

Gruppenrichtlinien auf einigen Computern ausschließen, Softwareverteilung differenzieren

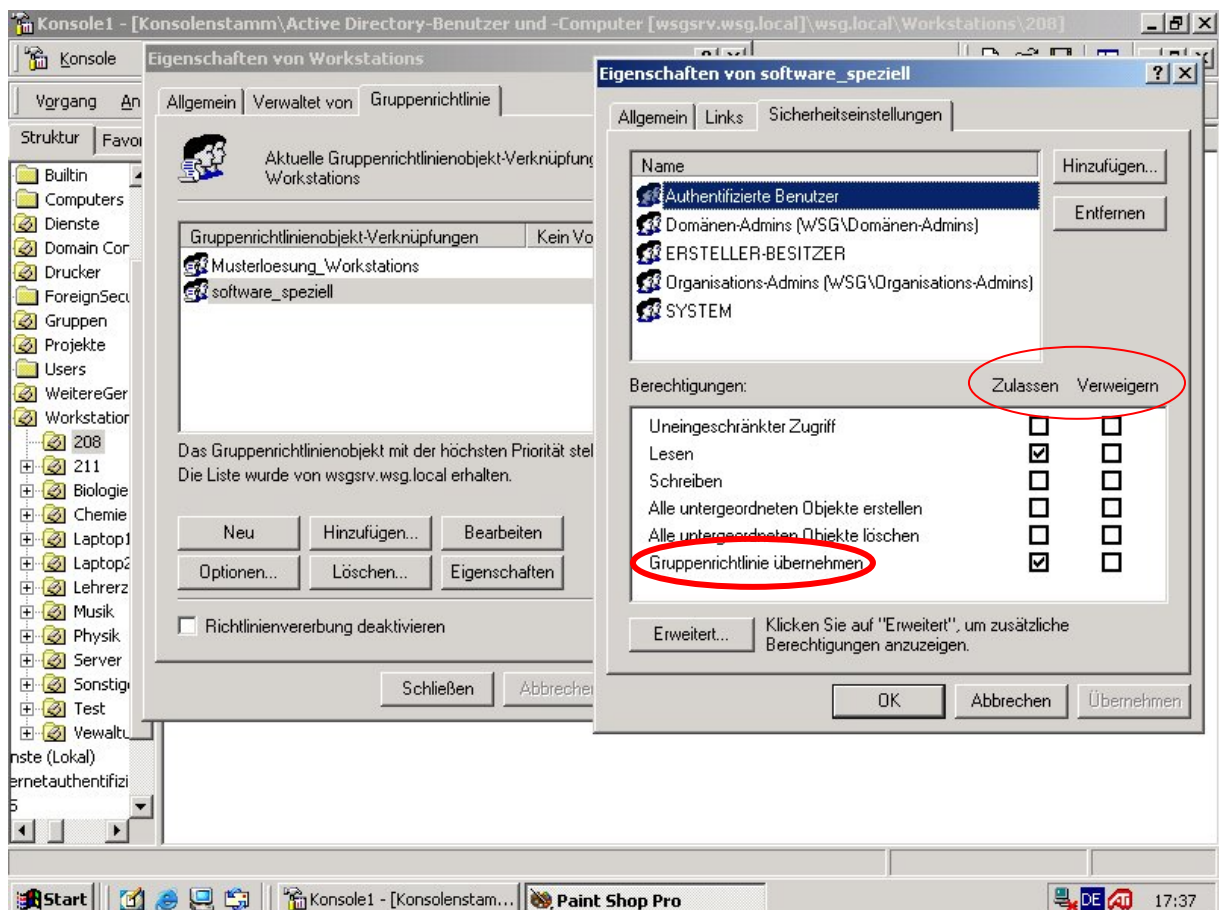
Diese Anleitung erläutert, wie man es erreichen kann, dass eine Gruppenrichtlinie nicht auf *alle* Mitglieder einer OU angewendet wird.

