://webdisk.ads.mwn.de> erreichbar ist. Eine Anmeldung erfolgt mit der LRZ-Kennung.

## **2.5.6 Laufwerksbuchstaben Konzept für Windows**

Um eine einheitliche Sprache innerhalb der Mandanten zu sprechen und damit eine einfachere Fehlerverfolgung für den Service-Desk zu erreichen, soll ein Laufwerksbuchstaben-Konzept für die Netzlaufwerke umgesetzt werden. Ein Vorschlag ist:

Laufwerksbuchstabe	Verwendung
H:	Persönliches Laufwerk des Nutzers
I:	Fakultät
T:	Temporäres Laufwerk der Uni und der Fakultäten

Alle weiteren Laufwerksbuchstaben sind frei.

## 2.5.7 Benutzerprofile

Für die Verwendung von Benutzerprofilen unter Windows sind drei Szenarien möglich.

### 2.5.7.1 Keine servergespeicherten Profile

Sollen keine servergespeicherten Profile verwendet werden, kann über Gruppenrichtlinien die Verwendung blockiert werden. Dies ist die Standardeinstellung bei allen Gruppenrichtlinien. Sollen servergespeicherte Profile verwendet werden, muss dieses über eine Gruppenrichtlinie wieder aktiviert werden.

### 2.5.7.2 Mandatory Profile

Soll ein Benutzer immer wieder ein vordefiniertes Profil verwenden, dessen Veränderungen beim Abmelden verworfen werden, dann verwendet man Mandatory Profiles. Die Zuordnung des Profils zum Nutzer wird über eine Umgebungsvariable `manprof` erreicht, die auf einem Ablageort an einem freiwählbaren Server liegt. Der Wert `manprof` ist der Default-Wert für das Attribut `Profilpfad` bei allen LRZ-Kennungen. Eine Anleitung findet sich im Kapitel 3.5 *Verwendung von Mandatory Profiles in der Domäne ads.mwn.de*.

### 2.5.7.3 Roaming Profile

Momentan werden Roaming Profile nicht in vollem Umfang unterstützt. Für Roaming Profiles müssen am Nutzerobjekt individuell Benutzerpfade eingestellt werden. Dies lässt sich aber aufgrund der zentralen Nutzerverwaltung nicht bewerkstelligen. Stattdessen ist wie bereits schon erwähnt eine Standardvariable `%manprof%` hinterlegt. Es ist möglich durch die Verwendung der `manprof` Variable Roaming Profile unter Windows XP für einen Benutzer pro Maschine einzustellen. Seit Vista ist es auch möglich über Gruppenrichtlinien allgemeine Pfade für servergespeicherte Profile anzugeben.

## 3 Howtos

### 3.1 Aufnahme von Windows Rechnern in die Domäne ads.mwn.de

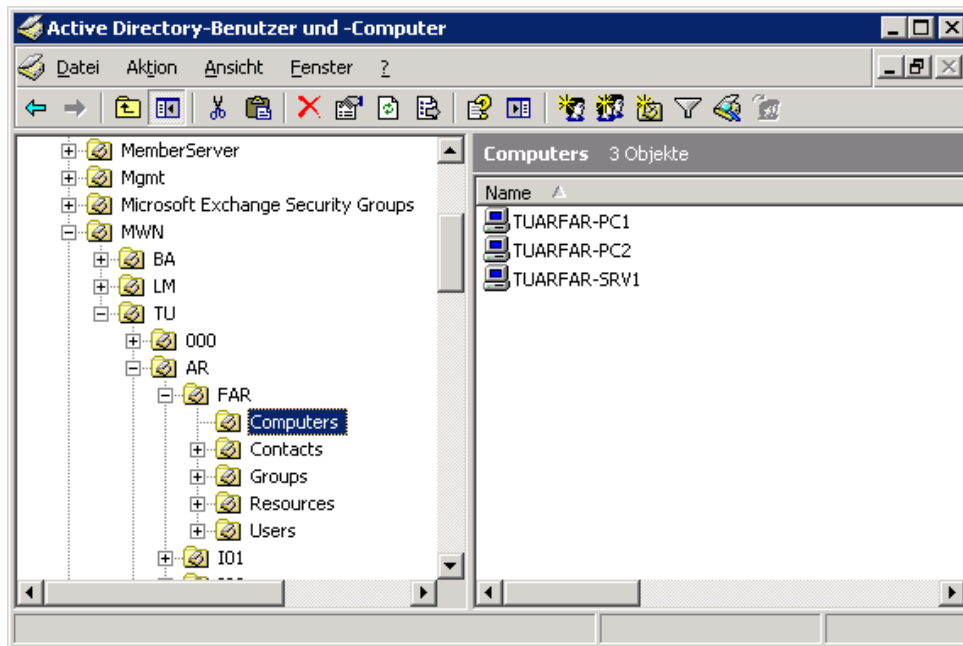
#### **Sinnvoller Einsatz:**

Durch die Aufnahme von Rechnern ergeben sich verschiedene Vorteile im Betrieb und in der Verwaltung von Rechnern:

- Nutzung von zentralen Gruppenrichtlinien über das Active Directory und damit einfachere Verwaltung von Systemeinstellungen an den einzelnen Rechnern
  
- Nutzung von An/Abmeldeskripten zum Verbinden von Ressourcen wie Dateiablagen oder Druckern
  
- Ausnutzung der zentralen Benutzerverwaltung
  
- Zugriffssteuerung auf Ressourcen
  
- Single Sign-on, eine Anmeldung um verschiedene zur Verfügung gestellte Ressourcen zu nutzen
  
- Anbindung von Servern als Memberserver in die Domäne um dezentral Dienste wie Druckerserver, Lizenz- oder Applikationsserver bereit zu stellen

#### **Schritt für Schritt Anleitung:**

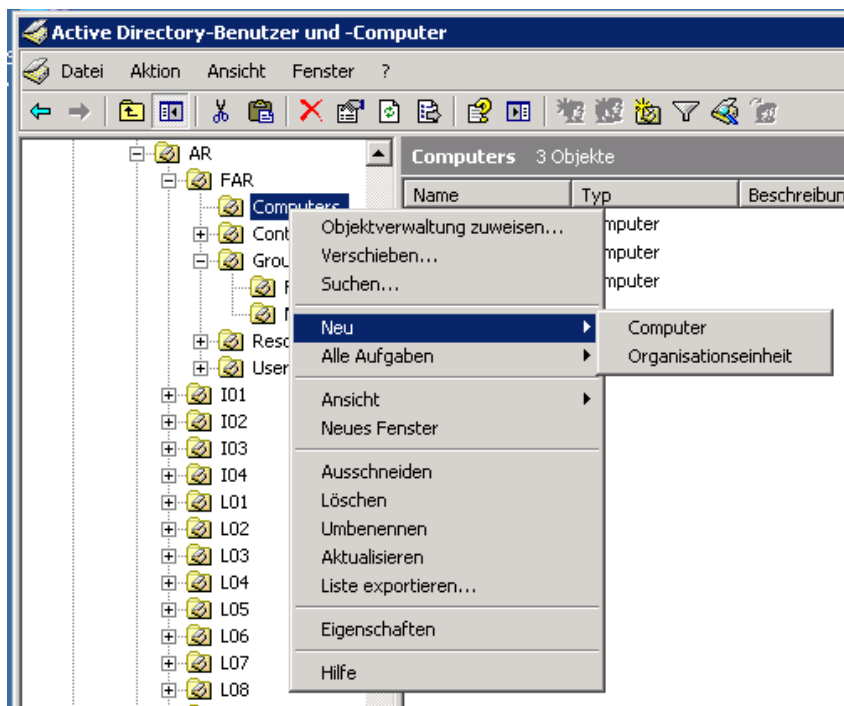
Aufgrund des Delegationskonzepts der Domäne ads.mwn.de ist es nicht wie üblich möglich einen Rechner einfach nur über die Systemsteuerung in die Domäne aufzunehmen. Bei diesem Verfahren muss der Teiladmin das Recht besitzen ein Computerobjekt in der allgemeinen OU Computers zu erzeugen. In der Domäne ADS ist darum nur eine Aufnahme von Rechnern unterhalb der OU des jeweiligen Teiladmins möglich.



3.1.1 Teilstruktur im Active Directory

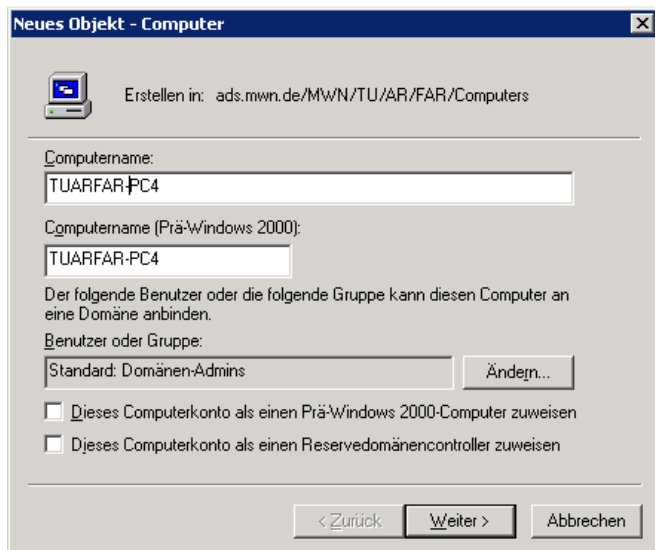
### 3.1.1 Nutzung der grafischen Oberfläche:

Die Aufnahme von Rechnern über die grafische Oberfläche besteht aus zwei Schritten. Im ersten Schritt müssen sie das Computerobjekt im Active Directory erzeugen. Starten sie dazu ADUC - Active Directory-Benutzer und –Computer Tool und wechseln Sie in Ihrem Teillast in die OU Computers. Durch einen Klick mit der rechten Maustaste auf die OU können Sie unter Neu – Computer ein neues Computerobjekt erzeugen.



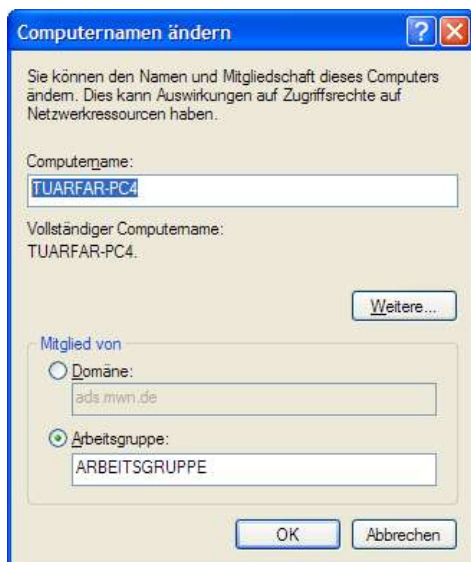
3.1.2 Anlegen eines Computerkontos

Geben Sie in dem Dialogfeld den Rechnernamen mit dem passenden Präfix für Ihre Organisation ein. Und schließen Sie danach den Assistenten ab.



### 3.1.3 Vergeben eines Computernamens

Im zweiten Schritt wechseln sie nun an den Rechner, den Sie in die Domäne aufnehmen wollen. Zunächst muss der Rechnername der Maschine an den Rechnernamen in der Domäne angepasst werden. Wechseln Sie dazu in die Systemsteuerung – System – Computername – Ändern. Im Dialogfenster Computernamen ändern passen sie nun den Rechnernamen dem Namen im Active Directory an. Groß- und Kleinschreibung ist dabei irrelevant. Nach Abschluss muss der Rechner gebootet werden. Der Neustart ist notwendig vor dem nächsten Schritt.



### 3.1.4 Ändern eines Rechnernamens

Nach dem Neustart wechseln Sie wieder nach Systemsteuerung – System – Computername – Ändern und ändern nun die Mitgliedschaft auf Domäne und geben den Namen der Domäne ads.mwn.de ein.



3.1.5 Aufnahme in die Domäne ads.mwn.de

Nach dem Bestätigen werden Sie zur Eingabe der Zugangsdaten für den jeweiligen Teiladmin aufgefordert.



3.1.6 Authentifizierung gegenüber der Domäne ads.mwn.de

Bei einer erfolgreichen Authentifizierung werden Sie in der Domäne ads.mwn.de willkommen geheißen. Danach ist noch ein weiterer Neustart notwendig.



3.1.7 Bestätigung der erfolgreichen Aufnahme in die Domäne

Nach dem Neustart können sie sich mit einer LRZ-Kennung am Rechner anmelden. Wollen sie den Rechner in Zukunft mit der Teiladminkennung verwalten, müssen Sie diese noch der lokalen Gruppe der Administratoren hinzufügen wie in Kapitel 3.2 Hinzufügen von Teiladmins zur lokalen Gruppe der Administratoren beschrieben.

### 3.1.2 Kommandozeile/Skript

Etwas einfacher ist die Aufnahme des Rechners über eine Kommandozeile oder per Skript. Über die Kommandozeile nutzen Sie den Befehl netdom. Dazu müssen Sie die Teiladminzugangsberechtigung angeben und den Ort im Active Directory als Distinguished Name in dem das Computerkonto angelegt werden soll.

