Netz-Weise
Lernen von den Besten.

Windows Gruppenrichtlinien

von Holger Voges

Freundallee 13 a
30173 Hannover
www.netz-weise.de

Inhalt

AD-Verwaltungswerkzeuge

Active Directory stellt 4 grafische Oberflächen zur Verwaltung des AD zur Verfügung, und zwar:

- Active Directory Users and Computer (Benutzer und Computer)
- Active Directory Domains and Trusts (Domänen und Vertrauensstellungen)
- Active Directory Sites and Services (Standorte und Dienste)

Sowie in Windows Server 2012 neu dazu gekommen:

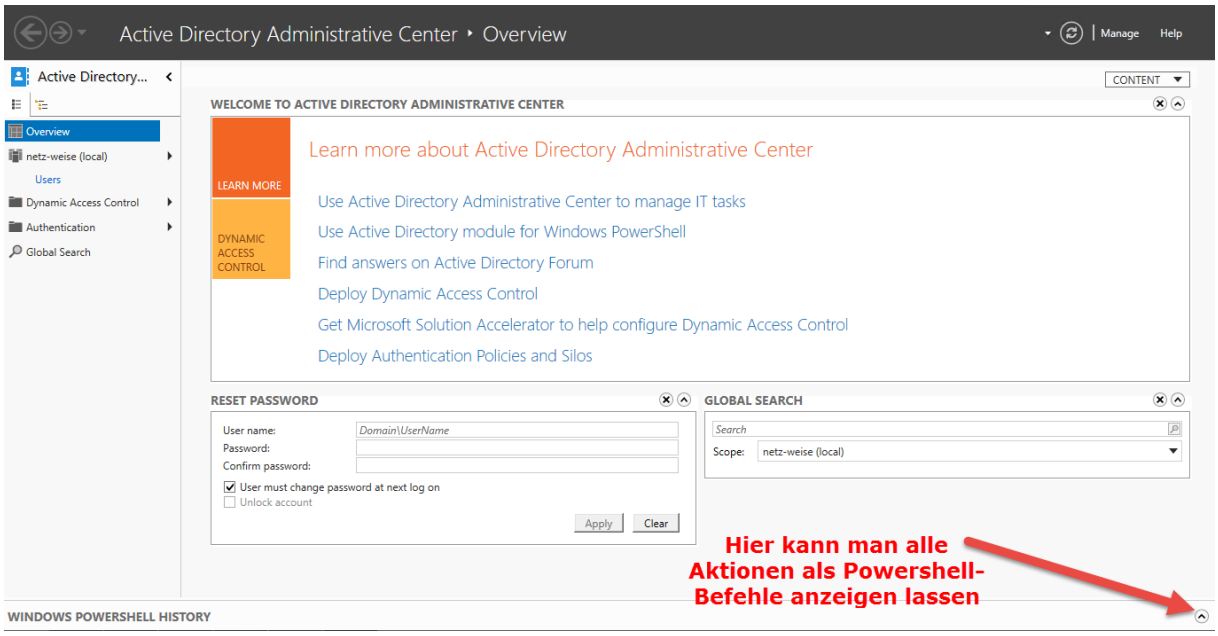
- Active Directory Administrative Center

AD Domains and Trusts und AD Sites and Services werden nur selten benötigt. Die Hauptarbeit erledigen Sie mit AD Benutzer und Computer bzw. dem Administrative Center, je nach Vorliebe. Das Administrative Center hat grundsätzlich ähnliche Fähigkeiten wie AD Benutzer und Computer, allerdings stehen noch einige zusätzliche Funktionen zur Verfügung.

AD Administrative Center

Das Administrative Center ist wie der Server-Manager PowerShell-basiert, also eigentlich ein Startprogramm für PowerShell-Befehle. Daher bietet das administrative Center einige Funktionen, die über die Powershell verfügbar sind, die Microsoft aber nicht ins Active Directory Benutzer und Computer eingebaut sind. Das sind im Einzelnen:

- Eine grafische Oberfläche für Fine Grained Password Policies
- Die Möglichkeit, den Active Directory Papierkorb zu aktivieren
- Die Konfiguration von Dynamic Access Control



Außerdem kann das Administrative Center auch noch alle Aktionen, die es ausführt, als Powershell-Befehl anzeigen lassen.

Weiterhin gibt es noch eine ganze Reihe von Kommandozeilenwerkzeugen zur Verwaltung des AD. Die wichtigsten sind:

- Die Windows Powershell

- Die Windows Powershell
- Die Windows Powershell
- Und dann noch dsquery, dsadd, dsget, dsmod, dsmove, dsquery, dsrm, csvde, ldifde und ntdsutil. Die Funktionalität der DS-Tools sowie csvde und ldifde lässt sich aber – sie werden es schon erraten haben – viel einfacher über Powershell durchführen.

Mehr Informationen über die Commandline-Tools finden Sie im Technet-Artikel Managing Active Directory from the command line. Eine ganze Reihe von zusätzlichen, sehr nützlichen AD-Tools findet man kostenlos auf der Website joewaretools.com.

Benutzerkonten und Gruppen

Die Domänencontroller verwalten in Ihren Domänendatenbanken in erster Linie Informationen über Benutzerkonten, Computerkonten und Gruppen. Diese werden zur Anmeldung benötigt. Ein Computer bzw. Benutzer, der kein Konto in der Domäne hat, kann nicht authentifiziert werden.

Beim Anlegen eines Benutzers sind eine Reihe von Informationen wie der NT4-Anmeldename (Domäne\Benutzername), ein Kennwort und eine Reihe von Kennworteigenschaften Pflicht. Tatsächlich hat das Benutzerkonto aber eine ganze Reihe von Informationen, die es verwaltet, die weit über die Anmeldeinformationen hinausgehen. Active Directory stellt nämlich nicht nur die Anmeldefunktionalität zur Verfügung, sondern als vollwertiger Verzeichnisdienst können auch eine Reihe Metainformationen verwaltet werden wie Adressinformationen, Telefonnummern, Abteilungszugehörigkeiten, Hierarchien (Manager) usw. Diese Informationen können mit einer Software abgefragt werden, die die LDAP-Abfragesprache beherrscht (LDAP-Queries). LDAP oder Lightweight Directory Access Protocol ist ein herstellerunabhängiges Protokoll, um Daten in Verzeichnisdiensten wie Active Directory, Open LDAP, Novell NDS usw. zu speichern. Um alle AD-Informationen auszulesen, können Sie neben den grafischen Verwaltungstools auch die Programme ADSIEDIT.MSC oder LDP.EXE verwenden oder auf Fremdhersteller-LDAP-Browser zurückgreifen.

Um Zugriff auf das Netzwerk zu bekommen, muss sich ein Benutzer zuerst an einem Computer anmelden, der selbst Mitglied einer Domäne im Forest ist – was nichts weiter heißt, als dass der Computer ebenfalls ein „Benutzerkonto“ in einer Domäne hat. Nur wenn der PC Mitglied der Domäne des Benutzers oder einer vertrauten Domäne ist, kann der Benutzer diesen PC verwenden, um sich an der Domäne anzumelden.

Der Anmeldevorgang

Bei der Domänenanmeldung besteht der Benutzername grundsätzlich aus der Domäne des Benutzers, in der sich der Benutzer befindet, plus seinem Benutzernamen : *netz-weise\Holger.* Wird kein Domänenname angegeben, verwendet der Computer entweder ein lokales Benutzerkonto, wenn er unter dem angegebenen Namen eines finden kann, oder er versucht eine Anmeldung an seiner eigenen Domäne. Alternativ kann man einen sogenannten User Principal Name (UPN) verwenden, der forestweit eindeutig ist und daher keinen zusätzlichen Domänennamen benötigt. Dieser UPN sieht aus wie eine Email-Adresse und kann, je nach Konfiguration, auch dieser entsprechen: *Holger@netz-weise.de* **.**

Wenn der Benutzer seine Anmeldeinformationen eingibt, schickt der Computer diese zur Überprüfung an den Domänencontroller. Hierbei wird jedoch nie das Kennwort selber übertragen. Der Domänencontroller speichert im Normalfall auch nicht das Kennwort, sondern nur einen berechneten

Wert, den sogenannten Hash. Aus dem Hash kann das Kennwort eindeutig wieder erkannt, aber nicht zurück gerechnet werden.

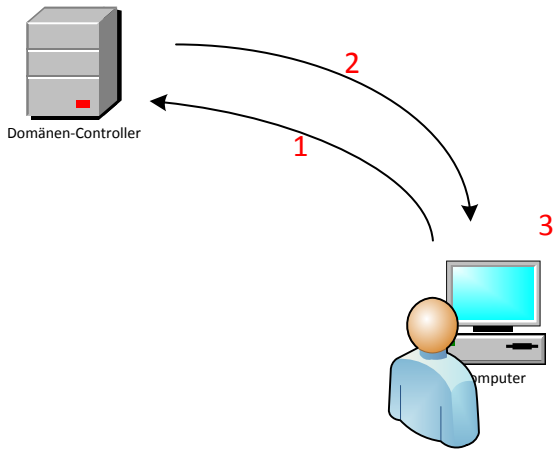
Sind der Benutzername und das Kennwort korrekt, schickt der Domänencontroller die Informationen über sämtliche Gruppenmitgliedschaften an den PC zurück, und dieser erstellt aus diesen Informationen eine Art Personalausweis (Access Token), der alle wesentlichen Sicherheitsinformationen enthält. Dieses Access-Token wird jetzt bei jedem Zugriff auf eine Ressource auf dem PC verwendet, um zu prüfen, ob ein Benutzer in den korrekten Gruppen ist, um Zugriff zu erhalten.

Wichtig! Da das Access-Token nur bei der Anmeldung erstellt und danach nicht aktualisiert wird bis der Benutzer sich neu angemeldet hat, werden Änderungen an Gruppenmitgliedschaften eines Benutzers erst mit einer Neuanmeldung gültig! Alle anderen Änderungen wie NTFS-Berechtigungen sind sofort wirksam, aber das Hinzufügen oder Entfernen von Rechten und Berechtigungen über Gruppenmitgliedschaften erfordert immer eine Neuanmeldung des Benutzers!