Man kann dadurch z.B. einen oder mehrere Computer eines Raums von der Softwareverteilung ausschließen, oder genauso einen Schüler einer Klasse mit speziellen Einschränkungen versehen oder davon ausnehmen.

In allen Fällen muss man diese Festlegungen in einer *eigenen Gruppenrichtlinie*¹ vornehmen. Diese GPO wirkt sich ja zunächst auf *alle* Objekte der OU aus, an die sie gekoppelt ist.

Einschränken kann man dieses Verhalten jedoch über die Sicherheitseinstellungen des Gruppenrichtlinienobjekts.

So sehen die Defaulteinstellungen aus: An den „Raum“, hier also die OU 208, sind zwei Gruppenrichtlinien gebunden. Die untere, software_speziell, soll Software an alle Computer in diesem Raum *mit einer Ausnahme* verteilen.



System, Administratoren und ERSTELLER haben Zugriffs- und Änderungsrechte auf das Objekt, ähnlich wie die Rechte bei einer Datei. Das ist für die weitere Vorgehensweise irrelevant.

¹ Ausnahme: Softwareverteilung. Siehe Ende dieser Anleitung.

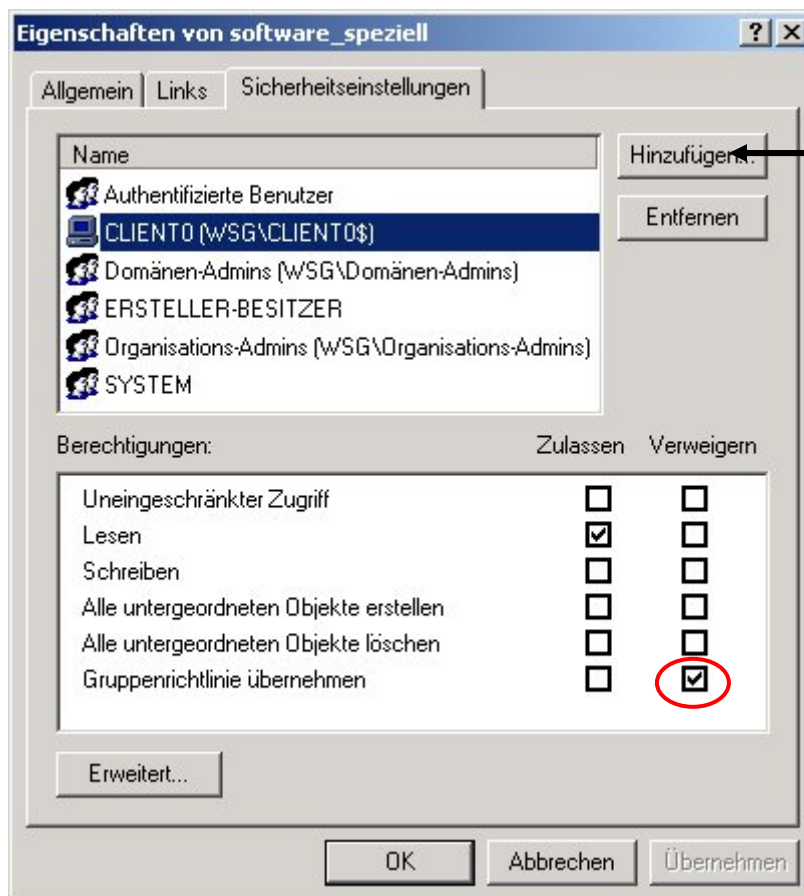
Interessant wird es bei „Authentifizierter Benutzer“. Zu diesen gehören alle *Benutzer*, aber auch *Workstations*, die das System kennt, die also an irgendeiner Stelle in der ADS eingetragen sind.

Und hier findet man – eingetragen als unterstes Recht – die Möglichkeiten, die Gruppenrichtlinie zu übernehmen oder aber auch die Übernahme zu verweigern.

