EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration von Dateiberechtigung über Active Directory-Gruppen

20.01.2012, Markus Reigl

Inhalt

- Strategie bei der Rechtevergabe und allgemeines Vorgehen
- Administration der Gruppen
- Administration der Dateiberechtigungen

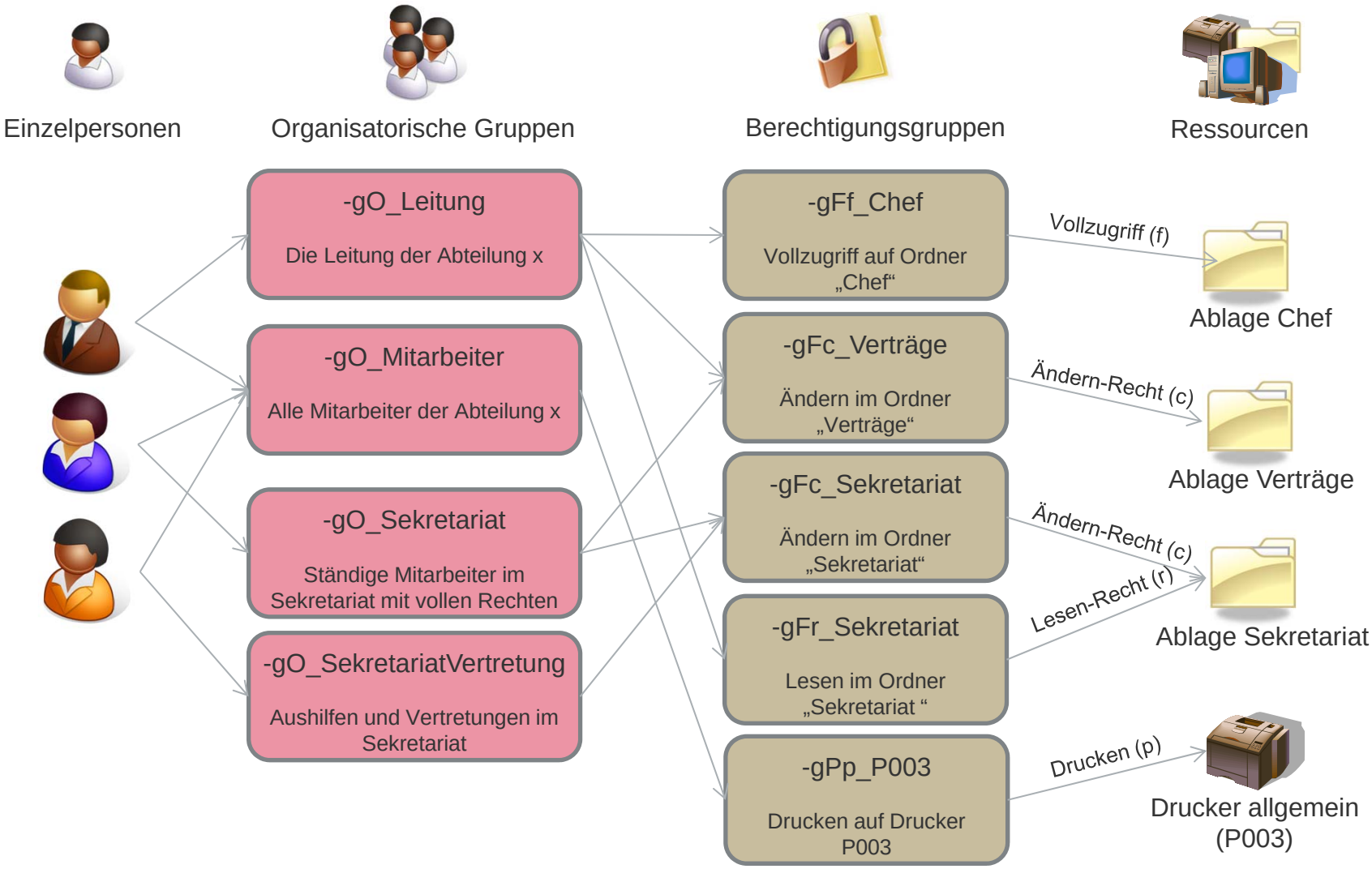
EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

1. Teil
Allgemeine Zielsetzungen und Strategie

- Berechtigungen im Dateisystem sind kompliziert zu setzen und schwer zu verwalten
  → Wenig Änderungen im Dateisystem durchführen