Um sich die Gruppenmitgliedschaften des angemeldeten Benutzers anzeigen zu lassen, kann man den Befehl

```
whomai /groups
```

verwenden. Er liest das Access-Token aus und gibt eine Auflistung aller Gruppen an.



1. Der PC gibt die Benutzerinformationen an den DC
2. Der DC verifiziert die Benutzerdaten und schickt ein Ticket mit den Benutzergruppen zurück
3. Der erstellt ein lokales (!) Access Token, das für alle lokalen (!) Zugriffe des Benutzers zur Berechtigungsüberprüfung verwendet wird.

Gruppen

Ein wesentliches Konzept bei der Berechtigungsvergabe von Windows sind Gruppen. Gruppen fassen Benutzer zu Einheiten zusammen. Den Gruppen kann man dann Berechtigungen vergeben, anstatt jeden Benutzer einzeln zu berechtigen. Die Vorteile liegen auf der Hand:

- Die Dokumentation von Berechtigungen ist deutlich einfacher
- Das Entfernen von Berechtigungen beschränkt sich darauf, den Benutzer aus einer Gruppe zu entfernen

- Das Erweitern von Berechtigungen beschränkt sich auf das Hinzufügen von Benutzern zu Gruppen, anstatt jedes Objekt einzeln anzufassen, auf das Berechtigungen vergeben werden sollen.

Das beste Beispiel für die Nützlichkeit von Gruppen liefert Microsoft selber. In dem Moment, in dem ein Computer in eine Domäne aufgenommen wird, wird nämlich die Gruppe der *Domänen-Benutzer* (Domain Users) Mitglied der Gruppe *Benutzer* auf dem PC, sowie die Gruppe der *Domänen-Administratoren* (Domain Admins) Mitglied in den *lokalen Administratoren*. Dadurch wird jeder Benutzer, der in der Domäne angelegt wird, automatisch berechtigt, den PC zu benutzen, da ein neuer Benutzer in der Domäne automatisch Mitglied der *Domänen-Benutzer* wird. Genauso hat jedes Mitglied der *Domain Admins* automatisch Administrative Rechte auf allen Workstations und Servern der Domäne.

Windows unterscheidet grundsätzlich 4 Typen von Gruppen:

Typ	Beschreibung	Speicherort
Lokale Gruppen	Werden in der lokalen Benutzerdatenbank (SAM = Security Accounts Manager) gespeichert. Eine lokale Gruppe existiert jeweils nur auf dem PC selbst und kann auf anderen PC´s nicht zur Berechtigungsvergabe verwendet werden. Viele lokale Gruppen werden bereits bei der Windows Installation vom System mit Standard-Berechtigungen angelegt wie z.B. Benutzer, Administratoren, Hauptbenutzer, Server-Administratoren…	PC
Lokale Domäne	Wie lokale Gruppen, aber nicht nur auf einem PC, sondern innerhalb der gesamten Domäne sichtbar, allerdings nicht in vertrauten Domänen. Den lokalen Gruppen sollen direkt Berechtigungen und Rechte vergeben werden.	AD
Globale	Standardgruppe, um Benutzerkonten hinzuzufügen. Im Unterschied zu lokalen Domänengruppen können Sie nur Benutzer und globale Gruppen aus der eigenen Domäne als Mitglieder haben, sind aber in allen vertrauten Domänen sichtbar und können also auch in Fremddomänen für die Berechtigungsvergabe verwendet werden	AD
Universale	Wie globale Gruppen, können aber Mitglieder aus allen Domänen (!) aufnehmen. Globale Gruppen werden auf einem speziellen Domänencontroller, dem globalen Katalog, gespeichert.	AD

Dass von Microsoft empfohlene Konzept zur Berechtigungsvergabe lautet, Benutzer-Konten in globale Gruppen, und diese dann lokalen bzw. Domänen-lokalen Gruppen hinzufügen. Berechtigungen werden nur an die beiden Typen von lokalen Gruppen direkt vergeben. Dieses Konzept wird auch mit A-G-P bzw. A-G-DL-P abgekürzt. Hierbei steht A für Account (Benutzer-oder Computerkonto), G für global Group, DL für Domain Local Group, L für Local Group und P für Permission.

Windows Gruppenrichtlinien zur Server- und Clientverwaltung

Zweck von Gruppenrichtlinien

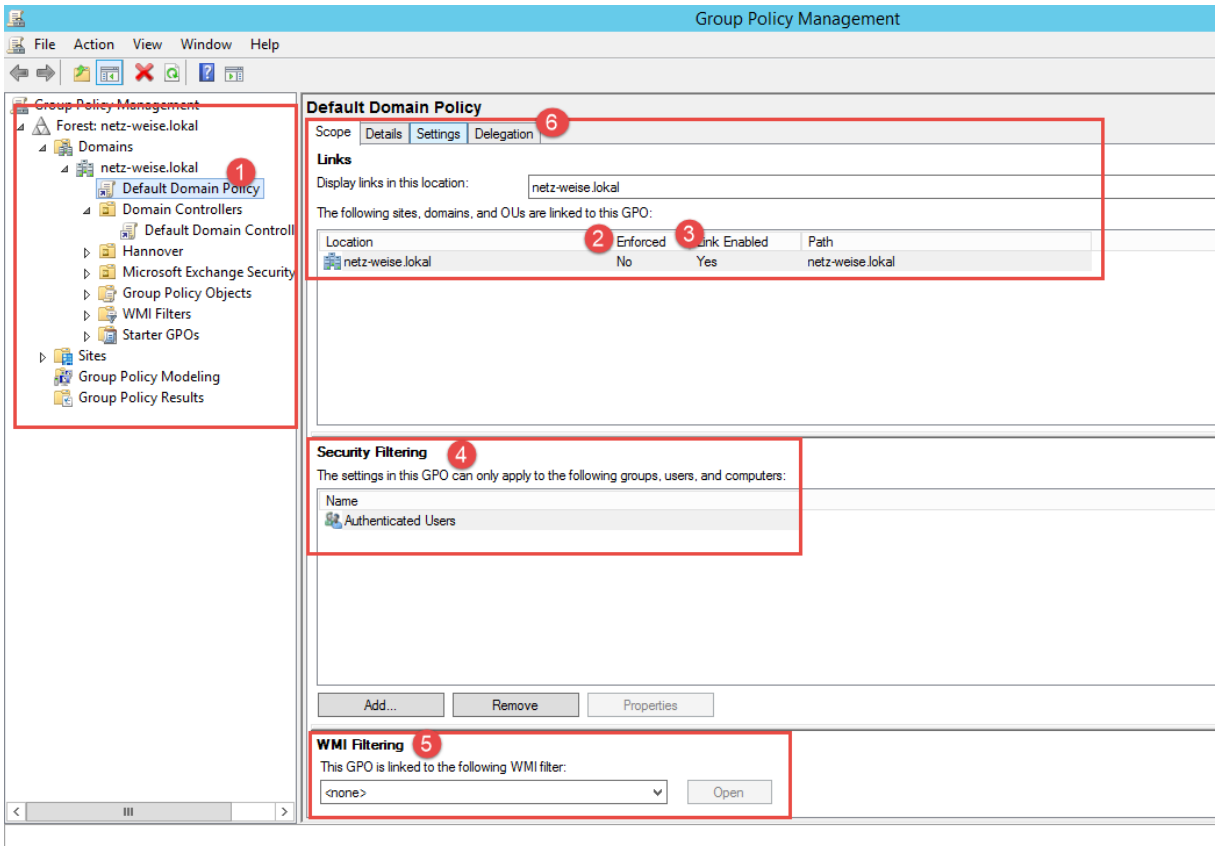
Die Windows Gruppenrichtlinien oder Group-Policies sind dazu da, Clients und Server zentral von einer Konsole aus zu konfigurieren. Mit Gruppenrichtlinien kann man eine sehr rudimentäre Form der Softwareverteilung durchführen, Sicherheitseinstellungen auf Computern zentral vorgeben und erzwingen, Dienste konfigurieren, Dateien und Registry-Einstellungen setzen, An- und Abmeldescripte konfigurieren, die Oberfläche des Benutzers umkonfigurieren und Funktionen an- oder abschalten sowie konfigurieren, Zertifikate verteilen und noch vieles mehr.

Voraussetzung für den Einsatz von Gruppenrichtlinien ist Active Directory. Die zu konfigurierenden Clients oder Benutzer müssen Mitglied einer Domäne sein, da die Gruppenrichtlinien direkt in das AD integriert sind. Ihren Ursprung haben Gruppenrichtlinien in den NT4 Policies, die aber sehr viel rudimentärer waren als die heutigen Gruppenrichtlinien.

Konfigurieren von Gruppenrichtlinien mit der Group Policy Management Console

Um die Einstellungen der Gruppenrichtlinien zu konfigurieren, nutzt man die Group Policy Management-Konsole oder kurz GPMC. Die GPMC ist ein Server-Feature und muss auf Nicht-Domänencontrollern nachinstalliert werden. Auf Windows Clients bekommt man die Konsole, indem man die RSAT-Tools (Remote Server Administration Tools) installiert. Da es für jede Windows-Version eine eigene Version der RSAT-Tools gibt (die nur die Funktionen des jeweils komplementären Windows-Servers Systems unterstützt), suchen Sie sich Ihren Download am besten selber, indem Sie im Internet einfach nach RSAT und Windows suchen. Die RSAT-Tools für Windows 7, SP 1 finden Sie hier:

http://www.microsoft.com/en-us/download/details.aspx?id=7887



Die Group Policy Management Konsole

Die GPMC erleichtert die Administration deutlich – bei Windows Server 2000 mußte man die Richtlinien noch per AD Benutzer und Computer konfigurieren.

Die Konsole zeigt im linken Fenster im Tree-View den Forest, die Domänen, die Standorte (Sites) sowie einige zusätzliche Ordner, auf die wir noch eingehen werden. Die erste wichtige Information, die wir aus diesem Tree-View ziehen ist, dass Gruppenrichtlinien ausschließlich auf Domänen-Objekten und Organizational Units angelegt werden können. Nicht einmal Container (wie der Container Users und Computer im AD) können als Grundlage für Gruppenrichtlinien verwendet werden. Es müssen OUs sein!