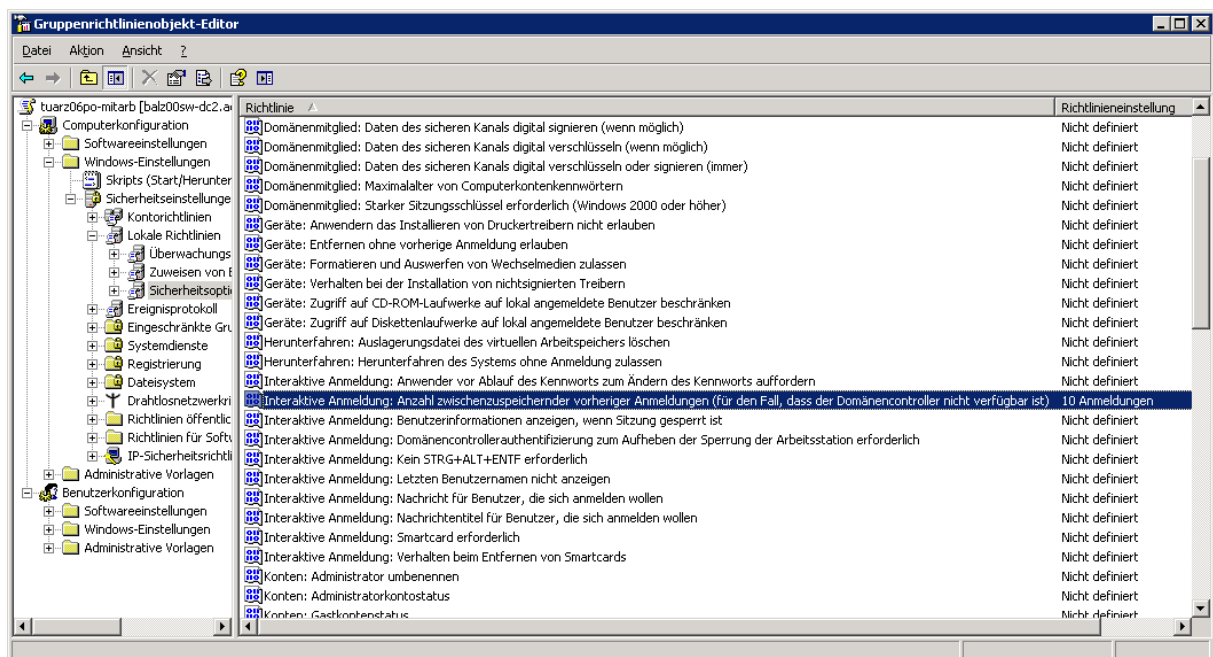
Beispielaufruf für netdom für die Beispieleinheit TUARFAR:

```
netdom join %computername% /domain:ads.mwn.de /userd:TUARFARLO-admin0  
/passwordd:*****  
/OU:OU=Computers,OU=FAR,OU=AR,OU=TU,OU=MWN,DC=ads,DC=mwn,DC=de  
/reboot
```

Alternativ kann natürlich auch ein vbs-Skript verwendet werden. Ein Beispiel kann unter [\\ads.mwn.de\NETLOGON\Scripte\Domänenmitgliedschaft](#) gefunden werden.

### 3.1.3 Notebooks mit zentraler Nutzerverwaltung der Domäne ads.mwn.de

Es ist natürlich auch möglich Notebooks in die Domäne ads.mwn.de aufzunehmen. Dabei gibt es eine Besonderheit zu beachten. Damit ein Nutzer sich auch ohne Verbindung zu der Domäne ads.mwn.de am Notebook mit seiner LRZ-Kennung anmelden kann, muss in den Gruppenrichtlinien eine Sicherheitsoption konfiguriert werden. Sie finden die Option unter Computerkonfiguration – Windows-Einstellungen-Sicherheitseinstellungen-Lokale Richtlinien-Sicherheitsoptionen. Stellen sie für die Option Interaktive Anmeldung: Anzahl zwischenspeichernder vorherige Anmeldungen eine beliebige Anzahl von Anmeldungen ein. Danach muss sich jeder Nutzer, der mit dieser Option arbeiten will, noch einmal an dem Rechner anmelden, damit die Zugangsdaten vom System gecached werden.



3.1.8 Sicherheitsoption für interaktive Anmeldung

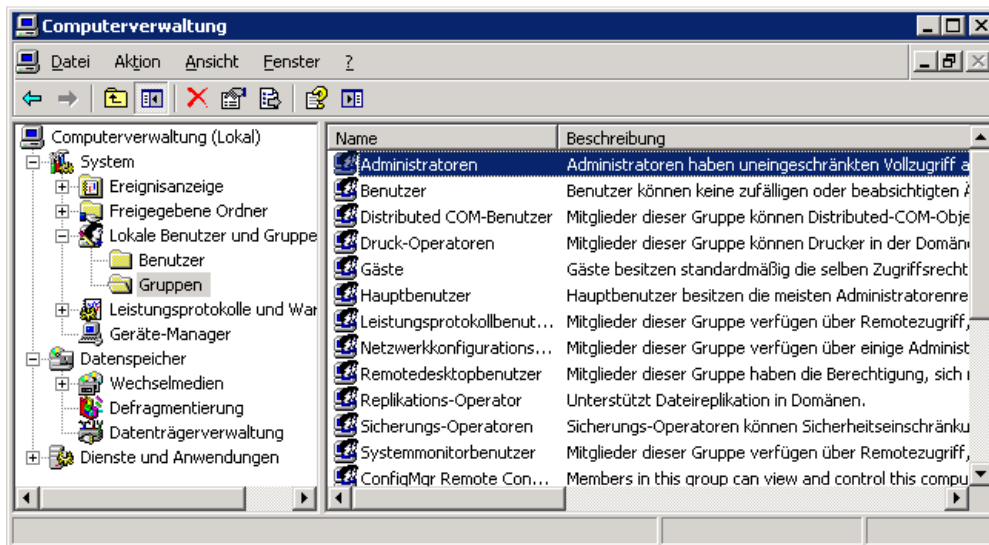
## 3.2 Hinzufügen von Teiladmins zur lokalen Gruppe der Administratoren

### Sinnvoller Einsatz:

Wenn eine Vielzahl von Rechner verwaltet werden soll, ist es einfacher mit einer einzigen Kennung dies zu tun. Diese Kennung sollte nur für die Administration verwendet werden und nicht im Alltagsbetrieb.

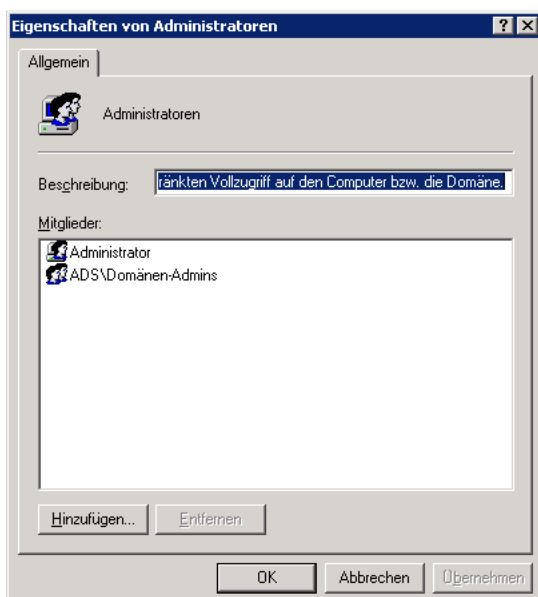
### Schritt für Schritt Anleitung:

Melden sie sich an dem lokalen Rechner mit einem lokalen Administrator an und starten dann die Computerverwaltung. Diese finden sie unter anderem in der Systemsteuerung – Verwaltung.



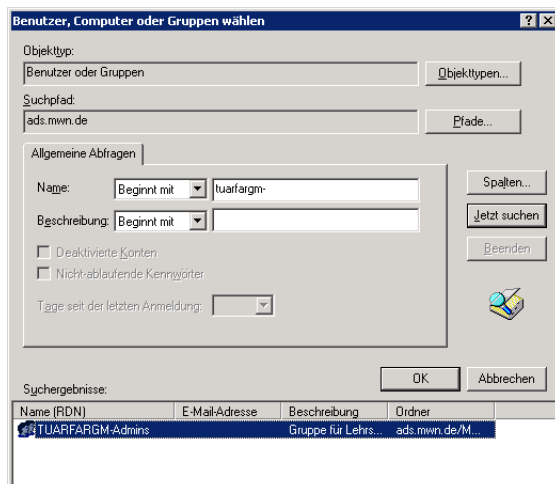
3.2.1 Benutzer und Gruppen in Computerverwaltung

Wechseln sie dann nach System – Lokale Benutzer und Gruppen und wählen dann die Gruppe Administratoren mit einem Doppelklick aus.



3.2.2 Mitglieder der lokalen Gruppe Administratoren

Über hinzufügen können sie dann nach dem gewünschten Benutzer oder Gruppe suchen lassen und danach zur Gruppe der Administratoren hinzufügen.



3.2.3 Suchen von Nutzern und hinzufügen zur Gruppe der Administratoren

## 3.3 Gruppenrichtlinien

### Sinnvolle Verwendung:


Mit Gruppenrichtlinien ist es für einen Teiladministrator möglich verschiedene Einstellungen zentral für die Computer oder Nutzer, die sich an einem Rechner im Active Directory anmelden vor zu nehmen. Solche Einstellungen können sein: Skripte, Steuerung der Benutzeroberfläche oder aber auch Einstellungen, die die Sicherheit des Rechners betreffen. Mit der Veröffentlichung von Windows Vista haben sich die Gruppenrichtlinien verändert darum werden im Folgenden beide Möglichkeiten zum erzeugen und verwalten von Gruppenrichtlinien beschrieben.

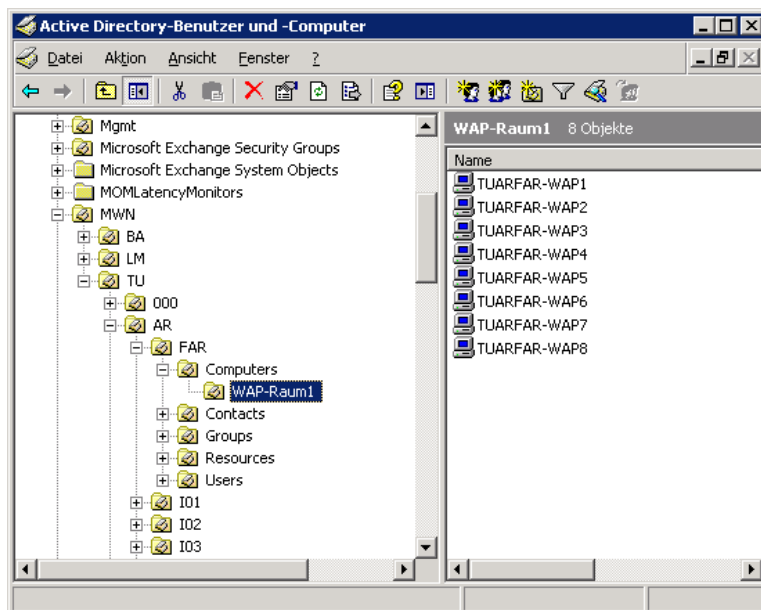
### Allgemeines:

Gruppenrichtlinien können immer nur mit OUs verknüpft sein. In der Domäne ads.mwn.de gibt es noch eine weitere Einschränkung. Sie können Gruppenrichtlinien nur unterhalb der der OU Computers in Ihrem Teilbereich anlegen.

### 3.3.1 Win 2000, XP und 2003

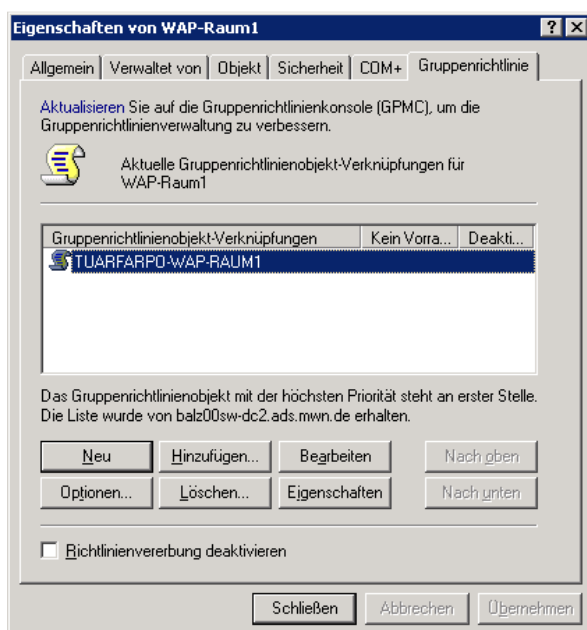
Die Gruppenrichtlinien für Win 2000, XP und 2003 können Sie über den Managementserver BADWLRZ-SWGMT1.ads.mwn.de verwalten. Starten sie dazu das ADUC - Active

Directory-Benutzer und –Computer Tool. Sie finden das Tool als  Verknüpfung auf dem Desktop mit Beschreibung Domäne ads.mwn.de. Wechseln sie zu ihrem Teilbereich im Active Directory.