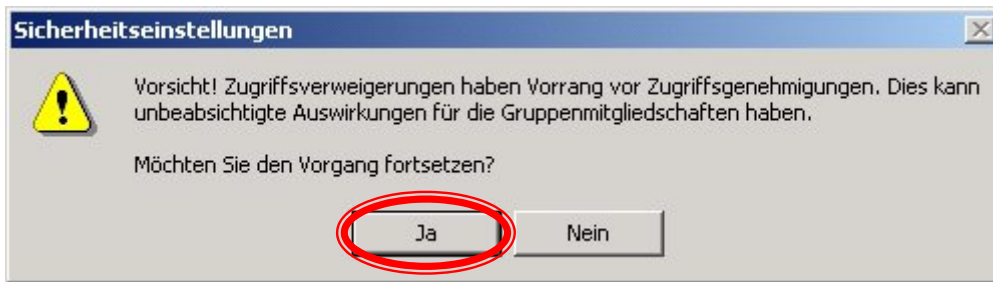
Nochmals: per Standard übernehmen *alle* Benutzer/Workstations, die in besagter OU stehen, die GPO; alle anderen nicht.

Aber: man kann Ausnahmen davon definieren. So könnte es sein der LehrerPC, der wegen BSA dem selben Raum wie die Schülerrechner zugeteilt sein muss, soll eine bestimmte Überwachungssoftware nicht aufinstalliert bekommen.

Ganz einfach: dann verbieten wir bei ihm halt die Übernahme der MSI-Verteilungs-GPO!