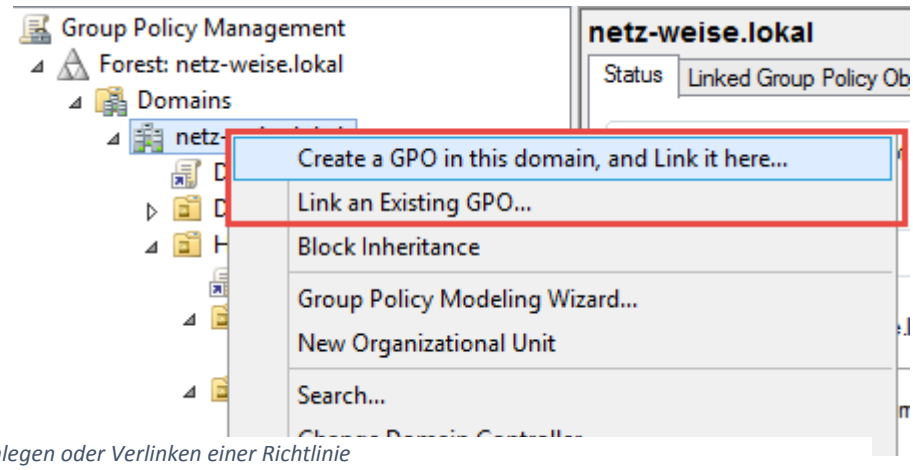
Auf einer OU können mehrere Richtlinien konfiguriert sein. In unserer Abbildung sind es aber nur 2 in der gesamten Domäne – die Default Domain Policy (1) und die Default Comain Controllers Policy. Beide Richtlinien sollten sie niemals bearbeiten!

Im Detail-Fenster rechts daneben sieht man die Orte, an denen die Gruppenrichtlinie zum Einsatz kommt oder verknüpft ist. Eine Richtlinie wird erst erstellt und dann nur mit den OUs verknüpft, auf denen sie verwendet werden soll. Dadurch kann eine Gruppenrichtlinie beliebig oft wiederverwendet werden. Das Löschen einer Verknüpfung hat keinen Einfluss die übrigen Verknüpfungen. Erst das Löschen der Richtlinie selber (in der Tree-View links im Ordner „Group Policy Objects“) führt dazu, dass alle Verknüpfungen ins Leere laufen. Eine Richtlinie kann außerdem bestimmte zusätzliche Konfigurationen wie „Enforced“ (2) oder im deutschen „Erzwungen“ empfangen. Auf dieses und andere Features gehe ich später noch ein. Ob der Link aktiviert ist und die Richtlinie damit angewendet wird oder nicht, zeigt der Eintrag „Link Enabled“ (3).

Gruppenrichtlinien werden grundsätzlich auf Organizational Units, Standorte oder Domänen angewendet. Alle Benutzer (oder Computer), die sich in einer OU befinden, auf der eine Richtlinie konfiguriert ist, werden von dieser betroffen. Allerdings kann man verhindern, dass ein Benutzer (oder Computer) eine Richtlinie überhaupt lesen darf. Ohne Leserechte kann eine Richtlinie natürlich auch nicht angewendet werden. Microsoft spricht dann von Security-Filtern (4). Security-Filter sind also nur eine einfache Form, Benutzern den Zugriff auf Richtlinien zu gestatten oder zu verbieten. Die Ausführliche Konfiguration findet man im Reiter „Delegation“. (6)

Erstellen und bearbeiten von Richtlinien

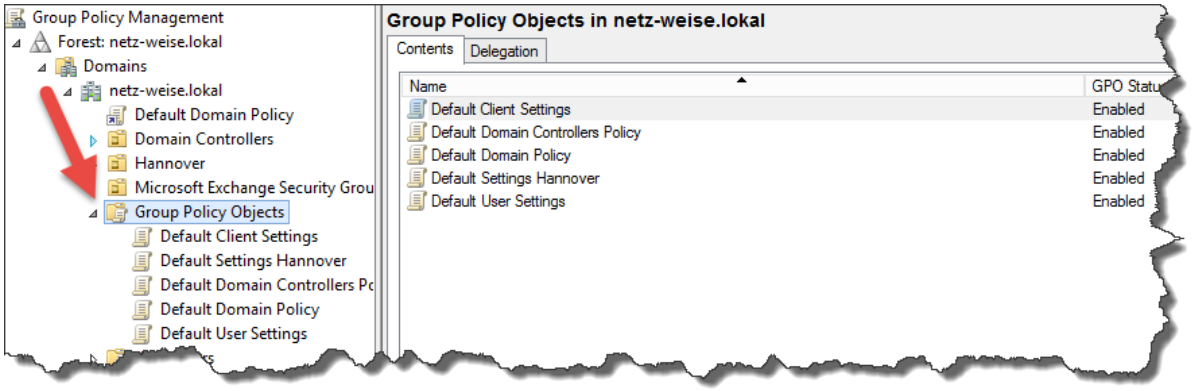
Wenn Sie eine neue Gruppenrichtlinie erstellen wollen, klicken Sie mit der rechten Maustaste den Ort an, an dem die Richtlinie angelegt werden soll, und wählen „Create a GPO in this domain, and link it here“. Dadurch erstellen Sie ein neues Gruppenrichtlinienobjekt, und verlinken sie mit der Organizational Unit oder Domäne, auf der Sie sich befinden. Tatsächlich werden durch diesen Eintrag also zwei Aktionen ausgeführt.



Anlegen oder Verlinken einer Richtlinie

Wenn Sie in den Ordner „Group Policy Objects“ unterhalb Ihrer Organizational Units wechseln, können Sie sehen, dass Sie jedes Mal beim Erstellen und Verknüpfen einer neuen Richtlinie in diesem Ordner eine neue Richtlinie erstellen. Für diese wird

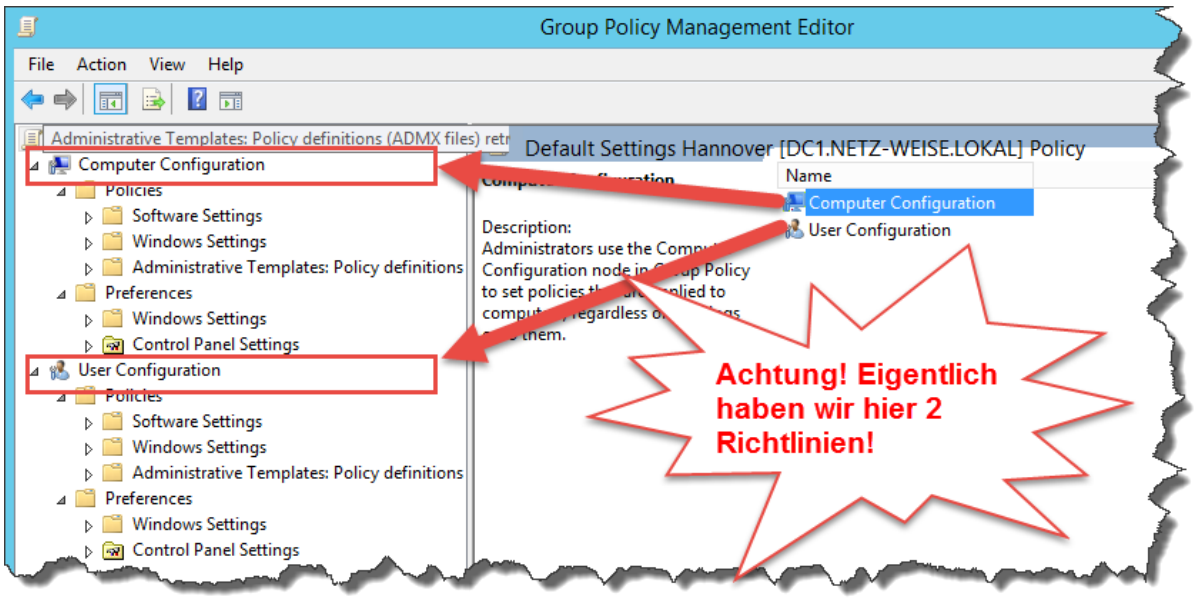
dann eine Verknüpfung mit der Domäne oder OU erstellt. Dieses Vorgehen hat verschiedene Vorteile, denn so können Sie eine Richtlinie problemlos von einer OU „entlinken“, ohne dabei die Richtlinie selber löschen zu müssen. Außerdem können Sie die Gruppenrichtlinie so auch an verschiedenen Orten verwenden, indem Sie sie einfach mehrfach verlinken. Dafür haben Sie im Kontextmenü auf einer OU oder der Domäne die Möglichkeit, statt „Create a gpo and link it here“ die Option „link an exisiting gpo“ auszuwählen. Daraufhin geht ein Fenster mit den vorhandenen Richtlinien auf, und Sie können die Richtlinie auswählen, die Sie verlinken möchten.



Der Ordner Group Policy Objects enhält alle Richtlinienobjekte

Wenn Sie eine neue Richtlinie angelegt haben, können Sie diese im Gruppenrichtlinieneditor bearbeiten, indem Sie aus dem Kontextmenü der Richtlinie die Option „Edit“ oder „Bearbeiten“ auswählen. Hier werden Sie 2 Einträge finden: *Computerconfiguration* und *User Configuration* bzw. Computerkonfiguration und Benutzerkonfiguration.

Wie Sie sich wohl schon denken können, kann man mit der Computerkonfiguration Computer konfigurieren, mit der Benutzerkonfiguration Benutzer. So trivial das klingt, so schwerwiegend ist es aber auch – denn eigentlich haben wir es hier nicht mit einer, sondern mit 2 Gruppenrichtlinien zu tun, da die Computereinstellungen und die Benutzereinstellungen nicht gleichzeitig vorgenommen werden!