3.3.1 Ansicht des Teilbaums im Active Directory zur Verwaltung von Computern

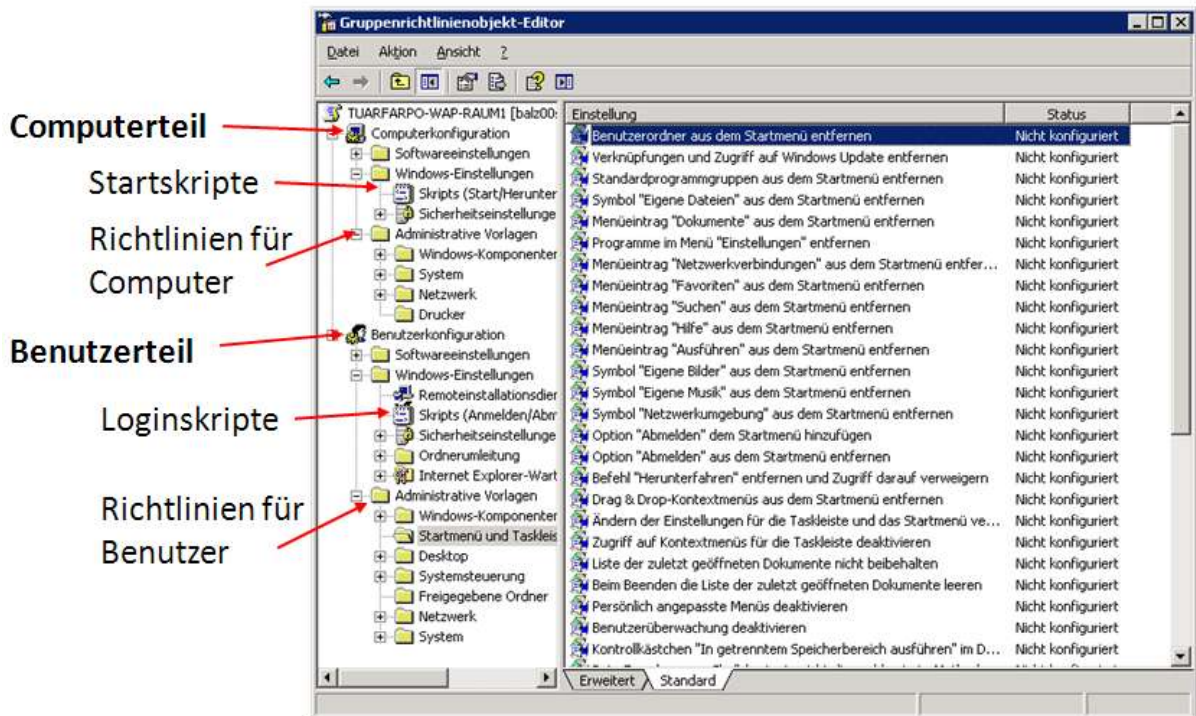
Markieren sie den gewünschten Container und wählen mit der rechten Maustaste im Kontextmenü den Punkt Eigenschaften aus. Wählen Sie dann den Reiter Gruppenrichtlinien.



3.3.2 Maske für die Verwaltung von Gruppenrichtlinien

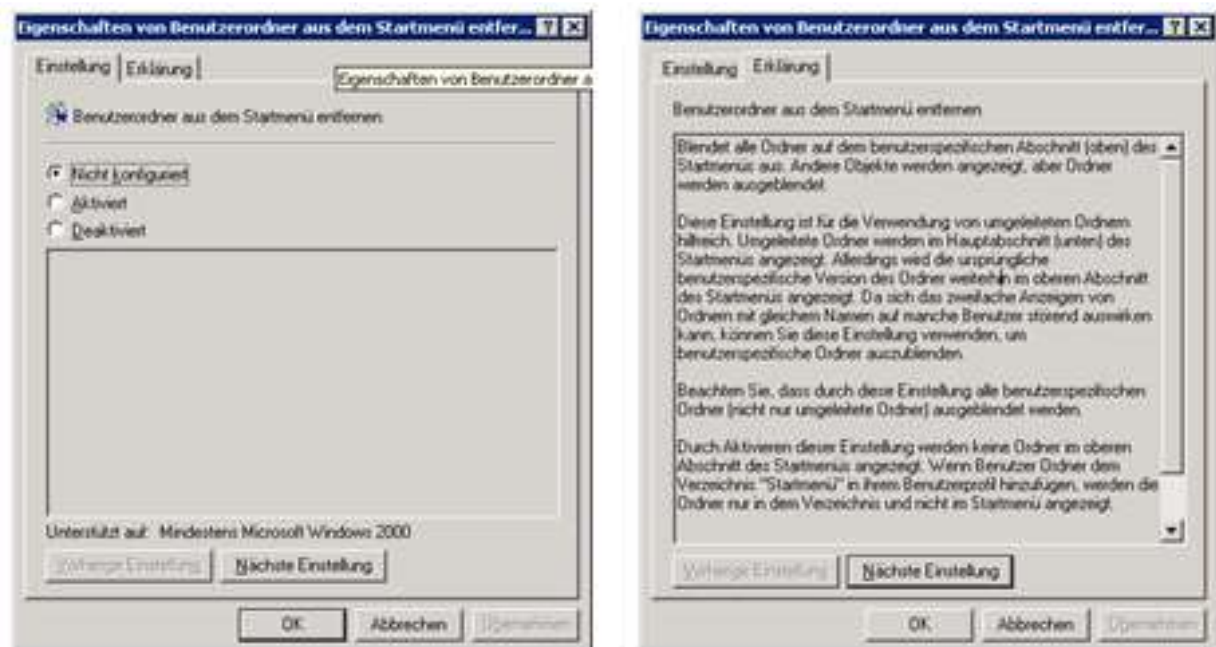
Sie können nun hier über Neu eine Gruppenrichtlinie anlegen und über Bearbeiten sich die Gruppenrichtlinie anzeigen und dann verändern.

Die Gruppenrichtlinien gliedern sich in einen Maschinenteil für den Computer und in einen Benutzerteil für den jeweils angemeldeten Anwender. Je nachdem stehen unterschiedliche Einstellungen zur Verfügung. Die Richtlinien finden sie jeweils unterhalb von Administrativen Vorlagen. Die Konfiguration von Login- und Startskripte finden sie im Kapitel 3.4 Loginskripte in der Domäne ads.mwn.de.



### 3.3.3 Struktur einer Gruppenrichtlinie

Suchen Sie sich die gewünschte Richtlinie raus und mit einem Doppelklick können sie die Einstellungen bearbeiten. Über den Reiter Erklärungen erhalten sie eine ausführliche Erklärung der jeweiligen Richtlinie und deren Auswirkung.



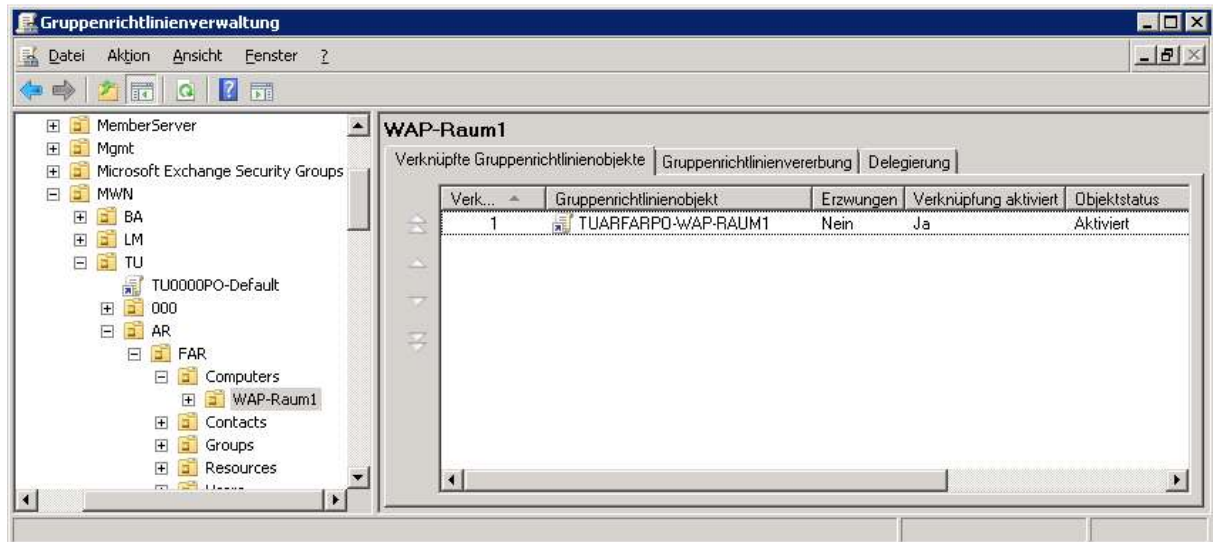
### 3.3.4 Einstellungen und Erklärung einer Gruppenrichtlinie

### 3.3.2 Änderungen ab Vista

Mit dem Release von Windows Vista hat sich die Verwaltung und die Möglichkeiten von Gruppenrichtlinien verändert. Sie können die neuen erweiterten Gruppenrichtlinien über den Managementserver BADWLRZ-SWGMT2.ads.mwn.de verwalten. Auf dem Managementserver finden sie auf dem Desktop eine Verknüpfung Group Policy Management

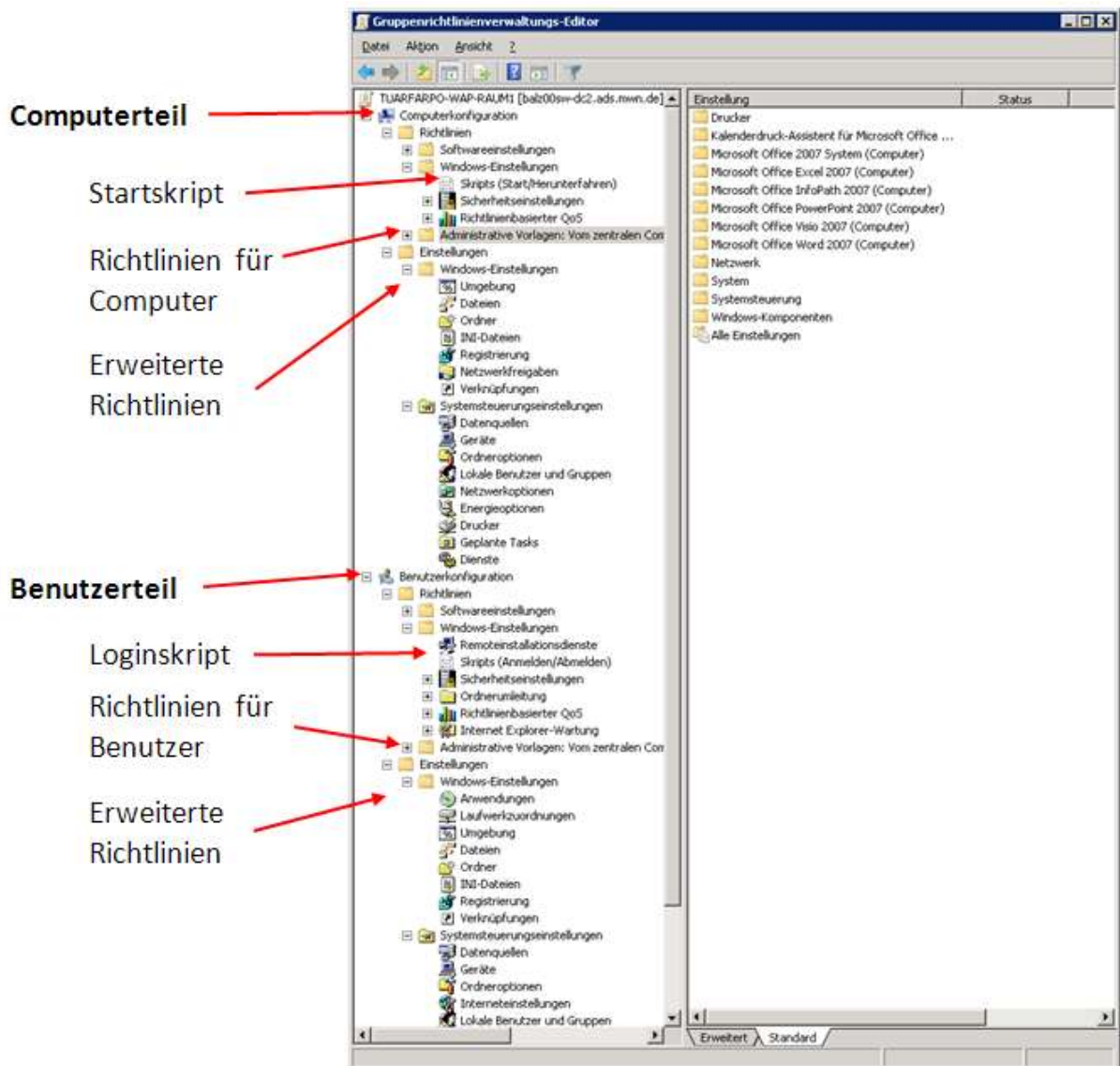


mit der sie die Gruppenrichtlinienverwaltung starten können.



### 3.3.5 Gruppenrichtlinienverwaltung ab Windows Vista

Im linken Teil sehen sie die Struktur des Active Directory. Navigieren sie in die gewünschte OU. Im rechten Teil finden sie dann die Gruppenrichtlinien bzw. können sie über die rechte Maustaste und das Kontextmenü eine neue Gruppenrichtlinie gemäß dem Namenskonzept anlegen oder bearbeiten.



### 3.3.6 Erweiterte Gruppenrichtlinien mit zusätzlichen Einstellungen

Die Gruppenrichtlinien sind wie bereits in 3.3.1 beschrieben in einen Computerteil und in einen Benutzerteil untergliedert. Zusätzlich kommen bei den erweiterten Gruppenrichtlinien die Erweiterten Einstellungen zum Tragen. Mit diesen zusätzlichen Einstellungen haben sie nun die Möglichkeit verschiedene neue Konfigurationen für Benutzer, Registryeinstellungen oder Startmenüeinträge zu verwalten. Die weitere Verwaltung erfolgt analog zu den bisherigen Gruppenrichtlinien.

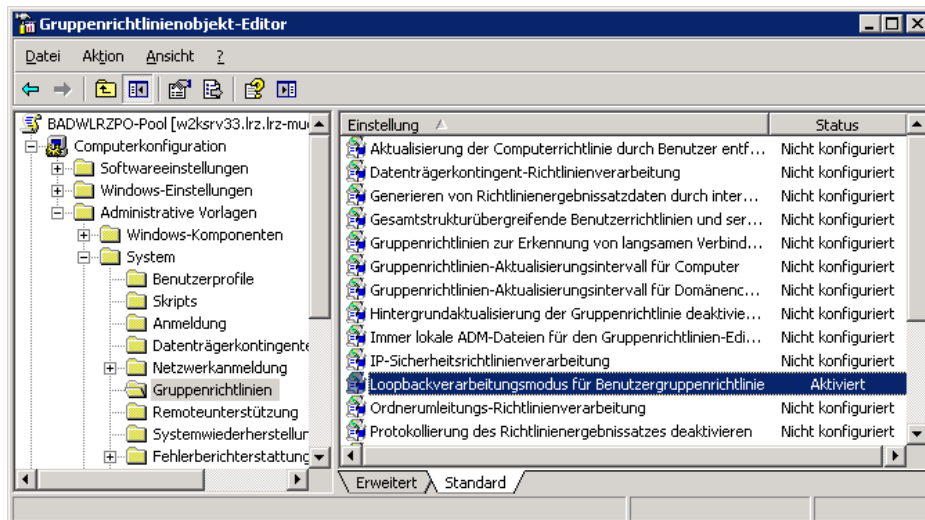
Die erweiterten Einstellungen können von allen Clients ab Vista genutzt werden. Ältere Clients können einen Teil dieser Einstellungen interpretieren, vorausgesetzt es wurde auf dem Client clientseitige Gruppenrichtlinienerweiterungen [MS KB 943729](#) installiert.

