**Einführung in Gruppenrichtlinien**

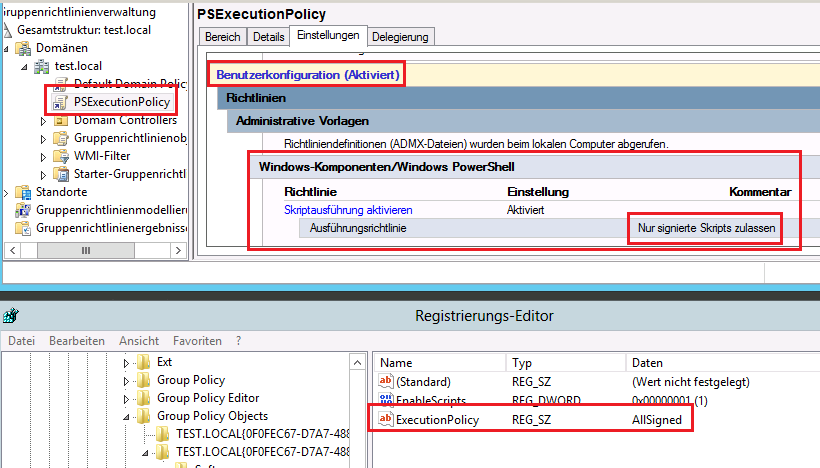
Eines gleich vorab: das Ganze ist immer ein PULL-Verfahren: Der Client holt sich etwas vom Server. Der Server kann nicht pushen. Dazu müsste er nämlich wissen, was auf dem Client fehlt – geht nicht…

Richtlinien schreiben in den Policy-Zweig der Registry. Benutzer haben hier nur Lese-Rechte, können die Richtlinien also nicht aushebeln.

Das Schreiben in den Policy-Zweig bringt einen weiteren Vorteil: die Originalwerte werden nicht angetastet (kein Tattooing).

Die aus dem GPO übernommenen Werte werden lokal in der ntuser.dat auf dem Client gespeichert. Die ntuser.dat enthält den benutzerspezifischen Teil von HKEY\_Current\_User.

Als erstes Beispiel nehmen Sie eine GPO, die Registry-Settings setzt und checken dann mit regedit:



Jedes Mal, wenn Sie Einstellungen in einer Policy ändern, werden diese Einstellungen außerdem in eine registry.pol geschrieben. Diese Dateien sind – vereinfacht gesprochen – kompilierte Sammlungen aller Registryeinstellungen des GPOs.

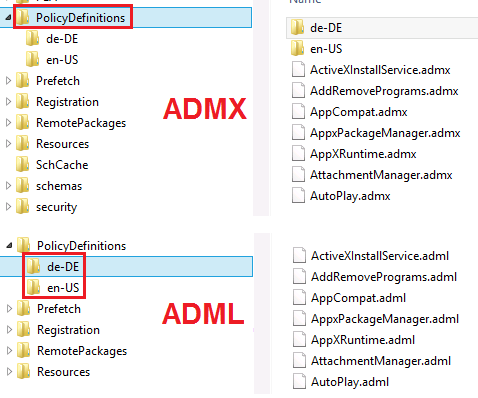
Lokale GPO: c:\windows\system32\GroupPolicy\User\Registry.pol

GPO: [\\FQDN\SYSVOL\FQDN\Policies\{GUID-GPO}\[User][Machine]\Registry.pol](file:///\\FQDN\SYSVOL\FQDN\Policies\%7bGUID-GPO%7d\%5bUser%5d%5bMachine%5d\Registry.pol)

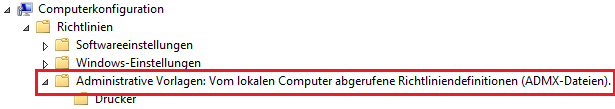
**Administrative Vorlagen**

Die allermeisten Registry-Einstellungen verbergen sich hinter den sog. Administrativen Vorlagen. Bis Vista waren die durchaus ein Problem: Im Verzeichnis c:\windows\inf lagen bis XP die adm-files. Wann immer ein GPO erstellt oder geändert wurde, landeten Teile als Unterordner „adm“ in jedem GPO im SYSVOL– da kamen schnell etliche MB zusätzliche Replikationslast zusammen. Mit Einführung des admx-Formats hat sich dies Vorgehen komplett erledigt.

Die Administrativen Vorlagen liegen jetzt unter Windows\Policydefinitions. Darunter gibt es länderspezifische Ordner, in denen die adml-Dateien liegen. Die passen die GPMC für die jeweilige Sprache an (Konfigurationen, Hilfetexte usw.).



Diese Dateien werden dann in der GPMC einfach vom lokalen Computer gelesen:

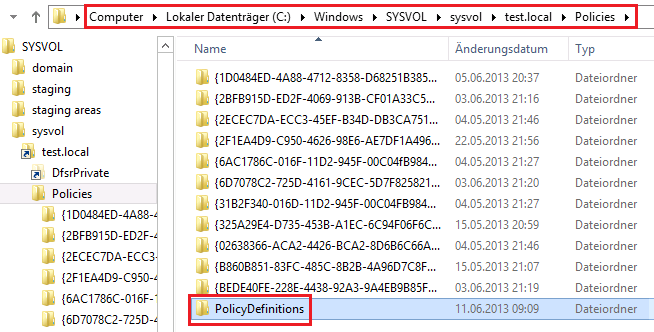


Zentraler Speicher – Central Store

Problematisch wird es, wenn ein Admin Änderungen an seinem PolicyDefintions-Ordner vornimmt, also z.B. eine eigene ADMX erstellt. In Bezug auf die Richtlinie selbst wird es da nicht zu Schwierigkeiten kommen. Aber wenn dann ein Admin auf einer anderen Maschine das neue GPO öffnet, sieht er die Einstellungen nicht – es fehlt ihm ja die admx Datei. Es wird hier nichts mehr via SYSVOL repliziert! Die sauberste Lösung dafür ist der Central Store: Sie sorgen dafür, dass *alle* ADMX-Dateien von *jeder* Admin-Maschine von einem *zentralen* Ort geladen werden.

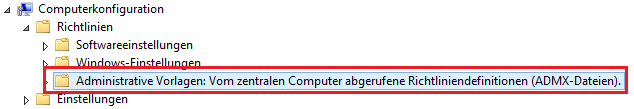
Der zentrale Speicher muss im SYSVOL eines DCs angelegt werden. Dieser repliziert ihn dann auf die anderen DCs. Zwar erhöhen Sie damit wieder das Replikationsvolumen, aber im Gegensatz zu adm-Unterordnern für jedes GPO haben Sie nur einen (überschaubaren) Ordner ohne unnötige Redundanz.

Erstellen Sie also einen Ordner „PolicyDefinitions“ im SYSVOL. Am besten machen Sie das gleich auf dem PDC-Emulator – die GPMC und gpedit.msc schauen immer dort zuerst nach!



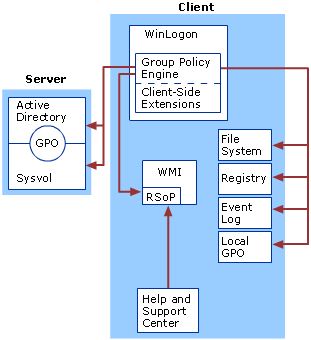
Jetzt kopieren Sie alle Dateien aus c:\Windows\PolicyDefinitions dort rein: Fertig!.

Von nun an wird der Abruf aus dem Central Store bevorzugt werden, d.h. evtl. noch vorhandene lokale Kopien werden ignoriert.

****

**Gruppenrichtlinien Architektur**

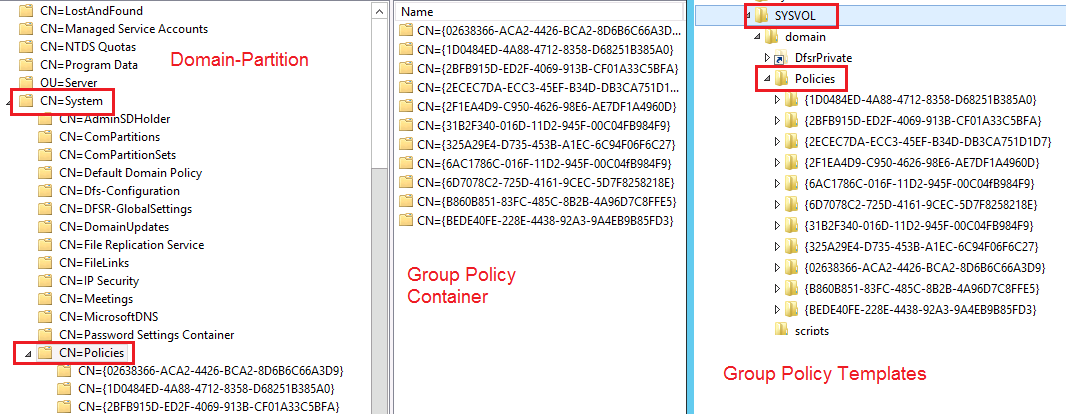
Zwei grundlegende Komponenten sind die Group Policy Engine und die Client Side Extensions. Im Zusammenspiel organisieren diese beiden das sog. Group Policy Processing – die Abarbeitung der Gruppenrichtlinien.