Wenn ein Computer gestartet wird, dann fängt der Gruppenrichtlinienclient an, den Computer anhand der Computerrichtlinien zu konfigurieren. Hierfür schaut er nach, in welcher Organisationseinheit sich das Computerkonto befindet, listet die Gruppenrichtlinien auf, die für den Computer gültig werden, und liest danach die Einstellungen vom Domänen-Controller. Hierfür liest er nur die Einstellungen aus den Computerkonfigurationen aus – logisch, es handelt sich ja um einen Computer.

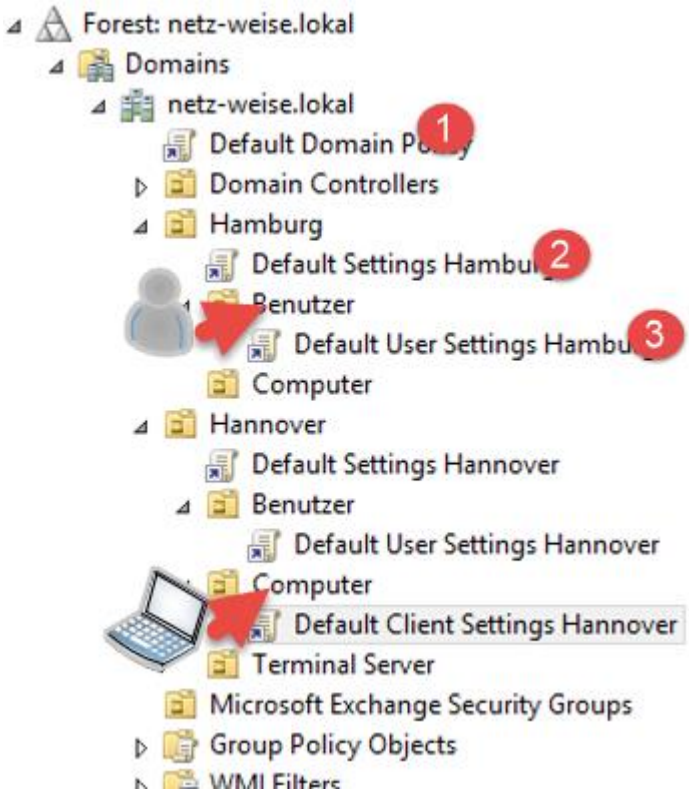
Wenn sich jetzt ein Benutzer am Computer anmeldet, dann startet der Gruppenrichtliniendienst das Gleiche Prozedere. Er schaut nach, wo im AD der Benutzer sich befindet, listet alle Gruppenrichtlinien auf, die für den Benutzer gelten, liest die Einstellungen (dieses Mal die Benutzerkonfiguration) vom Domänencontroller und wendet die Einstellungen auf den Benutzer an. Wenn sich der Benutzer und der PC nicht in der gleichen OU befinden, bedeutet dies aber, dass für den Benutzer und den Computer völlig unterschiedliche Gruppenrichtlinien gezogen wurden! Es gibt also faktisch eigentlich in jeder Gruppenrichtlinie immer zwei Gruppenrichtlinien – eine für Computer (Computerkonfiguration) und eine für Benutzer (Benutzerkonfiguration). Diese haben miteinander nichts zu tun!

Ein kleines Beispiel zur Verdeutlichung:

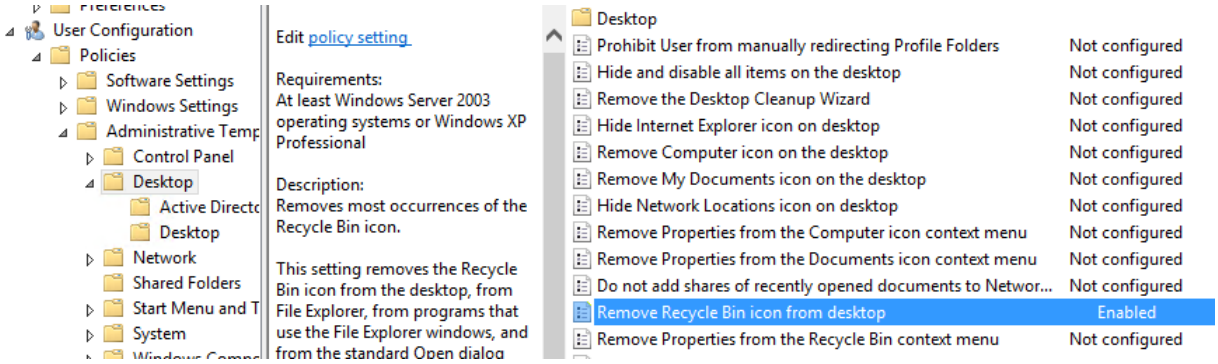
Der Benutzer Hans befindet sich in der Organisationseinheit Benutzer in Hamburg. Für einen Besuch in Hannover meldet er sich am Laptop seines Kollegen an. Der Laptop befindet sich in der OU Computer in Hannover. Wenn der Benutzer Hans sich am Laptop anmeldet, wertet der aus, in welcher OU sich der Benutzer befindet, und wendet dann (in dieser Reihenfolge) die Gruppenrichtlinien

1. Default Domain Policy
2. Default Settings Hamburg
3. Default User Settings Hamburg

an.



Wenn sich in der Richtlinie Default Settings Hannover die Einstellung aus der unten stehen Abbildung befindet, wirkt sich diese Einstellung auf den Benutzer aus?



Die Antwort lautet nein, da sie zwar in der Benutzerkonfiguration gesetzt ist, aber in der des Computers, und die wird für den Benutzer gar nicht angewendet!

Die Einstellungen

Gruppenrichtlinien bestehen aus verschiedenen Typen von Einstellungen. Die Haupttypen sind für Benutzer und Computer gleich – aber lassen Sie sich nicht täuschen, es handelt sich um jeweils unterschiedliche Einstellungen.

Software-Settings

Der erste Typ der Einstellungen sind die Software-Settings. Die Software-Settings erlauben das automatische Verteilen von Programmen, soweit diese im msi-Format vorliegen. MSI-Pakete enthalten alle notwendigen Dateien sowie in Form von Tabellen die Installationskonfiguration.

Die Möglichkeiten der Steuerung der Installation sind gering, daher ist eine Software-Verteilung mit Gruppenrichtlinien für größerer Unternehmen nicht zu empfehlen. Eine Software, die die Software-Verteilung des AD zu einem brauchbaren Werkzeug macht, ist Specops Deploy.

Security Settings

Security-Settings stellen eine Reihe von Optionen zur Verfügung, um die Sicherheit des Windows Betriebssystems zu konfigurieren. Security Settings stellen folgende Optionen zur Verfügung:

Policiy	auch User	Zweck
Account-Settings		Kennwortrichtlinien, Kontosperrrichtlinien, Kerberos-Einstellungen[1]
Lokale Richtlinien		Benutzerrechte, Sicherheitsoptionen, Audit-Policy (ab Vista durch Advanced Audit Policy Configuration ersetzt, s.u. in der Tabelle)
Event-Log		Ereignisanzeige-Einstellungen wie Größe oder Überschreiben
Restricted Groups		Gruppenmitgliedschaften erzwingen(!) – diese Mitgliedschaften werden **anstatt** der lokalen Einstellungen gesetzt
System-Services		Dienste-Startmodus und Berechtigungen auf Diensten setzen
Registry		Registry-**Berechtigungen** setzen
File System		Dateisytem-**Berechtigungen** setzen
Wired Network Policies		Netzwerk-Authentifizierung an RADIUS-fähigen Switchen (802.1x) Technet: 802.1X Authenticated Wired Access Overview
Windows Firewall with Adv. Security		Firewall-Profil-Einstellungen festlegen
Network List Manager Policies		Festlegen, welche Netzwerkprofile bei der Netzwerkerkennung festgelegt werden sollen und ob ein Benutzer den Typ ändern kann Network Location Awareness (NLA) and how it relates to Windows Firewall Profiles
Wireless Network Policies		Netzwerk-Authentifizierung an RADIUS-fähigen Accesspoints konfigurieren
Public Key Policies	+	Verteilt Zertifikate und konfiguriert Verschlüsselungsfeatures wie EFS und Bitlocker

[1] Die Konto-Einstellungen werden für Domänen-Konten nur dann gültig, wenn man Sie direkt unterhalb der Domäne definiert. Daher kann für die Domäne über Gruppenrichtlinien nur eine Kennwortrichtlinie erzwungen werden. Die Einstellungen müssen (und sollten) nicht in der Default Domain Policy geändert werden. Konto-Einstellungen, die auf einer OU definiert sind, werden auch angewandt, allerdings nur auf die lokalen Computer-Konten: http://cbfive.com/local-and-domain-user-password-policy/

Software Restriction Policies	+	Legt PC-weit fest, welche Programme von Benutzern gestartet werden dürfen. Diese Einstellungen gelten für alle User.
Application Control Policies (Applocker)		Ähnlich den Software Restriction Policies, allerdings genauer konfigurierbar (u.a. für Gruppen). Ab Windows Server 2008R2 Standard oder Windows 7 Enterprise Edition
IP Security Policies		Zentrale IP-SEC Steuerung
Adv. Audit Policy Configuration		Erweitertes Auditing, benötigt mind. Windows Vista/Server 2008 und darf nicht mit dem Standard-Auditing kombiniert werden

