paed**ML**® Windows

Gruppenrichtlinien für Fortgeschrittene

Anwendungen der GPOs einschränken,
Bildschirmschoner, Hintergrundbilder

Stand: 21.04.2013

zkn
Zentrale Konzeptionsgruppe Netze

Impressum

Herausgeber
Zentrale Konzeptionsgruppe Netze (ZKN)
an der Landesakademie für Fortbildung und Personalentwicklung an Schulen

Autoren
Andreas Mayer,
Martin Resch

Endredaktion
Martin Resch

Weitere Informationen
http://www.lehrerfortbildung-bw.de/netz/

Veröffentlicht: 2012

Inhaltsverzeichnis

1. Vorbemerkungen/Vorbereitungen

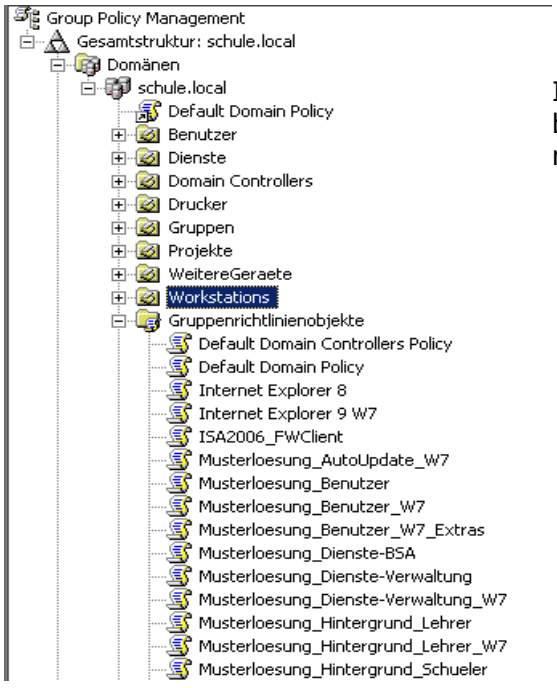
Gruppenrichtlinie sind eine feine Sache – der Administrator kann damit vom Server aus zentrale Vorgaben an alle Computer im Netz zuordnen.

Einige Einstellungen, besonders Beschränkungen im Zugriff auf systemrelevante Einstellungen, sind bereits von der paedML vorgegeben.

Standardmäßig nimmt jeder Administrator außerdem die Zuweisung seiner Softwarepakete (MSI) auf diese Weise vor. Mit Gruppenrichtlinien geht jedoch noch viel mehr - diese Anleitung möchte Ihnen ein paar Beispiele dazu geben. Sie ist ausdrücklich an fortgeschrittene Netzwerkbetreuer gerichtet, denn Fehlkonfigurationen in den Gruppenrichtlinien lassen sich nicht in jedem Fall ohne Weiteres rückgängig machen und können das Netzwerk stark beeinträchtigen.

1.1. Der Gruppenrichtlinien-Editor

Alle Einstellungen an den Gruppenrichtlinien werden über den Gruppenrichtlinienverwaltung vorgenommen (*gpmc.msc*) vorgenommen, die man über *Start*|*Programme*|*Verwaltung* aufrufen kann.

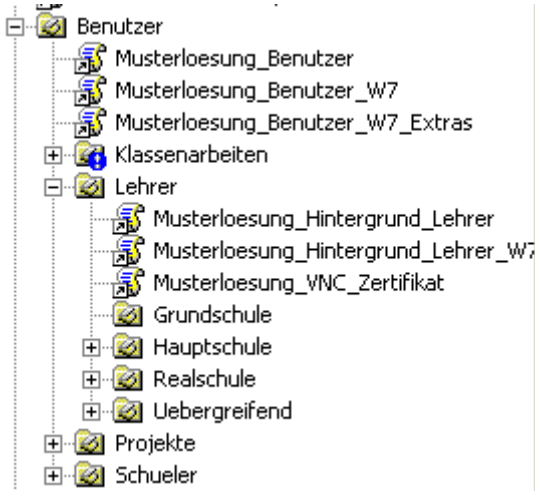


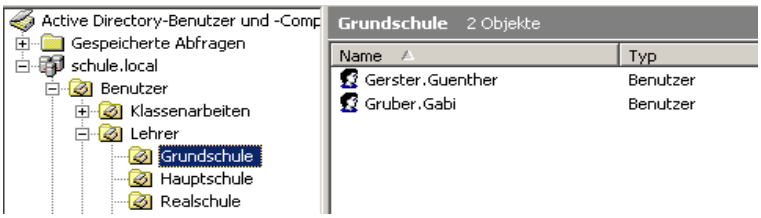
Im oberen Bereich finden Sie ein Abbild der Domänenstruktur, die für uns relevanten Zweige sind *Benutzer* und *Workstations*.

Weiter unten sind alle Gruppenrichtlinie aufgeführt, die überhaupt vorhanden sind. Alle, die mit „*Musterloesung_*" beginnen, sollten Sie nach Möglichkeit unverändert lassen. Sie können bei einem Update überschrieben werden.

1.2. Die Wirkung von GPOs

GPO ist die Abkürzung von *GroupPolicyObjekt*, also einer einzelnen Gruppenrichtlinie. GPOs werden immer an eine OU (also einen „Ast" in der Domänenstruktur) angebunden und wirken dann auf alle Objekte, die sich in diesem Bereich oder einen darunter liegenden befinden (sogenannte Vererbung).



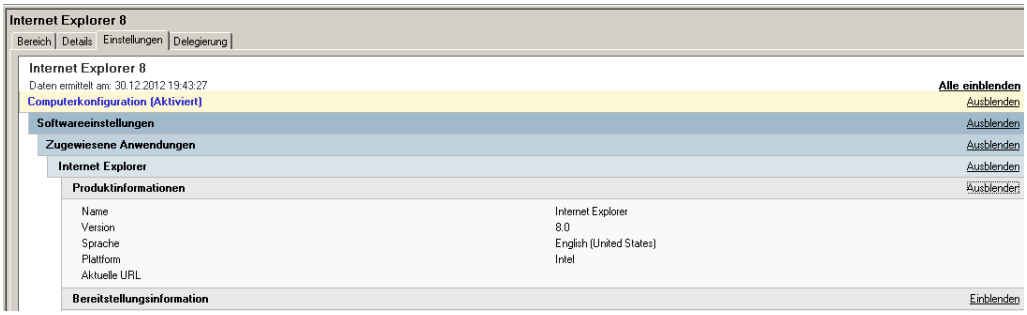


GPOs Active Directory

In der Abbildung sieht man zum Beispiel, dass die *GPOs Musterloesung_Benutzer*, *Musterloesung_Benutzer_W7* und *Musterloesung_Benutzer_W7_Extras* Auswirkung auf alle Lehrer, Projekte und Schueler haben, auch wenn sich die Lehrer erst in der Untereinheit Grundschule befinden. Welche Lehrer das konkret sind, kann man in dieser Ansicht nicht erkennen, dazu muss man in der Active Directory nachsehen (rechtes Bild). Für die Lehrer kommen außerdem drei zusätzliche GPOs dazu.
Das blaue Ausrufungszeichen bei den Klassenarbeiten bedeutet, dass hier die Vererbung der Gruppenrichtlinien unterbunden wurde; die drei erstgenannten wirken sich also auf diese Benutzer nicht aus.

1.3. Einstellungen von Gruppenrichtlinien

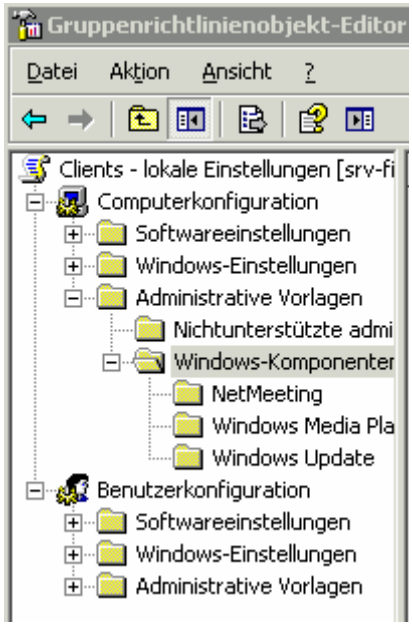
Eine einzelne Gruppenrichtlinie kann man per rechtem Mausklick an einer OU neu erstellen, man kann bereits vorhandene GPOs an eine neue OU ankoppeln oder man kann bestehende Gruppenrichtlinien bearbeiten.
Klickt man links auf eine bestehende Gruppenrichtlinie, kann man sich im Hauptfenster die vorgenommen Einstellungen anzeigen lassen (Reiter *Einstellungen*) .



Auf den Reiter *Bereich* werden wir später zurückkommen.

1.4. Wirkungsweise von Gruppenrichtlinien

Gruppenrichtlinien (GPO) bestehen aus zwei verschieden Abschnitten:



- einem Teil, in dem Einstellungen für Computer vorgenommen werden, und dem
- anderen Teil, in dem Einstellungen für Benutzer vorgenommen werden.

Es macht keinen Sinn, in *einer* GPO beide Einstellungen einzutragen, da sie ja später entweder Benutzern oder PCs zugeordnet ist, nicht aber beiden zugleich. Um GPOs sowohl Benutzern als auch *gleichzeitig* PCs zuzuordnen, sind ziemliche Verrenkungen notwendig, darauf wird später eingegangen.

Beim **Hochfahren** übernimmt ein PC die Einstellungen aus dem Bereich Computer-konfiguration, Einstellungen im Bereich Benutzerkonfiguration werden dabei ignoriert.

Meldet sich ein Benutzer dann an einem Computer an, werden nur die Einstellungen aus dem Bereich Benutzerkonfiguration übernommen, Einstellungen im Bereich Computerkonfiguration werden ignoriert.

Es ist also sehr wichtig, die jeweiligen Einstellung immer nur den zutreffenden OUs im Active Directory zuzuordnen. Benutzereinstellungen bei Workstations wirken sich nicht aus.

1.5. Die unterschiedlichen Einstellmöglichkeiten

Zunächst sind die Einstellmöglichkeiten in drei Hauptpunkte unterteilt:

1. **Softwareverteilung**. Die paedML sieht das nur computerbezogen vor, und das Verfahren ist unter [7] ausführlich dokumentiert.
2. **Windowseinstellungen**. Hier geht es insbesondere um Berechtigungen, Start- und Anmeldeskripte (siehe hierzu [4] und [5]), eingeschränkte Gruppen (sind in der Regel ohne Relevanz, ein Beispiel zu den lokalen Administratoren finden Sie aber unter [6]), Datei- und Registryberechtigungen ([8]) und einige sehr spezielle Einstellungen zum Thema Sicherheit und lokalen Diensten etc.
3. **Administrative Vorlagen**: hier werden im weitesten Sinne Software- (auch Windowseinstellungen) vorgenommen. Diese Einstellmöglichkeiten sind erweiterbar. Sie wirken sich auf die Registry des Clients aus.