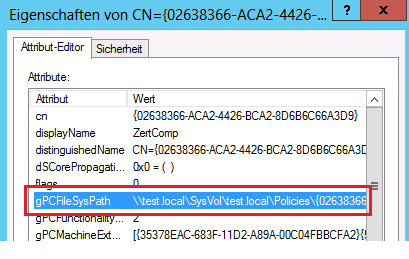
**aus:** [**http://technet.microsoft.com/en-us/library/cc784268%28v=ws.10%29.aspx**](http://technet.microsoft.com/en-us/library/cc784268%28v=ws.10%29.aspx)

Group Policy Templates und Group Policy Container

Auf Serverseite ist folgendes zu beachten: ein GPO setzt sich immer aus zwei Teilen zusammen: dem Group Policy Container (GPC, im AD) und dem Group Policy Template (GPT, im SYSVOL). Im folgenden Screenshot sehen Sie die beiden Speicherorte:



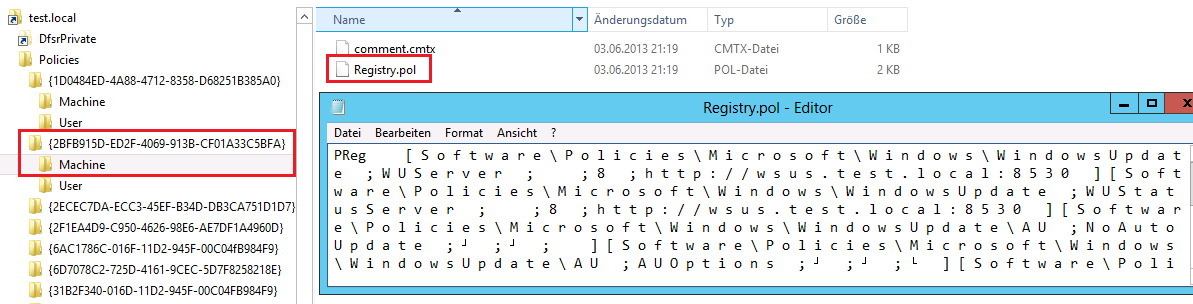
Im GPC steht in den Eigenschaften im Attribut gPCFileSysPath der dazugehörige Speicherort im SYSVOL:



Im GPC liegen ansonsten nur relativ wenig Informationen, die vor allem AD-relevante Eigenschaften (DN, Name, GUID, USN usw.) des GPOs betreffen.

Das GPT enthält die meisten Informationen: alle administrativen Vorlagen, grundlegende Richtlinien, Sicherheitseinstellungen, Skripte und mögliche Software-Verteilungen. Die GPTs werden seit Server 2008 R2 über DFS-R zwischen den DCs (mit dem ganzen SYSVOL) repliziert.

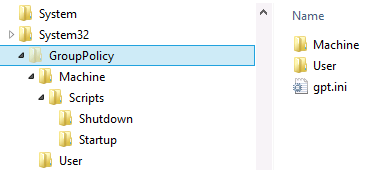
Unterhalb des Template-Ordners finden Sie Unterordner. Unter „Machine“ finden Sie die Datei registry.pol. Dort stehen die Pfade in der Registry, die durch dieses GPO angewendet werden sollen:



Dasselbe gilt natürlich auch für den „User“-Unterordner.

Lokales GPO und Multiple Local Group Policy (MLGPO)

Eine Besonderheit stellt das lokale GPO dar: Es liegt versteckt im Verzeichnis windows\system32\grouppolicy. Das lokale GPO gilt auch für Domänenmitglieder, unterliegt aber grundsätzlich den Domänen-Policies. Es existiert vor allem für den Fall, dass lokale Anmeldungen am System zulässig sind.

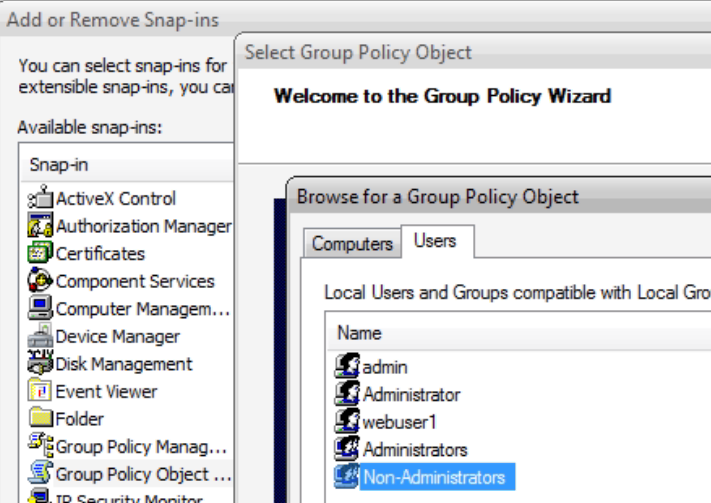


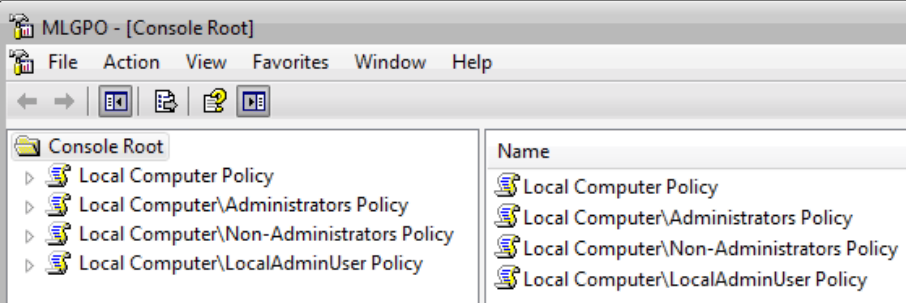
Seit Vista gibt es MLGPOs. Diese erlauben, verschiedene lokale GPOs für verschiedene User an einer Maschine einzurichten. Das richtet sich vor allem an das Szenario Administrator und Non-Administrator Group Policy.

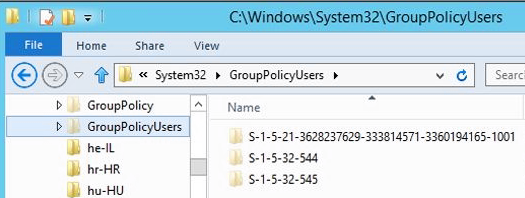
MLGPOs gliedern sich nach drei Ebenen. Einstellungen werden „Top-Down“ abgearbeitet:

|  |  |  |
| --- | --- | --- |
| **Layer** | **Art der Policy** | **Einstellung** |
| First Layer | die lokale Standard-GPO | deaktiviert |
| Second Layer | Administrator- und Non-Administrator Policy | nicht konfiguriert |
| Third Layer | Policies für spezifische User | aktiviert |
| **Ergebnis** |  | **aktiviert** |

Da es in diesem Papier maßgeblich um Domänenumgebungen geht, wird nicht näher auf das Einrichten eingegangen. Um einen Eindruck zu gewinnen:



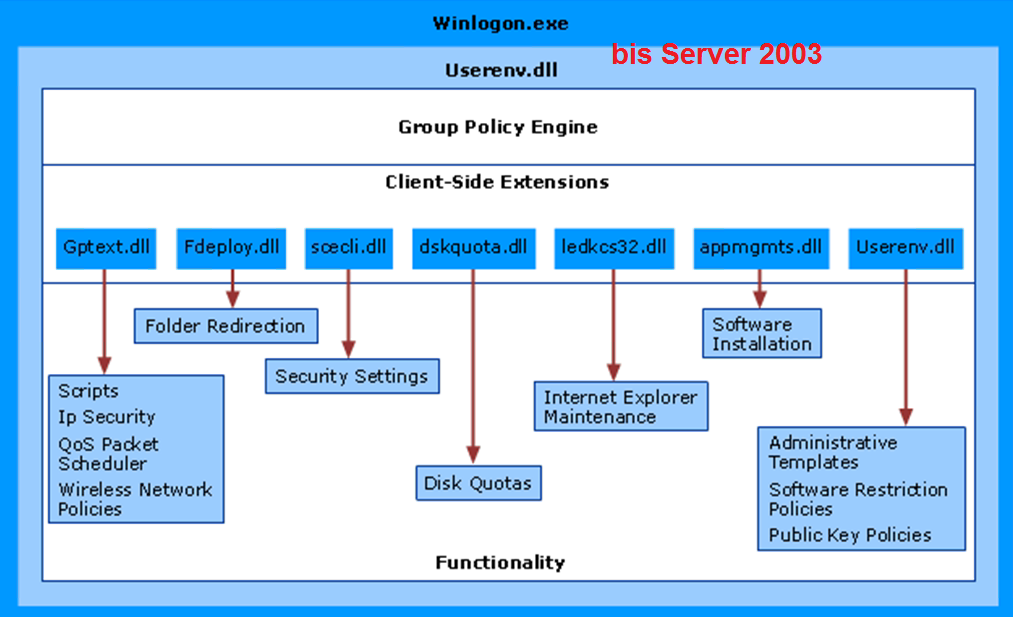




Eine detaillierte Anleitung finden Sie hier: <http://technet.microsoft.com/de-de/library/cc766291%28v=ws.10%29.aspx>

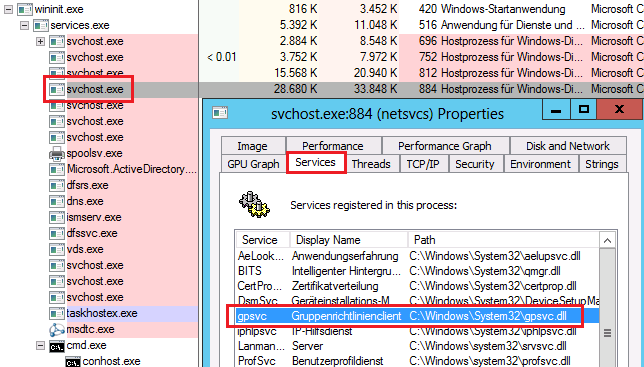
**Die Group Policy Engine**

Die Group Policy Engine ist *die* zentrale Komponente. Unter Server 2003 sah das Ganze noch so aus:

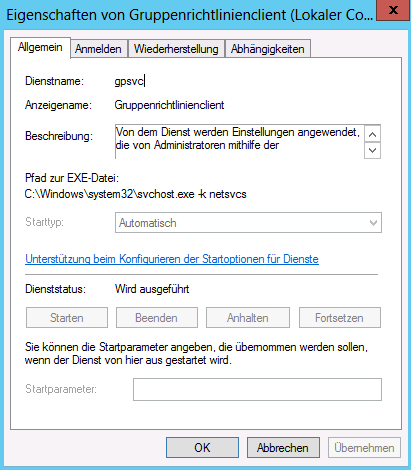


**aus:** [**http://technet.microsoft.com/en-us/library/cc784268%28v=ws.10%29.aspx**](http://technet.microsoft.com/en-us/library/cc784268%28v=ws.10%29.aspx)

Mit Einführung von Server 2008 /Vista hat sich dieses Konzept grundlegend geändert. Nun läuft die Engine im Kontext des Dienstes GroupPolicyClientService (GPSVC). Dieser läuft innerhalb eines svchost-Prozesses. Ein Blick in den Process-Monitor:



Dieser GPSVC verhält sich etwas eigentümlich. Werfen Sie mal einen Blick in Services.msc:

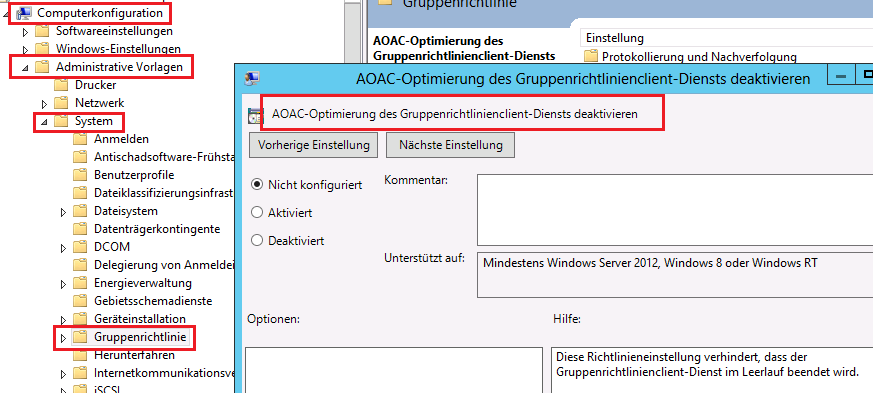


Hier ist alles ausgegraut – ein untrügliches Zeichen dafür, dass Windows nicht will, dass Sie hier rumspielen! Wenn Sie’s unbedingt wollen: hier steht wie: <http://www.winfaq.de/faq_html/Content/tip2000/onlinefaq.php?h=tip2344.htm>

Auf einem Windows 8 sieht der Dienst so aus:



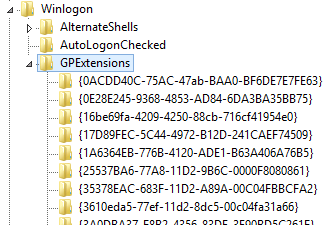
Er läuft gar nicht die ganze Zeit – er legt sich alle 10 Minuten schlafen! Microsoft nennt das allen Ernstes Energiesparen: Das Ganze firmiert unter AOAC (Always-on, Always-Connected), kann aber per GPO ausgeschaltet werden:



Client Side Extensions

In der Registry liegen im folgenden Pfad die sog. GPExtensions – hier auf einem Server 2012:



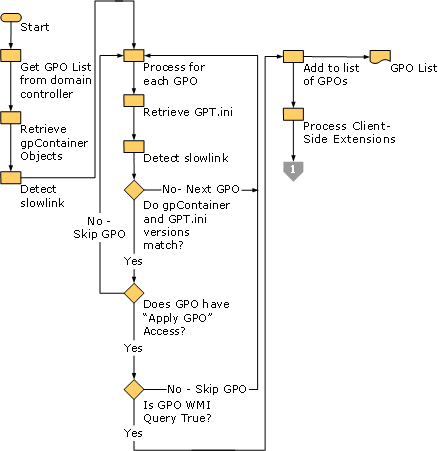


Eine komplette Liste, welche CSEs hinter welcher GUID stehen und welche dlls beteiligt sind, findet sich hier: <http://evilgpo.blogspot.de/search/label/client%20side%20extensions>

Was machen diese CSEs? Wie schon gesagt, der Server stellt GPOs nur bereit – der Client holt sich die GPOs und verarbeitet sie lokal. Das CSE organisiert dabei, wie und wo Konfigurationen aus den GPOs umgesetzt werden müssen. Dabei werden sie von den ihnen zugeordneten dlls gesteuert. Die Reihenfolge richtet sich dabei aufsteigend nach den GUIDs. Das Ganze erfolgt ausschließlich im Kontext des SYSTEM-Kontos.

Ablauf der GPO-Anwendung

Das Ganze funktioniert dann so: Zunächst muss der Client sich die Infos holen, welche GPOs auf ihn zur Anwendung kommen:



**aus:** [**http://technet.microsoft.com/en-us/library/cc784268%28v=ws.10%29.aspx**](http://technet.microsoft.com/en-us/library/cc784268%28v=ws.10%29.aspx)

Mit diesem Verfahren sollten Sie sich detaillierter vertraut machen.

**Abarbeitungsregel: LSDOU**

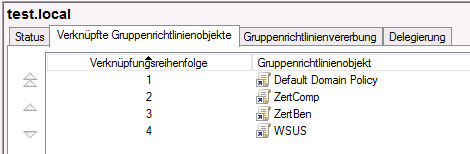
Sie können GPOs auf vier Ebenen verknüpfen: Lokales GPO – Standort – Domäne – OU

Sie können sich das mit der Abkürzung LSDOU merken. Einstellungen vererben sich dabei von lokal bis zur OU: solange also nichts Gegenteiliges konfiguriert wird, können sich die lokalen Einstellungen behaupten.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ebene** | **GPO1 - Einstellung** | **GPO2 – Einstellung** | **GPO3 – Einstellung** |
| Lokal | Aktiviert | nicht konfiguriert | nicht konfiguriert |
| Standort | nicht konfiguriert | nicht konfiguriert | aktiviert |
| Domäne | nicht konfiguriert | Aktiviert | deaktiviert |
| OU | nicht konfiguriert | deaktiviert | aktiviert |
| **Ergebnis** | **Aktiviert** | **deaktiviert** | **aktiviert** |

Vorrang (Precedence)

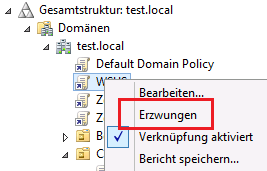
Auf jeder dieser Ebenen können natürlich mehrere Objekte verknüpft sein. In diesem Fall entscheidet die Verknüpfungsreihenfolge:



Dabei wird aufsteigend verarbeitet, d.h. die Einstellungen von dem WSUS-GPO oben in der Abbildung haben den niedrigsten Vorrang.

Erzwungen /Enforced (no override)

Wenn ein GPO „Erzwungen“ wird, dann kann seine Konfiguration auf der nächsten Ebene nicht überschrieben werden.



Ein Beispiel:

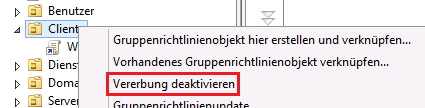
|  |  |  |
| --- | --- | --- |
| **Ebene** | **GPO – Einstellung xyz („normal“)** | **GPO – Einstellung xyz („Erzwungen“)** |
| Domäne | aktiviert | aktiviert |
| OU | deaktiviert | deaktiviert |
| **Ergebnis** | **deaktiviert** | **aktiviert** |

Mit Hilfe eines „Erzwungen“ kann der Domänenadmin also Einstellungen wirklich sicher festlegen. Evtl. delegierte Berechtigungen an einer OU ermöglichen deren Admins evtl. das Anlegen eigener GPOs – die Einstellungen einer *erzwungenen* Richtlinie bleiben dann aber in jedem Fall gewährleistet (was ja im default nicht so wäre).

Im Prinzip bewirkt ein „Erzwungen“, dass dies GPO in jedem Fall als letztes abgearbeitet wird.

Vererbung deaktivieren / Block inheritance

Wenn Sie auf Domänenebene ein GPO verknüpfen, dann vererbt sich dessen Konfiguration auf alle OUs. Wenn sie diese Einstellung für eine bestimmte OU aber nicht wollen (IT, Leiter o.ä.), dann können Sie für diese OU die Vererbung deaktivieren:



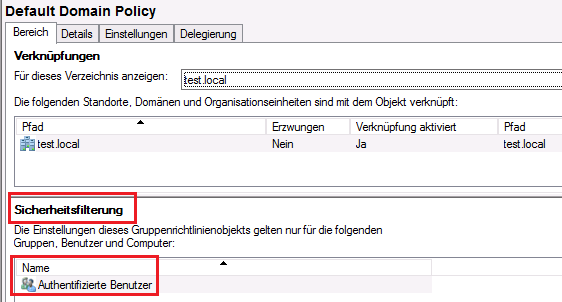
Die Deaktivierung der Vererbung kann ein „Erzwungen“ *nicht* aushebeln!

Dasselbe könnten Sie auch auf Domänenebene machen, dann würde nichts vom Standort übernommen werden.

Sicherheitsfilterung

Die Sicherheitsfilterung dient der Feinabstimmung: Hier können Sie festlegen, auf welche Objekte (Benutzer, Gruppen, Computer) in einem Container (Standort, Domäne, OU) das GPO wirken soll.

Wenn ein GPO wirken soll, dann muss das Objekt sowohl das GPO lesen können, als auch die Berechtigung „Gruppenrichtlinie übernehmen“ haben. Im default gilt das immer für „Authentifizierte Benutzer“, d.h. alle Domänenbenutzer- *und Computer* sind erfasst:



Bevor ein GPO abgearbeitet wird, wird seine ACL überprüft. Grundsätzlich gilt auch hier, dass eher mit geringem „Zulassen“ und nur im Notfall mit einem „Verweigern“ gearbeitet werden sollte.