- Neuen Mitarbeitern einfach notwendige Berechtigen zuweisen
  → Rollenbasiert arbeiten

- Berechtigungen möglichst zentral managen
  → Weitgehend mit Gruppen im AD arbeiten



EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Die verschiedenen Servicemodelle des ZDV für Gruppenlaufwerke

Simple	

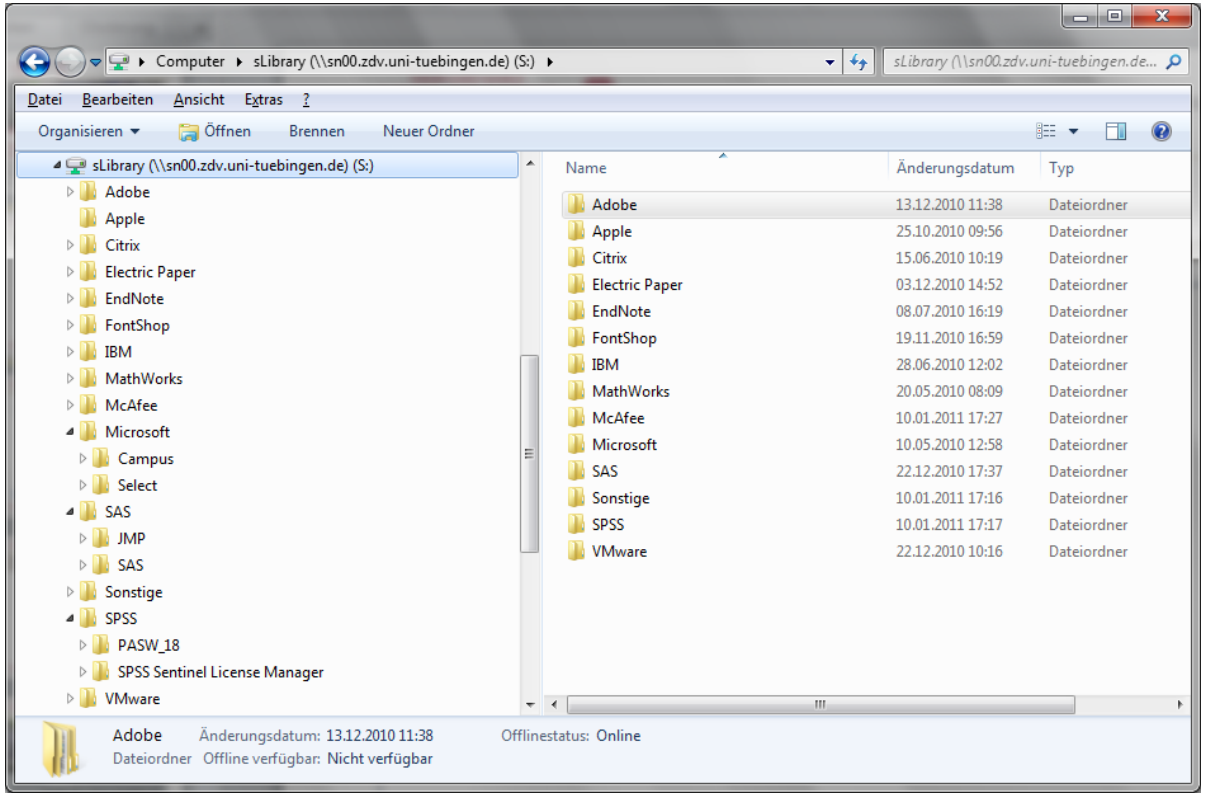
EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Die verschiedenen Servicemodelle des ZDV für Gruppenlaufwerke

	simple	advanced	delegated	managed
Verwaltung Gruppen	nein	Nein	je	ZDV
Zuweisen Berechtigungen	nein	an User	an Gruppen	Nein
Unterschiedliche Ordner-Berechtigungen	nein	Möglich	ja	Ja
Zugriff auf Berechtigungen im Hauptordner	nein	nein	ja	

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Beispiel:
Rechtevergabe für die Software-Library (sLibrary)



EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

1. Schritt: Software nach unterschiedlichen Berechtigungen gruppieren

Gruppe	Verzeichnis		Zugriff für
Adobe	/Adobe		ZDV
Microsoft-Campus	/Microsoft/Campus		ZDV, UB, WiWi
Microsoft-Select	/Microsoft/Select		CICS
Campus	/Endnote /Mathworks /McAfee /SAS/JMP /SPSS/PASW		Uni-Angestellte
IT	/Apple /Citrix /Fontshop /IBM /Vmware	/ElectricPaper /SAS/SAS /SPSS/License Man /Sonstige /MS/Campus intern	ZDV

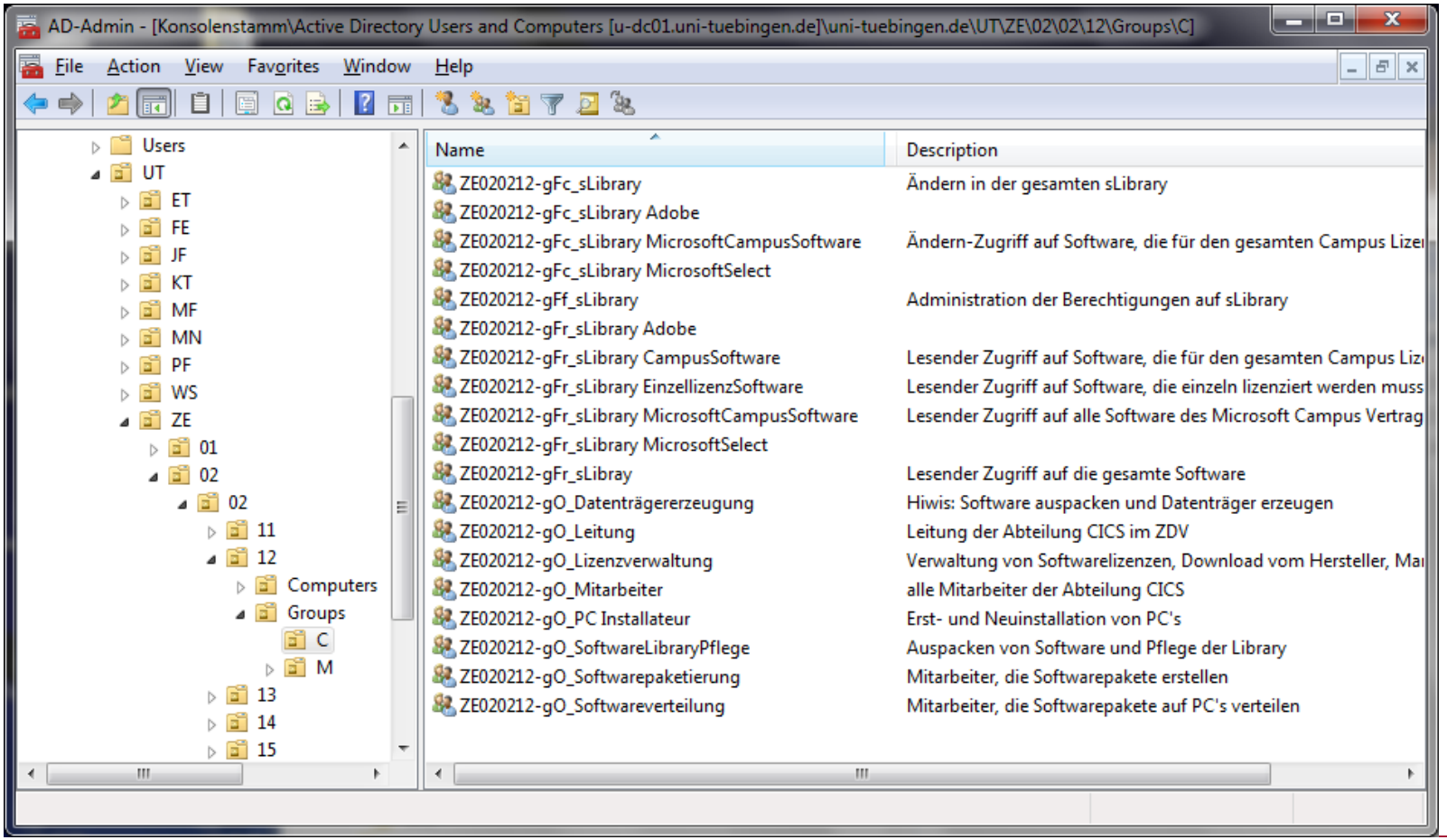
EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