1.6. Vererbung; gpresult auf den Clients

Die Standardvorgabe von Gruppenrichtlinien ist, dass sie von einer OU auf die darunter liegenden weitergereicht wird, eine auf *Workstations* definierte Gruppenrichtlinie wirkt also auch auf alle Rechner, die in den Räumen *EDV1, EDV2* usw. sind.

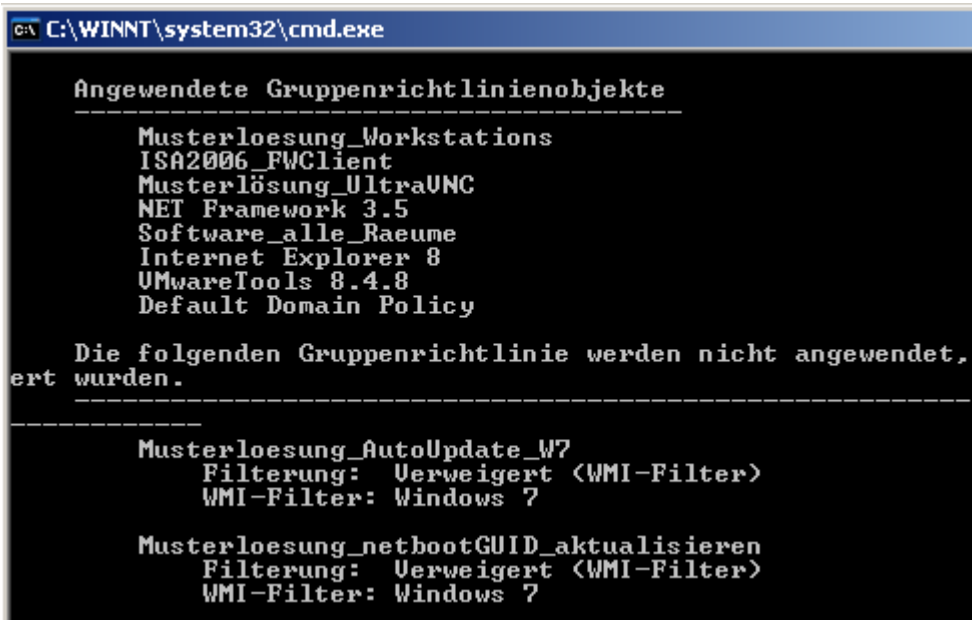
Dieses Verhalten ist in der Regel auch sinnvoll. Es kann aber auch für Ausnahmefälle ausgeschaltet werden, dann aber nur global für alle GPOs.

Auf den Clients kann mit dem Tool *gpresult* abgerufen werden, welche Gruppenrichtlinie tatsächlich beim Hochfahren angewendet wurde.

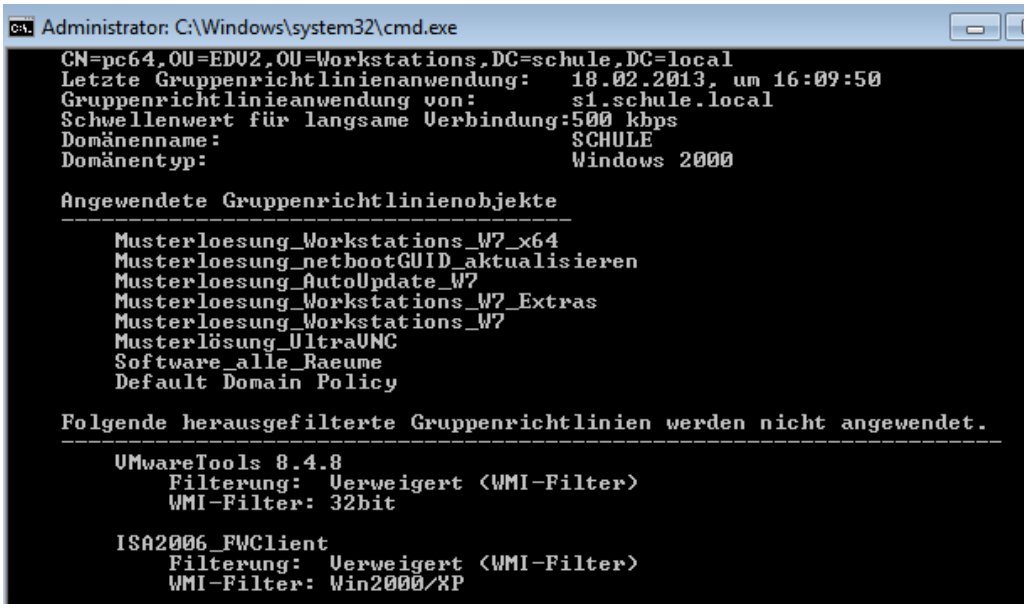
Übung 1:

1. Melden Sie sich an einem Client als *pgmadmin* an.
2. Öffnen Sie über *Start|Ausführen|cmd* ein Eingabefenster.
3. Geben Sie *gpresult* (XP) bzw. *gpresult /r* (Windows 7) ein.
4. Analysieren Sie die Ausgabe.

Je nach Situation wird sich die Ausgabe unterscheiden: Auf einem XP-Client könnte sie in etwa so aussehen:



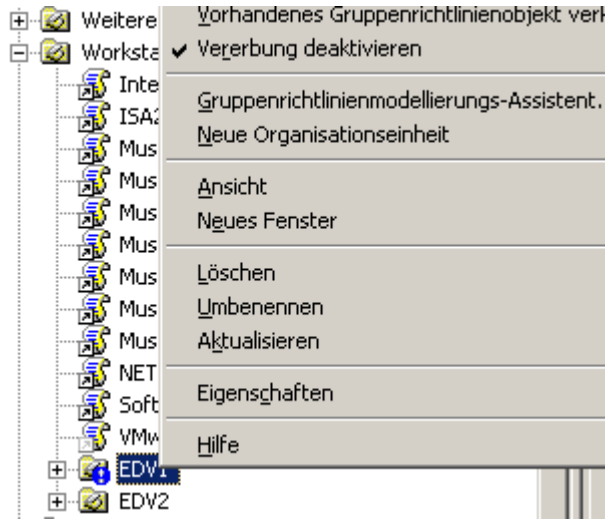
Man erkennt deutlich, welche GPOs auf den Client wirken. Außerdem sind diejenigen aufgeführt, die durch einen WMI-Filter keine Wirkung auf den entsprechenden Client zeigen. Bei einem Windows 7-Client mit 64bit-Betriebsystem ändert sich das Bild entsprechend:



Über WMI-Filter später mehr.

Übung 2:

1. Deaktivieren Sie die Vererbung der Gruppenrichtlinien auf *EDV1*. Klicken Sie dazu in der Gruppenrichtlinienverwaltung mit der rechten Maustaste auf *EDV1* und wählen Sie die Zeile *Vererbung deaktivieren*.
   In der GPO erscheint dann ein blaues Ausrufungszeichen und der Haken bei Vererbung deaktivieren (s.u.).



2. Starten Sie den Client neu. Melden Sie sich als *pgmadmin* an und überprüfen Sie mit *gpresult* die Änderung.

Leider kann man die Vererbung nicht nur für einzelne GPOs deaktivieren. Umgekehrt kann man aber erzwingen, dass die Deaktivierung der Vererbung für einzelne GPOs nicht durchgeführt wird.

Übung 3:

1. Klicken Sie auf einzelne GPOs mit der rechten Maustaste und aktivieren Sie *Erzwungen*.
2. Starten Sie wiederum den Client neu und überprüfen Sie das Ergebnis mit *gpresult*.
3. Machen Sie anschließend die Änderungen der beiden Übungen wieder rückgängig.

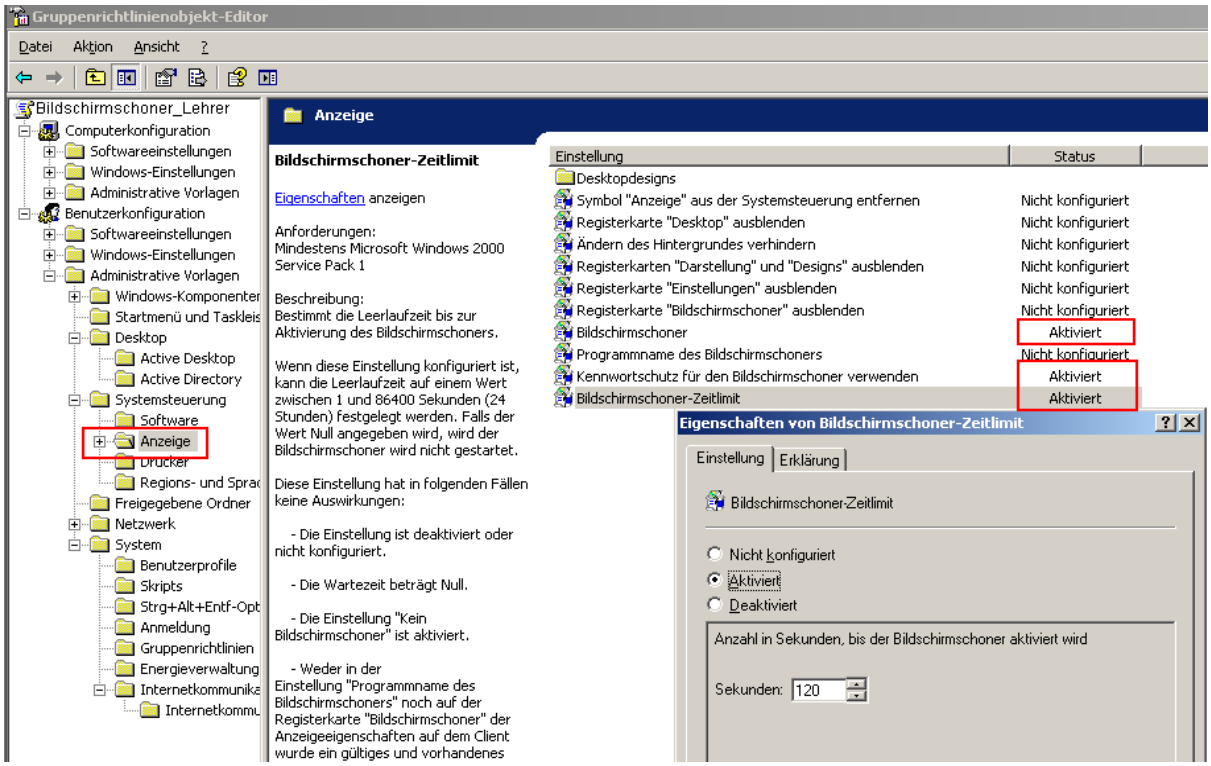
1.7. Konfiguration von Bildschirmschonern

Vieles in den folgenden Abschnitten geht um das praxisnahe Thema Bildschirmschoner. Um an diesem Beispiel einige Möglichkeiten zu erklären, werden im Folgenden ein paar Vorbereitungen getroffen.