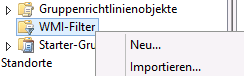
WMI-Filter

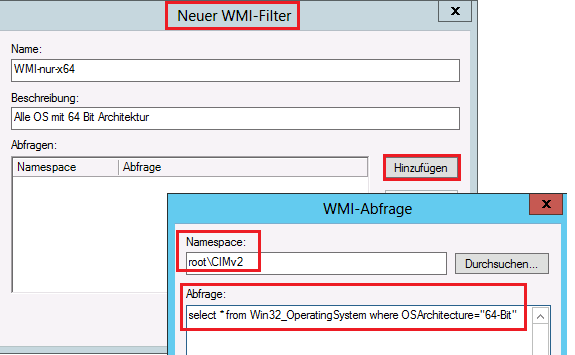
Mittels WMI können bestimmte Hardware- oder Softwareinformationen als Kriterium für das Anwenden eines GPOs herangezogen werden. Erfüllt das Objekt den Filter (TRUE), wird das GPO angewendet – erfüllt es ihn nicht, eben nicht (FALSE). Jedes GPO kann mit einem WMI-Filter verknüpft werden. Clients mit Windows 2000 ignorieren WMI-Filter!

WMI-Filter basieren auf der WQL – der WMI Query Language, die große Ähnlichkeit zu SQL-Queries hat. Die Windows Management Instrumentation ist eine Microsoft-Implementierung des Common Information Models (CIM). Es handelt sich im Wesentlichen um eine Schnittstelle, über die umfängliche Hard- und Softwareinformationen verwaltet werden können.

WMI-Filter Beispiel – GPO nur auf Computer mit x64-Architektur anwenden

WMI-Filter werden in der GPMC zunächst erstellt und dann einem GPO zugewiesen:

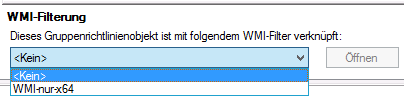




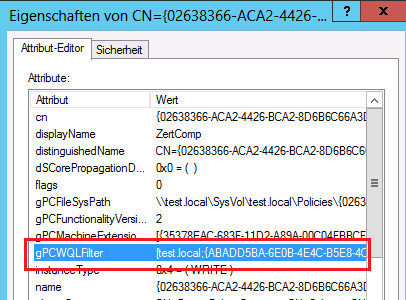
Leider bietet die GPMC keine Möglichkeit, die Query zu generieren. Deshalb sollte man hier entweder aufs Internet vertrauen oder z.B. von Microsoft den WMI Code Creator herunterladen.

<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=8572>

Der WMI-Filter kann dann über den Reiter „Bereich“ einem GPO zugeordnet werden:



Bei der Abarbeitung wird das Attribut gPCWQLFilter im GP-Container überprüft:



**First Contact: Initial-GPO-Processing**

Was während des Processings (also der Abarbeitung der Richtlinien) geschieht, müssen Sie für das Troubleshooting unbedingt verstanden haben. Vor allem Fragen wie „Warum zieht die Richtlinie nicht?“ erklären sich danach wie von selbst.

Computerstart

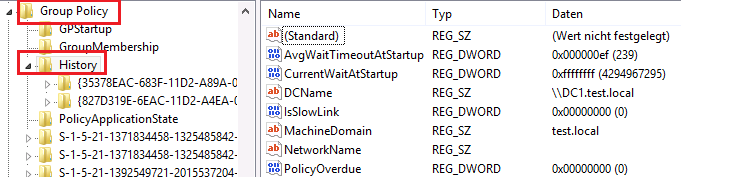
Die Kommunikation zwischen Client und DC startet mit dem Zugriff auf das SYSVOL-Verzeichnis. Dort liegen unter Policies die GPTs.



Zu diesem Zeitpunkt sind ausschließlich die Computerkonfigurationen interessant. Außerdem überprüft der DC den Standort und die OUs, in denen der Client Mitglied ist. So werden die GPOs bestimmt, die auf den Client Anwendung finden müssen.

Der Client merkt sich diese GPOs auch in der Registry. Damit kann der Client bei einem Update überprüfen, ob sich tatsächlich eine Änderung an bereits bekannten GPOs ergeben hat.

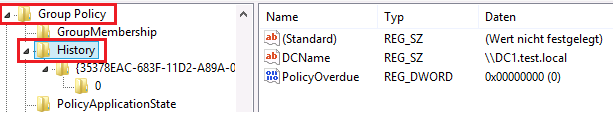
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History



Benutzeranmeldung

Bei der Benutzeranmeldung werden die benutzerrelevanten Teile der GPOs verarbeitet. Auch diese werden in der Registry gemerkt:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy\History



Nun lohnt es sich (jaja, tut es), bis zu Windows 2000 zurückzublicken:

Synchrone Abarbeitung bei Windows 2000

Computer startet -> DNS-Client sucht DC -> DC ordnet Client Site, Domäne und OU zu -> “Computereinstellungen werden übernommen” (sollte also eigentlich heißen: Computerkonfiguration der GPOs werden übernommen)

Anmeldedialog wird präsentiert (STRG-ALT-ENTF) -> Benutzerkonfiguration der GPOs werden übernommen

Diese Abarbeitung nennt man *synchronous processing*: Der Benutzer landet erst dann auf dem Desktop, wenn alle Einstellungen nacheinander abgearbeitet wurden! Zunächst müssen die Compuereinstellungen fertig sein, erst dann startet die Abarbeitung der Benutzerkonfigurationen. Erst wenn diese wiederum abgearbeitet worden sind, wird der Desktop angezeigt.

Bei XP, Windows 7 und Windows 8 gibt es hier keinen Unterschied zu Windows 2000: auch hier findet eine synchrone Abarbeitung statt.

Background Refresh (asynchronous)

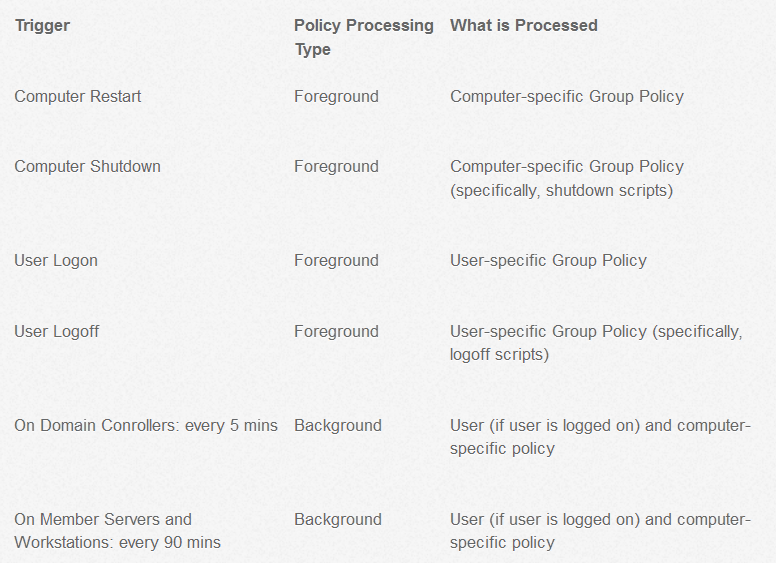
Bei einer Änderung von GPOs während einer aktiven Benutzeranmeldung kommt das sog. Background Refresh zum Tragen. Dies ist eine sog. *asynchrone Abarbeitung*.

Background refreshs finden alle 90 Minuten mit einer Zufallsverzögerung von 0 bis 30 Minuten (es kann also schlimmstenfalls 120 Minuten dauern) statt. Erschwerend kommt hinzu, dass diese Intervalle getrennt für Computer- und Benutzerkonfigurationen laufen.

Für DCs sind diese Intervalle kürzer: hier wird alle 5 Minuten neu überprüft.

Background und Foreground-Refresh

Dennoch gibt es weiterhin foreground-refreshs: Foreground refreshs finden aufgrund bestimmter Ereignisse statt, background refreshs auf Basis des festgelegten Intervalls.

  
**aus:** [**http://gpoguy.com/whitepapers/understanding-foreground-and-background-gpo-processing/**](http://gpoguy.com/whitepapers/understanding-foreground-and-background-gpo-processing/)

Ordnerumleitung, Software-Installationen, Disk-Quotas und Skripte können nur im foreground-processing angewendet werden.

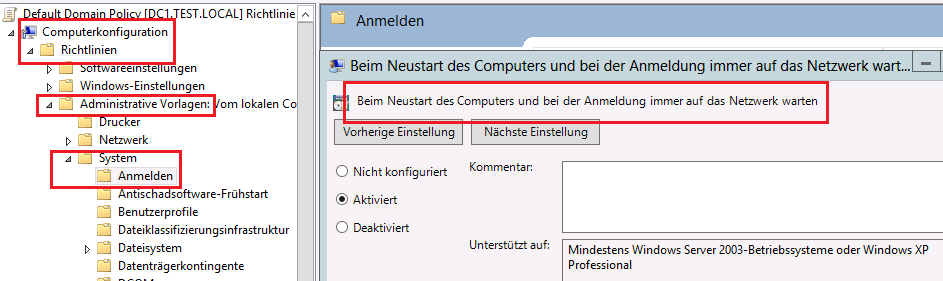
Unterschied im background-processing seit Windows XP: Fast logon optimization

Bislang galt, dass beim Systemstart ein foreground-processing stattfindet. Das ist aber nur bei Windows 2000 so. Windows XP (und Vista, und 7 und 8…) wurde vor allem mit dem schnelleren Start vermarktet. Sobald das initial-processing einmal durchlaufen wurde, arbeitet jedes OS ab XP anders als 2000: GPOs werden jetzt immer asynchron verarbeitet! Schlimmer noch: das OS wartet gar nicht erst den Kontakt zu einem DC ab, wenn das Netzwerk etwas braucht. Es nimmt einfach die letzten bekannten GPOs als Basis (History-Zweige der Registry!). Das gilt sowohl für den Computerstart als auch für die Benutzeranmeldung. Neuere Richtlinien finden also u.U. trotz eines Systemstarts mit neuem Logon (noch) keine Anwendung!