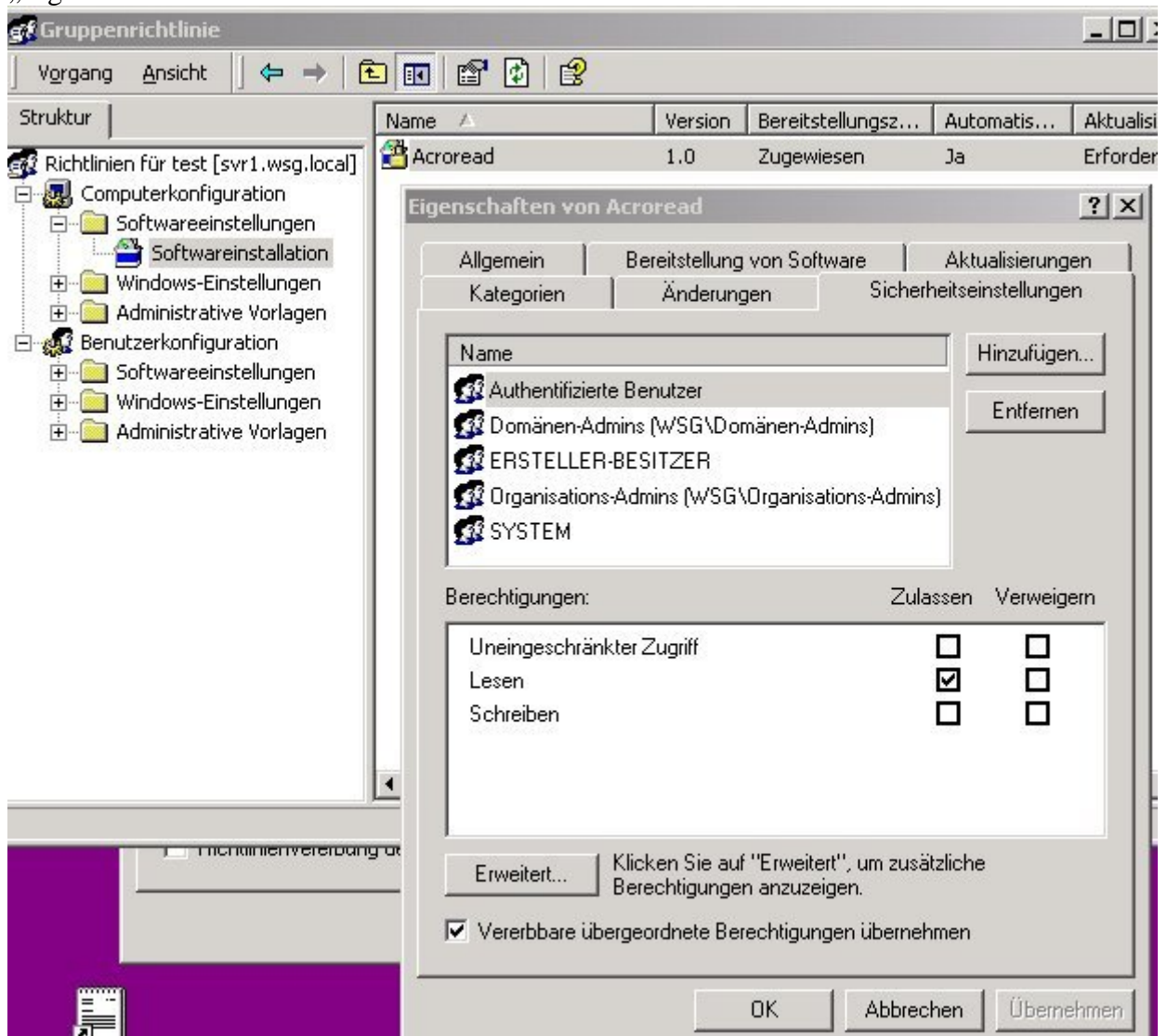
Über den Button „Hinzufügen“ wählt man ein Objekt (oder ein Gruppe, die man zuvor aus mehrere Objekten zusammengestellt hat) aus der ADS aus und verweigert ihm die Übernahme der Richtlinie. Der entsprechende PC „Client0“ bliebe dann in unserem Beispiel von der Verteilung der Software ausgenommen. Hat man z.B. 25 PCs in einem Raum aber nur 20 Lizenzen für eine Software, so könnte man PC20-PC25 in eine Gruppe zusammenfassen und dieser Gruppe die Übernahme der GPO verweigern. Zwar sind sie immer noch bei den authentifizierten Benutzern dabei, aber im Zweifelsfall ist die Maßnahme „verweigern“ die, die sich durchsetzt.



Wollen Sie hingegen nur einem oder wenigen Computern/Benutzern eine Richtlinie zuteilen, so löschen Sie den Eintrag „Authentifizierte Benutzer“ und fügen Sie dann das Objekt/die Objekte mit dem Kreuz bei „GPO übernehmen – zulassen“ hinzu.

Geht es Ihnen nur um die Zuweisung eines einzigen Softwarepaket, können Sie dieselbe Methode auch für dieses Paket anwenden.

Wählen Sie dazu in der ADS das Softwarepaket mit der rechten Maustaste, klicken Sie „Eigenschaften“.



Wählen Sie den Reiter „Sicherheitseinstellungen“ und gehen Sie an dieser Stelle genauso vor, wie oben beschrieben.



Solche Änderungen sollten Sie gut dokumentieren. Ansonsten werden Sie in einigen Monaten evtl. viel „Spaß“ und wenig Erfolg bei der Fehlersuche haben!

Weitere Beispiele und eine ausführliche Erklärung findet man auf der sehr empfehlenswerten Internetseite www.gruppenrichtlinien.de unter howto- Richtlinien für Benutzergruppen. Hier geht es dann in erster Linie um Ausgrenzung von Benutzer(gruppen), sowie unter Softwarezuweisung.

Autor: Martin.Resch@pythi.de, Stand: 11/2003

Haftungsausschluss: Diese Anleitung wurde mit großer Sorgfalt erstellt, trotzdem erfolgt die Anwendung bei Ihrem System auf eigenes Risiko.