### 3.3.3 Besonderheiten in der Domäne ads.mwn.de

#### 3.3.3.1 Loopbackverarbeitungsmodus

Durch die Strukturierung des Active Directories in einen OU für die Nutzer und eine OU für die Teiladministration können Gruppenrichtlinien nicht wie gewohnt auf Benutzerobjekte angewandt werden. Hierzu muss die Loopbackverarbeitungsmodus in den Gruppenrichtlinien

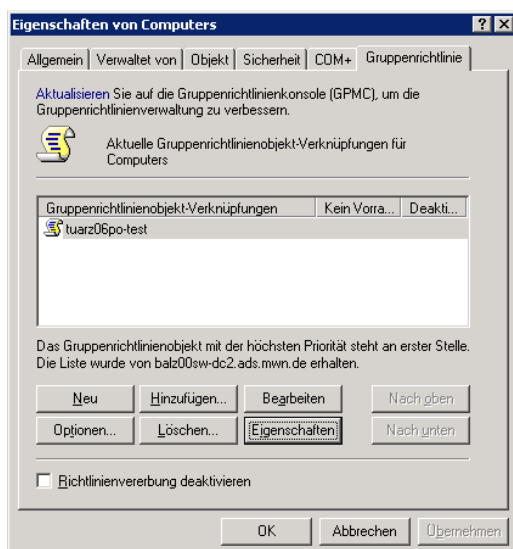
verwendet werden. Sie finden diesen in den Administrativen Vorlagen – System – Gruppenrichtlinien - „Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien“. Durch aktivieren werden die Benutzergruppenrichtlinien für jeden Domänenbenutzer angewandt, der sich an dem Rechner anmelden kann.



3.3.7 Wichtige Gruppenrichtlinie: Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien

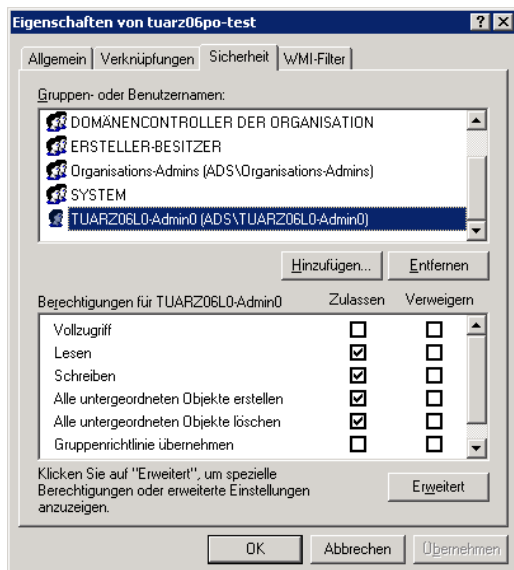
### 3.3.3.2 Rechte auf Gruppenrichtlinien

Soll eine Gruppenrichtlinie für einzelne Nutzer oder Gruppen nicht angewandt werden, können sie die Berechtigungen über Eigenschaften - Sicherheit der jeweiligen Gruppenrichtlinien steuern.



3.3.8 Eigenschaften einer Gruppenrichtlinie

Sie können über Hinzufügen Gruppen oder auch einzelne Nutzer aus dem Active Directory erlauben die Gruppenrichtlinie zu lesen, zu bearbeiten oder zu übernehmen. Wollen Sie verhindern, dass ein Nutzer oder eine Gruppe die Gruppenrichtlinien übernimmt, können sie dieses explizit verweigern. Verweigern schlägt hierbei immer das Recht Zulassen.



3.3.9 Sicherheitskonfiguration einer Gruppenrichtlinie

### 3.3.3.3 Fehlende Rechte auf Gruppenrichtlinien für Teiladmins

Wenn ein Mitglied der Teiladmingruppe eine Gruppenrichtlinie anlegt, bekommt sein Teiladminkonto automatisch das Recht die Gruppenrichtlinie zu bearbeiten wie in der Abbildung 3.3.9 Sicherheitskonfiguration einer Gruppenrichtlinie dargestellt. Die anderen Mitglieder der Teiladmingruppe bekommen das Recht nicht. Sollen diese auch die Gruppenrichtlinie verändern können, muss die Gruppe der Teiladmins explizit berechtigt werden. Dies ist leider eine Einschränkung der delegierten Administration im Active Directory.

## 3.4 Loginskripte in der Domäne ads.mwn.de

### Sinnvoller Einsatz:

Loginskripte können vielfältig in der Rechneradministration verwendet werden. Häufige Verwendung für Skripte ist das Anbinden von Laufwerken oder Druckern bei Nutzern, die Installation von Software, die Anpassung von Benutzern oder Rechnerkonfigurationen, Austausch von Dateien oder Ändern von Registryeinträgen. Mit Skripten können auch komplexere Aufgaben bewerkstelligt werden. Man unterscheidet in:

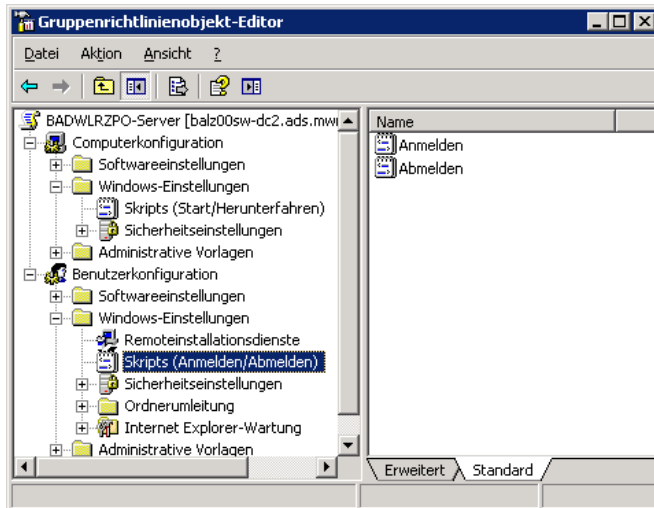
- Computerskripten - laufen im Kontext des Systemaccounts
- Benutzerskripten - laufen im Kontext des angemeldeten Benutzers

Skripte können wahlweise beim Starten oder Herunterfahren des Rechners oder beim An- oder Abmelden eines Nutzers ausgeführt werden. Als Skripte können alle ausführbaren Dateien angegeben werden.

### Schritt für Schritt Anleitung:

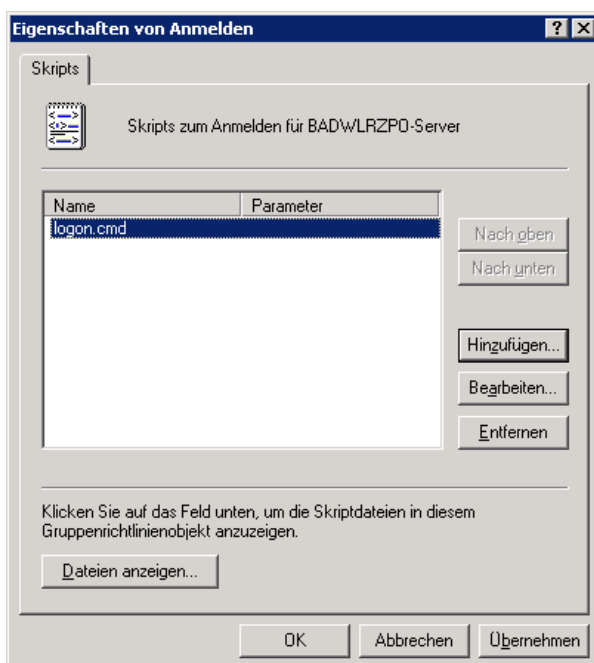
Loginskripte werden in den Gruppenrichtlinien hinterlegt. Öffnen sie dazu den Gruppenrichtlinieneditor für die gewünschte Gruppenrichtlinie. Eine Kurzeinführung zu den Gruppenrichtlinien finden Sie im Kapitel 3.2.

Unter Computerkonfiguration – Windows Einstellungen Skripts finden Sie die Skripte für den Start oder das Herunterfahren des Rechners. Unter Benutzerkonfiguration – Windows Einstellungen Skripts sind die Skripte für das An- und Abmelden des Benutzers hinterlegt.



3.4.1 Skripte in den Gruppenrichtlinien

Mit einem Doppelklick auf An- oder Abmelden öffnen sich die Eigenschaften. Über Hinzufügen öffnet sich ein Explorer-Fenster und sie können ein Skript in die Gruppenrichtlinie einbinden. Das Skript wird dann mit der Gruppenrichtlinie abgespeichert. Es können alle ausführbaren Dateien (.exe, .vbs, .cmd usw.) hinterlegt werden.



3.4.2 Verwalten von Skripten für eine Gruppenrichtlinie

Ein paar einfache Beispiele für Aufrufe in einer Batchdatei als Loginskript:

```
Net use h: \\nas.ads.mwn.de\%username%
```

Bindet das persönliche Laufwerk eines Nutzers ein

```
Net use i: \\nas.ads.mwn.de\tuarfar$
```

Bindet das Projektverzeichnis für die Einrichtung TUARFAR an

```
%logonserver%\tools\netlogon\tools\con2prt\con2prt.exe /cd \\Druckserver\Drucker1
```

Bindet freigegebenen Drucker als Standard an

Im Verzeichnis [\\ads.mwn.de\NETLOGON\Scripte\Loginskript](https://ads.mwn.de/NETLOGON/Scripte/Loginskript) finden sich ein paar Beispiele von Skripten.

### 3.5 Verwendung von Mandatory Profiles in der Domäne ads.mwn.de

Mit Mandatory Profiles kann man einem Benutzer ein vordefiniertes Profil vorgeben. Das Profil wird beim Login eines Nutzers vom Server geladen. Der Nutzer kann Veränderungen am Profil dann vornehmen. Mit dem Abmelden wird das Profil vom Rechner gelöscht und jegliche Änderungen am Profil gehen verloren.

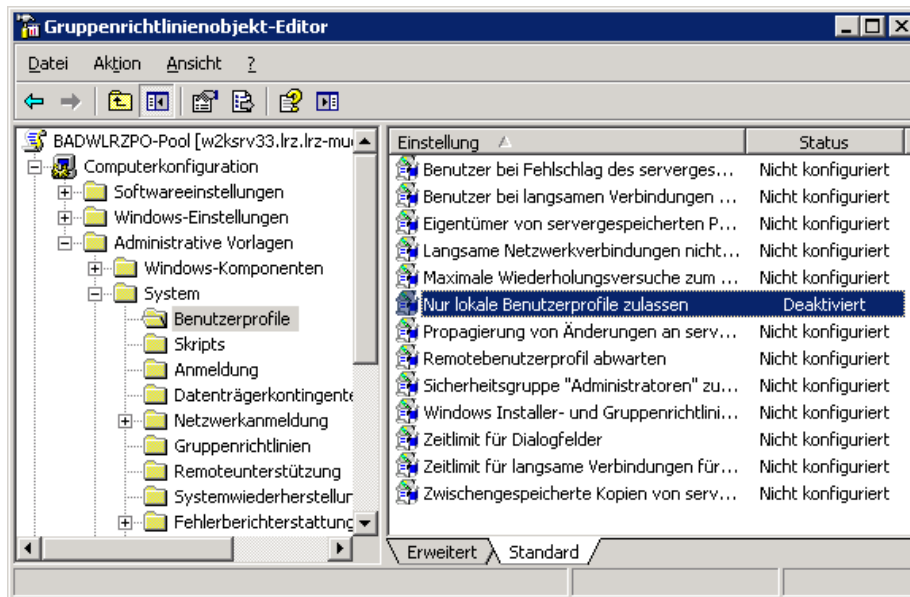
#### **Sinnvoller Einsatz:**

Mandatory Profiles kommen an Windows Arbeitsplätzen zum Einsatz an denen man vermeiden möchte, dass Nutzer Veränderungen am System vornehmen können. Auch bietet sich dadurch die Möglichkeit Voreinstellungen für Anwendungen zentral vorzugeben. Dies ist vor allem bei öffentlichen Arbeitsplätzen, Kursräumen oder Kiosk-PCs der Fall.

#### **Voraussetzungen:**

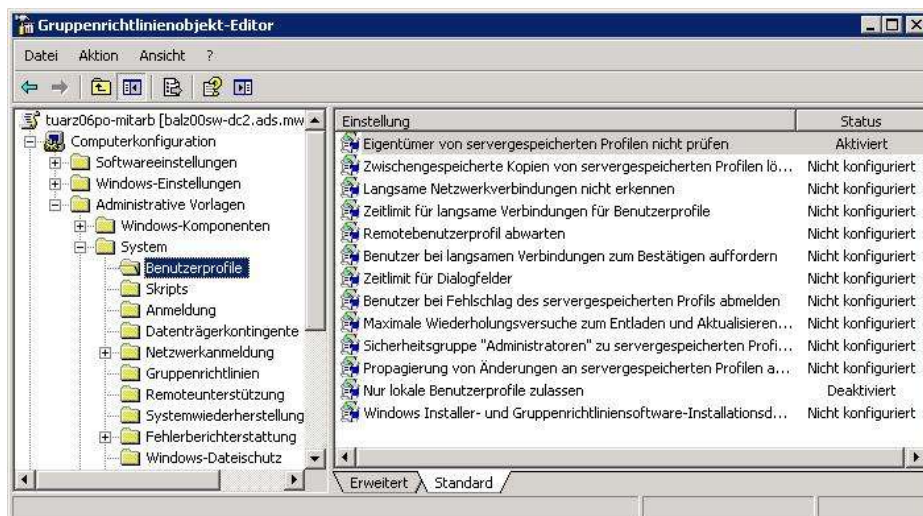
Um Mandatory Profiles in der Domäne ads.mwn.de nutzen zu können müssen vier Voraussetzungen erfüllt sein:

-Servergespeicherte Profile müssen zugelassen sein, dies kann man über die Gruppenrichtlinie Computerkonfiguration – Administrative Vorlagen – System – Benutzerprofile - „Nur lokale Benutzerprofile zulassen“ deaktivieren erreichen.