Als ob das noch nicht unschön genug ist: was ist mit den GPOs, die nur im foreground-processing abgearbeitet werden können? Microsoft geht hier einen etwas faulen Kompromiss ein: der Computer oder Benutzer bekommen während des background-refreshs einen sog. tag, dass für den kommenden Start bzw. das kommende Logon eine synchrone-Abarbeitung stattfinden muss. Für Softwareverteilung wird das also in zwei Starts/ Abmeldungen münden, bis ein GPO zieht.

Nähere Infos hier: <http://support.microsoft.com/kb/305293/en-us>

Meiner Meinung nach, ist dieses Verhalten inakzeptabel. Die Beschleunigung des Anmeldeerlebnisses des Users geht auf Kosten der sauberen Abarbeitung der Richtlinien. Zum Glück können Sie alle Maschinen zum alten Windows 2000 Verhalten zwingen, also der standardmäßig synchronen Abarbeitung von Richtlinien. So verhält sich jeder Neustart, jeder Logon wie beim Initial-Processing. Erst wenn alle Computer-GPOs sauber abgebarbeitet wurden, kann sich der Benutzer anmelden. Und den Desktop sieht er erst dann, wenn die Benutzer-GPOs durch sind. Einfach eine GPO dafür konfigurieren:

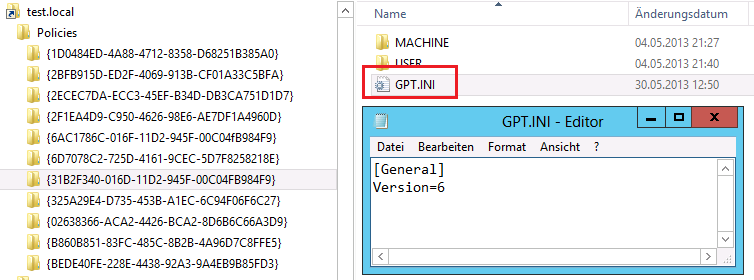


Oder Sie konfigurieren für bestimmte CSEs das erzwungene Abarbeiten (synchron) bei jedem Start:

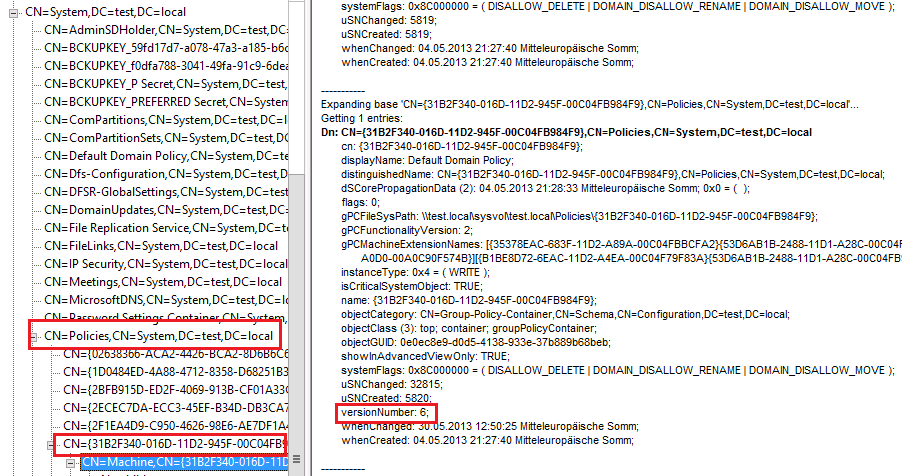
**Computerkonfiguration\Administrative Vorlagen\System\Gruppenrichtlinie**

**Versions-Nummern**

Wie stellt das OS fest, ob eine GPO neu angewendet werden muss, wenn es in der History etwas findet? GPOs haben eine Versions-Nummer (siehe oben Screenshot Registry). Bei jeder Art von Refresh wird diese Nummer abgeglichen, um Änderungen festzustellen. Der DC speichert diese Versionsnummer zum einen in der Datei GPT.ini unter der GUD des GPOs im SYSVOL-Verzeichnis:



Und in der AD-DB:



Durch den Abgleich der Versionsnummer im GPC und im GPT vergewissert sich der DC, dass das GPO in einem konsistenten Zustand ist.

**Gpupdate**

Natürlich können Sie ein OS zwingen, sofort nach geänderten Richtlinien zu fragen: mit gpupdate.

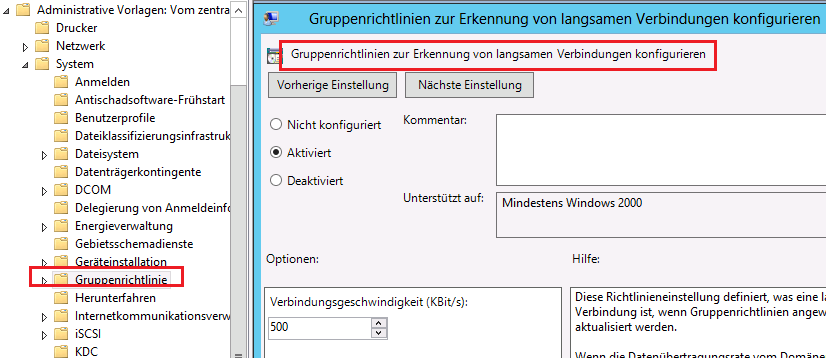
|  |  |
| --- | --- |
| /force | Initiiert einen refresh unabhängig von der Versionsnummer aller GPOs. Es ist ein weitverbreitetes Missverständnis, dass /force etwas mit dem *sofortigen* Updaten zu tun hätte. |
| /target:{Computer|User} | Entweder nur Computer- oder nur User-Konfigs abarbeiten |
| /wait:{value} | gpupdate wartet standardmäßig 10 Min. auf das Abarbeiten des Befehls; ein „-1“ an dieser Stelle würde unendlich warten. |
| /logoff | wenn GPOs gefunden werden, die einen foreground-refresh benötigen (SW-Install, Ordnerumleitung) erfolgt ein automatisches logoff. |
| /boot | dasselbe wie /logoff, nur eben für Computerkonfigurationen |
| /sync | Macht dasselbe wie die oben erwähnte Richtlinie „Auf das Netzwerk warten“ – nur eben einmalig und manuell. |

**Slow-Link-Detection**

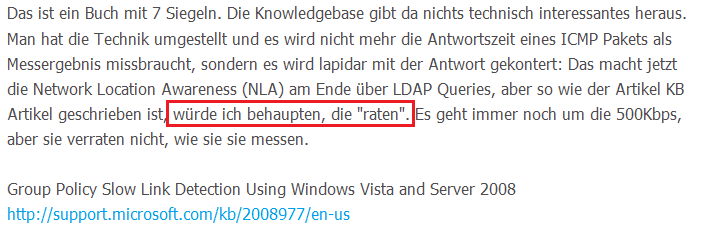
Wenn während des Processings ein „Slow-link“, also ein langsames Netzwerk erkannt wird, dann werden folgende CSEs angewiesen, keine Abarbeitung durchzuführen:

|  |  |
| --- | --- |
| **CSE** | **Default** |
| Sicherheitseinstellungen | an (kann nicht ausgestellt werden) |
| Administrative Vorlagen | an (kann nicht ausgestellt werden) |
| Software Installation | aus |
| Skripte | aus |
| Ordnerumleitung | aus |

Das Verhalten der Slow-link-Detection wird über GPOs gesteuert.



Wie die Berechnung der Verbindungsgeschwindigkeit erfolgt? Hier ein Zitat vom Kollegen Heitbrink:



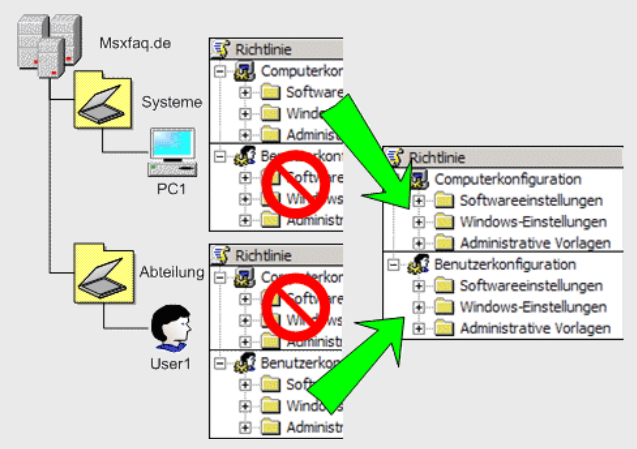
**aus:** [**http://www.gruppenrichtlinien.de/artikel/slow-link-detection-erkennung-langsamer-verbindungen/**](http://www.gruppenrichtlinien.de/artikel/slow-link-detection-erkennung-langsamer-verbindungen/)

Zu NLA hier: <http://technet.microsoft.com/de-de/library/cc749203%28v=ws.10%29.aspx>