Übung 4: Erstellen Sie eine Gruppenrichtlinie für Lehrer, die nach 2 Minuten einen Bildschirmschoner veranlasst, bei dessen Reaktivierung man ein Kennwort benötigt.

1. Starten Sie die Gruppenrichtlinienverwaltung (*Start – Programme – Verwaltung*).
2. Erstellen Sie eine neue Gruppenrichtlinie „*Bildschirmschoner_Lehrer*" für die Benutzergruppe „Lehrer".
3. Navigieren Sie zu: *Benutzerkonfiguration – Administrative Vorlagen – Systemsteuerung – Anzeige*

4. Konfigurieren Sie diese Gruppenrichtlinie so, dass nach z.B. 60 Sekunden[1] der Bildschirmschoner eingeschaltet wird und bei der „Wiederbelebung" das Kennwort eingegeben werden muss.
(Siehe Markierungen im Screenshot)



Übung 5: Melden Sie sich als Lehrer an einem PC an und testen Sie, ob der Bildschirmschoner wie gewünscht aktiviert wird.

Da ohne eine kennwortgeschütze Bildschirmsperre unmittelbar auf private Daten des angemeldeten Benutzers zugegriffen werden kann und je nach Situation die Privilegien des Benutzers auch missbraucht werden könnten, ist eine Bildschirmsperre für den Administrator Pflicht, für die Lehrer sehr empfehlenswert. Das Sperren der Arbeitsstationen hat jedoch auch Nachteile, denn nur der angemeldete Benutzer selbst kann die Sperre wieder aufheben, der Administrator könnte ihn gegebenenfalls zwangsabmelden. Ist der PC nicht der einzige in einem Raum, könnte ein anderer Lehrer in auch von einem anderen Rechner per Schulkonsole aus abmelden[2]. Die letzte Möglichkeit wäre es noch, den Rechner per Ausschalter herunterzufahren und dann neu zu starten.

1 Im Schulbetrieb sind eher 5 Minuten sinnvoll.
2 Diese Möglichkeit sollte dann im Kollegium geschult werden. Ein gesperrter Rechner schafft sonst unmittelbar Frust und Verdruss, insbesondere wenn der „Schuldige" die Schule vielleicht schon in Richtung nach Hause verlassen hat...

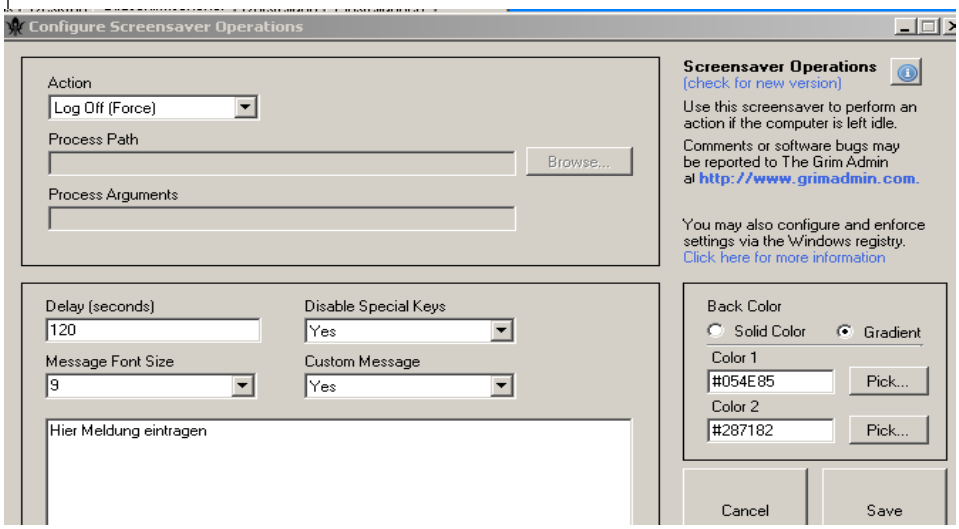
Als Alternative wäre es denkbar, statt dem Bildschirmschoner eine Abmeldung vorzunehmen. Auch das hat natürlich Nachteile, denn in diesem Fall gehen nicht gespeicherte Änderungen verloren. Sicherlich keine so gute Idee für den Computerraum, wo der Lehrer nach der Beantwortung einer Schülerfrage seinen Rechner abgemeldet wieder vorfindet...

Diese Möglichkeit lässt sich über zwei spezielle Bildschirmschoner verwirklichen.

- Der aus dem Microsoft NT Resource Pack stammende *winexit.scr*, der allerdings nur bis Windows XP funktioniert oder
- *Screensaver Operations.scr* von Grimsoft [3] bietet erweiterte Möglichkeiten und funktioniert auch mit Windows 7.

Übung 6: Abmeldebildschirmschoner installieren und konfigurieren

1. Verteilen Sie das MSI-Paket *ssoperations_1.3_setup* an alle Workstations.
2. Starten Sie den PC1 (neu) und melden Sie sich als Administrator an.
3. Wählen Sie den neuen Bildschirmschoner *Screensaver Operations* aus (rechte Mautaste auf den Desktop, Eigenschaften - Bildschirmschoner) und konfigurieren Sie ihn über Einstellungen so, dass er nach 2 Minuten eine ansprechende Meldung[3] ausgibt und einer weiteren Minute ein forced logout[4] durchführt (s. Bild auf der Folgeseite).
   Über *Vorschau* können Sie die Einstellungen testen.



Die jetzt vorgenommene Konfiguration gilt nur für den Administrator. Man könnte sie jetzt auch als aproflehrer und -schueler durchführen und dann das Profil kopieren. Das hat jedoch einige Nachteile:

1. Das Verfahren ist sehr unübersichtlich und muss ggf. recht oft durchgeführt werden (Lehrer, Schüler, Klassenarbeiten, nochmals alles für Win7...)
2. Wird ein Programm deinstalliert, wird das Profil nicht bereinigt, hier sammelt sich mit der Zeit sehr viel Müll in der Registry an.
3. Kleine Änderungen können nur durchgeführt werden, indem man das komplette Verfahren nochmals durchläuft.

3 Verändern Sie die Standardmeldung – so können Sie später den Erfolg leicht kontrollieren.

4 Hier wird ohne Rücksicht auf Verluste abgemeldet. Nicht gespeicherte Daten gehen verloren.

2. Manipulation der Registry und Administrative Vorlagen

Nicht für jeden Zweck gibt es eine geeignete Gruppenrichtlinie – das kann ja auch gar nicht sein, da fast jede Software ihre eigenen Registryeinträge mit sich bringt, über die Einstellungen vorgenommen werden können. Für diesen Zweck wurden die administrativen Vorlagen, kleine Textdateien mit der Endung .adm, erdacht. Diese bieten eine Möglichkeit, direkt Registryeinstellungen an den Clients zentral über GPOs vorzunehmen. Sie werden mitunter mit der entsprechenden Software bereits bereitgestellt[5], können im Internet gefunden werden oder lassen sich (im bescheidenen Maß) auch selbst erstellen. Eine ausführlicher Anleitung findet man unter [1c].

Administrative Vorlagen können nach Belieben zu einer GPO hinzugefügt oder wieder entfernt werden. Durch das Hinzufügen entstehen neue Konfigurationsmöglichkeiten.

Zwei Dinge müssen dabei besonders beachtet werden:

- Die meisten Einstellungen sind erst dann sichtbar, wenn die Ansicht des GPO-Editors entsprechend angepasst wird,
- Die Einträge in der Registry eines Clients durch adm-GPOs bleiben größtenteils auch dann bestehen, wenn die entsprechende Gruppenrichtlinie deaktiviert oder entfernt wird. Änderungen müssen also aktiv zurückgesetzt werden.

Als Alternative lassen sich auch (allerdings mit weniger Komfort) Registry-Auszüge per Start- oder Anmeldeskript importieren. Letztlich geht das dann auch wieder über eine Gruppenrichtlinie und ist für den Anfänger leichter zu realisieren.

Die folgenden Übungen bauen aufeinander auf. Sie sollten sie also unbedingt in der angegebenen Reihenfolge abarbeiten.

2.1. Einen Registryeintrag verteilen

Die im Abschnitt 1.7 vorgenommenen Einstellung sollen jetzt an alle Benutzer weitergegeben werden. Da sie allesamt in der Registry stehen, bietet sich das in der folgenden Übung vorgestellte Verfahren an:

> **Übung 7:** Einen Registryabschnitt exportieren
> 1. Melden Sie sich am *PC1* als Administrator an.
> 2. Starten Sie den Registyeditor *Start|Ausführen → regedit*
> 3. Navigieren Sie zum Abschnitt *HKCU|Software|GrimAdmin.com*
> 4. Klicken Sie mit der rechten Maustaste auf diesen Abschnitt, wählen Sie Exportieren und geben Sie als Dateinamen `\S1\netlogon\GrimAdmin` an.

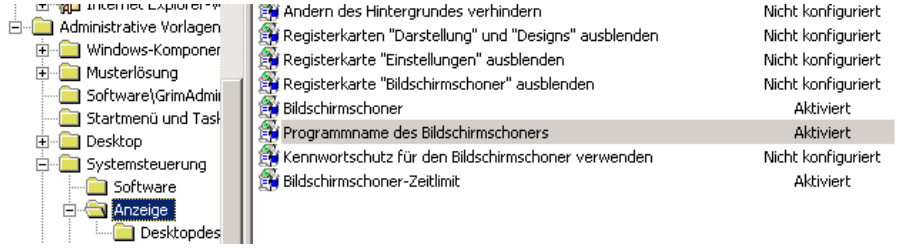
5 Meistens bei Software von Microsoft.

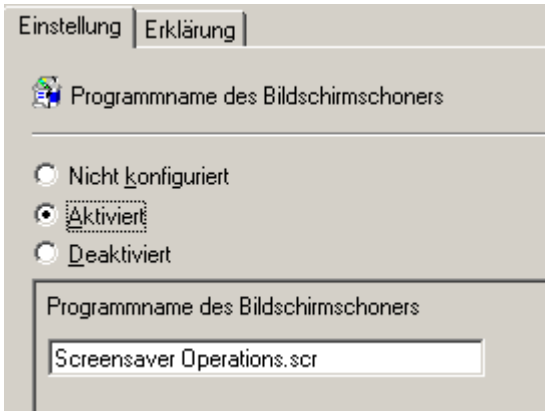
Sie haben dadurch auf dem Server eine neue Textdatei erstellt, in der die Informationen aus der Registry eingetragen worden sind. Auf einem anderen Rechner oder mit einem anderen Benutzerkonto könnten diese durch Doppelklick übernommen werden, der Bildschirmschoner wäre dann für den ausführenden Benutzer genauso eingestellt wie in der Vorlagekonfiguration. Dies ist aber kein geeigneter Weg für ein Schulnetzwerk. Die Übertragung an alle Benutzer erfolgt daher per Gruppenrichtlinie.

Mit dem Wissen, was jeder einzelne Schlüssel bedeutet (das steht bei diesem Programm in der beiliegenden Dokumentation) könnten Sie die Einträge vor der Verteilung auch noch anpassen. Da sie unabhängig vom Profil bestehen, sind sie leichter zu organisieren.