2. Schritt:
Zugriffsgruppen definieren

Softwaregruppe	Berechtigungsgruppe
/	ZE020212-gFf_sLibrary ZE020212-gFc_sLibrary ZE020212-gFr_sLibray
Adobe	ZE020212-gFc_sLibrary Adobe ZE020212-gFr_sLibrary Adobe
Microsoft-Campus	ZE020212-gFc_sLibrary MicrosoftCampusSoftware ZE020212-gFr_sLibrary MicrosoftCampusSoftware
Microsoft-Select	ZE020212-gFc_sLibrary MicrosoftSelect ZE020212-gFr_sLibrary MicrosoftSelect
Campus	ZE020212-gFr_sLibrary CampusSoftware
IT	ZE020212-gFr_sLibrary EinzellizenzSoftware

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

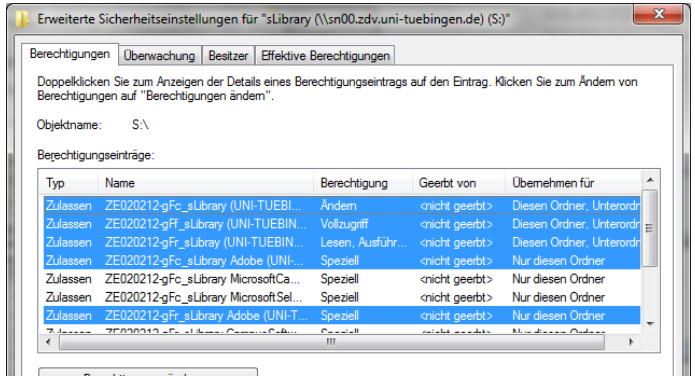
Beispiel:
Gruppen im AD

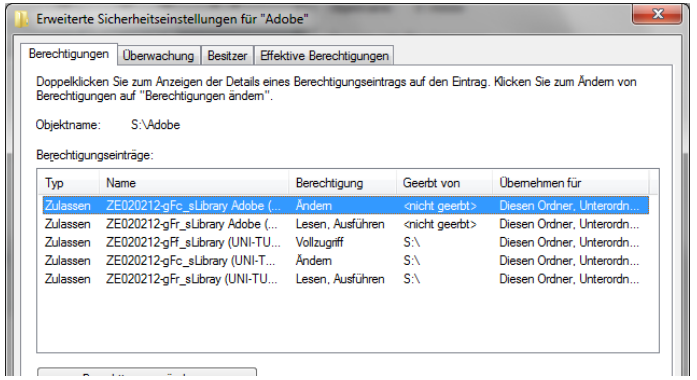


EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

3. Schritt
Berechtigungsgruppen den Ordnern zuweisen

Ordner	Gruppe	Berechtig.	Vererben
/	gFf_sLibrary gFc_sLibrary gFr_sLibray	Voll Ändern Lesen	Ja Ja Ja
/	gFc_sLibrary Adobe gFr_sLibrary Adobe	Anzeigen Anzeigen	Nein Nein
/Adobe	gFc_sLibrary Adobe gFr_sLibrary Adobe	Ändern Lesen	Ja Ja





EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

3. Schritt
Berechtigungsgruppen den Ordnern zuweisen

Ordner	Gruppe	Berechtig.	Vererben
/	gFr_sLibrary CampusSoftware	Anzeigen	Nein
/Endnote	gFr_sLibrary CampusSoftware	Lesen	Ja
/Mathworks	gFr_sLibrary CampusSoftware	Lesen	Ja
/McAfee	gFr_sLibrary CampusSoftware	Lesen	Ja
/SAS	gFr_sLibrary CampusSoftware	Anzeigen	Nein
/SAS/JMP	gFr_sLibrary CampusSoftware	Lesen	Ja
…			

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

3. Schritt
Berechtigungsgruppen den Ordnern zuweisen

Ordner	Gruppe	Berecht.	Vererb.
/	gFc_sLibrary MicrosoftSelect gFr_sLibrary MicrosoftSelect gFc_sLibrary MicrosoftCampusSoftware gFr_sLibrary MicrosoftCampusSoftware	Anzeigen	Nein Nein Nein Nein
/Microsoft	gFc_sLibrary MicrosoftSelect gFr_sLibrary MicrosoftSelect gFc_sLibrary MicrosoftCampusSoftware gFr_sLibrary MicrosoftCampusSoftware	Anzeigen	Nein Nein Nein Nein
/Microsoft/ Campus	gFc_sLibrary MicrosoftCampusSoftware gFr_sLibrary MicrosoftCampusSoftware	Ändern Lesen	Ja Ja
/Microsoft/ Select	gFc_sLibrary MicrosoftSelect gFr_sLibrary MicrosoftSelect	Ändern Lesen	Ja Ja

