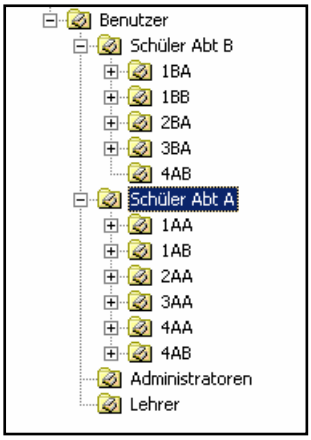
4. Einrichten der ADS

4.1 Die Container in der ADS

Die Planung der ADS sollte sehr gründlich überlegt werden. Vor allem wenn man Aufgaben an Kollegen und Kustoden delegieren will, sollte auf eine saubere Struktur geachtet werden, damit nur gewollte Administrationsrechte übergeben werden können.

Bitte erarbeiten Sie vor der Installation einen eigenen Entwurf. Nachträgliche Änderungen sind sehr aufwändig. Für diesen Entwurf kann mein Vorschlag als Ausgangspunkt dienen. Dieser muss aber unbedingt an die jeweilige Schulsituation angepasst werden.

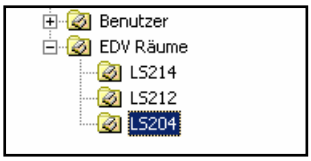


Ich gehe hier von 2 Abteilungen aus, die wiederum mehrere Klassen enthalten.

Vorgangsweise: Im Snap-In Active *Directory-Benutzer und –Container*. Kontextmenü neuer Container: Namen eingeben.

Je nach Bedarf kann der Lehrercontainer auch in Abteilung A und B aufgeteilt werden.

Für die EDV – Räume werden ebenfalls eigene Container angelegt.



4.2 Erstellung der Sicherheitsgruppen in der ADS

Sicherheitsgruppen werden vor allem zur Vergabe von Datei Zugriffsrechten verwendet. Niemals sollten Rechte einzelnen Benutzern zugewiesen werden. Benutzer sind lediglich Mitglieder von Sicherheitsgruppen und erhalten dadurch ihre Zugriffsrechte.

Man unterscheidet Universelle, Globale und Lokale Gruppen. Bitte informieren Sie sich in 18.1 auf der Seite 169

Für unsere Schul-Domäne reicht es aus, **Globale Sicherheitsgruppen** zu verwenden.

Im Container Benutzer gibt es folgende Globale Gruppen:

- **GG_BPA_Schueler**
- **GG_BPA_Admins** Mitglied von *Administratoren* und *Domänen-Admins* und *Schema-Admins*
- **GG_BPA_Lehrer**

Im Container Schüler Abt A gibt es folgende Globale Gruppe:

- **GG_Schueler_A** Mitglied von GG_BPA_Schueler

Im Container Schüler Abt B gibt es folgende Globale Gruppe:

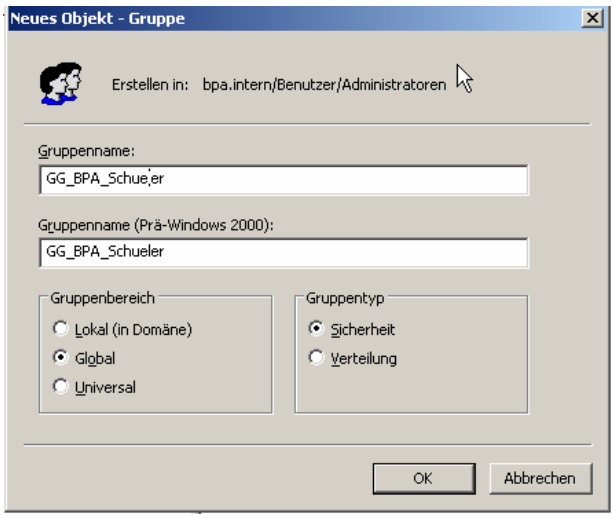
- **GG_Schueler_B** Mitglied von GG_BPA_Schueler

Im Container 1AA es folgende Globale Gruppe:

- **GG_1AA** Mitglied von GG_Schueler_A

Für die anderen Klassen gibt es die entsprechenden Sicherheitsgruppen. Diese können auch automatisiert mit **TJ's Usermanager**[13] angelegt werden.

Vorgangsweise: Im Snap-In **Active *Directory-Benutzer und –Container*** den gewünschten Container wählen.