Übung 8:

1. Modifizieren Sie die Gruppenrichtlinie aus Übung 1 so, dass der neue Bildschirmschoner *Screensaver Operations.scr* verwendet wird.





2. Testen Sie, ob die Änderung funktioniert hat.

Auf diese Art haben Sie jetzt zwar den Bildschirmschoner umgestellt, aber noch nicht die Konfiguration vorgegeben.

Übung 9:

1. Stellen Sie in der selben Gruppenrichtlinie unter *Benutzer*|*Windowseinstellungen*|*Skripts*|*Anmelden*|*Hinzufügen* das folgende neue Anmeldeskript[6]

2. Melden Sie sich an dem Rechner als Lehrer an und testen Sie das Ergebnis.

Der Aufruf des Programms *regedit* mit dem Parameter */s* bewirkt, dass die nachfolgend angegebene Registryauszugsdatei ohne Rückfrage zur Registry hinzugefügt wird.

Die Einträge im Benutzerzweig werden nur temporär in das Profil aufgenommen. Nach dem Abmelden werden sie wieder durch die Standardwerte aus dem servergespeicherten Profil überschrieben. Sie können das testen, indem Sie die GPO deaktivieren und sich dann neu anmelden.

Auf die gleiche Weise lassen sich jedoch auch computerbezogene Registryeinträge verteilen. Das geht allerdings nicht beim Anmelden, da dem Benutzer in der Regel die Berechtigungen fehlen, dort Einträge vorzunehmen. Statt dessen müssen Sie – raumbezogen oder für alle Workstations – unter der Computerkonfiguration ein Startskript eintragen. Bei unserem Beispiel ist es möglich (nicht jedes Programm unterstützt das), die Einstellungen im Computerteil der Registry einzutragen und dadurch für jeden Benutzer gelten zu lassen.

Übung 10:

1. Kopieren Sie die Registrydatei und benennen Sie die Datei um in *GrimAdmMachine.reg* um.
2. Ändern Sie zweimal den Teil *HKEY_CURRENT_USER* in *HKEY_Local_Machine*.
3. Entfernen Sie das Loginskript aus der in der vorigen Übung erstellten GPO.
4. Erstellen Sie eine neue GPO für EDV1 und weisen Sie diesmal analog der vorangegangenen Übung *regedit /s* `\\s1\netlogon\GrimmAdmMachine.reg` diesmal computerbezogen als Startskript zu.
5. Fahren Sie den Rechner PC2 (neu) hoch und melden Sie sich als Lehrer (oder als Administrator) an. Testen Sie den Bildschirmschoner.

Registryeinträge können ebenso einfach wieder aus der Registry gelöscht werden. Sie löschen einen Schlüssel samt Unterschlüsseln und Einträgen, indem Sie unmittelbar nach der öffnenden eckigen Klammer ein Minuszeichen ergänzen.

6 Genaueres siehe auch [4] bzw. [5]

Übung 11: Registryeintrag löschen

1. Kopieren Sie die Datei *GrimAdmin.Reg* und benennen Sie die Kopie in *delGrimAdmin.reg* um.
2. Ändern Sie die erste Textzeile (Zeile 3) um, indem Sie ein „-" ergänzen: [*-HKEY_Local_Machine|Software|GrimAdmin.com*]
3. Löschen Sie alles unterhalb stehende.
4. Ändern Sie das Startskript aus der letzten Übung so ab, dass jetzt der Registryeintrag wieder gelöscht wird.
5. Starten Sie den Rechner neu und überprüfen Sie das Ergebnis.

2.2. Ergänzendes Beispiel aus der Praxis (optional)

Einige Schulen setzen den Arduino-Microprozessor[7] im Informatik- oder NWT-Unterricht ein. Dabei wird die kleine Platine über USB an einen Rechner angeschlossen. Man muss dann zunächst den Treiber installieren, damit das Gerät erkannt und man mit ihm arbeiten kann, man benötigt dafür Administratorberechtigungen. Grund dafür ist, dass Treiberdaten im Computerbereich der Registry eingetragen werden.

Dabei ergibt sich ein sehr ärgerliches Verhalten: wird ein anderes Board angesteckt, erkennt Windows nicht, dass die Treiber schon installiert sind und möchte die Installation durchführen – geht aber wieder nur als Administrator. Für den Unterricht ein ziemlich unbrauchbares Verfahren.

Der Grund dafür liegt in der USB-Seriennummer. Jedes Board hat zwar die gleiche Verkäufer- und Produkt-ID (vid, pid), aber eine unique Seriennummer und ist dadurch für Windows unterscheidbar. Für jedes Gerät muss daher ein eigener Schlüssel eingetragen werden.

Dieses Verfahren lässt sich zum Glück beeinflussen[8]. Durch einen eigenen Regkey wird die zusätzliche Seriennummernauswertung unterdrückt und diese spezielle Gerät nur Noch über vis und pid zugeordnet. Die Einstellung lässt sich auch über Gruppenrichtlinen verteilen. In der Praxis hat man meist schon einmal den Treiber installiert; damit das Verfahren funktioniert, muss das teilweise rückgängig gemacht werden.

Übung 12: Vorbereitung (Simulation)

1. Melden Sie sich als Administrator an einem Client an. Importieren Sie die Registrydatei *arduino1.reg* durch einen Doppelklick.
2. Starten Sie *regedit*. Suchen Sie den (normalerweise durch Installation verursachten) Eintrag *[HKEY_LOCAL_MACHINE|SYSTEM|CurrentControlSet|Enum|USB|Vid_2341&Pid_0043]*, versuchen Sie diesen Eintrag zu löschen.

Selbst als Administrator haben Sie nicht die Berechtigung, diesen Eintrag zu löschen. Das geht ausschließlich mit Systemberechtigungen. Per Gruppenrichtlinie ausgeführte Startskripte haben aber die benötigte Berechtigung.

Durch eine weitere Regdatei wird

7 http://arduino.cc/en/Main/ArduinoBoardUno

8 Siehe hierzu http://www.ftdichip.com/Support/Documents/AppNotes/AN_107_AdvancedDriverOptions_AN_000073.pdf (S.22) bzw. http://www.uwe-sieber.de/usbtrouble.html (ziemlich am Ende).

- Dieser Schlüssel gelöscht, denn er enthält die Daten für ein spezifisches Gerät,
- Die Prüfung auf die Seriennummer in Zukunft abgeschalten. Damit muss nur noch *einmal* [9]der Treiber installiert werden und steht dann für alle Boards zur Verfügung.

```
Windows Registry Editor Version 5.00

[-HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\VID_2341&PID_0043]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\usbflags]
"IgnoreHWSerNum23410043"=hex:01
```

Übung 13:

1. Verteilen Sie die Registrydatei arduino2.reg per GPO.
2. Sehen Sie auf dem Client nach, ob der alte Eintrag verschwunden ist und ob der 2. eingetragen wurde.

Hinweis: Sie finden in der Registry der Schulungsumgebung evtl. einen weiteren Ignore..eintrag und den Key GlobalDisableSerNumGen. Vermutlich handelt es sich dabei um Einstellungen von vmware.

Für die Anwendung in der Praxis müssen Sie die Gruppenrichtlinie wieder deaktivieren, nachdem sie bei jedem Client einmal abgearbeitet wurde. Erst dann installieren Sie als Administrator an jedem Port den Treiber. Bei einem neuen Ausführen der GPO würde sonst durch die erste Zeile der Treiber wieder gelöscht.

2.3. Beispiel für den Einsatz einer adm-Datei

Aus Registrydateien können mit etwas Nacharbeit adm-Dateien erstellt werden. Das geht z.B. mit dem Tool **reg2adm**[10]. Das sprengt aber den Rahmen dieser Dokumentation. Statt dessen wenden wir eine fertige adm-Datei an.

Übung 14:

1. Kopieren Sie die Datei *Screensaver.adm* irgendwohin auf Ihren Server.
2. Löschen Sie die computerbezogene Richtlinie für das Eintragen/Löschen der reg-Datei.
3. Gehen Sie zu der vorher erstellten Lehrer-GPO Bildschirmschoner und wählen Sie *Bearbeiten*. Klicken Sie im linken Bereich ganz unten auf *Administrative Vorlagen* mit der rechten Maustaste und wählen Sie *Vorlagen hinzufügen/entfernen*.
4. Gehen Sie auf *Hinzufügen* und suchen Sie die unter 1. kopierte Datei. Klicken Sie auf *Schließen*.

Wenn Sie jetzt die Administrative Vorlage erweitern, scheint der neu entstandene Menüpunkt leer zu sein und Sie werden vergeblich nach neuen Einstellmöglichkeiten suchen. Um Sie zu sehen, müssen Sie zuerst die Ansicht entsprechend erweitern. Leider wird diese Einstellung nicht gespeichert, sie müssen Sie jedes Mal von neuem vornehmen.

9 Gegebenenfalls für jeden USB-Port (manchmal geht das aber für die anderen Ports dann als Benutzer).

10 Zu finden u.a. unter http://www.novell.com/coolsolutions/tools/13885.html

Übung 15:

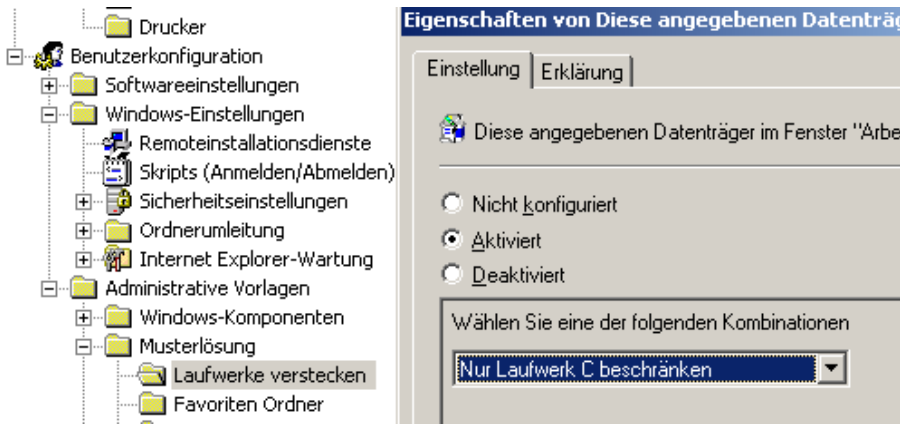
1. Wählen Sie durch einen einfachen Klick *Administrative Vorlagen* aus und klicken Sie dann oben im Menü *Ansicht|Filterung*. Entfernen Sie den Haken ganz unten bei *Nur vollständig verwaltbare Richtlinien anzeigen*.
2. Nach dem Klick auf *OK* erscheint ein neuer links Menüpunkt *Software/Grimsoft.com*. Nehmen Sie hier ein paar Einstellungen vor, melden Sie sich am Client neu an und überprüfen Sie das Ergebnis.