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

4. Schritt
Rollen definieren und Personen zuweisen

Rolle	Beschreibung	Mitglieder
Mitarbeiter CICS ZE020212-gO_Mitarbeiter	Alle Mitarbeiter	JS, UK, PS, MR, WH, JE, RF, SB, BL
Softwareinstallateur ZE020212-gO_PC Installateur	Software auf Clients installieren, also Zugriff auf alle Clientsoftware benötigen	PS, WH, JE, RF, SB
Datenträgererzeugung ZE020212-gO_Datenträgererzeugung	Auspacken von Software, ISO erzeugen, CD/DVD brennen	Hiwi‘s, WH
Leitung ZE020212-gO_Leitung		JS
Lizenzverwaltung ZE020212-gO_Lizenzverwaltung	Download von Software	WH, JS
sLibrary-Pflege ZE020212-gO_SoftwareLibraryPflege	„Kehrwoche“…	MR

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

5. Schritt: Rollen mit Berechtigungen versehen

Softwaregruppe / Rolle	Gesamt	Adobe	MS-Campus	MS-Select	Campus	Einzel-lizenz	
Mitarbeiter CICS	R						
Softwareinstallateur						R	
Datenträgererzeugung		C		C	C		
Leitung							
Lizenzverwaltung	C	F	C				
sLibrary-Pflege	C						
ZDV Mitarbeiter							
Angestellte					R		
Admin, MR	F						
Softwarepaketierung						R	
Softwareverteilung						R	
ZE, CTC			R				
PC-Installateur	R						

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

2. Teil: Administration der Zugriffsgruppen
Überblick

- Verbinden mit dem Terminalserver
- Starten der Administrationskonsole
- Erstellen der Gruppen für den Zugriff auf das gesamte Laufwerk
- Erstellen der Gruppen für spezielle Ordner
- Erstellen von Organisatorischen Gruppen
- Zuordnen der User-Accounts zu den Org. Gruppen
- Zuordnen der Org. Gruppen zu den Zugriffsgruppen

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Zugriffsgruppen Verbinden mit dem Terminalserver

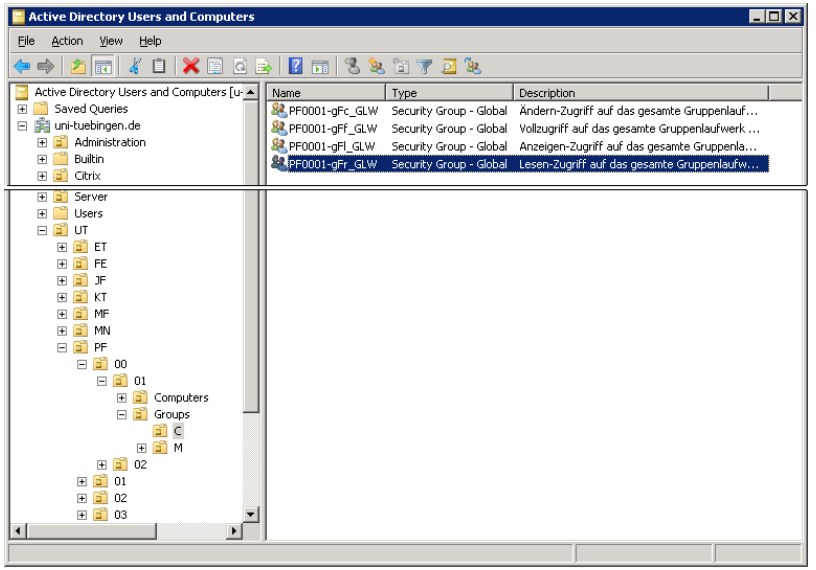
Die Administration wird in einer gesicherten Umgebung ohne lokale Installation von Software durchgeführt