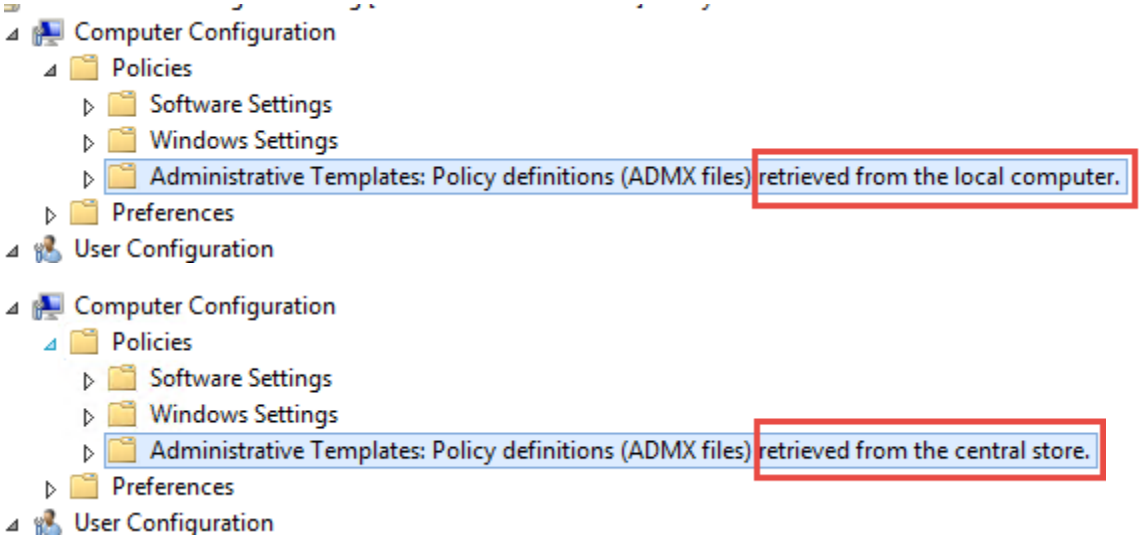
Administrative Templates

Administrative Templates oder Administrative Vorlagen sind Registry-Einstellungen, die von den Gruppenrichtlinien gesetzt werden und deren Beschreibung und Konfiguration aus Text-Dateien kommt. Diese Textdateien werden als Administrative Vorlagen bezeichnet und können auch erweitert werden. Bis Windows XP lagen die Vorlagen als reine Textdateien (.adm) vor, ab Vista hat Microsoft auf XML-Notation in der Datei gewechselt (.admx). Die XML-Notation hat den Vorteil, dass die Beschreibungen, die im Group-Policy Editor angezeigt werden, mehrsprachig sein können. Dafür wird außerdem eine Sprach-Definitionsdatei mitgeliefert (.adml).

Standardmäßig sind die admx-Dateien im Windows-Ordner jedes Rechners unter „PolicyDefinitions“ abgelegt, und die Group Policy Management-Konsole lädt die Dateien von hier. Dieses Verfahren hat allerdings den Nachteil, dass man nur jeweils die Policy-Einträge sehen kann, die der jeweilige Client unterstützt bzw. die man in den PolicyDefinition-Ordner gelegt hat. Um die admx-Dateien für alle Administratoren zentral zur Verfügung zu stellen genügt es, den PolicyDefinitions-Ordner in den Sysvol-Ordner eines Domänen-Controllers zu kopieren:

\\<Domäne>\SYSVOL\<Domäne>\Policies\

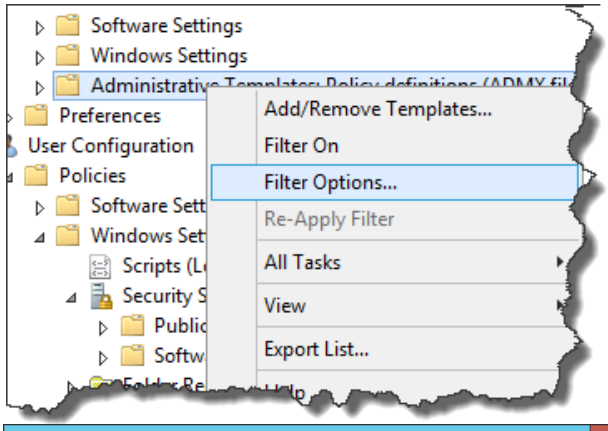
Die GPMC sucht immer zuerst an diesem Pfad, bevor es den lokalen Pfad zum Laden der Vorlagen benutzt. Welchen Pfad die Konsole verwendet hat, zeigt Sie an:

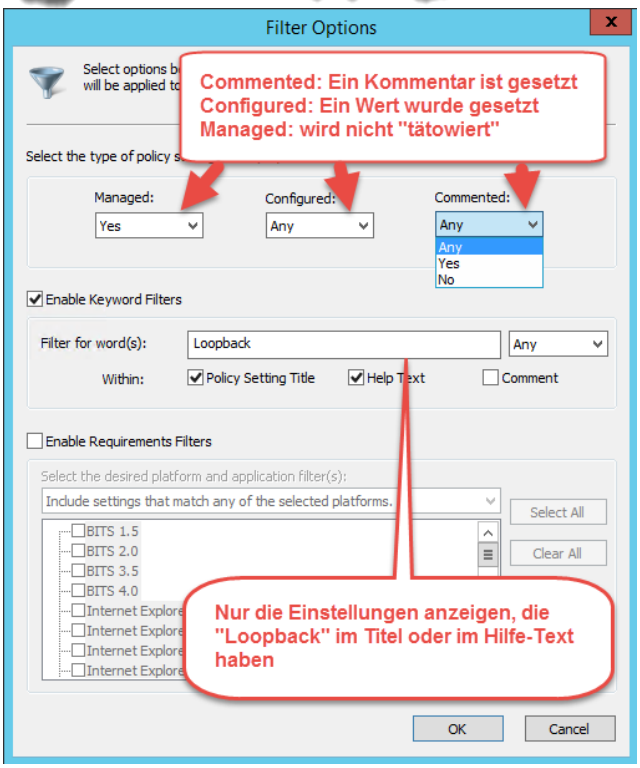


Für die Erstellung eigener ADMX-Dateien kann man den AMDX-Editor verwenden, der Bestandteil des kostenlosen ADMX-Migrators ist:

http://www.microsoft.com/en-us/download/details.aspx?id=15058

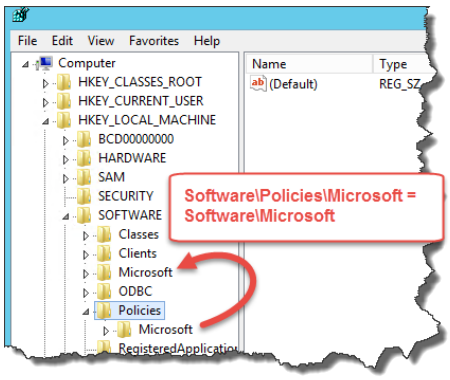
Da die Administrativen Vorlagen sehr zahlreich sind, und noch viel zahlreicher werden, wenn man weitere administrative Vorlagen z.B. für Office oder Chrome hinzufügt, bringt die GPMC die Möglichkeit mit, Filter auf die Ansicht der administrativen Vorlagen zu setzen. Wählen Sie hier im Kontextmenü von „Administrative Templates“ die Filter-Options. Im Fenster Filter Options können Sie jetzt auswählen, welche Richtlinien noch angezeigt werden sollen. Als Optionen stehen Ihnen zur Verfügung:





Managed (Yes/No/Any)

Unter Windows NT wurden alle Richtlinieneinstellungen direkt in den entsprechenden Wert in der Registry geschrieben. Das hat allerdings den Nachteil, dass die Einstellungen alle vorhanden bleiben, wenn die Richtlinie entfernt wird. Um den Ursprungszustand wiederherzustellen, muss man also manuell alle Werte wieder zurücksetzen. Man spricht hier auch von „tätowieren“ oder „tatooing“. Deshalb hat Microsoft mit Windows 2000 neue Registry-Schlüssel eingeführt, die den Namen „Policies“ tragen. Registry-Einträge, die hier gesetzt werden, werden nach entfernen der Richtlinie ebenfalls entfernt, und die Ursprungseinstellung tritt wieder in Kraft. Die Anwendung, die über die Richtlinien konfiguriert wird, muss dieses Feature allerdings unterstützen – der Schlüssel Policies wird also nicht von Microsoft in den Original-Schlüssel gespiegelt, sondern die Anwendungen, die die Policies-Schlüssel verwenden, müssen zuerst im Policies-Schlüssel nach Ihrer Konfiguration schauen, und wenn Sie dort nicht fündig werden, den „normalen“ Schlüssel durchsuchen. Windows stellt dafür an 4 Stellen einen Policy-Ordner bereit:



HKCU\Software\Policies (preferred location)
HKLM\Software\Policies (preferred location)
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies

Einstellungen, die nicht in einem dieser Schlüssel liegen, können nach Entfernen der Richtlinie nicht mit entfernt werden, da das System den Ursprungszustand der Schlüssel nicht kennt. Sie sind wie die alten NT4-Einstellungen tätowiert. Man spricht auch von ungemanagten Einstellungen gegenüber den gemanagten Einstellungen, die in den Policies-Schlüsseln gesetzt werden. Managed im Filter

bedeutet also, dass man sich alle Einstellungen anzeigen lassen kann, die nicht wieder selbständig aus der Registry entfernt werden.

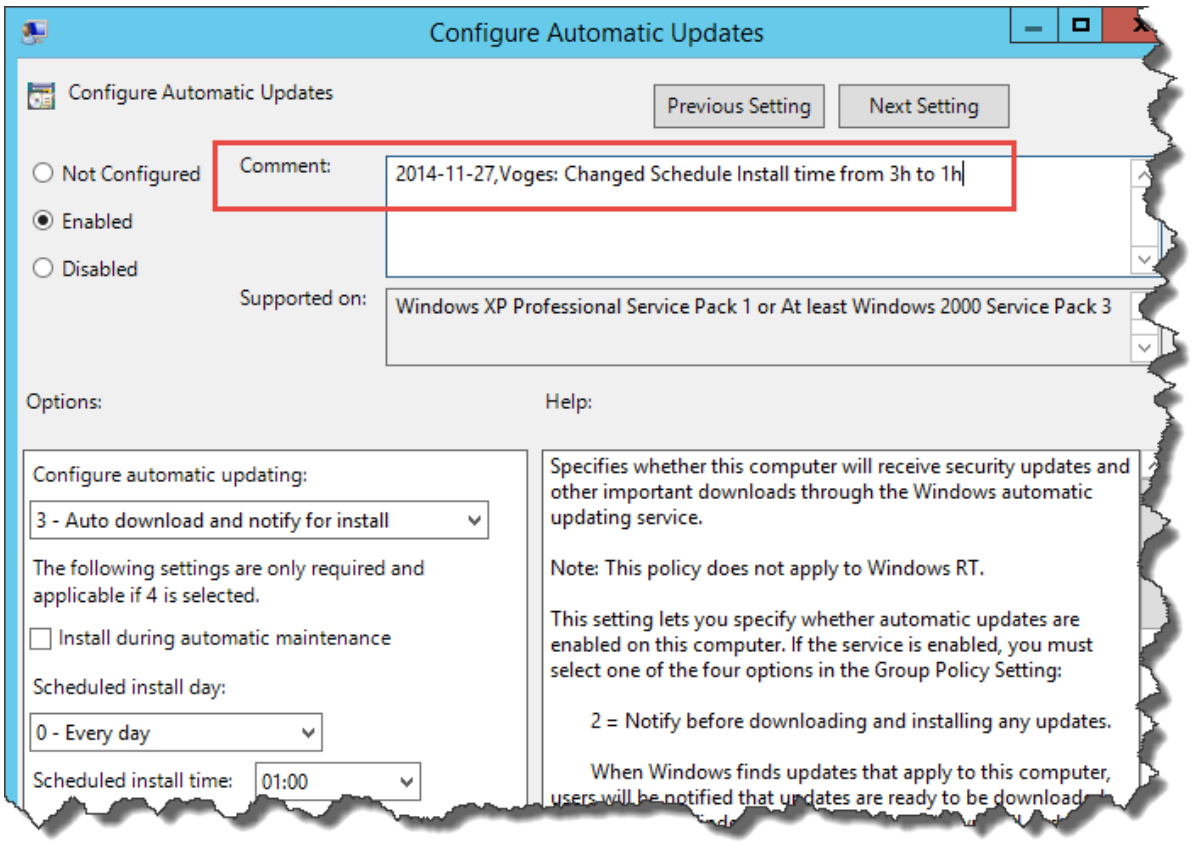
Mehr bei MSDN: [Implementing Registry-based Policy]