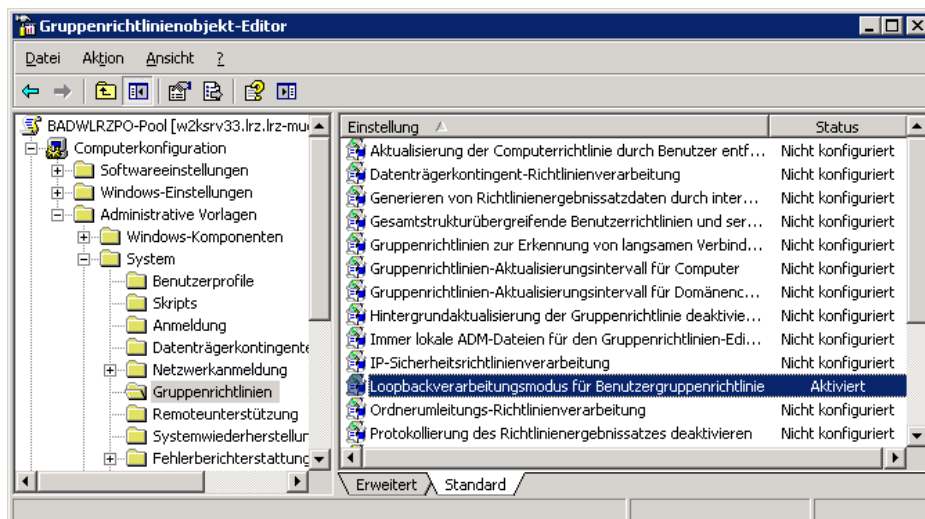
3.5.1 Wichtige Gruppenrichtlinie: Nur lokale Benutzerprofile zulassen

-Der Eigentümer von servergespeicherten Profilen darf nicht überprüft werden. Das kann man erreichen, indem man die Gruppenrichtlinie Computerkonfiguration – Administrative Vorlagen – System – Benutzerprofile – „Eigentümer von servergespeicherten Profilen nicht prüfen“ aktiviert.



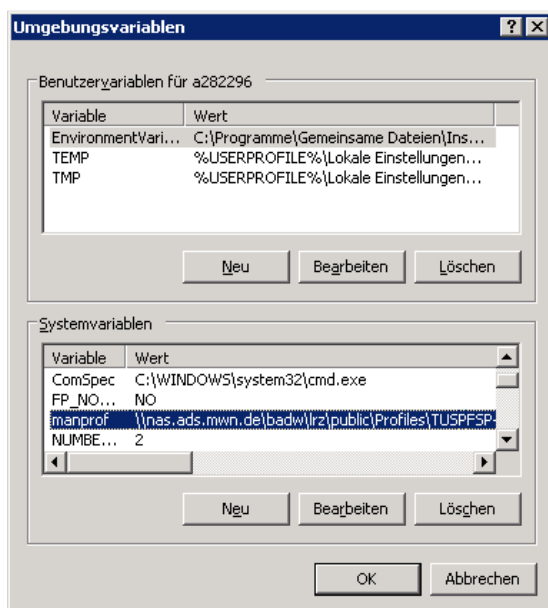
3.5.2 Wichtige Gruppenrichtlinie: Eigentümer von servergespeicherten Profilen nicht prüfen

-Loopbackverarbeitung für Computerkonfiguration – Administrative Vorlagen – System – Gruppenrichtlinien - „Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien“ aktivieren einschalten



### 3.5.3 Wichtige Gruppenrichtlinie: Loopbackverarbeitungsmodus für Benutzergruppenrichtlinien

- Lokale Umgebungsvariable manprof muss am lokalen Computer gesetzt sein und auf den Pfad zu dem Profil verweisen.



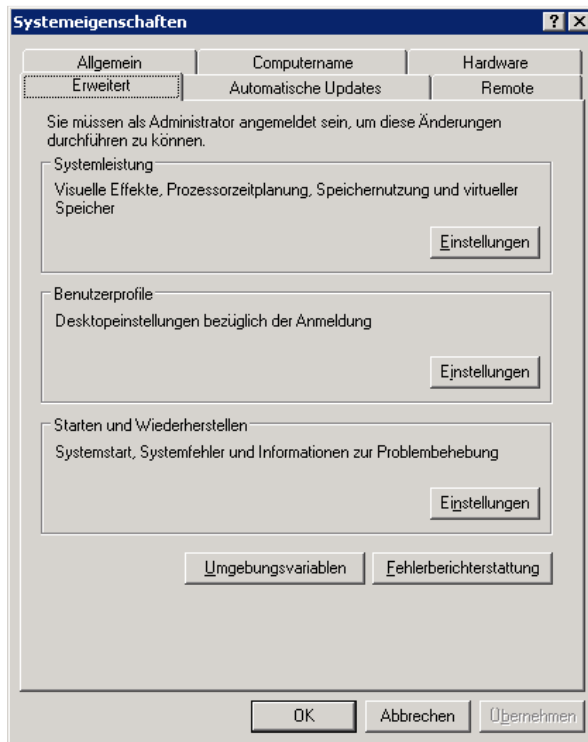
### 3.5.4 Hinzufügen einer Umgebungsvariable

#### Schritt für Schritt Anleitung:

Sie brauchen dazu ein Nutzerkonto A zum Anlegen des Profils und ein Nutzerkonto B mit lokalen Adminrechten zum Erzeugen des Mandatory Profiles.

- Melden Sie sich an einem Rechner mit dem Nutzer A an, dies kann ein lokaler oder ein Domänenutzer sein.
- Konfigurieren Sie das Benutzerprofil nach Ihren Vorstellungen. Einige Einstellungen wie die Ordneroptionen können Sie bequem im Profil anpassen. Auch manche Einstellung von Programmen lassen sich im Profil leichter konfigurieren. Häufig müssen beim ersten Start Eulas bestätigt oder Assistenten noch abgearbeitet werden. Dies können sie so dem Profil mit geben.

- Wenn Sie mit der Konfiguration des Profils nach Ihren Vorstellungen fertig sind, melden Sie sich ab.
- Melden Sie sich mit dem Nutzer B an der Maschine an.
- Wechseln Sie nach Systemsteuerung – System – Erweitert
- 



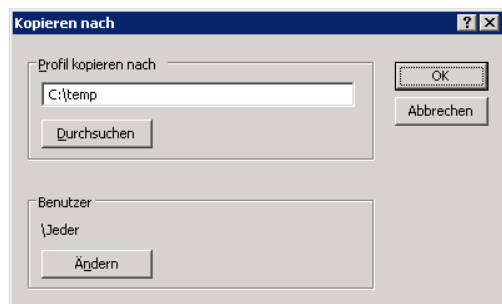
3.5.5 Systemeigenschaften aus der Systemsteuerung

### -Starten Sie Benutzerprofile - Einstellungen



3.5.6 Übersicht über die lokalen Benutzerprofile am Rechner

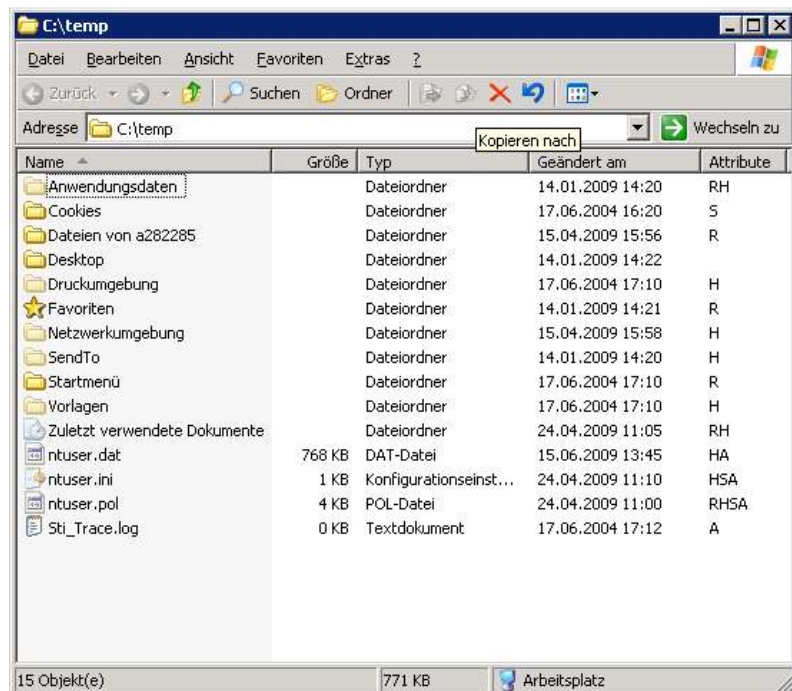
-Markieren Sie das vorhin erzeugte Benutzerprofil und wählen Sie „Kopieren nach“.



### 3.5.7 Verallgemeinern und kopieren des Profils in einen freien Ordner

-Hier müssen Sie nun ein Verzeichnis hinterlegen, in welches die Dateien des Profils kopiert werden. **Vorsicht, alle Dateien in dem Verzeichnis werden überschrieben.** Als zweiten Punkt müssen Sie die Benutzergruppe auswählen, die mit dem Profil arbeiten soll. Hier müssen Sie die lokale Gruppe Jeder auswählen. Es folgt dann noch eine Warnung, die Sie bestätigen und dann wird das Verzeichnis in das angegebene Verzeichnis kopiert.

-In dem Verzeichnis finden Sie nun das Profil mit der üblichen Profil-Ordnerstruktur.



### 3.5.8 Übersicht über ein Nutzerprofil für Windows XP

-Kopieren Sie nun den Inhalt des Ordners auf einen zentralen Ablageort, der von jedem Benutzer, der die Rechner nutzen soll, erreicht werden kann. Wir empfehlen dafür auf dem NAS-Filer den Public-Ordner in Ihrem Projektverzeichnis. Das wäre z.B. für die Fakultät AR die Ablage <\\nas.ads.mwn.de\tuar\far\public\Profil\Pool.man>.

-Damit das Profil auch ein Mandatory wird, muss noch die Datei ntuser.dat in ntuser.man umbenannt werden.

-Den Pfad müssen Sie in der Variable manprof lokal am Rechner einstellen. Sie können dies manuell über die Systemsteuerung – System – Erweitert – Umgebungsvariablen oder per Skript über die Kommandozeile:

```
\\ads.mwn.de\NETLOGONTools\setx\setx.exe -m manprof  
\\nas.ads.mwn.de\tuar\far\public\Profil\Pool.man
```


-Sie können das Profil auch in einem bestimmten Rahmen nachträglich ändern. Es ist möglich weitere Desktopverknüpfungen oder Favoriten hinzuzufügen und Konfigurationen für Anwendungen in dem Ordner Anwendungsdaten zu verändern. Erfahrene Administratoren können auch die ntuser.man mit dem Tool regedit laden und dort direkt Registrykeys verändern.

### Troubleshooting:

Es gibt verschiedene Gründe warum ein Mandatory Profil nicht geladen wird. Anbei noch ein paar Tipps zur Fehlersuche.

gpreult:

Der Kommandozeilenbefehl gpreult liefert sehr gute Informationen für die Fehleranalyse. Im oberen Teil können Sie unter zwischengespeicherte Profile sehen, ob der Pfad zu dem Profil erkannt wird und unter den angewendeten Gruppenrichtlinienobjekten muss Ihre Gruppenrichtlinie auftauchen, in der Sie den Loopback und die Verwendung von Servergespeicherten Profilen erlauben.



```
gpreult  
-----  
RSOP-Daten für LRZ\282296 auf W2KTSRU1: Protokollmodus  
-----  
Betriebssystemtyp:      Microsoft(R) Windows(R) Server 2003 Standard Editio  
n  
Betriebssystemkonfiguration: Mitgliedsserver  
Betriebssystemversion:  5.2.3790  
Terminalservermodus:  Anwendungsserver  
Standortname:         Standardname-des-ersten-Standorts  
Zwischengespeichertes Profil: \\10.156.7.10\tse-prof$\W2K3\282296.LRZ  
Lokales Profil:       N:\Dokumente und Einstellungen\282296  
Langsame Verbindung? Nein  
-----  
COMPUTEREINSTELLUNGEN  
-----  
CN=W2KTSRU1,OU=W2k3TSE,DC=lrz,DC=lrz-muenchen,DC=de  
Letzte Gruppenrichtlinienanwendung: 15.06.2009, um 13:33:27  
Gruppenrichtlinienanwendung von:    w2ksrv34.lrz.lrz-muenchen.de  
Schwellenwert für langsame Verbindung: 500 kbps  
Domänenname:                        lrz  
Domärentyp:                          Windows 2000  
-----  
Angewendete Gruppenrichtlinienobjekte  
-----  
W2k3-TSE-Server  
LRZ-Default  
Richtlinien der lokalen Gruppe  
-----  
Der Computer ist Mitglied der folgenden Sicherheitsgruppen
```