- Starten des Terminal-Server Clientprogramms Startmenü > Ausführen > „mstsc“
- Name des Administrations Terminal-Servers: u-ts02.uni-tuebingen.de
- Authentifizieren mit dem Domänen-Account der Uni-Tübingen, der für die Administration vom ZDV zugelassen wurde

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Zugriffsgruppen
Starten der Administrationskonsole

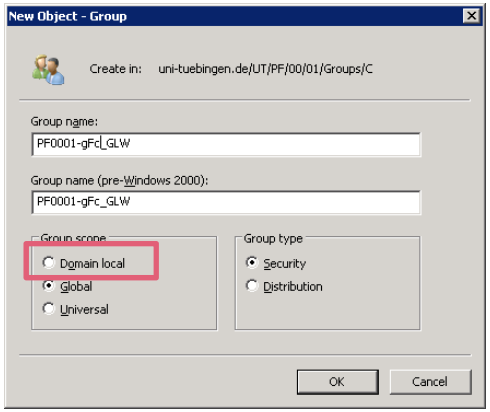
- Start über einen Link auf dem Desktop oder
  Startmenü > Administrative Tools > Active Directory Users and Computers
- Navigieren zur jeweiligen Org. Einheit
  Beispiel: PF0001
  UT > PF > 00 > 01
- Gruppen werden in Unter-OU
  Groups > C
  administriert

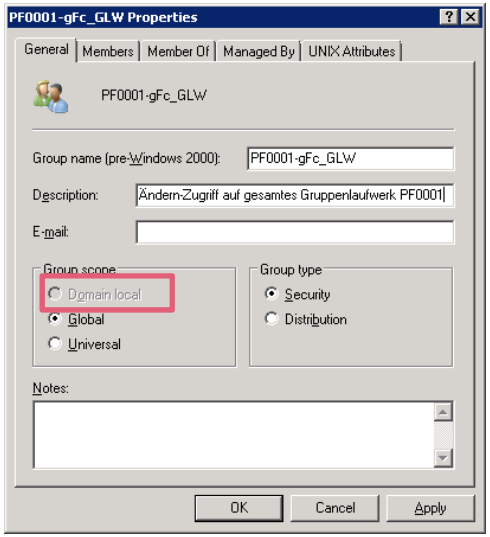


EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Zugriffsgruppen
Erstellen der Gruppen für den Zugriff auf das GLW

- Bei in der Konsole markierter OU folgendes Menü aufrufen:
  Action > New > Group
- Name entsprechend der Konvention vergeben
  Beispiel: Ändern-Zugriff auf gesamtes GLW
  → PF0001-gFc_GLW
- Group Scope: „Domain local“
- Group Type: „Security“
- Mit OK Gruppe erstellen
- Ergänzen einer Beschreibung nachträglich durch Menü Action > Properties





EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Zugriffsgruppen
Erstellen der Gruppen für spezielle Ordner

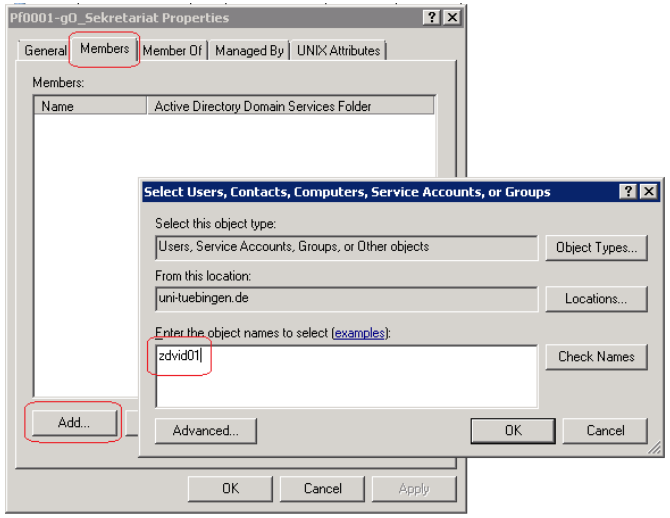
- Werden für Daten spezielle Zugriffsrechte benötigt, so sollten diese Daten in einer Unterordner Struktur zusammengefasst werden.
- Für diesen Ordner eine/mehrere Zugriffsgruppen angelegen
  Beispiel: Ordner „Verträge“ → PF0001-gFr_GLW Verträge
- Empfehlung:
  höchstens bis zur Unterordner Ebene 2 unterschiedliche Rechte vergeben