Ein Blick in die ADM-Datei zeigt den engen Zusammenhang mit der zugrundeliegenden REG-Datei. ADM-Dateien sind vor allem dann von Vorteil, wenn die Konfiguration öfter geändert werden muss, weil dann eine grafische Bedienoberfläche zur Verfügung steht. Einfacher ist allerdings die Methode über den Import von REG-Dateien.

Als weiteres Beispiel wird noch eine weitgehend unbekannte ADM-Datei der paedML vorgestellt.

Übung 16:

1. Erstellen Sie eine neue GPO, die alle Schüler betrifft.
2. Fügen Sie wie in Übung 9 die Vorlage *Musterlösung.adm* hinzu (sie ist direkt in dem Ordner, der sich bei *Hinzufügen* öffnet).
3. Vergessen Sie nicht Ansicht-Filterung!
   Nehmen Sie die abgebildete Einstellung vor.



4. Melden Sie sich als Schüler an einem Client an und bestätigen Sie, dass das Laufwerk C im Arbeitsplatz oder Explorer nicht mehr sichtbar ist.

3. Bestimmte Benutzer an bestimmten Computern

3.1. Ziel dieses Kapitels

Diese Anleitung erklärt, wie man die Wirkungsweise von Gruppenrichtlinien weiter einschränken kann. So sollen sie nur auf wenige Rechner in *einem* Raum oder im Netz, bestimmte Schüler *einer* Klasse oder sogar nur dann gelten, wenn ein gewisser Benutzerkreis auf bestimmten PCs im Netz angemeldet ist.

Also zum Beispiel für alle *Lehrer*, die an einem Rechner im Raum *EDV1* angemeldet sind. Schüler oder Lehrer in einem anderen Raum sollen nicht betroffen sein.

Mögliche Anwendungen wären die eingeschränkte Verteilung von Software, die Zuweisung eines Anmeldeskripts für eine Projektgruppe oder, als ausführlich dokumentierte Beispiele, die Zuordnung eines Hintergrundbilds für einen Raum oder die Einrichtung eines Bildschirmschoners für alle Lehrer, der aus Gründen des Datenschutzes bei der Reaktivierung das Kennwort des angemeldeten Benutzers verlangt.

So soll verhindert werden, dass Unbefugte Zugang zu Daten des Lehrers erhalten, wenn dieser vergessen hat sich abzumelden oder den PC zu sperren.

Dieses Verhalten ist jedoch nicht allen Räumen oder an allen PCs erwünscht. Im Lehrerzimmer beispielsweise kommt es immer wieder vor, dass ein Kollege vergisst sich abzumelden. Durch den Bildschirmschoner wird dieser PC dann gesperrt und steht erst dann wieder zur Verfügung, nachdem der angemeldete Kollege oder ein Administrator die Sperrung aufhebt.

Auch an einem Computer, der zu Präsentationszwecken verwendet wird, ist es lästig, wenn man während eines Vortrags immer wieder die Sperrung aufheben muss.

Mit dem herkömmlichen Verhalten der Gruppenrichtlinien ist dies jedoch nicht realisierbar, da Einstellungen in einer Gruppenrichtlinie für bestimmte Benutzer (z.B. für alle Lehrer) immer gelten, egal an welchem PC er sich anmeldet. Dies sei im folgenden Abschnitt nochmals kurz dargelegt.

In unserem Beispiel möchten wir jedoch erreichen, dass Benutzereinstellungen auf unterschiedlichen PCs anders vorgenommen werden. Meldet sich ein Lehrer in einem

Computerraum ein, soll er einen Bildschirmschoner mit anschließender Kennwortabfrage erhalten; im Lehrerzimmer dagegen nicht.

Um dieses Ziel zu realisieren benötigt man etwas vertiefte Kenntnisse der Thematik der Gruppenrichtlinien.

3.2. Eine Gruppenrichtlinie soll nur für bestimmte Computer im Netz gelten

Beispielsituation: An gewissen Rechnern im Schulnetzwerk sollen sich Schüler nicht anmelden können. Die Rechner sind keinen bestimmten gemeinsamen kriterien unterworfen – also nicht in einem Raum zusammengefasst. Es könnten z.B. die Lehrercomputer in mehreren Computerräumen sein.

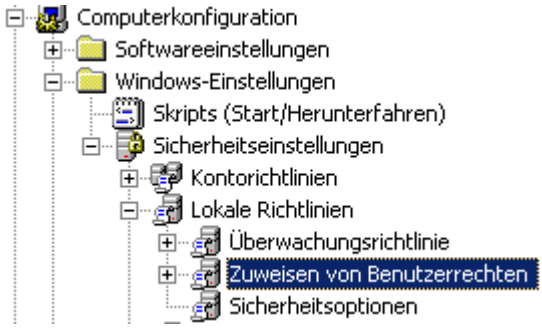
Problem: Gruppenrichtlinien können prinzipiell nur an OUs, also komplette Räume geknüpft werden.

Lösung: Auch die Gruppenrichtlinien verfügen (wie Dateien oder Ordner) über Sicherheitseinstellungen. Nur die Objekte, die das Recht sie zu lesen besitzen, können die Einstellungen übernehmen. Von allen anderen Objekten werden sie ignoriert.

In Lösung besteht aus den folgenden beiden Übungen: zunächst wird das Anmelderecht für Schüler bei allen Rechnern entfernt. Anschließend wird die GPO so modifiziert, dass sie sich nur noch auf PC2 auswirkt.

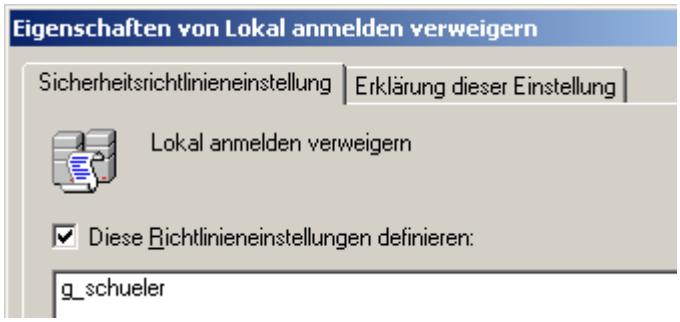
Übung 17: Schüleranmeldung verbieten

1. Erstellen Sie an der OU Workstations eine neue GPO mit dem Namen *Schüleranmeldung verhindern*.
2. Navigieren Sie links an die abgebildete Stelle unten den Computerkonfigurationen *Zuweisen von Benutzerrechten*.



3. Suchen Sie im rechten Fesnsterbereich die Einstellung Lokal anmelden verweigern und doppelklicken Sie auf diesen Punkt, um die Einstellung zu bearbeiten.

4. Aktivieren Sie diese Einstellung und fügen Sie die Gruppe *g_schueler* hinzu. Schließen Sie anschließend den Gruppenrichtlinieneditor.



5. Starten Sie PC1 und PC2 neu und versuchen Sie, sich als Schüler anzumelden.

Natürlich ist die Einstellmöglichkeit so noch nicht sinnvoll. Sie könnten allenfalls einige Benutzer von der Anmeldung in einem ganzen Raum aussperren, was in Schulen mit mehrern Schularten eventuell interessant ist.

Übung 18: GPO-Zuweisung eingrenzen

1. klicken Sie auf die in der vorherigen Übung erstellte Gruppenrichtlinie.
2. Wählen Sie im rechten Fenster den Reiter „Bereich".
   Entfernen Sie unter „Sicherheitsfilterung" die Authentifizierten Benutzer.
   Wählen Sie *Hinzufügen*. Da Computer standardmäßig nicht angezeigt werden, müssen Sie nun zunächst auf Objekttypen klicken und dort den Haken bei *Computer* setzen.[OK]
3. Geben Sie nun pc2$ ein und bestätigen Sie.
   Die neue GPO wird jetzt nur auf genau diesen Rechner angewendet.
4. Starten Sie PC1 und PC2 (neu) und überprüfen Sie, bei welchem sich jetzt ein Schüler anmelden kann.

5.

3.3. Lösungsstrategien für komplexere Situationen

Um das oben definierte Zeil umsetzen zu können, genügt diese Methode leider noch nicht. Es gibt aber weitere Lösungsmöglichkeiten. Diese verwenden jeweils einen technisch unterschiedlichen Lösungsansatz, führen jedoch beide letztendlich zum gewünschten Ergebnis.

Dies ist zum einen der Weg über den so genannten Loopbackverarbeitungsmodus, der zweite Weg arbeitet mit einem WMI Filter.

Hier eine kurze Gegenüberstellung der beiden Möglichkeiten

Bezeichnung	Loopbackverarbeitungsmodus	WMI Filter
Eignung	▪ Für alle PCs einer OU	▪ Für einzelne PCs in einer oder verschiedenen OUs, verschiedene Bedingungen auf diesen PCs.
Funktion	▪ In einer GPO für Computer kann man bei aktiviertem Loopbackverarbeiungsmodus auch Benutzereinstellungen vornehmen. Diese Benutzereinstellungen werden nach dem „normalen" Einlesen der eigentlichen Benutzereinstellungen gelesen und ersetzen oder ergänzen diese Einstellungen.	▪ Man erstellt einen Filter, z.B. über PC-Namen und kann damit steuern, ob eine GPO (auch für Benutzer) an den betroffenen PCs überhaupt angewendet wird.

4. Loopbackverarbeitungsmodus

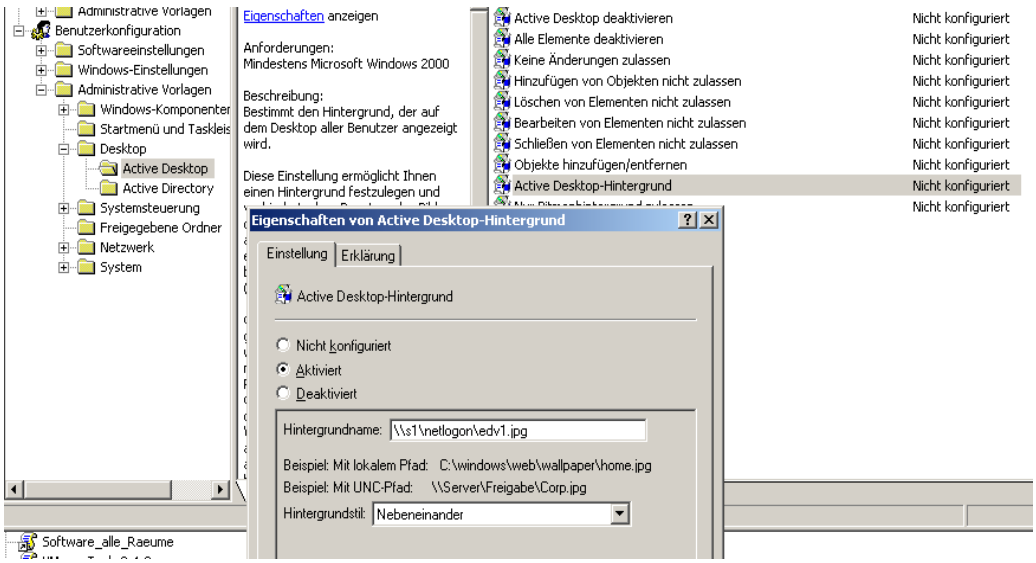
Prinzipiell dient der Loopbackverarbeitungsmodus dazu, *Computern* Einstellungen mitzugeben, die sich auf angemeldete *Benutzer* auswirken. Bei der eines Benutzers an einem PC, der einer solchen GPO unterliegt, werden dann die entsprechenden Einstellungen zugewiesen. Wir beginnen mit einem sehr einfachen Beispiel