Configured (Yes/No/Any)

Die Einstellung Configured filtert alle Einstellungen heraus, in denen eine Einstellung vorgenommen wurde. So ist es sehr einfach, sich die Einstellungen anzeigen zu lassen, die gesetzt worden sind. Durch die Menge der Einstellungen ist es sonst schwierig, diese Richtlinien zu finden.

Commented (Yes/No/Any)

Es werden nur die Richtlinieneinstellungen angezeigt, für die ein Kommentar hinterlegt wurde. Wenn man Einstellungen vornimmt, kann man Kommentare eingeben. Dies ist z.B. ein guter Ort, um den Zeitpunkt, den Ersteller und den Grund der Einstellung zu hinterlegen.



Weitere Infos zur ADMX-Dateien für Office und Chrome:

http://www.gruppenrichtlinien.de/artikel/google-chrome-sichere-und-empfohlene-konfiguration/

Administrative Vorlagendateien für Gruppenrichtlinien (ADMX, ADML) und Dateien des Office-Anpassungstools (OCT) für Office 2013

Office 2010 Administrative Template files

Office 2013 Administrative Template files

Lokale Sicherheitsrichtlinien

Die lokalen Sicherheitsrichtlinien existieren auf jedem Windows-PC und legen eine Reihe von Sicherheitseinstellungen fest. Hier finden sich z.B. die Kennwort-Richtlinien, die Systemrechte der Benutzer, eine Reihe von Systemeinstellungen, die Firewallkonfiguration und Netzwerk-Zugriffsregeln, die IP-Sec-Konfiguration und die Möglichkeit, die Ausführung von Software zu verhindern (Software-Restriction-Policies und App-Locker).

Die Lokalen Sicherheitsrichtlinien können zentral über das Active Directory mit Hilfe der Gruppenrichtlinien überschrieben werden. Alle Einstellungen, die in den Lokalen Sicherheitsrichtlinien festgelegt sind, gibt es in den Gruppenrichtlinien ebenfalls. Wird ein Computer in die Domäne aufgenommen, werden die Kennwortrichtlinien beispielsweise sofort nur noch aus der Domäne bezogen und die lokalen Richtlinien werden überschrieben. Die meisten anderen Richtlinien sind jedoch in der Domäne standardmäßig nicht konfiguriert, so dass die lokalen Richtlinien trotzdem Gültigkeit haben.

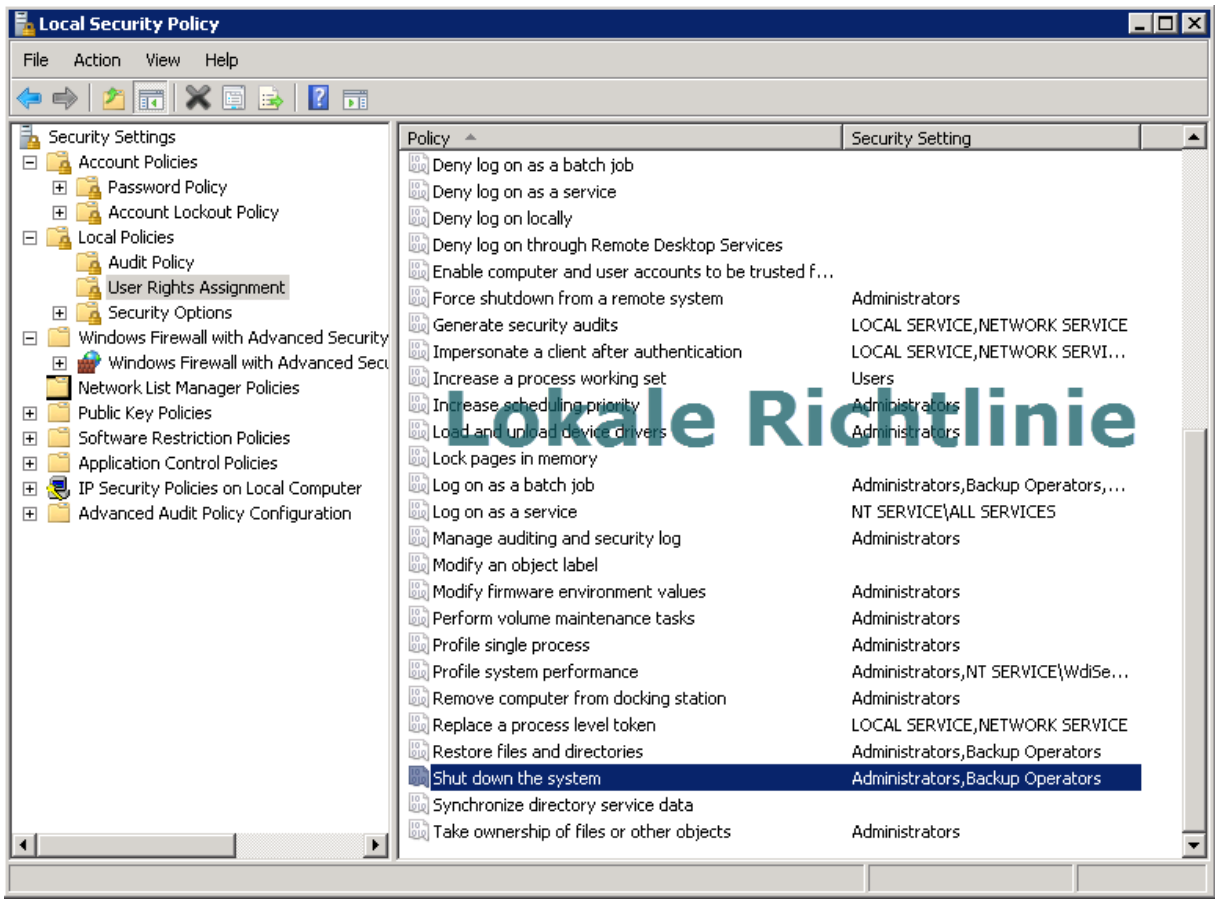
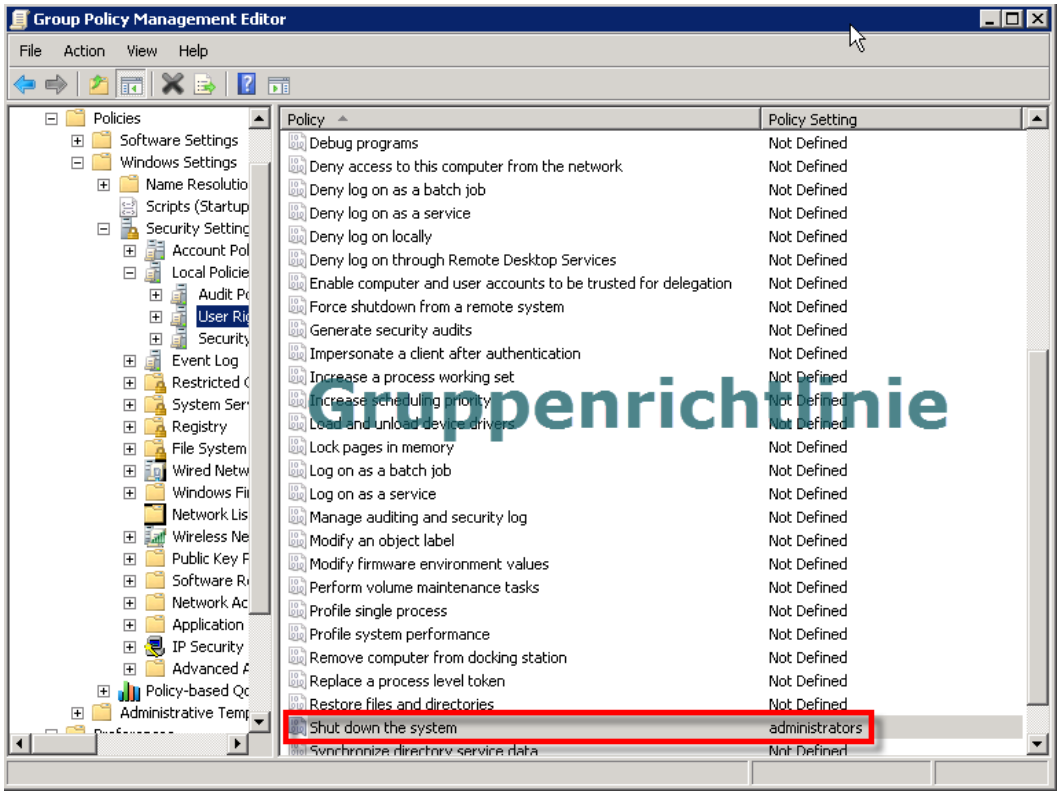