**Loopback-Verarbeitungsmodus**

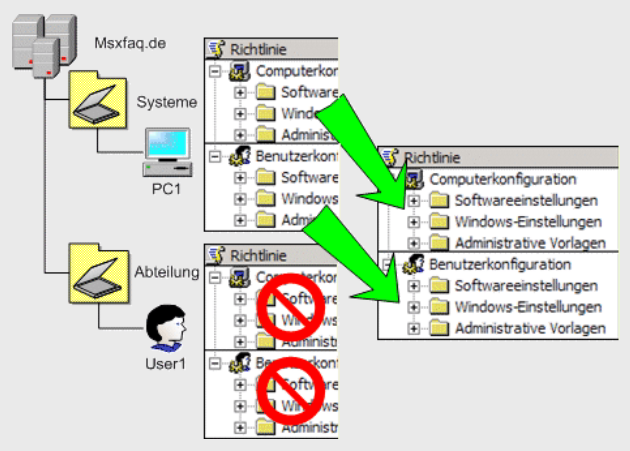
Im Prinzip geht es beim Loopback darum, Benutzerkonfigurationen abhängig vom Computer durchzusetzen. Der Loopback wird als GPO für die Computer implementiert, an denen die Benutzerkonfigurationen ignoriert oder ergänzt werden sollen. Ein gutes Beispiel wären Termminalserver, an denen keinesfalls bestimmte Benutzerkonfigurationen zum Zuge kommen dürfen. Folgende Skizzen verdeutlichen das sehr gut:

Normalerweise würde so abgearbeitet werden:



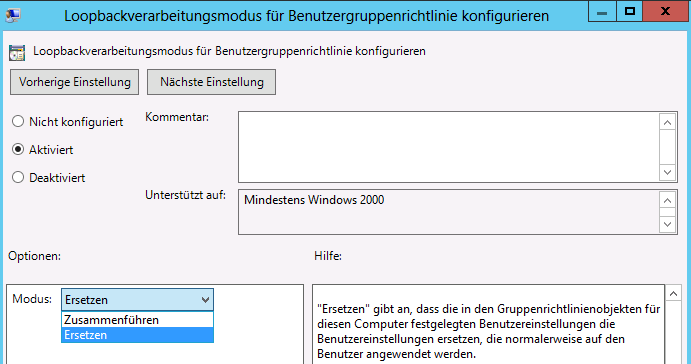
**aus:** [**http://www.msxfaq.de/verschiedenes/gpo.htm**](http://www.msxfaq.de/verschiedenes/gpo.htm)

Im Loopback sieht das Ganze dann so aus:



**aus:** [**http://www.msxfaq.de/verschiedenes/gpo.htm**](http://www.msxfaq.de/verschiedenes/gpo.htm)

Das obige Bild zeigt den Replace-Mode (Ersetzen). Es wäre auch ein Merge (Zusammenführen) möglich: **Computerkonfiguration\Administrative Vorlagen\System\Gruppenrichtlinie**



**Group Policy Preferences (GPP) – Gruppenrichtlinien Einstellungen**

Im Gegensatz zu den Policies und ihren Versionsnummern, werden die Preferences jedesmal verarbeitet. Außerdem schreiben Sie in den Originalpfad, manipulieren also die Defaultwerte!

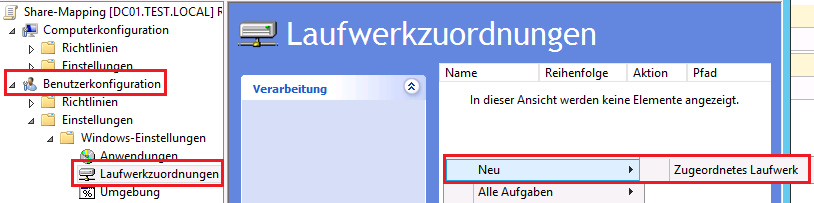
Das hat vor allem eine Konsequenz: User können Preferences fast immer umgehen, weil ja die Originalzweige (z.B. in CurrentUser) für den User beschreibbar sind.

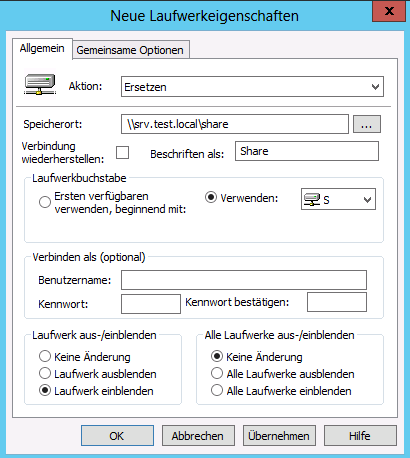
Klingt ja nicht so gut, oder? Im Gegenteil! Begreifen Sie Preferences erstmal als Vorschläge an den Benutzer.

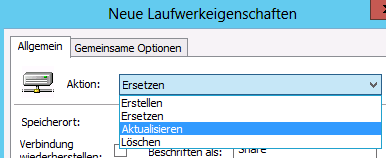
Laufwerkszuordnungen

Anmeldeskripte im NETLOGON oder das direkte Einpflegen von LogonScripts im AD-Konto sind seit der Einführung der GPPs Schnee von gestern.

In diesem Beispiel soll die Freigabe „SHARE“ auf srv.test.local für jeden Benutzer der Domäne gemapped werden.



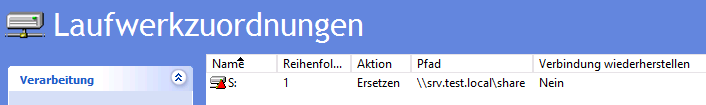




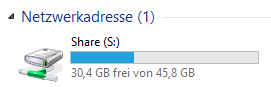
**Ersetzen**: Löscht bestehendes Mapping und legt das Neue mit seinen Konfigurationen an.

**Aktualisieren**: Löscht nicht, sondern ergänzt nur die Einstellungen.

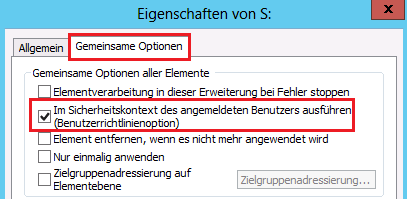
Fertig!



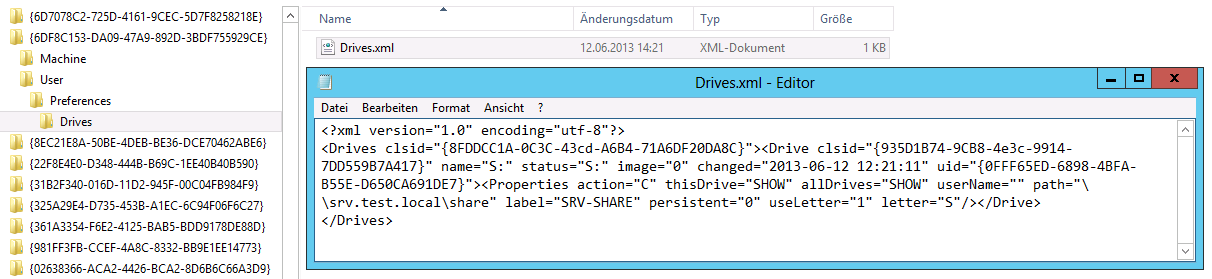
Ergebnis auf WIN8:



Normalerweise klappt das gut. Wenn Sie Probleme haben, könnte die Benutzerrichtlinienoption helfen. Normalerweise werden GPPs im Kontext des Systemkontos ausgeführt. U.U. hat das aber keinen Zugriff auf die Ressource, der Benutzer aber schon. Deshalb lässt sich die Benutzerrichtlinienoption konfigurieren. Dann wird das Mapping im Sicherheitskontext des Benutzers ausgeführt:



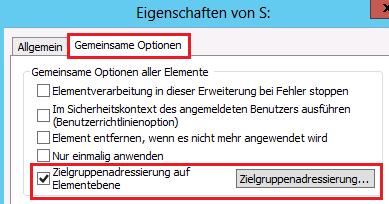
Die Konfiguration jedes GPPs wird im SYSVOL unterhalb des GPOs mit einer xml-Datei gespeichert:

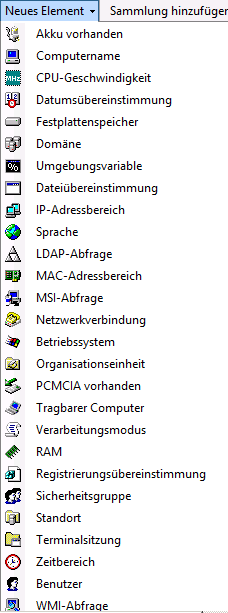


Noch nicht überzeugt? net use doch besser? Dann schauen Sie sich mal das Weitere an.

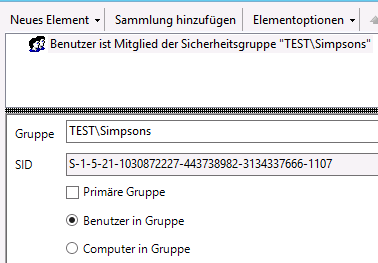
Laufwerkszuordnungen – Zielgruppenadressierung

Oben wurde ein Laufwerk für alle Benutzer einer OU gemapped. Jetzt wollen Sie, dass es nur für bestimmte Gruppen zugeordnet wird.

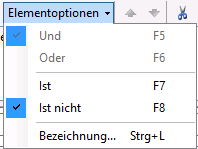


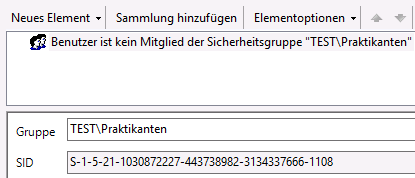


Sie entscheiden sich hier für das Element „Sicherheitsgruppe“. Mit folgender Einstellung würde das Laufwerk nur Mitgliedern der Gruppe „Simpsons“ zugeordnet.