4.1. Hintergrundbild - So wird's gemacht

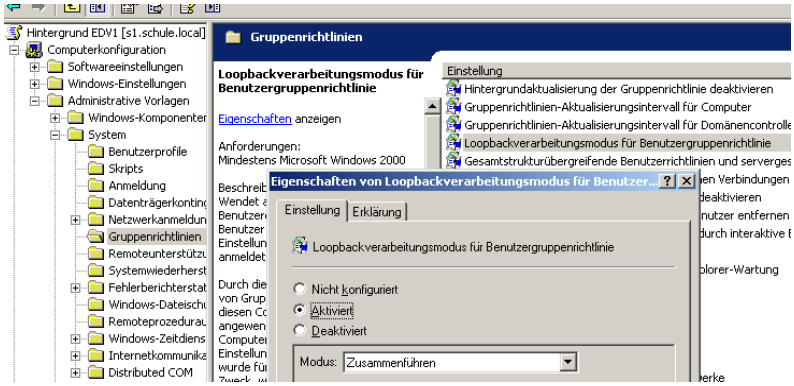
Das folgende Beispiel soll den PCs in jeweils einem Raum (OU) ein eigenes Hintergrundbild zuordnen. Das ist ohne Loopbackmodus nicht möglich, denn Hintergrundbilder sind eine Benutzereigenschaft, während der Raum mit den Computerobjekten in Zusammenhang steht.

Übung 19: Hintergrund raumspezifisch

1. Kopieren Sie die beiden Beispieldateien *edv1.jpg* und *edv2.jpg* auf dem Server in den Ordner
   `D:\Sysvol\sysvol\schule.local\scripts\Hintergrund`
2. Öffnen Sie die Gruppenrichtlinienverwaltung. Entscheiden Sie sich, ob Sie einen XP oder einen Windows 7-Rechner konfigurieren wollen. Deaktivieren Sie die bestehende Hintergrundrichtlinie (rechte Maustaste, Haken bei Verknüpfung aktivieren entfernen).
3. Erstellen Sie bei der OU *Workstations*| *EDV1* eine Richtlinie *Hintergrund_EDV1*.
   Nehmen Sie folgende Konfigurationen vor:



4. Aktivieren Sie den Loopbackverarbeitungsmodus im Computerteil der Gruppenrichtlinie mit „Zusammenführen“[11]:



5. Wiederholen Sie das Vorgehen analog für *EDV2*.
6. Testen Sie die Einstellungen, indem Sie sich als Lehrer, Schüler und Administrator an einem Rechner in einem dieser Räume anmelden.

Hinweis1: normalerweise unterliegt der Administrator ja keiner Gruppenrichtlinie. Auf diese Weise kann man ihm dann aber doch ein Hintergrundbild zuweisen.

Hinweis2: Mit BGinfo können weitere Informationen ausgewertet werden, siehe hierzu
http://lehrerfortbildung-bw.de/netz/muster/win2000/material/tipps/bginfo/
Allerdings überschreibt der nach der o.a. Methode eingetragene Hintergrundbildschirm den von Bginfo. Das Beispiel ist daher eher nur als Darstellung der Möglichkeiten zu sehen.

4.2. Funktionsweise beim Bildschirmschoner

Nochmal der Ablauf durch diese Gruppenrichtline im konkreten Detail: Soll der Bildschirmschoner auf allen PCs in bestimmten Räumen (Raum OU) wie z.B. dem Lehrerzimmer nicht angewendet werden, eignet sich der *Loopbackverarbeitungsmodus*.

Das Besondere am Loopbackverarbeitungsmodus ist, dass man in einer Gruppenrichtlinie für *Computer* Einstellungen für *Benutzer* vornehmen kann.

- Im Netz hat man eine GPO *Bildschirmschoner_Lehrer* erstellt , die für die Kennwortabfrage des Bildschirmschoners sorgt.
- Man erstellt eine zusätzliche GPO *Raum_kein_Bildschirmschoner* für die OU Lehrerzimmer. In dieser GPO aktiviert man den Loopbackverarbeitungsmodus und deaktiviert die Kennwortabfrage.

Was passiert nun bei der Anmeldung eines Lehrers?

- Zunächst werden die Benutzereinstellungen der GPO des Lehrers für den Bildschirmschoner übernommen, der Lehrer hätte also den Bildschirmschoner.

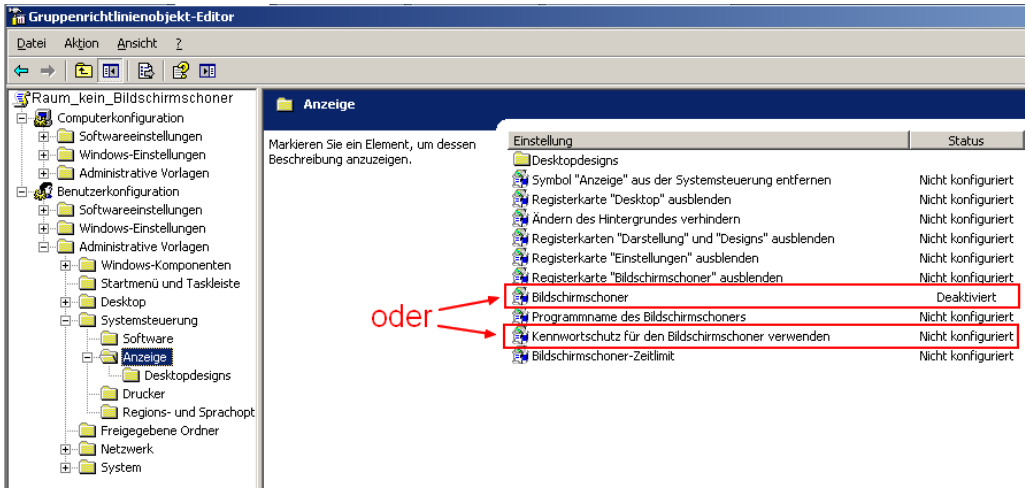
11 Ersetzen wäre eine ganz schlechte Idee. In diesem Fall werden *überhaupt keine* Benutzer-GPOs ausgeführt und statt dessen nur die hier definierten Einstellungen.

- Nun kommt der Loopbackverarbeitungsmodus ins Spiel. Dieser sorgt dafür, dass *nachdem* alle dem Benutzer zugeordneten GPOs abgearbeitet wurden, die in der GPO *Raum_kein_Bildschirmschoner* eingestellten Benutzereinstellungen gelesen werden. Hier wird nun festgelegt, dass kein Bildschirmschoner verwendet werden soll. Das Verbot *überschreibt* die Einstellungen aus der GPO *Bildschirmschoner_Lehrer*.
  So wird erreicht, dass in allen Räumen, denen die GPO *Raum_kein_Bildschirmschoner* der angemeldete Lehrer (bzw. jeder angemeldete Benutzer) keinen Bildschirmschoner erhält.

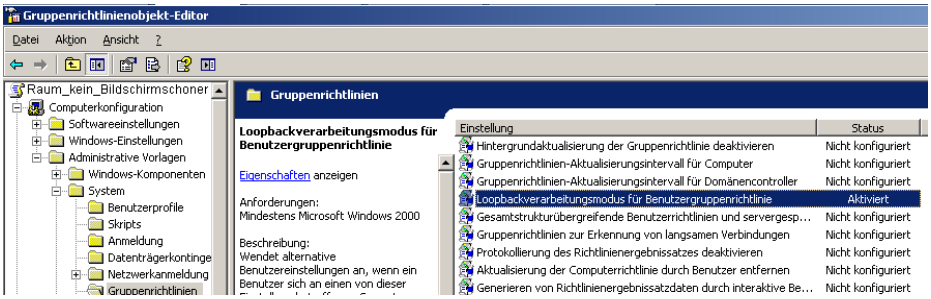
4.3. Bildschirmschoner - So wird's gemacht

Man erstellt eine neue Gruppenrichtlinie *Raum_kein_Bildschirmschoner*. In dieser Richtlinie nimmt man zwei Einstellungen vor:

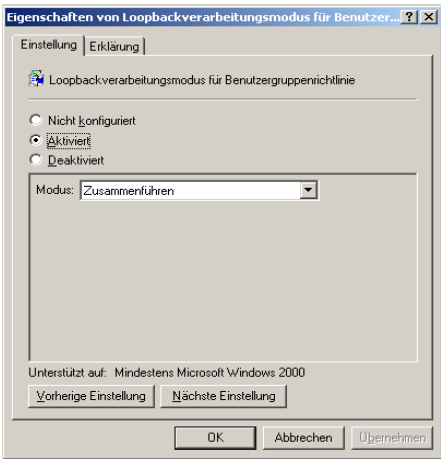
- Bildschirmschoner *Deaktiviert*[12] (*Benutzerkonfiguration* | *Administrative Vorlagen* | *Systemsteuerung* | *Anzeige*)



- Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie: *Aktiviert* – Modus: *Zusammenführen*
  (*Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Gruppenrichtlinien*)



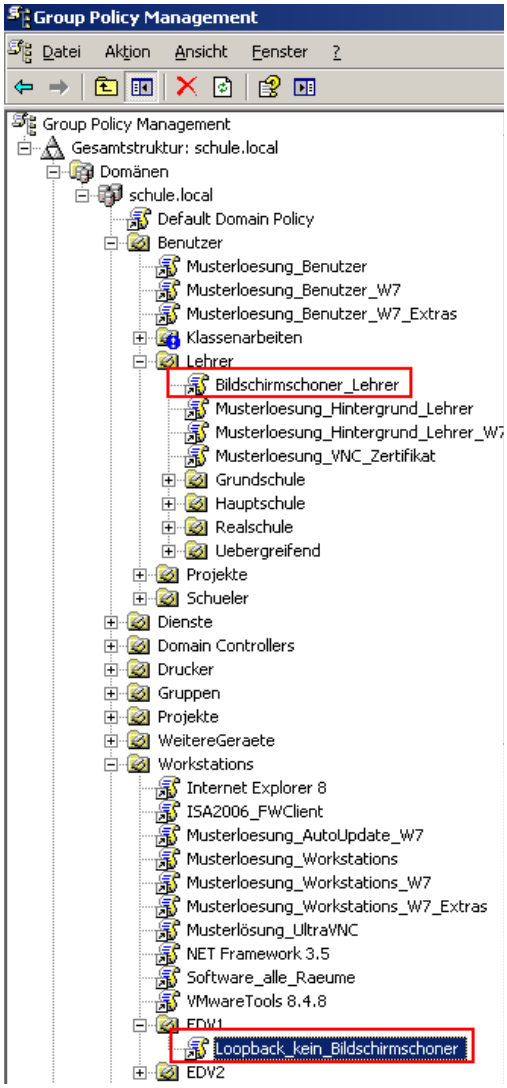
12 Alternativ kann man auch die Einstellung Kennwortschutz für den Bildschirmschoner verwenden *Deaktivieren*. Dann erscheint der Bildschirmschoner nach der Zeit, die in der GPO *Bildschirmschoner_Lehrer* vorgegeben wurde – nur eben ohne Kennwortschutz.