### 3.5.9 Ergebnis einer Abfrage mit gpreult

## 3.6 Vergaben von Rechten auf Ressourcen in der Domäne ads.mwn.de

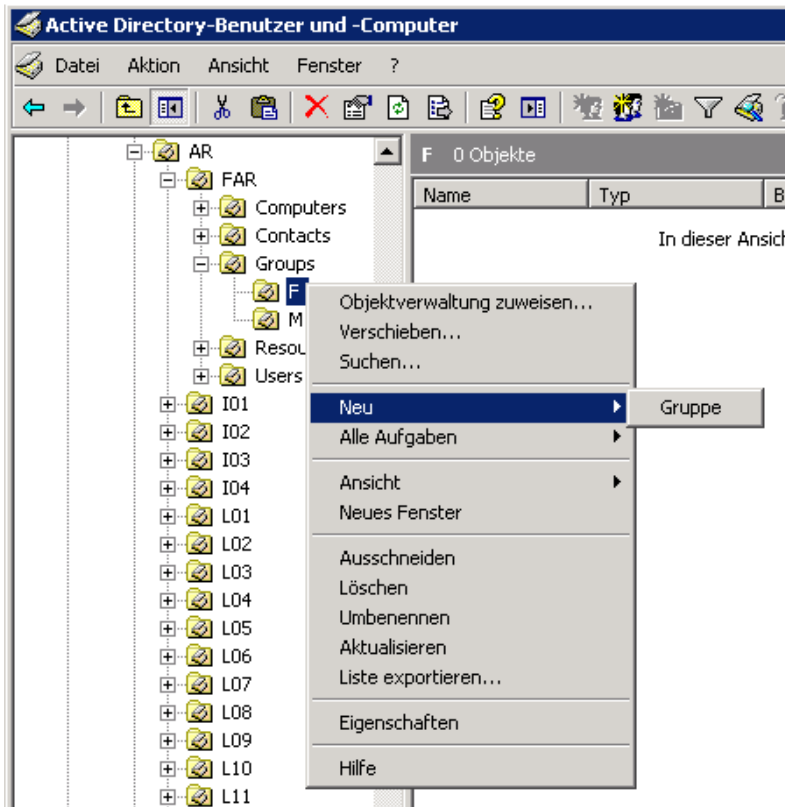
Eine der wichtigsten Aufgaben im Active Directory ist die zentrale Steuerung des Zugriffs auf Ressourcen in der Domäne ads.mwn.de. Wichtige Ressourcen, die alltäglich verwendet werden, sind dabei Drucker, Computer oder Dateiablagen. Das Active Directory bietet die Möglichkeit einzelnen Benutzern oder aber auch mehreren in Berechtigungsgruppen organisierten Nutzern den Zugriff auf Ressourcen zu erlauben, einzuschränken oder gar zu verbieten.

### Sinnvolle Verwendung

Rechte auf Ressourcen sollten wenn möglich immer über Gruppenmitgliedschaften vergeben werden. Dabei kann eine Gruppe eine Rolle am Lehrstuhl (z.B. Hiwis) darstellen, der man bestimmte Rechte auf verschiedene Ressourcen zuweisen möchte. Bei einer Änderung der Mitglieder dieser Rolle muss dann lediglich noch das jeweilige Benutzerobjekt aus der Gruppe entfernt oder hinzugefügt werden. Bei einer einzelnen Zuweisung von Rechten passiert es hingegen leicht, dass Rechte vergessen werden. Ein Nutzerobjekt kann natürlich auch Mitglied in mehreren Gruppen sein, oder eine Gruppe ist Mitglied in einer anderen Gruppe, dann kumulieren sich die Rechte des Nutzers, es sei denn ein Recht wurde explizit irgendwo verweigert.

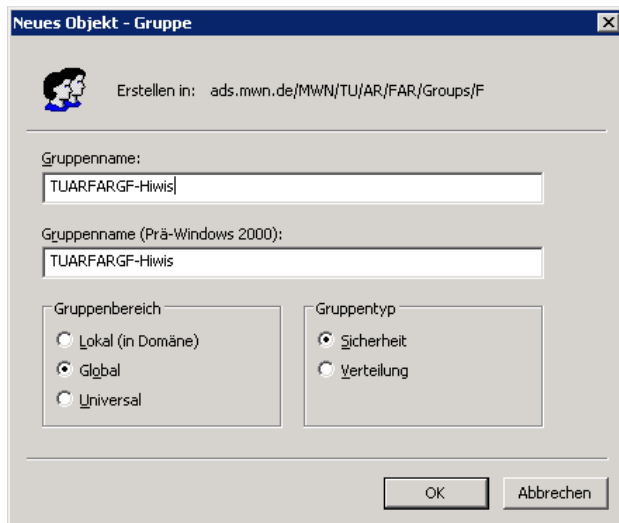
### 3.6.1 Anlegen einer Gruppe:

Starten Sie das ADUC - Active Directory-Benutzer und -Computer Tool und wechseln sie zu ihrem Teillast. Über einen Rechtsklick auf die OU mit der Bezeichnung F bekommen sie das Kontextmenü Neu – Gruppe.

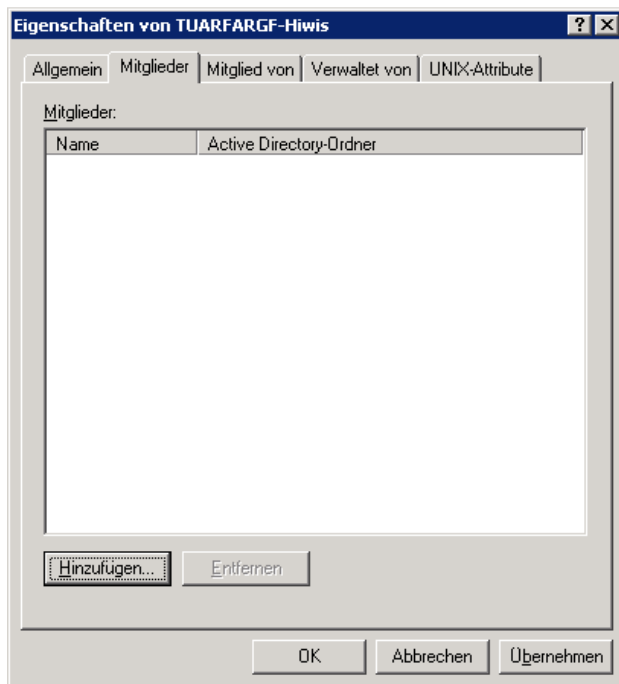


Vergeben Sie in dem folgenden Assistenten einen Gruppennamen. Beachten Sie dabei das verbindliche Namenskonzept für die ADS-Domäne. Wählen sie als Gruppenbereich Global

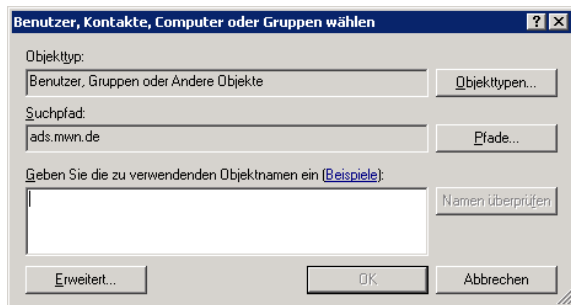
und als Gruppentyp Sicherheit (das sind die Standardeinstellungen) und bestätigen Sie den Assistenten.



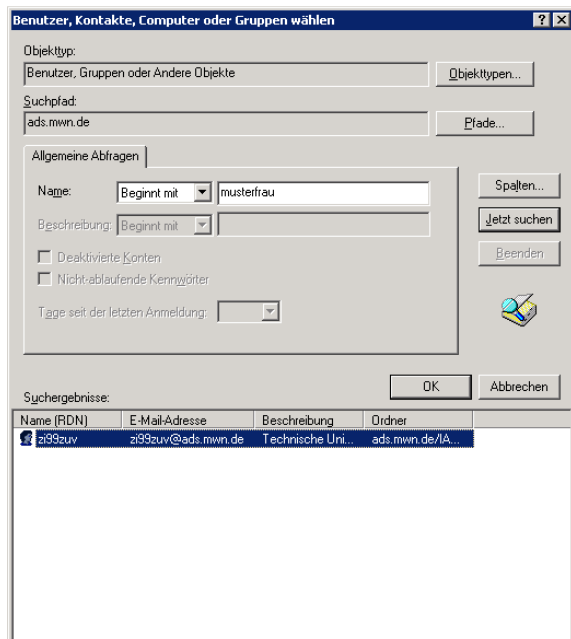
Als nächstes ändern Sie die Mitgliedschaft der Gruppe. Markieren Sie die Gruppe im ADUC - Active Directory-Benutzer und -Computer Tool und lassen sie sich über die rechte Maustaste die Eigenschaften der Gruppe anzeigen. Im Reiter Mitglieder finden Sie die aktuellen Gruppenmitglieder.



Über Hinzufügen startet ein Assistent, über den Sie einzelne Nutzer aus dem Active Directory der Gruppe hinzufügen können. Sie können die Kennung direkt eingeben und prüfen lassen, wenn Sie diese wissen, oder über erweitert nach einem Nutzer im Active Directory suchen lassen.

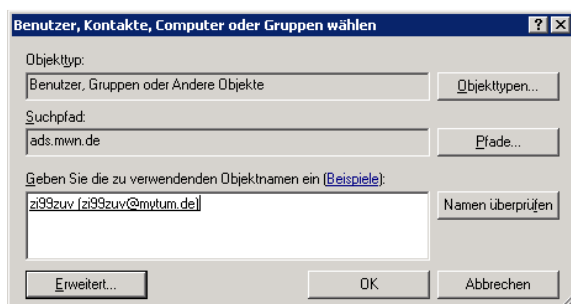


3.6.1 Hinzufügen von Objekten



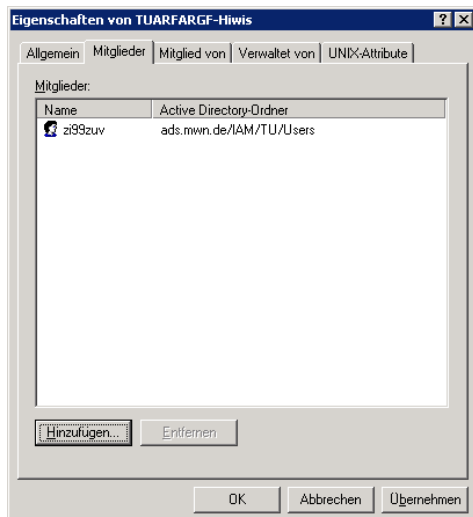
3.6.2 Erweiterte Suche von Objekten im Active Directory

Als Suchkriterium sind LRZ-Kennung oder Nachname möglich. Über „Jetzt suchen“ startet die Suche. Das Ergebnis wird im unteren Teil angezeigt. Wählen sie dann den gewünschten Nutzer aus und fügen sie ihn über OK der Gruppe hinzu.



3.6.3 Der Nutzernamen wird aufgelöst

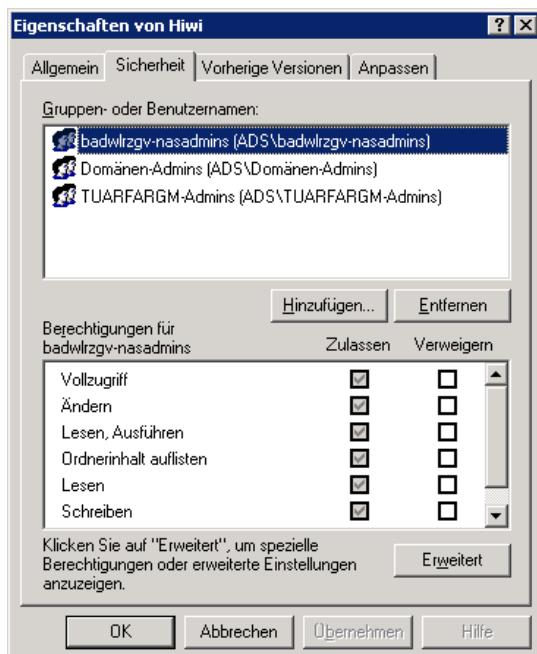
Zum Abschluss des Assistenten erfolgt eine Übersicht der aktuellen Mitglieder in der Gruppe.



3.6.4 Übersicht der aktuellen Mitglieder in der Gruppe

### 3.6.2 Vergabe von Rechten auf Dateiebene auf nas.ads.mwn.de

Starten Sie den Windows Explorer und navigieren in das Verzeichnis, für das Sie die Rechte setzen wollen. Markieren Sie den Ordner und wählen über das Kontextmenü über die rechte Maustaste den Punkt Eigenschaften aus. Im Reiter Sicherheit können Sie die bestehenden einfachen Berechtigungen für Dateien und Ordner unterhalb des aktuellen Verzeichnisses sehen und bearbeiten.



3.6.5 Verwalten von Berechtigungen für einen Dateiodner

Sie können nun über Hinzufügen weitere Gruppen oder Nutzer für diesen Ordner berechtigen. Dazu verwenden Sie wieder den gleichen Assistenten wie bereits oben beschrieben. Wenn möglich sollten Sie immer mit diesen Berechtigungen arbeiten. Im allgemeinen Betrieb reichen drei Berechtigungsstufen:

### Lesender Zugriff:

Vollzugriff	<input type="checkbox"/>	<input type="checkbox"/>
Ändern	<input type="checkbox"/>	<input type="checkbox"/>
Lesen, Ausführen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ordnerinhalt auflisten	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schreiben	<input type="checkbox"/>	<input type="checkbox"/>

#### 3.6.6 Leserecht für einen Nutzer oder Gruppe

Wenn Sie einer Nutzergruppe nur einen lesenden Zugriff geben wollen verwenden Sie diese Stufe. Die Nutzer können dann Dateien öffnen, den Inhalt lesen, aber nicht verändern. Dateien können an einen anderen Ort kopiert werden.

### Schreibender Zugriff:

Vollzugriff	<input type="checkbox"/>	<input type="checkbox"/>
Ändern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen, Ausführen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ordnerinhalt auflisten	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>

#### 3.6.7 Schreibrecht für einen Nutzer oder Gruppe

Wenn Sie möchten, dass die Nutzer die Dateien ändern oder neue Dateien und Ordner anlegen sollen, verwenden Sie dieses Recht.