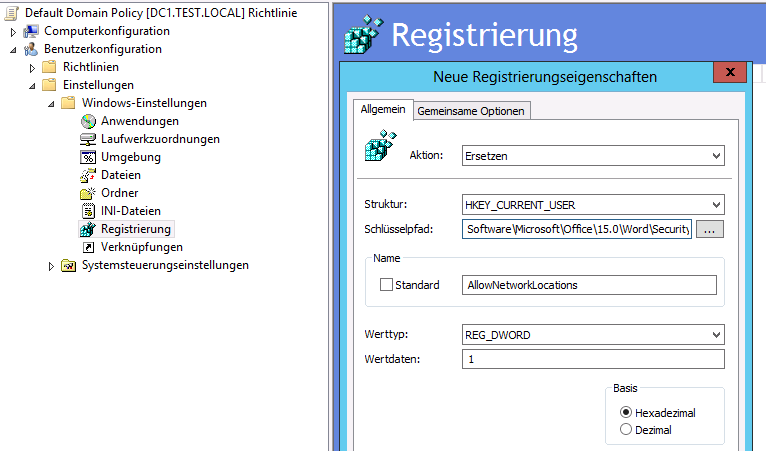
Unter „Elementoptionen“ können Sie auch negativ formulieren. Wenn also ein Benutzer Mitglied in mehreren Gruppen ist, dann kann eine Gruppenmitgliedschaft dafür sorgen, dass er das Laufwerk *nicht* bekommen wird:





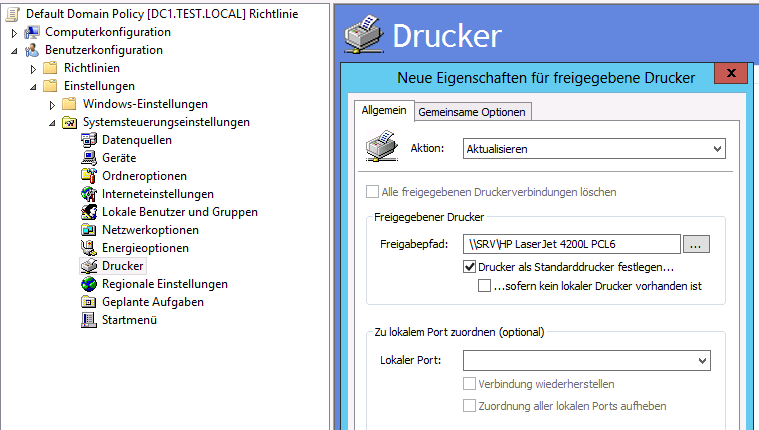
Setzen eines Registry-Keys auf bestimmte Computer

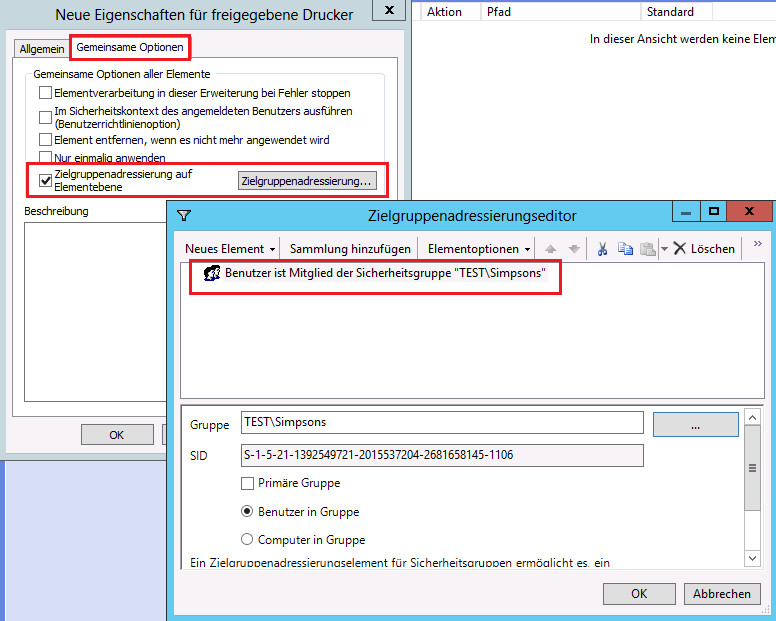
Hier wird als Beispiel ein vertrauenswürdiger Speicherpfad für Word gesetzt – auf Benutzerbasis:



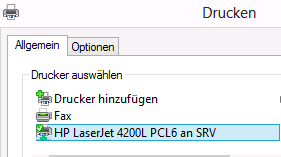
Freigeben von Standarddruckern in Abhängigkeit einer AD-Gruppenmitgliedschaft

Sie können über die Preferences Standarddrucker in Abhängigkeit einer bestimmten Gruppenmitgliedschaft festlegen:

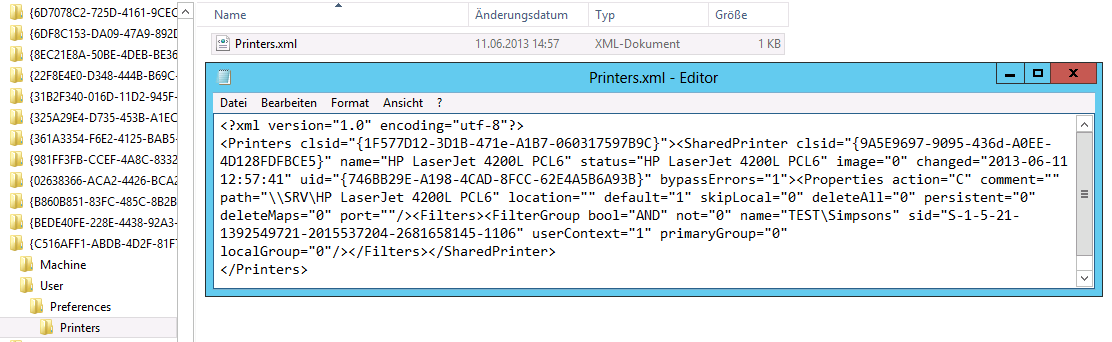




Ergebnis am Win8:



Im SYSVOL die xml-Datei:



Einstellungen Internet Explorer: Rot und Grün, F5-F6-F7-F8

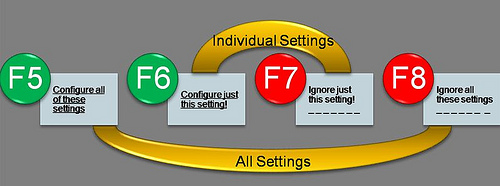
Die meisten Systemsteuerungseinstellungen bilden im Prinzip die Fenster ab, wie Sie auch in der Systemsteuerung selbst oder einer Anwendung zu sehen wären.

Nette Idee, aber: Wie wollen Sie entscheiden, ob eine Einstellung aktiviert, deaktiviert oder nicht konfiguriert ist? Wenn Sie ein Häkchen nicht setzen, was meinen Sie damit? Deaktiviert? Nicht konfiguriert? Was, wenn nur einige Einstellungen per GPP verändert werden sollen, andere nicht?

Microsoft löst dieses Problem über farbliche Markierungen und die Funktionstasten F5-F6-F7-F8.

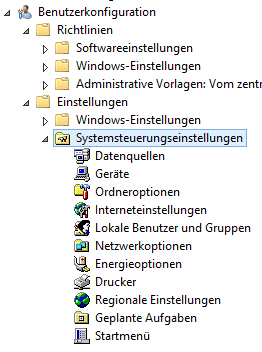
Grün = aktiviert, Rot = deaktiviert (kein Eintrag in xml-Datei im SYSVOL)  
keine Farbe = nicht konfiguriert

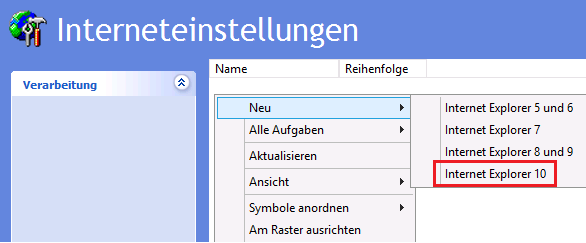
F5 – alle grün   
F6 – eine grün   
F7 – eine rot   
F8 – alle rot

  
**aus:** [**http://blogs.technet.com/b/grouppolicy/archive/2008/10/13/red-green-gp-preferences-doesn-t-work-even-though-the-policy-applied-and-after-gpupdate-force.aspx**](http://blogs.technet.com/b/grouppolicy/archive/2008/10/13/red-green-gp-preferences-doesn-t-work-even-though-the-policy-applied-and-after-gpupdate-force.aspx)

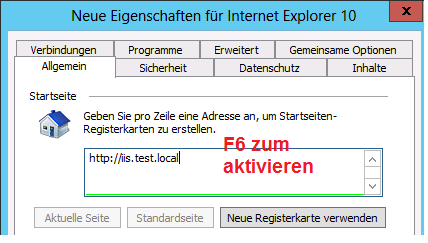
Schauen Sie sich das mal an einigen konkreten Konfigs an. Vorab eine Warnung: Mit dem IE 9 und GPPs gibt es Probleme! <http://matthiaswolf.blogspot.de/2012/08/gpp-und-der-internet-explorer-9-das.html> In den folgenden Beispielen konfigurieren Sie den IE 10 auf Win8.