Zusammenführen bedeutet, dass die Einstellungen die durch andere Gruppenrichtlinien vorgenommen Vorgaben ergänzen. Widersprechen sich zwei Einstellungen, setzt sich immer ein Verbot/Deaktivieren durch.

In unserem Beispiel setzt sich also das Deaktivieren des Bildschirmschoners durch.

Nun verknüpft man die Gruppenrichtlinie *Raum_kein_Bildschirmschoner* mit all den Räumen, in denen kein Bildschirmschoner (oder keine Kennworteingabe) aktiviert werden sollen.



Übung 20: Nehmen Sie die notwendigen Einstellungen vor, dass im Raum EDV1 kein Bildschirmschoner für Lehrer aktiviert wird. In Raum EDV2 soll der Bildschirmschoner aktiviert bleiben.

5. WMI Filter

5.1. Funktionsweise

Sollen die Einstellungen der GPO für Benutzer – in unserem Beispiel der Bildschirmschoner - nicht auf allen PCs einer OU angewendet oder ausgeschlossen werden, benötigt man ein anderes Werkzeug als den Loopbackverarbeitungsmodus. In diesem Fall kann man mit einem WMI Filter arbeiten.

WMI steht für *Windows Management Instrumentation*. Damit ist es möglich Filter auf Grundlage einer großen Zahl von Möglichkeiten zu erstellen. Verknüpft man solch einen Filter dann mit einer Gruppenrichtlinie, wird diese nur angewendet, wenn die Kriterien des Filters erfüllt werden. Hierbei ist es unerheblich, ob in der GPO Einstellungen für Benutzer oder für Computer vorgenommen wurden.

Für unser Beispiel verknüpfen wir die Gruppenrichtlinie *Bildschirmschoner_Lehrer* mit einem WMI Filter, der nach bestimmten PC-Namen filtert. Ein Filtern nach Zugehörigkeit zu einer OU ist übrigens leider nicht möglich.

Ab Schulkonsole 2.7 gibt es bereits zwei WMI Filter. Damit wird festgelegt, welche Gruppenrichtlinien nur auf Windows XP bzw. Windows 7 Computern ausgeführt werden.

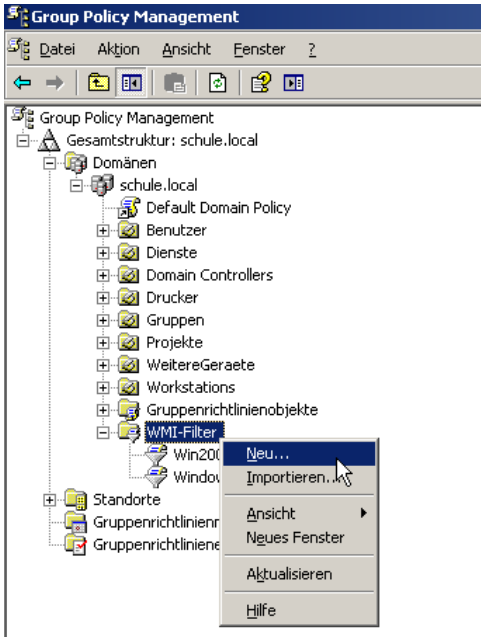
5.2. So wird’s gemacht

5.2.1. WMI Filter erstellen

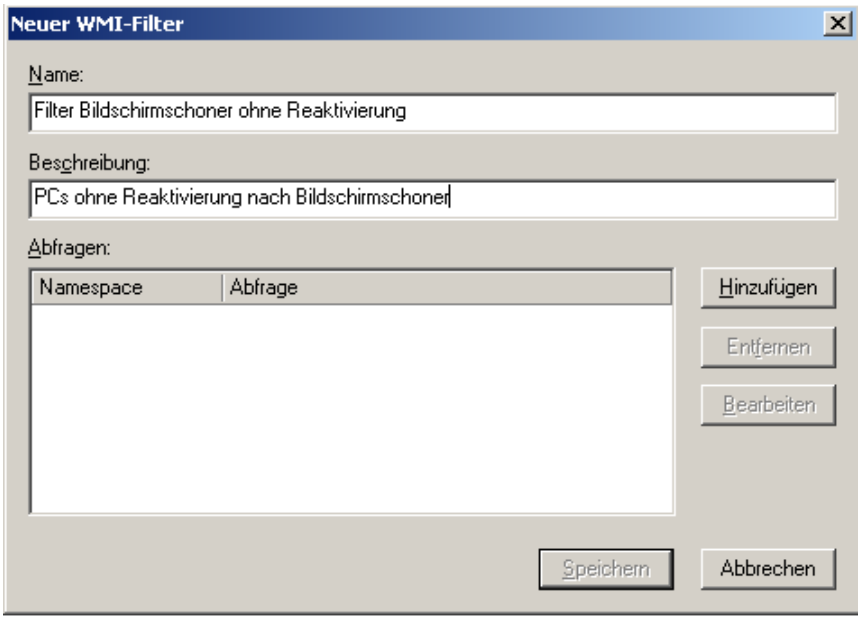
Um einen neuen WMI Filter zu erstellen, öffnet man die Gruppenrichtlinienverwaltung. Im linken Bereich geht man weit nach unten bis zum Punkt *WMI Filter*.

Seit der Version 2.7 der Schulkonsole gibt es dort bereits zwei Filter, nämlich den für Windows 2000/XP und für Windows 7, ggf. sogar noch einen für Win 7 64bit.

Um einen neuen Filter zu erstellen rechtsklickt man auf *WMI Filter* und wählt *Neu*.

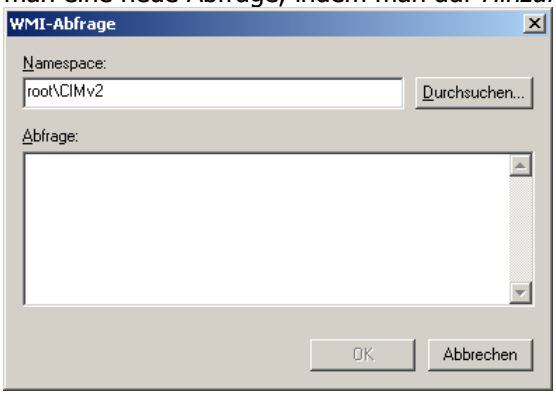


Zunächst gibt man dem WMI Filter einen Namen, zudem kann man eine passende Beschreibung eingeben.



5.2.2. Filterkriterien definieren

Nun muss man festlegen, nach welchen Kriterien gefiltert werden soll. Hierzu erstellt man eine neue Abfrage, indem man auf *Hinzufügen* klickt.



Im Bereich *Namespace* ändert man nichts. Im Bereich *Abfrage* gibt man nun den entsprechenden Befehl ein[13].

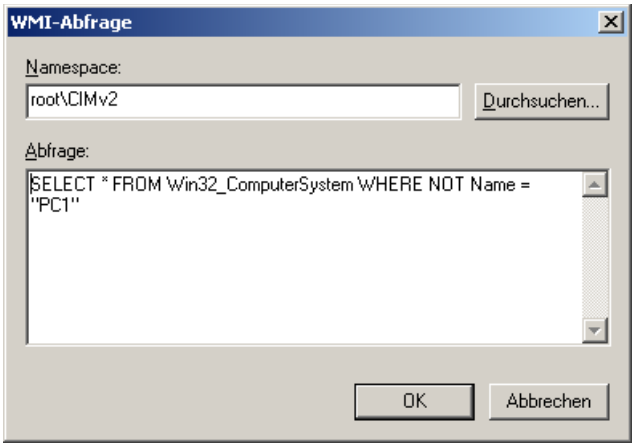
Hierzu nun einige Beispiele, die Sie auf Ihre Erfordernisse anpassen können.

1. Suche nach einem PC Namen

Wichtig ist zu Beginn, dass man sich nochmals über die Funktion des Filters Gedanken macht. Die Gruppenrichtlinie, auf die der Filter später angewendet wird, wird auf allen Computern angewendet, auf die der Filter zutrifft.

Im Beispiel soll nun der Bildschirmschoner auf allen Computern außer PC1 erscheinen. Der Filter lautet daher: Alle Computer außer PC1. Die Syntax hierzu lautet:

```
SELECT * FROM Win32_ComputerSystem WHERE NOT Name = "PC1"
```



2. Suche nach mehreren PCs

Man kann den Filter auf mehrere PCs ausweiten:

```
SELECT * FROM Win32_ComputerSystem WHERE NOT Name = "PC1" OR
Name = "PC2"
```

3. Suche mit Platzhaltern

Haben die PCs, auf denen der Bildschirmschoner nicht erscheinen soll, ähnliche Bezeichnungen, kann man mit Hilfe von Platzhaltern suchen. Im Beispiel werden alle PCs mit dem Namensbestandteil „Lehrer" ausgefiltert.

13 Programmiersprache ist *Windows Management Instrumentation Query Language (WQL)*

```
SELECT * from Win32_ComputerSystem WHERE NOT name
LIKE "%Lehrer%"
```

4. Weitere Möglichkeiten

In unserem Beispiel sollte eine Gruppenrichtlinie dann angewendet werden, wenn ein PC-Name nicht im Filter enthalten war. Dies funktioniert selbstverständlich auch umgekehrt. Mit dem Filter

`SELECT * FROM Win32_ComputerSystem WHERE Name = "PC1"` könnte man z.B. ein MSI Paket nur dem PC *PC1* zukommen lassen.

Die Filtermöglichkeiten sind äußerst umfangreich. Beispiele für Filterkriterien sind WiFi Netzwerkarte, bestimmter Festplattengröße, bestimmter Grafikkarte, bestimmte Software[14] etc.

Einige Beispiele:
- Nur PCs auf denen 32bit-Betriebsystem läuft (XP oder W7 oder …)

```
SELECT AddressWidth FROM Win32_Processor WHERE AddressWidth
='32'
```

- analog geht es natürlich auch für 64bit-Betriebsysteme.

- überprüfen, ob eine bestimmte Datei auf dem Client vorhanden ist

```
Select * From CIM_Datafile Where Name = 'C:\\Windows\\test.txt'
```

- weiter ausdifferenziert

```
SELECT path,filename,extension,version FROM CIM_DataFile WHERE
path="\\Program Files\\Internet Explorer\\" AND filename="iex-
plore" AND extension="exe" AND version>="8.0"
```

- überprüfen, ob ein bestimmter Ordner vorhanden ist

```
Select * From CIM_Directory Where Name = 'C:\\programme\\test'
```

(bitte die doppelten „\" beachten!)