### Vollzugriff:

Vollzugriff	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ändern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen, Ausführen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ordnerinhalt auflisten	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>

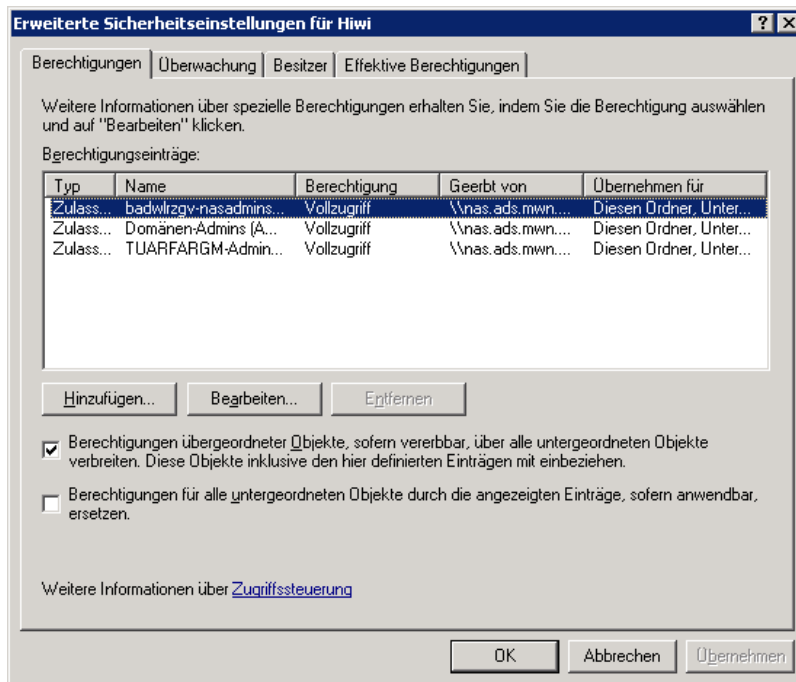
#### 3.6.8 Vollzugriff für einen Nutzer oder Gruppe

Vollzugriff sollten sie wenn möglich nicht vergeben. Über Vollzugriff hat der Nutzer die Möglichkeit selbst Rechte zu setzen und kann dem Teiladministrator die Zugriffsrechte entziehen.

### Erweiterte Sicherheit:

Die Schaltfläche Erweitert bietet zusätzliche Möglichkeiten Rechte zu setzen. Die erweiterten Rechte brauchen sie für folgende Tätigkeiten:

- Durchbrechen der Vererbung
- Berechtigungen nach unten im Dateibaum ersetzen
- Setzen von sehr feingranularen Rechten

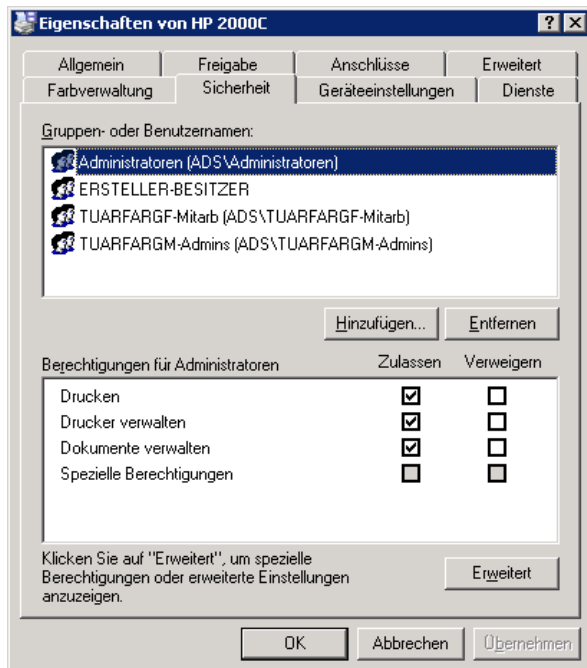


### 3.6.9 Erweiterte Dateirechte für komplexere Dateirechte

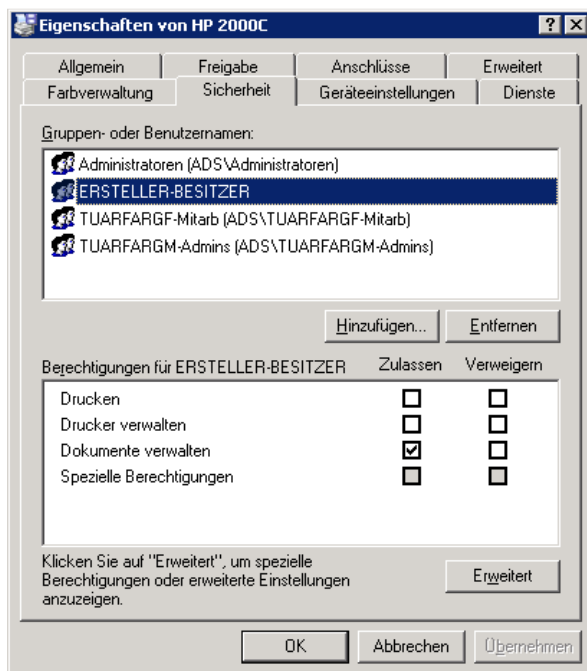
### 3.6.3 Vergeben von Rechten auf Drucker in der Domäne

Sie können auch die Berechtigungen auf Drucker über die Benutzerverwaltung des Active Directory steuern. Wenn Sie einen Netzwerkdrucker freigeben, dann müssen sie die Rechte auf diesen überarbeiten. Leider sind die Standardrechte nämlich hier sehr großzügig, sodass jeder Domänenbenutzer auf dem Drucker zunächst drucken könnte. Ändern sie dazu die Rechte für den Drucker wie folgt:

- Entfernen Sie die Gruppen Hauptbenutzer, Benutzer und Jeder falls vorhanden.
- Fügen sie explizit die Gruppen oder Benutzer hinzu, die Drucken sollen und berechtigen sie diese.
- Geben sie den Teiladmins das Recht die Drucker und Dokumente zu verwalten.
- Geben sie der Gruppe Ersteller-Besitzer das Recht die (eigenen) Dokumente zu verwalten. Ersteller-Besitzer sind jeweils die Nutzer die gerade einen Druckjob abgesetzt haben und die sollen ihren Druckjob selbst auch löschen können.



3.6.10 Vollzugriff für die Gruppe Administratoren

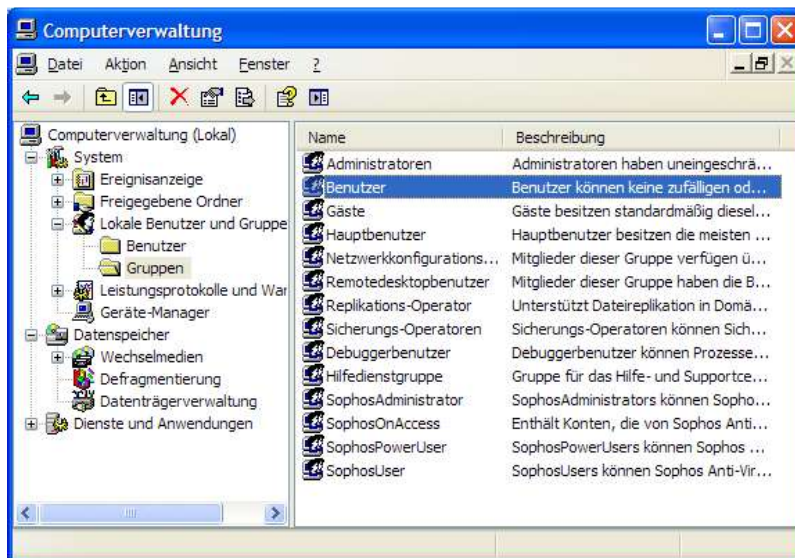


3.6.11 Dokumente Verwalten für die Gruppe Ersteller-Besitzer

### 3.6.4 Beschränken der Anmeldung an einem Rechner

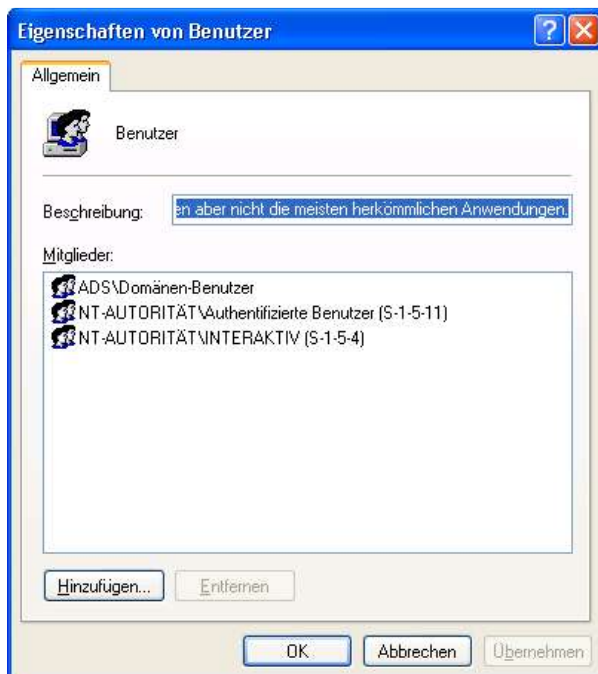
Nachdem ein Rechner in die Domäne ads.mwn.de aufgenommen ist, können sich alle Mitglieder der Gruppe Domänenbenutzer, dies sind im Prinzip alle Besitzer einer LRZ-Kennung, an dem Rechner lokal anmelden. Das ist leider eine Standardeinstellung. Möchte man das verhindern, kann man die Mitgliedschaft für die lokale Nutzergruppe „Benutzer“ anpassen.

Öffnen Sie dazu über Systemsteuerung – Verwaltung die Computerverwaltung.

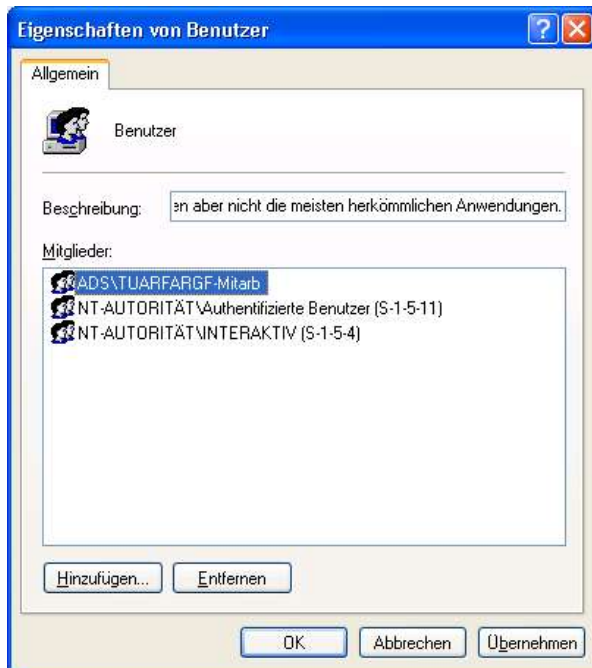


3.6.12 Lokale Benutzerverwaltung in der Computerverwaltung

Markieren sie die Gruppe Benutzer und öffnen über die rechte Maustaste die Eigenschaft der Gruppe. Es werden Ihnen die Mitglieder der Gruppe angezeigt. Unter den Mitgliedern befindet sich nun auch die Gruppe ADS\Domänen-Benutzer. Entfernen sie diese Gruppe nun und fügen die Benutzer oder Gruppen hinzu die sich in Zukunft an dem Rechner anmelden sollen.



3.6.13 Mitglieder der lokalen Gruppe Benutzer mit der vordefinierten Gruppe ads\Domänen-Benutzer



3.6.14 Mitglieder der lokalen Gruppe Benutzer mit einer explizit hinzugefügten Gruppe

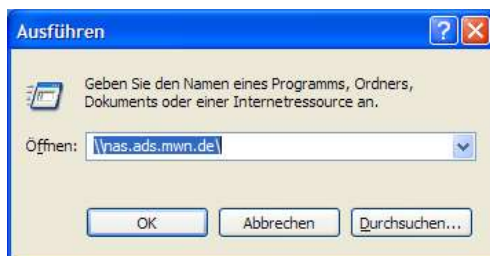
## 3.7 Anbinden des Storage nas.ads.mwn.de für nicht Domänenrechner

Für nicht in die Domäne integrierte Rechner ist es notwendig die Anbindung an den Storage nas.ads.mwn.de manuell vorzunehmen.

### 3.7.1 Einmaliges Anbinden des Storage

Manchmal ist es nötig von einem beliebigen Rechner im MWN auf die zentrale Dateiablage zuzugreifen. Dies kann man relativ unkompliziert erledigen.

Gehen Sie hierzu über Start – Ausführen (alternativ die Tastenkombination Windows + R) und geben hier den UNC-Pfad <\\nas.ads.mwn.de> ein.