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Zugriffsgruppen
Erstellen von Organisatorischen Gruppen

- Personen, die Zugriff erhalten sollen, sollten aufgrund ihrer Rolle gruppiert werden
- Hierfür Gruppen anlegen (gleiches Vorgehen, anderer Name)
- Beispiele:
  alle Hiwis → PF0001-gO_Hiwis
  Sekretariat → PF0001-gO_Sekretariat

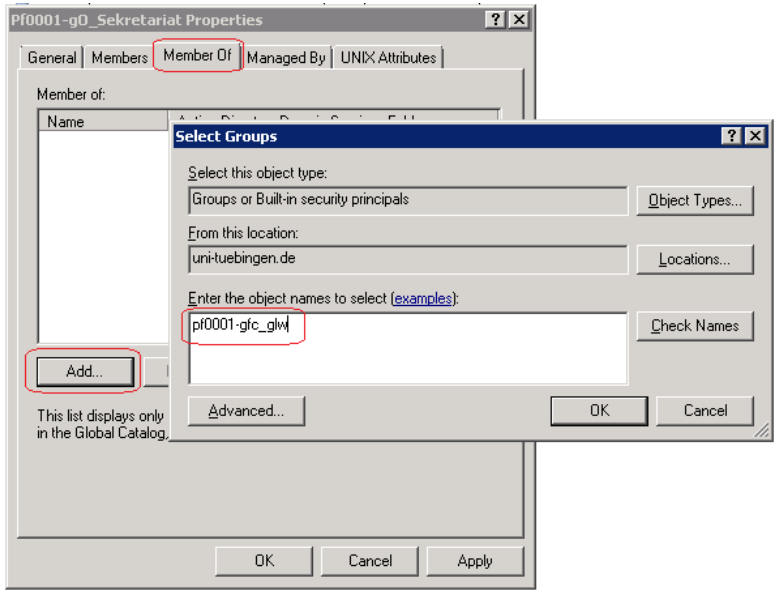
- Zuordnen der Personen in die Organisatorischen Gruppenüber:
  Members > Add > Logon-ID eingeben



EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Zugriffsgruppen
Zuordnen der Org. Gruppen zu den Zugriffsgruppen

- Zuletzt werden die Org. Gruppen entsprechend den benötigten Berechtigungen und die Zugriffsgruppen aufgenommen
- Org. Gruppe auswählen, Menü
  Action > Properties > Member Of > Add > Gruppenname eingeben



EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Dateiberechtigungen
Überblick

- Verbinden des Gruppenlaufwerks
- Zuweisen der Zugriffsgruppen auf Laufwerkebene
- Anlegen der Unter-Ordner
- Zuweisen von Zugriffsgruppen an spezielle Ordner

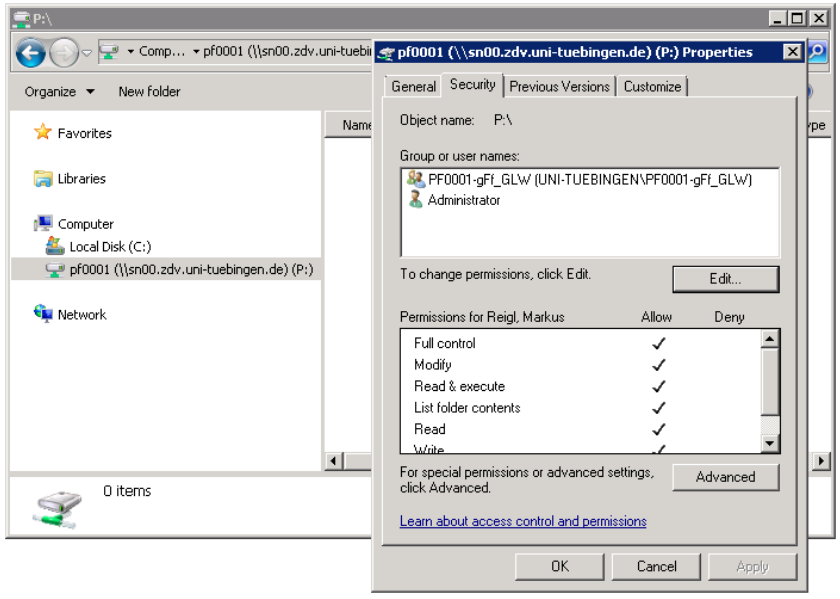
EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