Abbildung 1- Local Security Policy Editor

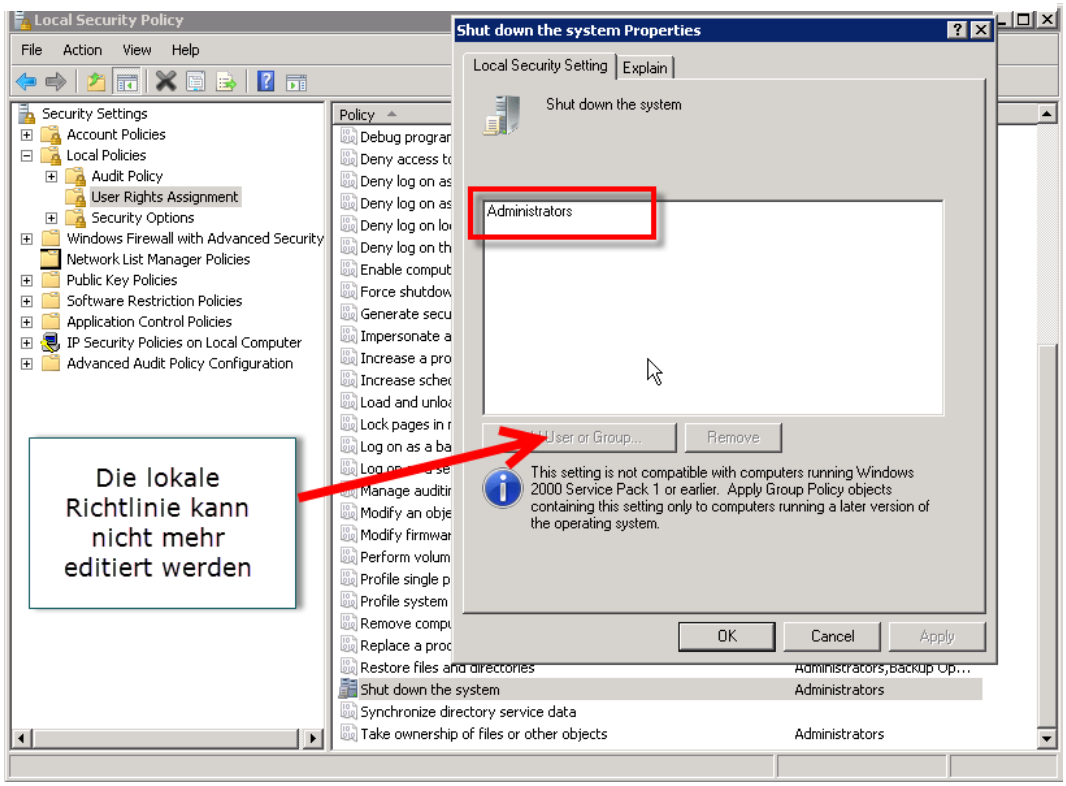
Für die Konfiguration der lokalen Sicherheitsrichtlinien gibt es die Konsole „*Local Security Policy*“ oder „*lokale Sicherheitsrichtlinien*“. In der Konsole befinden sich die Einstellungen in einzelnen Konfigurationsknoten oder – bildlicher gesprochen - Unterordnern.

Im Ordner *Local Policies -> User Rights Assignment* befinden sich alle Windows Systemrechte aufgelistet. Hier findet man z.B. die Rechte, die einem Benutzer das Anmelden per Remote Desktop (RDP) erlauben

– *allow log on through Remote Desktop Services* oder die Rechte, den Computer herunter zu fahren – *Shut down the system*.



es wird eine Gruppenrichtlinie konfiguriert, die das Herunterfahren nur Administratoren erlaubt



Die Gruppenrichtline hat die lokalen Einstellungen (s. Abb. 2) überschrieben. Eine Änderung ist lokal nicht möglich

Kennwortrichtlinien erstellen

Für die Sicherheit der Netzwerkumgebung ist wichtig, dass alle Computer mit einem Benutzernamen und einem Kennwort gesichert sind. Nur so kann sichergestellt werden, dass keine unbefugten Zugriff auf das Firmennetzwerk bekommen. Kennwortsicherheit ist ein heißes Thema, das vielfältig diskutiert wird. Ein Problem bei Benutzerkennwörter ergibt sich z.B. daraus, dass zu kurze Benutzerkennwörter mit gängigen Hacking-Tools sehr schnell geknackt werden können. Genauso sind Standard-Kennwörter über sogenannte Wörterbuchattacken einfach durch ausprobieren auflösbar. Bei einer Wörterbuchattacke probiert ein Programm einfach die gängigsten Kennwörter in verschiedenen Kombinationen und Abwandlungen aus.

Um es dem Angreifer möglichst schwer zu machen, Kennwörter zu hacken, ist es daher sinnvoll, ein möglichst schweres zu knackendes Kennwort zu nutzen. Eine Reihe von Kriterien für gute Kennwörter sind:

- Die Länge. Kennwörter mit 8 Zeichen oder weniger sind sehr einfach durch Brute Force (ausprobieren aller Buchstabenkombinationen) zu hacken.
- Die Komplexität. Je mehr Zeichenkombinationen möglich sind, umso komplexer wird das Kennwort. Nutzt man statt Kleinschreibung z.B. Groß- und Kleinschreibung, verdoppelt sich die Anzahl der Zeichen pro Kennwortstelle. Nutzt man dazu Sonderzeichen und Zahlen, vervielfacht sich die Anzahl der Kombinationen noch ein weiteres Mal. Jedes zusätzliche Zeichen verdoppelt die Anzahl der möglichen Kombinationen pro Stelle!
- Ähnlichkeit mit echten Wörtern vermeiden. Hacking-Tools wie Cain and Abel können anhand von sehr komplexen Wörterbüchern die Anzahl der auszuprobierenden Kombinationen stark einschränken.

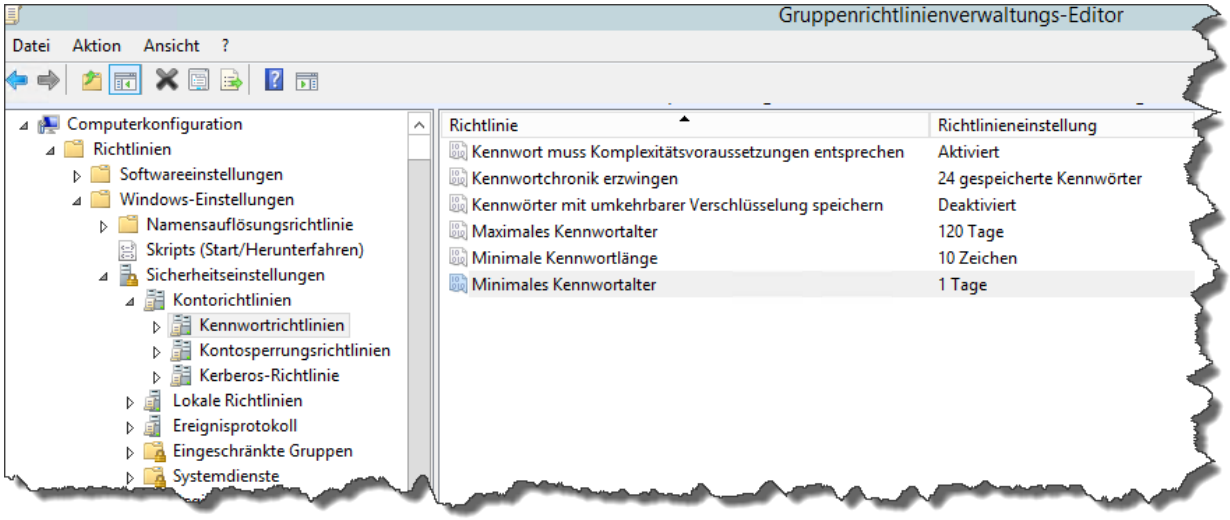
Windows bietet seit Windows 2000 die Möglichkeit, eine Kennwortrichtlinie zu definieren. Diese Kennwortrichtlinie legt fest, wie ein Kennwort auszusehen hat, damit Windows es akzeptiert. Außerdem wird über die Kennwortrichtlinie auch festgelegt, wie häufig der Benutzer sein Kennwort ändern muss.

Bis Windows Server 2008 war es nur über eine domänenweit konfigurierbare Richtlinie möglich, die Kennwortvorgaben zu setzen. Dadurch gab es nur eine einzige Richtlinie, die für alle Benutzer gültig war. Mit Windows Server 2008 hat Microsoft dieses Manko mit den granulierten Richtlinien (Fine grained Password Policies) endlich behoben. Die Einstellungsmöglichkeiten sind die gleichen wie bei den Domänenweiten Kennwortrichtlinien, können aber individuell vergeben werden.

Domänenweite Kennwortrichlinien konfigurieren per Group Policy

Um eine domänenweite Kennwortrichtlinie einzurichten, verwenden Sie Windows Gruppenrichtlinien. Öffnen Sie hierzu die Windows Gruppenrichtlinienkonsole (GPMC) und erstellen Sie auf Domänenebene eine neue Richtlinie. Stellen Sie sicher, dass die neue Richtlinie in der Bindungsreihenfolge (Priorität) der Default Domain Policy steht. Dies können Sie erreichen, indem Sie in der Gruppenrichtlinienkonsole die Domäne auswählen und dann den Reiter "verknüpfte Gruppenrichtlinienobjekte" auswählen. Über die Pfeile am Rand können Sie die Priorität ändern. Die Richtlinie mit der Verknüpfungsreihenfolge 1 wird als letzte angewendet und hat somit Priorität.