Bemerkung[15]:

Es ist nicht möglich, zu überprüfen ob

- eine bestimmte Datei oder ein bestimmter Ordner nicht existiert,
- ob ein bestimmter Registry-Eintrag existiert.

Weitere Anregungen finden Sie unter
http://www.zeda.nl/EN/Blog/018_Implementing_WMI_Filters/

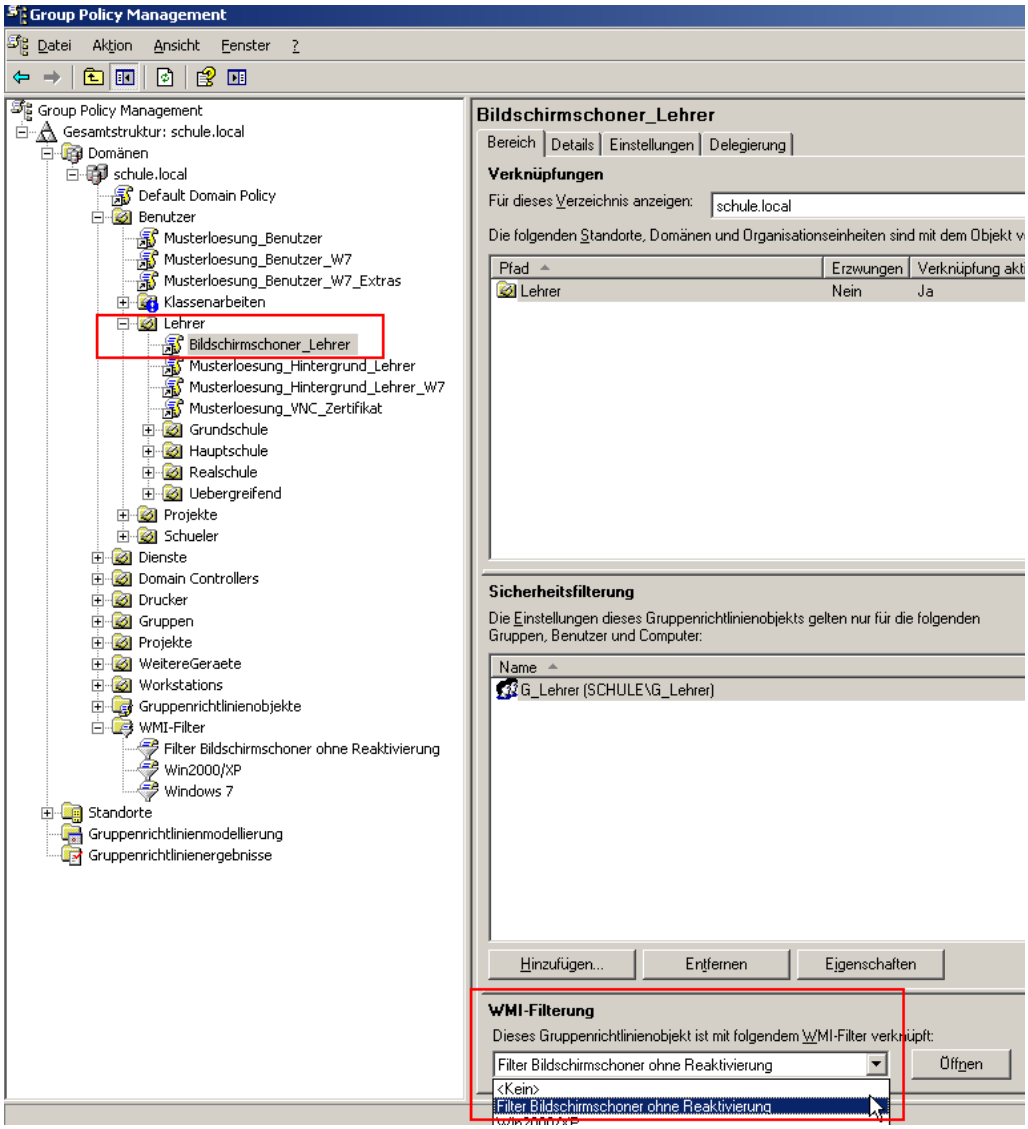
5.2.3. WMI Filter anwenden

Nun muss man noch dafür sorgen, dass der erzeugte WMI Filter auf die Gruppenrichtlinie für den Bildschirmschoner auch angewendet wird. Hierzu wählt man die GPO Bildschirmschoner_Lehrer.

Auf der rechten Seite unten wählt man unter WMI Filterung den erstellten WMI Filter aus.

14 Vom Filtern nach installierter Software wird allerdings aus Performancegründen von Microsoft dringend abgeraten.

15 Vgl. http://social.technet.microsoft.com/Forums/en/winserverGP/thread/5cd1b80a-2f90-4d46-bf65-dba52dcf0c56



Übung 21: Erstellen Sie einen WMI Filter der bewirkt, dass auf PC1 und PC3 kein Bildschirmschoner aktiviert wird. Entfernen Sie vorher ggf. noch Einstellungen aus dem vorangegangenen Kapitel (Loopbackverarbeitungsmodus)

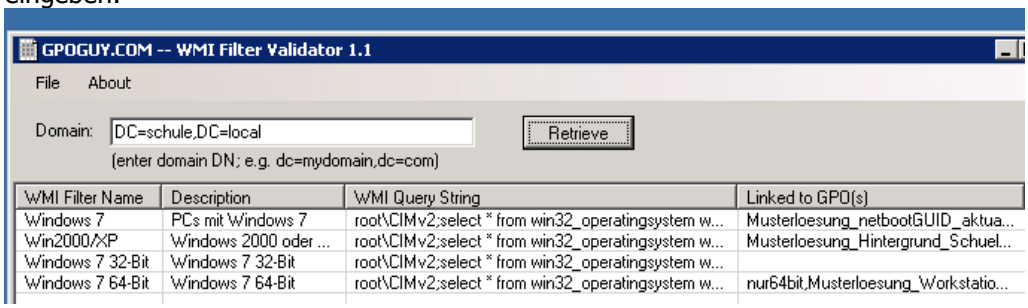
5.2.4. WMI-Filter testen - So wird's gemacht

Da die Syntax der WMI-Filter doch recht ungewohnt ist, kann man sich schon einmal unsicher sein, auf welchem Rechner der Filter nun tatsächlich greift.

Ein gute Hilfe kann das kostenlose Tool WMI-FILTER Validiator[16] sein. Damit können Sie auf dem Server ausprobieren, ob ein WMI-Filter auf einem vorgegebenen Client greifen würde oder nicht – der Client muss dazu lediglich eingeschalten sein. Sie sparen dadurch den Neustart beim Testen.

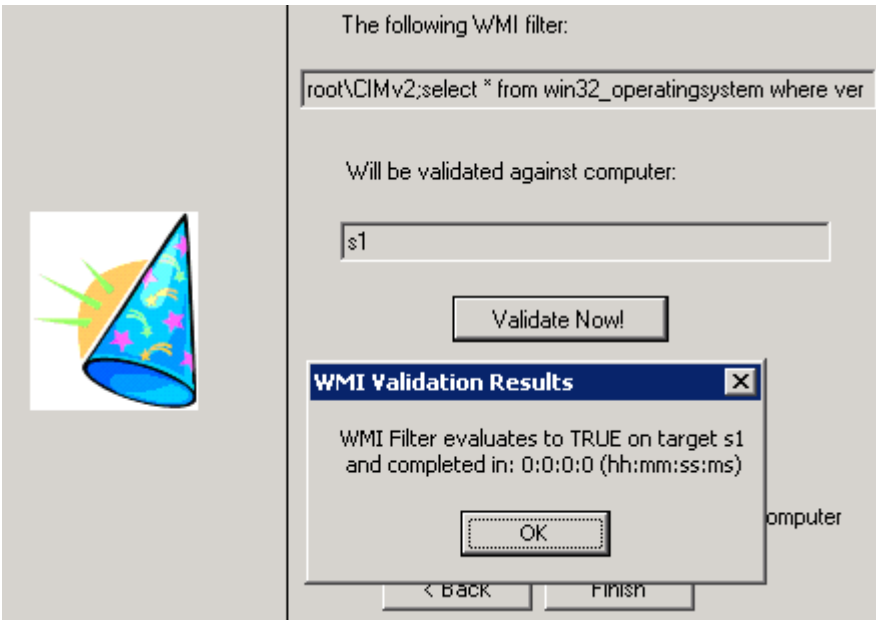
16 Download unter http://gpoguy.com/free-tools/free-tools-library/wmi-filter-validation-utility/

Nach dem Download und dem Entpacken kann das Tool auf dem Server ohne Installation gestartet werden. Dann muss zunächst die Domänenbezeichnung wie abgebildet eingeben:



Nach einem Klick auf den *Retrieve*-Button werden alle vorhandenen WMI-Filter aufgelistet. Durch Rechtsklick auf einen von ihnen und *Validiate* werden Sie aufgefordert, den Namen eines Rechnes einzugeben.

Nach *Next* können Sie den Test über Validiate now durchführen und erhalten als Ergebnis der durchgeführten WMI-Abfrage, ob die Regel zutrifft oder nicht.



Übung 22:

1. Probieren Sie das Tool aus.

6. Quellen und weiterführende Links

[1] http://www.gruppenrichtlinien.de/, insbesondere

a) http://www.gruppenrichtlinien.de/artikel/filtern-von-gruppenrichtlinien-anhand-von-benutzergruppen-wmi-und-zielgruppenadressierung/
b) http://www.gruppenrichtlinien.de/artikel/oreilly-uebersetzung-adm-templates-erstellen/

c) http://www.gruppenrichtlinien.de/artikel/loopbackverarbeitungsmodus-loopback-processing-mode/

[2] ADM-Dateien: Erklärungen von Microsoft http://support.microsoft.com/kb/816662/de und http://support.microsoft.com/kb/225087/de
[3] http://www.grimadmin.com/filemgmt/index.php

[4] http://lehrerfortbildung-bw.de/netz/muster/win2000/material/tipps/startup/anmeldeskripte/

[5] http://lehrerfortbildung-bw.de/netz/muster/win2000/material/tipps/startup/

[6] http://lehrerfortbildung-bw.de/netz/muster/win2000/material/tipps/administratoren.pdf

[7] Softwareverteilung im Basiskurs: http://lehrerfortbildung-bw.de/netz/muster/win2000/material/basis30/pdf/kap_14a_Softwareverteilung.pdf

[8] Datei- und Registryberechtigungen http://lehrerfortbildung-bw.de/netz/muster/win2000/material/software/berechtigungen_setzen_gpo

[9] http://www.waynezim.com/2009/07/how-to-use-wmi-filt-ring-to-improve-group-policy-administration/

[10] http://www.msxfaq.de/verschiedenes/gpo.htm