Es gibt die Einstellungen nur in der Benutzerkonfiguration:

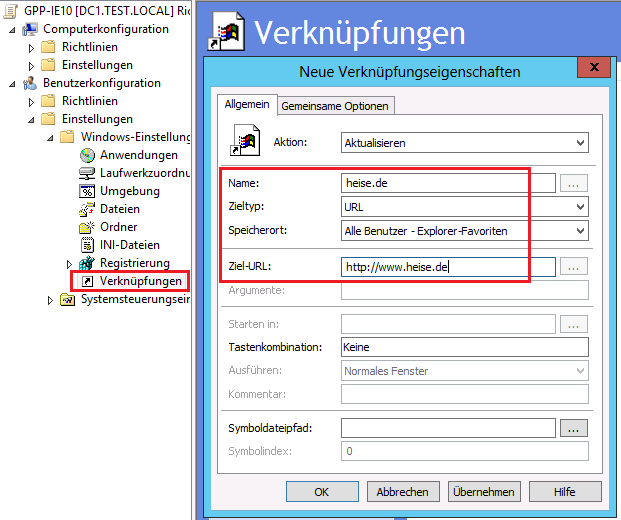




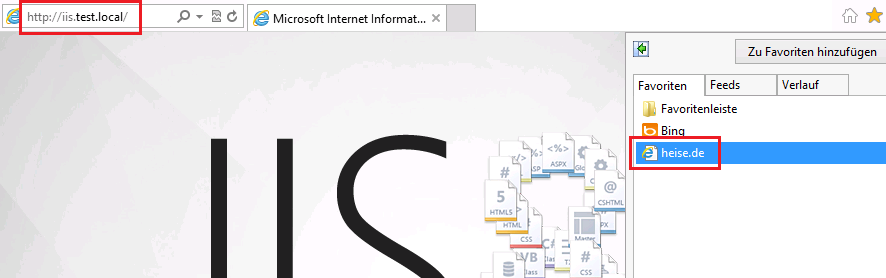
Sie richten eine Startseite ein:



Favoriten können folgendermaßen hinzugefügt werden:



Funzt:



**Neuerungen Gruppenrichtlinien Server 2012**

Force Refresh – Remote Group Policy Updates: Push it!

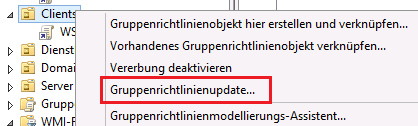
Auch mit Gpupdate dauert es manchmal gefühlte Stunden, bis eine aktualisierte Richtlinie zieht.

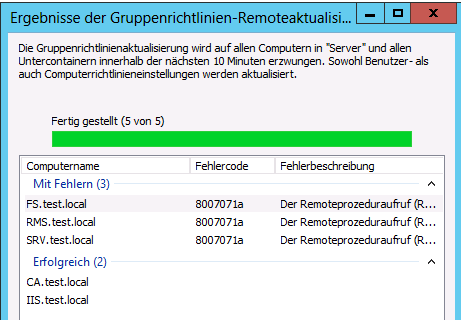
Server 2012 führt ein neues Feature ein, das gerade beim Testen neuer Einstellungen seine Stärken ausspielt. Sie können aus der GPMC von einer OU aus ein gpupdate rausschicken! 10 Minuten sollte man aber trotzdem einplanen.

Noch zu langsam? Mit folgendem neuen PS-cmdlet können Sie ein gpupdate gegen einen beliebigen Rechner *sofort* erzwingen:

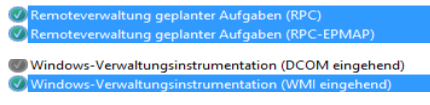
Invoke-gpupdate -computer <computername>

Mit -RandomDelayInMinutes lassen sich aber auch hier Verzögerungen definieren.

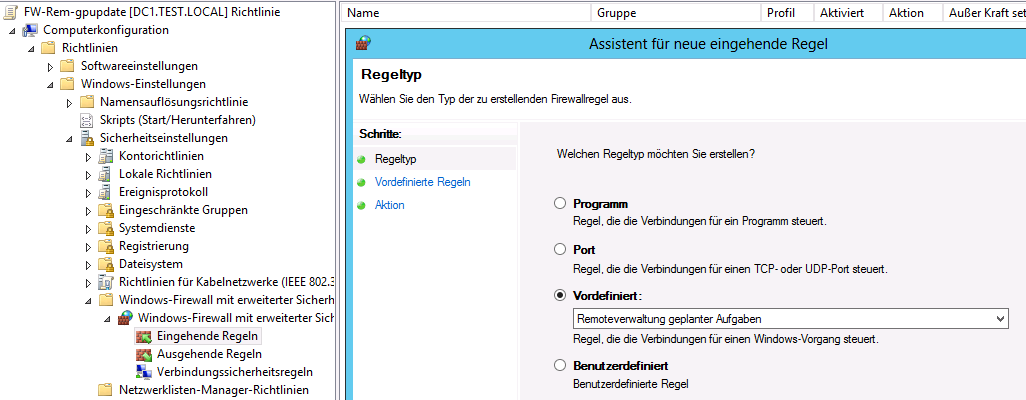




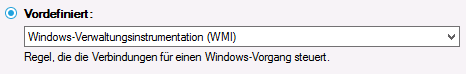
Im Screenshot oben sehen Sie Fehler bei drei Rechnern. Das liegt daran, dass auf denen die nötigen Firewallausnahmen nicht aktiviert wurden:

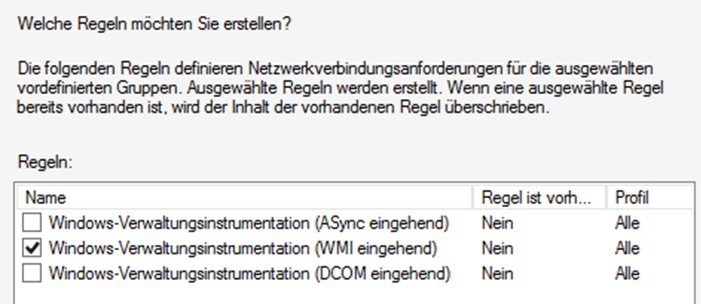


Das geht sehr einfach, denn es gibt vordefinierte Regeln, die sich dann bequem per GPO verteilen lassen:

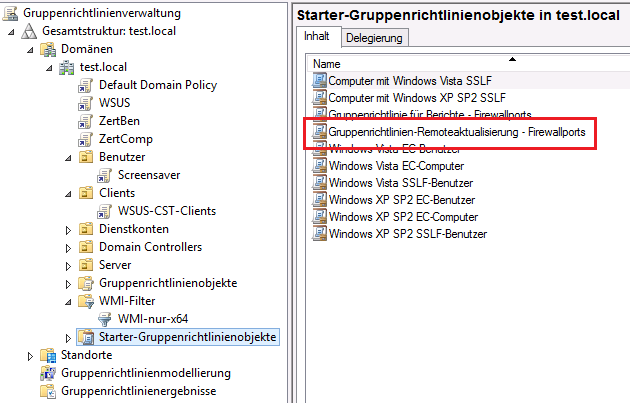


Und:

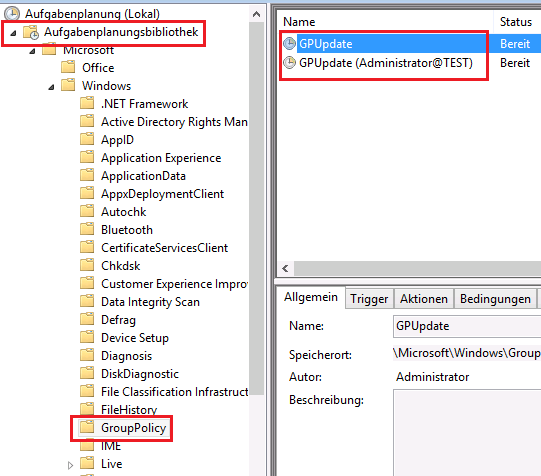




Das Ganze ginge auch über ein Starter-GPO:

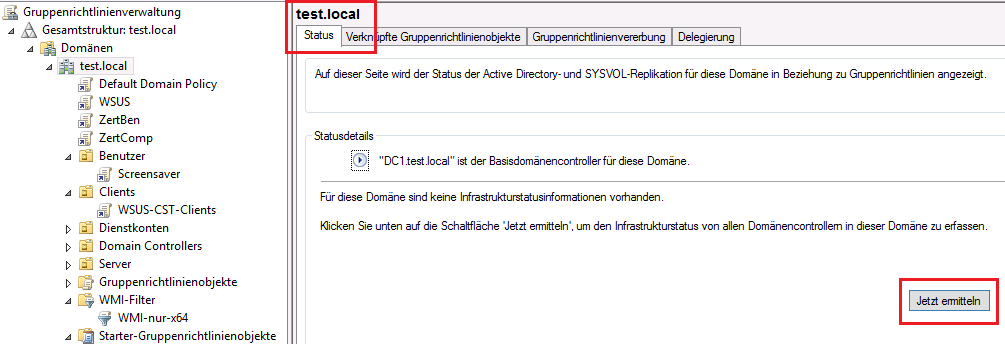


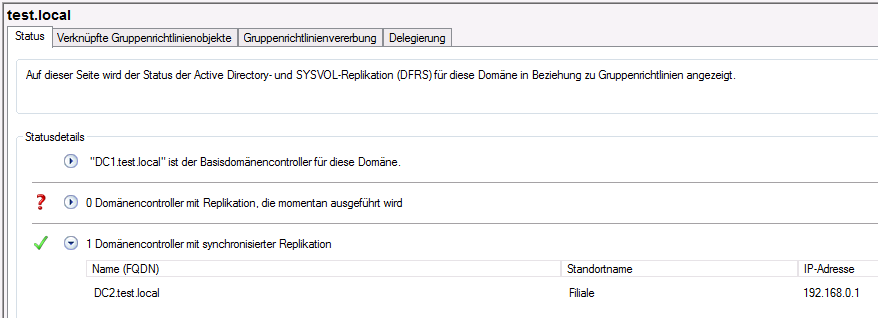
Die verschiedenen Ausnahmen lassen schon erahnen, wie das Remote-Update umgesetzt wird: es wird auf den Zielrechnern ein scheduled task angelegt:



Status Update

Ein „Ermitteln“ (Detect Now) führt dazu, dass alle DCs abgefragt werden und die SYSVOL-Einträge verglichen werden. Sehr brauchbar, um hier Replikationsproblemen auf die Spur zu kommen.





Policy Events

In den RSOP-Daten der GPMC finden Sie jetzt einen Tab zu Ereignis-IDs.