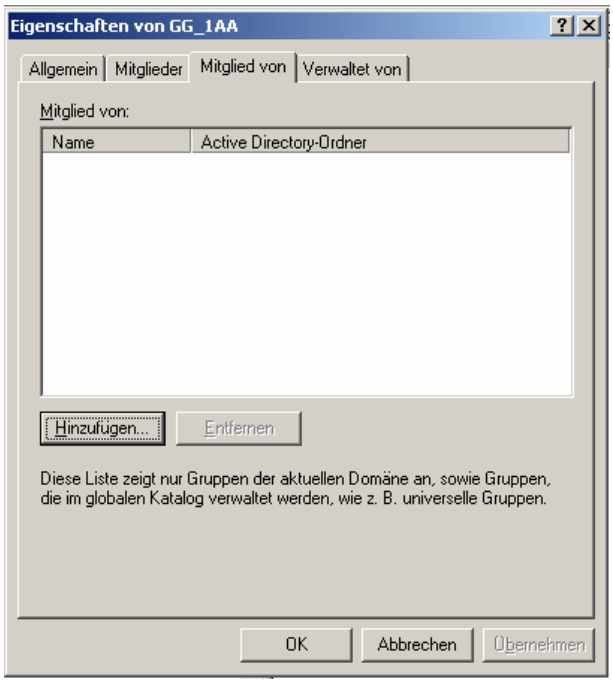
Im Kontextmenü: *NEU -> Gruppe* auswählen.

Gruppenname Eingeben

Gruppenbereich und Typ wie voreingestellt.

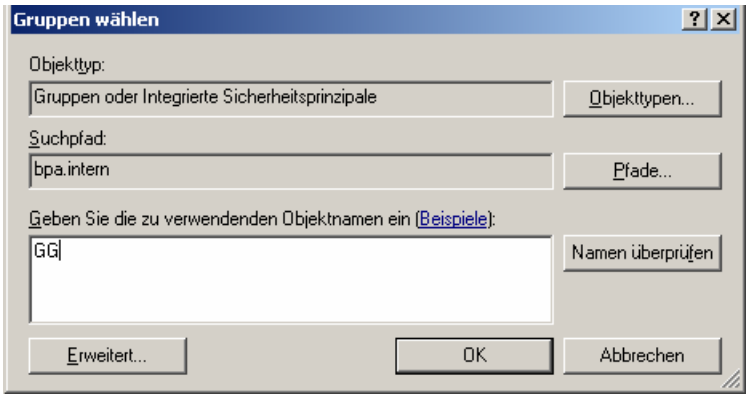
[13] Siehe 7.3

Gruppenmitgliedschaft schachteln:

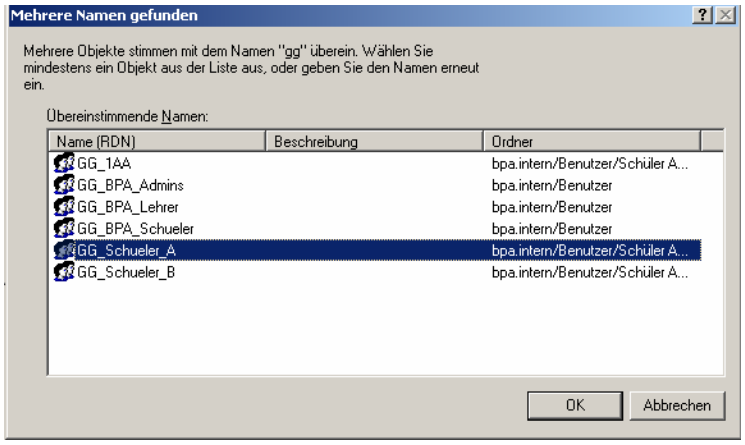


Eigenschaften der Gruppe wählen:
Register *Mitglied von*

Schaltfläche *Hinzufügen*.