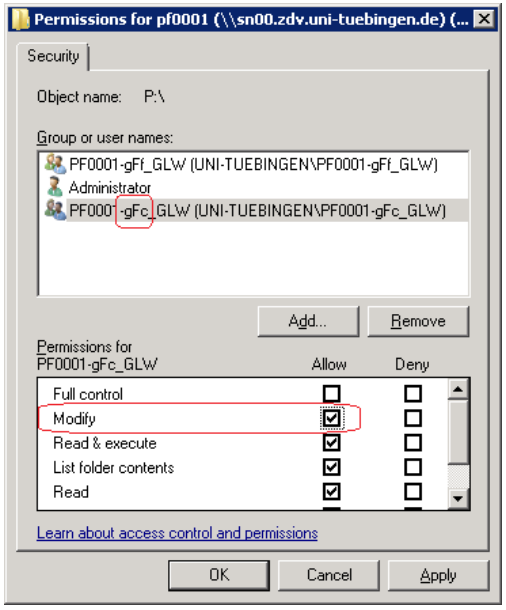
Administration der Dateiberechtigungen
Verbinden des Gruppenlaufwerks

- Die Gruppenlaufwerke erhalten den Namen der Organisatorischen Einheit,
  z.B. Dekanat Philosophische Fakultät → PF0001
- Mappen des Laufwerks über den Explorer
  „\\sn00.zdv.uni-tuebingen.de\PF0001“
- Alternativ über ein Zeilenkommando bzw. eine Batch-Datei
  `> net use G: \\sn00.zdv.uni-tuebingen.de\PF0001 /user:uni-tuebingen\zdvid01`
  hier User-ID „zdvid01“

Administration der Dateiberechtigungen
Zuweisen der Zugriffsgruppen auf GLW-Ebene

- Freigabe auswählen > rechte Maustaste > Properties > Security
- Edit > Add > Gruppenname eingeben
- Berechtigung entsprechend der Gruppe auswählen





EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Dateiberechtigungen
Anlegen der Ordnerstruktur

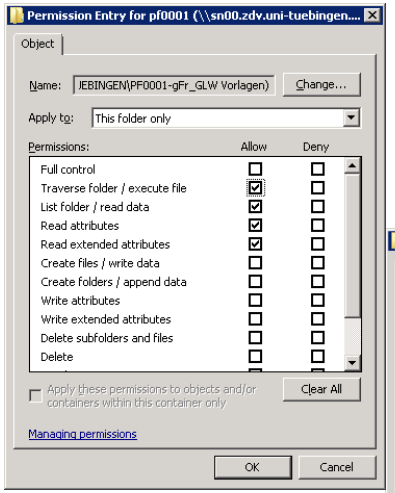
- Anlegen der Ordner der Ebene 1
- Evtl. noch unterschiedliche Berechtigungen auf Ordner-Ebene 2

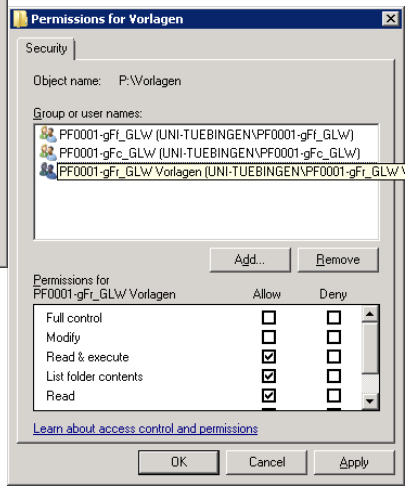
- Niemals: Benutzer-Accounts direkt Rechte auf Ordner geben
- Immer: Berechtigungen über Zugriffsgruppen vergeben
- Normalerweise: Benutzer in Org. Gruppen sammeln und diese in Berechtigungsgruppen aufnehmen
- In Ausnahmefällen: User direkt in Zugriffsgruppen, falls keine Org-Struktur besteht

EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Administration der Dateiberechtigungen
Zuweisen von Zugriffsgruppen an spezielle Ordner

- Zugriffsgruppe benötigt das Recht, den Hauptordner „auflisten“ zu können
- Zuweisen über „Advanced Security Settings“





PF0001\ Listen-Zugriff nur für diesen Ordner (nicht weitervererbt)

PF0001\Archiv Lesender Zugriff für Ordner und alle Unterordner