3.7.1 Verbinden mit nas.ads.mwn.de über Start - Ausführen

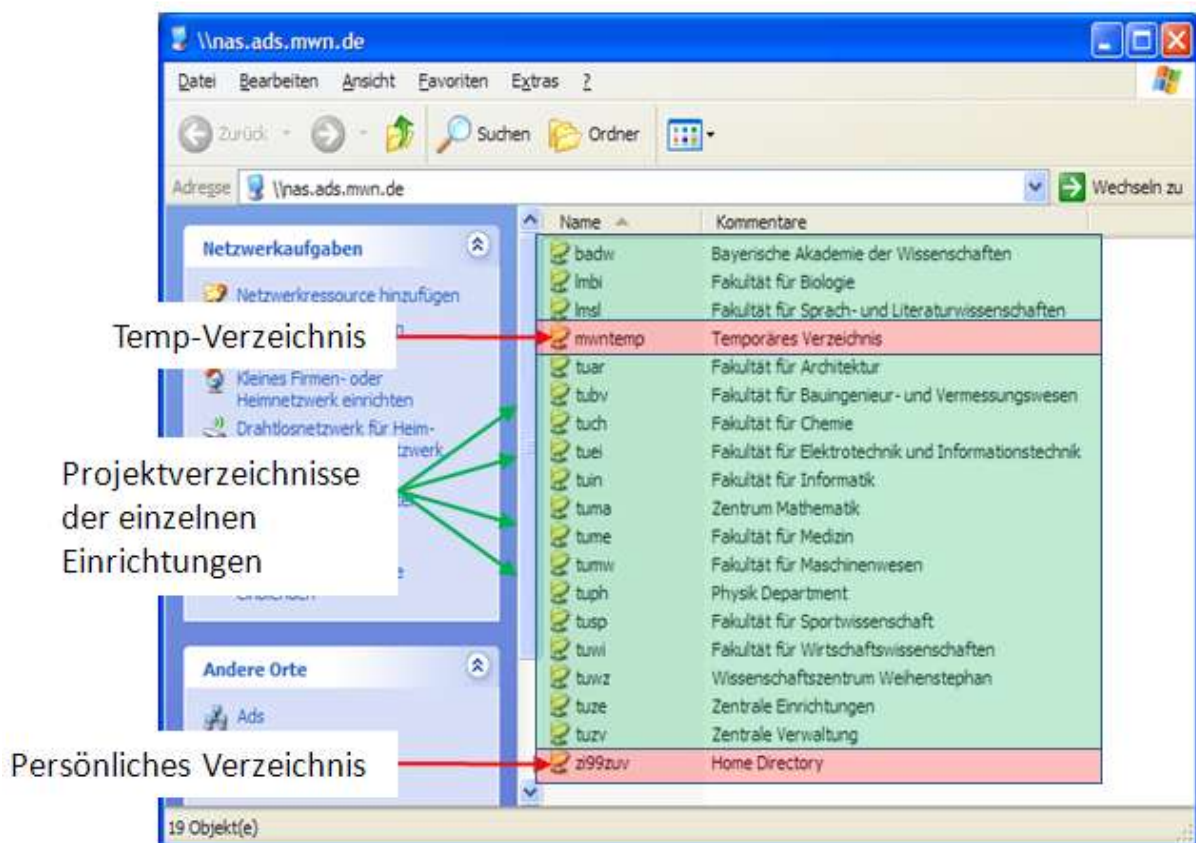
Nach kurzer Zeit (<30 sec) erscheint ein Anmeldefenster. Geben sie hier nun als Benutzername ihre LRZ-Kennung und ihr Passwort ein.



3.7.2 Anmeldedialog

Nach kurzer Zeit sollte im Windows Explorer eine Übersicht über alle freigegebenen Ordner auf dem zentralen Ablagesystem zu sehen sein. Sie finden dort unter anderem:

- Ihr persönliches Verzeichnis mit dem Namen ihrer LRZ-Kennung
- die Fakultätsverzeichnisse, darin verbergen sich die jeweiligen Institutsverzeichnisse
- mwntemp – ein Verzeichnis für die kurzzeitige Ablage von Dateien, eventuell für den Austausch innerhalb des MWN



3.7.3 Sichtbare Freigaben auf nas.ads.mwn.de

### 3.7.2 Netzlaufwerk – dauerhaftes Anbinden des Storage nas.ads.mwn.de

Öffnen sie dazu den Windows Explorer. Im Menü wählen sie unter Extras den Punkt Netzlaufwerk verbinden aus.



#### 3.7.4 Netzlaufwerk verbinden

Wählen sie nun ein freies Laufwerk aus und geben sie als Ordner den Pfad zu dem Ablagebereich ein. Beispiele für Pfade sind:

-Persönliches Verzeichnis für den Nutzer zi99zuv:  
\\nas.ads.mwn.de\zi99zuv

-Projektverzeichnis für den Lehrstuhl I01 in der Fakultät Architektur:  
nas.ads.mwn.de\tuar\far

Oder:  
\\nas.ads.mwn.de\tuarfar\$

-Temporäres Verzeichnis für das MWN  
[\\nas.ads.mwn.de\mwntemp](https://nas.ads.mwn.de/mwntemp)

Soll das Laufwerk nach einer erneuten Anmeldung für den Nutzer wiederhergestellt werden, dann markieren sie die Option „Verbindung bei Anmeldung wiederherstellen“

Als nächstes markieren sie den Punkt „anderem Benutzernamen“ und hinterlegen im nächsten Dialog die Zugangsdaten für den Ablagebereich. Beachten Sie dabei die Verwendung des Domänennamens vor der LRZ-Kennung.



3.7.5 Hinterlegen der Zugangsdaten für den Zugriff auf die Ablage

Danach sollte im Windows Explorer das Laufwerk eingeblendet werden und Sie können damit arbeiten. Beim nächsten Login und dem ersten Zugriff auf das Laufwerk werden Sie eventuell zu einer erneuten Eingabe ihrer Zugangsdaten aufgefordert.

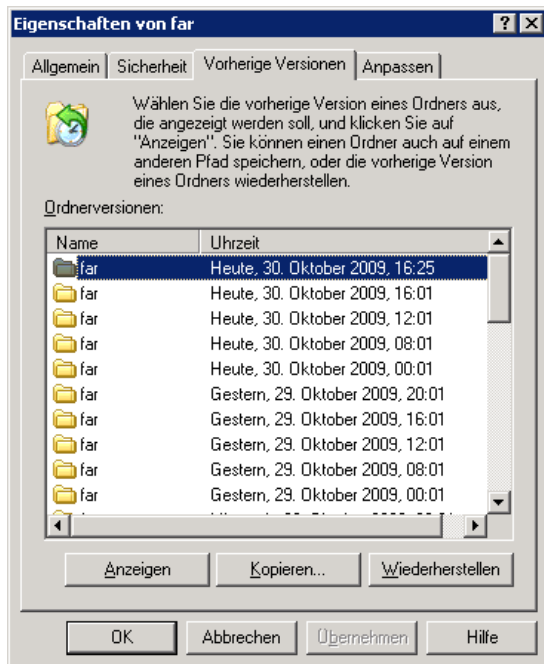


3.7.6 Windows-Anmeldedialog

### 3.8 Wiederherstellung von Dateien auf nas.ads.mwn.de über Snapshots

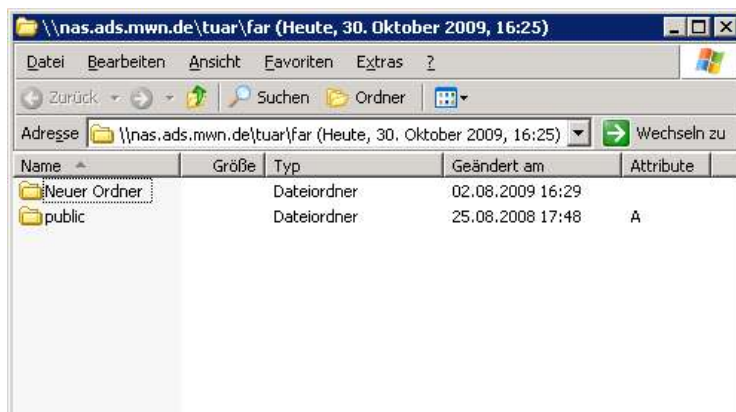
Der Nas-Filer bietet eine einfache Möglichkeit gelöschte Dateien bequem wiederherzustellen. Alle vier Stunden werden vom Nas-Filer sogenannte Snapshots, Abbilder des aktuellen Filesystems, erzeugt. Diese Snapshots reichen dann maximal vier Wochen zurück.

Dazu müssen sie sich die Eigenschaften des übergeordneten Ordners anzeigen lassen in dem die Dateien gelöscht wurden. Sie finden unter den Eigenschaften einen Reiter „Vorherige Versionen“. Hier werden Ihnen die verfügbaren Snapshots mit der jeweiligen Uhrzeit angezeigt.



3.8.1 Verfügbare Snapshots für einen Ordner

Markieren sie den gewünschten Snapshotstand und wählen dann die Option Anzeigen. In einem Explorer-Fenster wird Ihnen dann der Inhalt des Ordners zu dem Zeitpunkt angezeigt. Sie können dann den Inhalt einfach auf einen Ablage ihrer Wahl kopieren und weiterbearbeiten. Die Option Wiederherstellen sollten sie nicht benutzen, da sonst der Ordner auf den alten Stand zurückgesetzt wird und so Daten überschrieben werden könnten.



3.8.2 Inhalt eines Snapshots im Explorer angezeigt

## 4 FAQ

### 4.1 Benutzerverwaltung

#### 4.1.1 Frage: Wo sind meine Nutzer?

Antwort: Alle Nutzer eines Mandanten liegen flach unterhalb der OU=IAM. Nutzer werden dort vom zentralen IDM-System gepflegt

#### 4.1.2 Frage: Darf ich selber Nutzer hinzufügen?

Antwort: **Nein**, aber sie können im Rahmen ihrer Teilstruktur sogenannte Serviceaccounts anlegen. Diese gelten nur innerhalb des Active Directory und sind für dienstspezifische Anwendungen gedacht. Auch Kurzfristige Gäste müssen über die Gästeverwaltung oder über SIM am LRZ ins Active Directory gebracht werden.

#### 4.1.3 Frage: Woher bekomme ich meine LRZ-Kennung?

Antwort: Eine ausführliche Dokumentation findet sich auf den Seiten des TUM Helpdesk: [http://portal.mytum.de/iuk/service/faq/faq10/100\\_Wie\\_bekomme\\_ich\\_ein\\_Account](http://portal.mytum.de/iuk/service/faq/faq10/100_Wie_bekomme_ich_ein_Account)

#### 4.1.4 Frage: Was ist mit meinen alten Projektkennungen vom LRZ?

Antwort: Die Projektkennungen am LRZ behalten bis auf weiteres ihre Gültigkeit. Diese Kennungen sind auch in der Domäne ads.mwn.de vorhanden. Sie sollten aber mittelfristig diese Kennungen nicht mehr verwenden und nur noch mit Ihrer von der TUM vergebenen LRZ-Kennung arbeiten.

#### 4.1.5 Frage: Kann ich an meinem Benutzerobjekt im Active Directory Einstellungen vornehmen?

Antwort: Nein, es kann nur die Gruppenmitgliedschaft von den einzelnen Teiladmins angepasst werden.

#### 4.1.6 Frage: Wie ändere ich oder setze ich mein Passwort zurück?

Antwort: Wenn Sie Ihr Passwort vergessen haben, können Sie sich entweder an Ihren zuständigen Benutzerverwalter oder an den IT Service Desk wenden. Wenn Sie der Benutzerverwalter nicht persönlich kennt, wird er einen amtlichen Lichtbildausweis (Pass oder Personalausweis) von Ihnen überprüfen.

#### 4.1.7 Frage: Wer ist mein IO an der TUM?

Antwort: Eine aktuelle Liste der IOs an der TUM finden sie unter: [http://portal.mytum.de/iuk/navigation/20041717161745\\_81759/20041917161940\\_10224/iuk/gremium/mitglieder\\_html](http://portal.mytum.de/iuk/navigation/20041717161745_81759/20041917161940_10224/iuk/gremium/mitglieder_html)

#### 4.1.8 Frage: Meine Einrichtung fehlt noch im Active Directory, an wen kann ich mich wenden?

Antwort: Sollte ihre Einrichtung noch fehlen, stellen sie bitte eine Anfrage an den Service Desk der TUM.

## 4.2 Berechtigungen

### 4.2.1 Frage: Ich habe einen Nutzer zu einer Gruppe hinzugefügt, aber er hat keine weiteren Berechtigungen erhalten?

Antwort: Gruppenmitgliedschaften werden nur beim Login eingelesen und angewandt. Melden Sie sich mit dem Nutzer ab und wieder an, dann sollte der Zugriff funktionieren.

### 4.2.2 Frage: Wieso bekomme ich den Fehler „Dieser Netzwerkordner ist zurzeit unter Verwendung eines anderen Namens und Kennwortes verbunden“?

Antwort: Windows kann immer nur mit einer Benutzerkennung eine Verbindung zum Onlinespeicher mit dem Namen nas.ads.mwn.de herstellen. Eine weitere Verbindung mit einer anderen Nutzerkennung schlägt mit obigen beschriebenen Fehler fehl. Eine zweite Verbindung lässt sich nur unter der Verwendung der IP-Adresse von nas.ads.mwn.de – 10.156.7.27 herstellen.

## 4.3 Gruppenrichtlinien

### 4.3.1 Frage: Warum wird meine Gruppenrichtlinie immer ausgefiltert wenn ich mir gresult anzeigen lasse?

Antwort: Wenn die Gruppenrichtlinie leer ist, dann wird diese in gresult als herausgefiltert dargestellt. Ändern sie eine Einstellung und dann sollte die Gruppenrichtlinie angewandt werden.

### 4.3.2 Frage: Warum kann ich als Teiladmin eine Gruppenrichtlinie nicht bearbeiten, die von einem anderen Teiladmin der Einheit erstellt wurde?

Antwort: Beim Anlegen einer Gruppenrichtlinie wird der Erzeuger automatisch berechtigt. Leider werden die anderen Mitglieder der Teiladmingruppe nicht automatisch berechtigt. Damit die anderen Mitglieder auch diese Gruppenrichtlinie bearbeiten können, muss die Teiladmingruppe hinzugefügt werden.

## 4.4 Woher krieg ich Hilfe zu verschiedenen Themen?

Antwort: Für die TUM ist der Service Desk der TUM erster Ansprechpartner. Erreichbar unter:

E-Mail: [it-support@tum.de](mailto:it-support@tum.de)

Telefon: 089-28917123

WWW: <http://portal.mytum.de/iuk/service/servicedesk/support/>