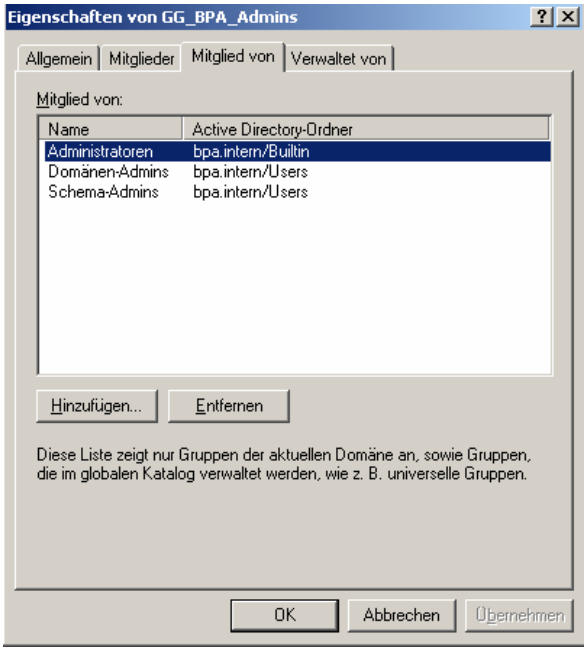
Geben Sie den gesamten Namen oder einen Teil des Namens ein und bestätigen sie mit *OK*.



Werden mehrere Namen gefunden so kann man zwischen diesen auswählen.

Mit *OK* bestätigen.

Erstellen Sie nun die Sicherheitsstruktur.



Nebenstehend sehen Sie die Mitglieder der Gruppe *GG_BPA_Admins*

Weitere Gruppen

Erstellen Sie im Container Benutzer noch folgende Gruppen:

- **GG_Passwort_Admins** Mitglieder dürfen Passwörter zurücksetzten
- **GG_Admins_Abt_A** dürfen Schüler in Abteilung A anlegen
- **GG_Admins_Abt_B** dürfen Schüler in Abteilung B anlegen
- **GG_Test_Schueler** Schüler, die Tests schreiben[14]. Diese Gruppe ist Mitglied von GG_BPA_Schueler

4.3 Profile und Basisordner am Fileserver

Die Freigaben und Dateiberechtigung am FILE Server bedürfen einer ebenso sorgfältigen Planung wie die ADS.

Auf welchem Server die Daten gespeichert werden, ist eigentlich egal. Dies können die Domänencontroller sein, oder ein eigenständiger FILE Server.

Ob die Lehrerdaten und Schülerdaten auf der selben Partition liegen ist ebenfalls „Geschmackssache“. Ein Vorteil von einer Partition ist sicherlich, dass kein Speicherplatz verschwendet wird. Ein Nachteil ergibt sich, wenn man jedes Jahr die Schülerdaten löscht, dies geht dann nicht durch einfaches Formatieren. Außerdem werden die Quotas (Speicherplatzbeschränkungen) komplizierter zu handhaben, da diese nur pro Abteilung einstellbar sind.

[14] siehe 4.4

Wir legen für die Lehrerdaten einen Ordner mit dem Namen **ldat** an. Darunter gibt es die Verzeichnisse **lhomes** für das Basisordner (Homelaufwerk) und das Verzeichnis **lprofiles** für das Profil[15] der Lehrer.
Analog benötigen wir das Verzeichnis **sdat** mit den Unterverzeichnissen **shomes** und **sprofiles** für die Schülerdaten. Das ganze ist in der nebenstehenden Abbildung dargestellt.

4.4 Freigaben und Dateiberechtigungen

Homeverzeichnis (=Basisordner) Schüler

Das Homeverzeichnis des Schüler Max Muster in der Klasse 1AA der Abteilung A würde in folgendem Netz-Pfad liegen:

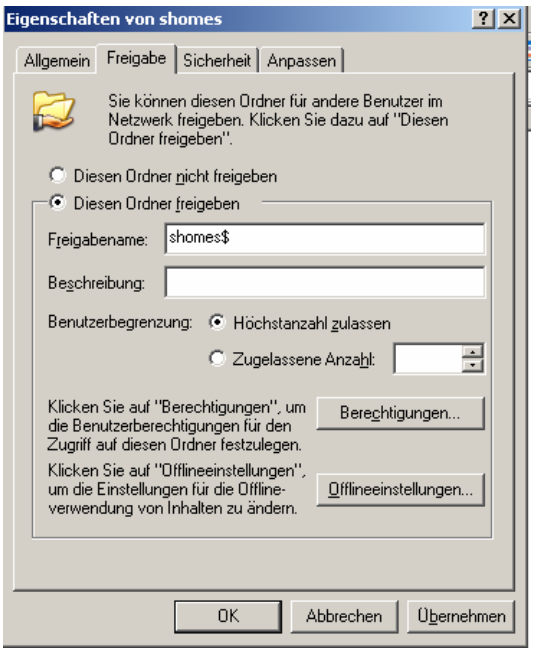
\\srv01\shomes$\AbtA\1AA\max.muster

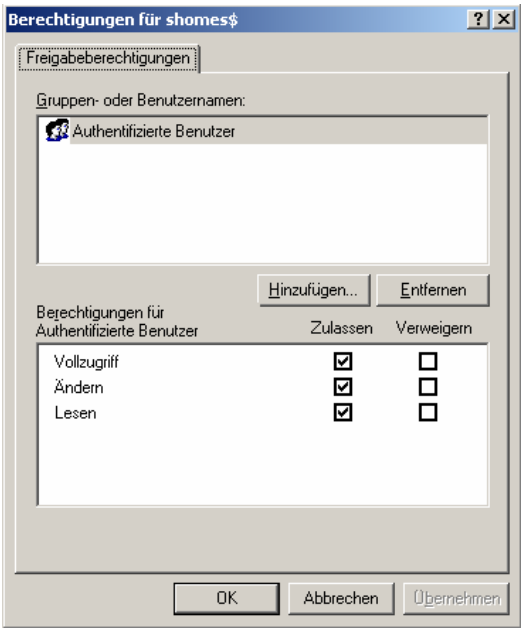
Dies würde am Server z.B. folgenden Pfad entsprechen:
\\e:\sdat\shomes\AbtA\1AA\max.muster

Damit die Schüler nicht auf die Homeverzeichnisse der anderen Schüler zugreifen können, müssen einige Einstellungen getroffen werden.
Durchführung:
Geben Sie den Ordner **shomes** unter folgenden Namen frei: **shomes$**.
Das $ Zeichen bedeutet, dass es sich um eine „versteckte“ Freigabe handelt. Diese wird nicht automatisch in der Netzwerkumgebung aufgelistet.
Für die Berechtigungen einer Freigabe gibt es zwei verschiedene Methoden:
Grobe Einstellungen können unter den **Freigabeberechtigungen** vergeben werden. Feinere Berechtigungen werden über die **NTFS – Einstellungen** (Register Sicherheit) vergeben. Es empfiehlt sich aber nur an einer Schraube zu drehen und keine Mischung zwischen Freigabe und NTFS Berechtigungen durchzuführen. Deshalb werden ich hier nur die NTFS Berechtigungen benutzten.

[15] siehe 18.19

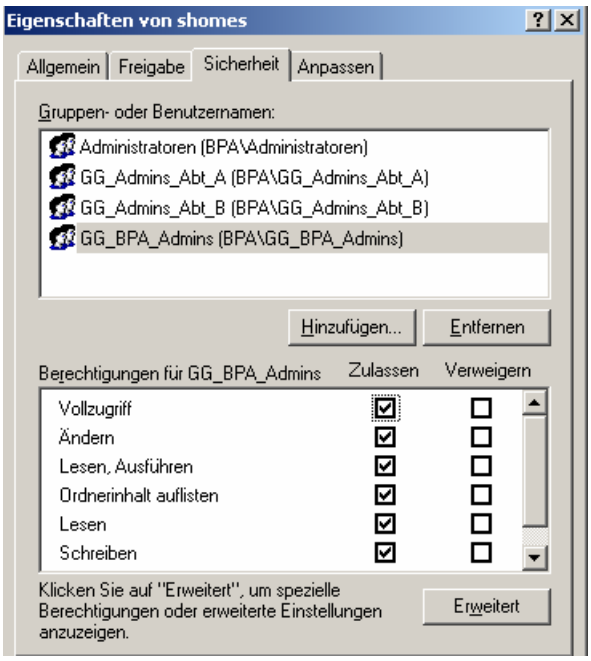
Klicken Sie auf die **Berechtigung** der **Freigabe:** Entfernen sie Jeder[16] und fügen Sie die Gruppe **Authentifizierte Benutzer** hinzu. Geben Sie dieser Gruppe Vollzugriff.





Die Gruppe *Authentifizierte Benutzer* entspricht der Gruppe *jeder* ohne anonymen Benutzern oder Gästen.

Unter dem Register **Sicherheit** stellen Sie nun die NTFS Berechtigung ein.



Löschen Sie alle bestehenden Einträge und geben Sie den Gruppen **Administratoren**, **GG_BPA_Admins**, **GG_Admins_Abt_A** sowie **GG_Admins_Abt_B** Vollzugriff.

Wenn man die Berechtigungen jetzt betrachtet könnte man meinen, dass die Schüler keinen Zugriff auf ihr Homeverzeichnis bekommen. Dies ist jedoch falsch. Das Homeverzeichnis wird nämlich durch das System (mit den Rechten eines Benutzers aus der Gruppe der Administratoren), beim Anlegen eines Benutzers erstellt.

[16] Im Unterschied zu Windows 2000 hat in 2003 die Gruppe *Jeder* nur Lesezugriff.

Anschließend wird dem Benutzer Vollzugriff gewährt.

Damit dies funktioniert müssen allerdings die Ordner **AbtA** und dessen Unterordner **1AA** existieren. Die Einstellungen für den Basisordner lauten dann
\\srv01\shomes$\AbtA\1AA\%username%
Leichter geht das Ganze wenn die Benutzer durch *TJ's Usermanager* (siehe 7.3) angelegt werden. Mit diesem Programm wird die Ordner Struktur selbstständig erstellt. Es müssen lediglich die Freigaben bestehen.

Durch die oben beschriebenen Einstellungen ist es sichergestellt, dass die Schüler einerseits keine anderen Homeverzeichnisse lesen können und anderseits auch keine eigenen Ordner in *shomes* anlegen können. Der Schüler kann sich nicht einmal dorthin verbinden.

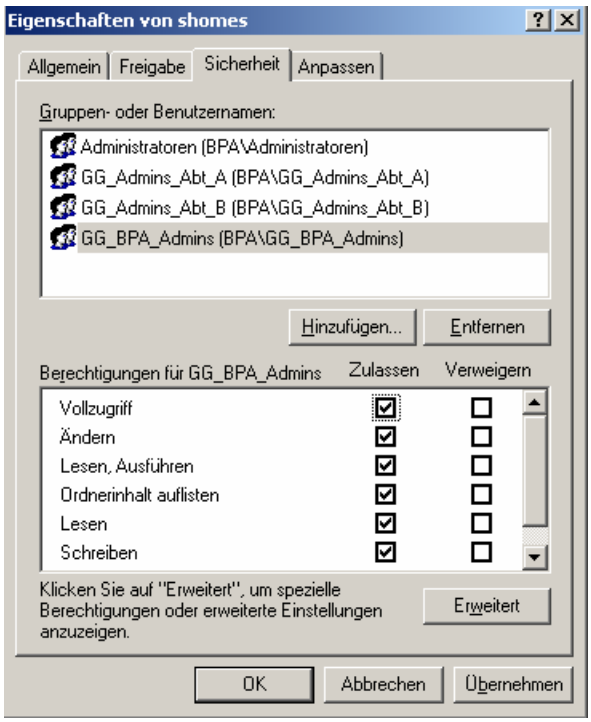
Homeverzeichnis (=Basisordner) Lehrer

Das Homeverzeichnis der Lehrer wird analog zum Homeverzeichnis der Schüler angelegt. Der Basisordner für den Lehrer *Thorsten Jarz* ist im Netz unter folgendem Pfad erreichbar:

\\srv01\lhomes$\thorsten.jarz

Dies würde am Server z.B. folgendem Pfad entsprechen:
\\e:\ldat\lhomes\thorsten.jarz

Damit Schüler und andere Lehrer nicht auf die Homeverzeichnisse der anderen Lehrer zugreifen können, müssen die folgenden Einstellungen getroffen werden.



Durchführung:
Geben Sie den Ordner **lhomes** unter folgenden Namen frei: **lhomes$**.

Klicken Sie auf die **Berechtigung** der **Freigabe:** Entfernen Sie *Jeder* und fügen Sie die Gruppe **Authentifizierte Benutzer** hinzu. Geben Sie dieser Gruppe Vollzugriff.

Unter dem Register Sicherheit stellen Sie nun die NTFS Berechtigung ein. Löschen Sie alle bestehenden Einträge und geben Sie den Gruppen **Administratoren**, **GG_BPA_Admins**, **GG_Admins_Abt_A** sowie **GG_Admins_Abt_B** Vollzugriff.