Bearbeiten Sie die Richtlinie nun, indem Sie sie mit Rechts anklicken und Bearbeiten im Kontextmenü aufrufen. Navigieren Sie im Editor unter Computerkonfiguration zu Richtlinien ->Windows Einstellung -> Sicherheiteinstellungen -> Kontorichtlinien -> Kennwortrichtlinien. Hier können Sie definieren, welche Kennworteinstellungen gültig sein sollen:



Kennwort muß Komplexitätsvoraussetzungen ensprechen

Das Kennwort muß aus den 4 Gruppen Großschreibung, Kleinschreibung, Sonderzeichen und Zahlen mindesten 3 enhalten. Passwort wäre also kein valides Kennwort (nur Groß- und Kleinschreibung), P@sswort aber schon. Außerdem darf der Benutzername nicht Bestandteil des Kennworts sein

Kennwortchronik erzwingen

Die letzten verwendeten Kennwörter werden gespeichert und können so lange nicht verwendet werden. Die Anzahl der letzten Kennwörter, die Windows sich merkt, ist die Kennwortchronik. Daher kann ein altes Kennwort nach <Kennwortchronik> Änderungen wieder verwendet werden. Das Maximum, das eingestellt werden kann, ist 24.

Kennwörter mit umkehrbarer Verschlüsselung speichern

Standardmäßig speichert der Domänen-Controller nur einen Kennwort-Hash. Ein Hash ist ein Fingerabdruck des Kennwortes – eine *Zeichencode*, der eindeutig dem Kennwort zuzuordnen ist, aber aus dem sich das Kennwort nicht ermitteln lässt. Sollte das AD jemals geknackt werden, kann ein Hacker also nur an den Kennwort-Hash kommen, nicht aber an das Kennwort selber. Das ist wohlgemerkt immer noch eine Katastrophe, weil er innerhalb des Netzwerkes mit dem Hash arbeiten kann, als hätte er das Kennwort selber erlangt. Aber wenn das Kennwort auch außerhalb des Netzwerkes verwendet wird, kann der Benutzer sicher sein, dass der Angreifer das Original-Kennwort nicht auch noch nutzen konnte, um bei amazon das Lager leer zu kaufen.

Manche Authentifizierungsverfahren benötigen allerdings auch auf dem Server das Klartext-Kennwort. Ein Beispiel ist CHAP (Challenge Handshake Protocol). Wenn Sie CHAP einsetzen, muss das Kennwort des jeweiligen Benutzers mit umkehrbarer Verschlüsselung gespeichert sein.

Maximales Kennwortalter, Minimales Kennwortalter

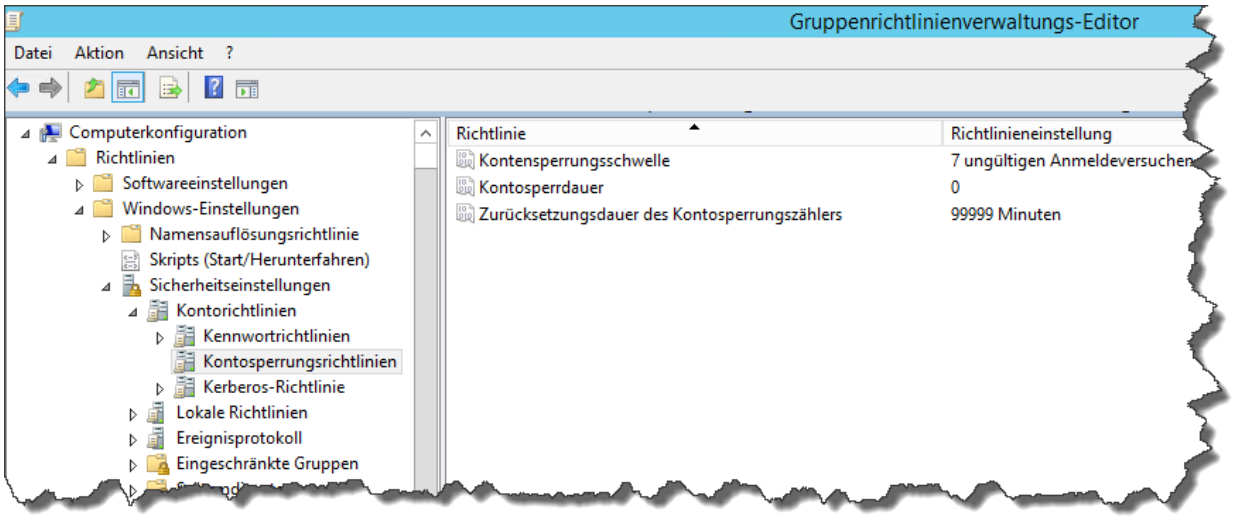
Mit dem Maximalen Kennwortalter legen Sie fest, wie lange der Nutzer sein Kennwort nutzen darf, bis er es ändern muß. Mit dem minimalen Kennwortalter legen Sie fest, dass er nicht sein Kennwort einfach 24 Mal (Kennwortchronik) sein Kennwort ändern, um sein altes Kennwort wieder verwenden zu können – Benutzer sind findig!

Die Standardeinstellung, die Windows für das Minimale Kennwortalter festlegt, halte ich allerdings für sinnlos. 1 Tag sollte hier für das minimale Alter Normalerweise reichen. Wir wollen unsere paranoiden Kollegen ja nicht davon abhalten, wirklich 100%ig sicher zu sein.

Minimale Kennwortlänge

Die Minimale Länge legt fest, aus wie vielen Zeichen das Kennwort mindestens bestehen muss. 8 sollte das absolute Minimum sein.

Nun können Sie noch die Kontosperrungsrichtlinien festlegen. Sie definieren, was passieren soll, wenn ein Benutzer sein Kennwort mehrfach falsch eingegeben hat.



Kontosperrungsschwelle

Die Schwelle legt fest, nach wie vielen Kennworteingaben das Kennwort gesperrt wird – der Benutzer kann sich dann nicht mehr anmelden, sondern bekommt eine Fehlermeldung, dass er sich an den

Administrator zur Entsperrung wenden soll. Ein Wert zwischen 7 und 10 scheint mir hier sinnvoll. Das stellt sicher, dass auch der dümmste Benutzer merkt, dass seine CAPS-Lock-Taste aktiviert ist oder dass er sein Kennwort letzte Woche geändert hat.
Wichtig! Eine Sperrung wirkt wie eine Deaktivierung des Kontos, kann aber nicht manuell erzeugt werden. Wenn also eine große Anzahl von Konten plötzlich gesperrt sind, und die Benutzer haben angeblich nichts gemacht, könnte das in diesem Fall vielleicht wirklich mal stimmen und Sie haben ein größeres Problem.

Kontosperrdauer

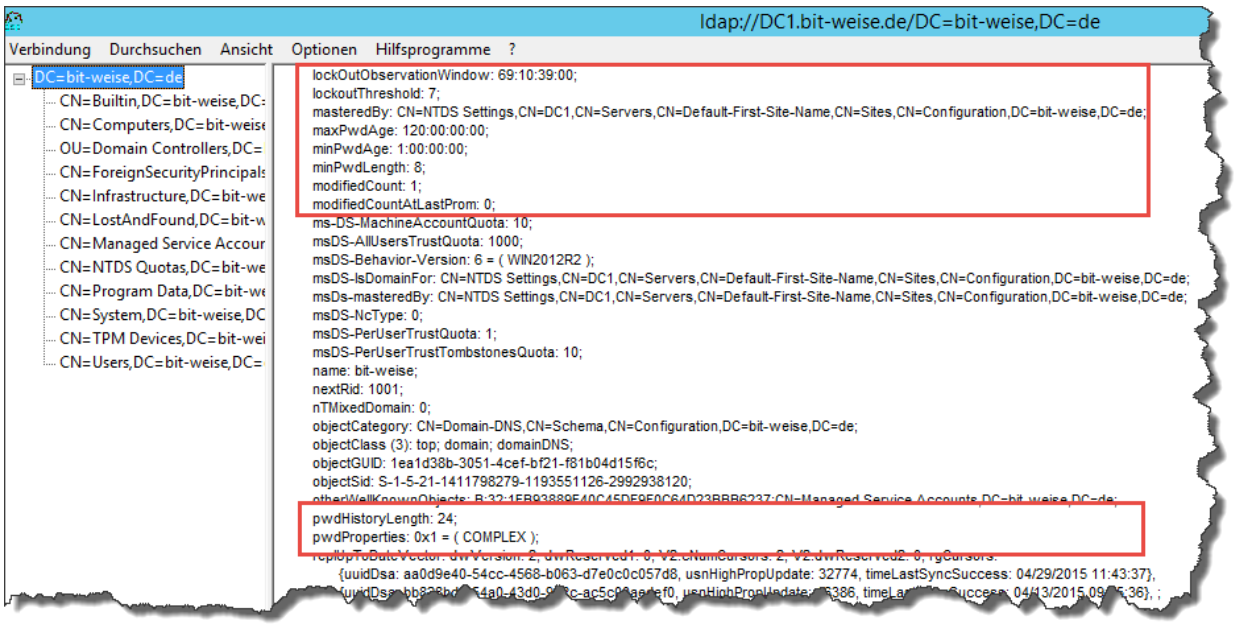
Legt fest, wie lange die Konten gesperrt bleiben, bevor das System Sie automatisch entsperrt. Standardmäßig schlägt Windows 30 Minuten vor – ich empfehle, hier eine Null einzutragen. 0 bedeutet, dass das Konto nur manuell entsperrt werden kann. Wenn ein Benutzer x mal sein Kennwort falsch eingegeben hat, ist es eher unwahrscheinlich, dass es ihm plötzlich wieder einfällt, aber es stellt sicher, dass das Hacker-Tool nicht alle 30 Minuten einen neuen Versuch starten kann.

Zurücksetzungsdauer des Kontosperrungszählers

Dieser Wert legt fest, wann der Zähler, der die Falscheingaben des Kennworts hochzählt, wieder auf Null gesetzt wird. Standardmäßig passiert das, sobald ein Benutzer sein Kennwort richtig eingegeben hat, aber auch nach Ablauf der hier eingetragenen Frist. Hier kann keine Null eingegeben werden, aber der Maximalwert ist 99999, was ca. 70 Tagen entspricht. Auch hier denke ich, dass der Benutzer wohl eher nicht 30 Minuten warten wird, bevor er sein Kennwort nochmal falsch eingibt, und für ein Hackertool ist das zurücksetzen nach 30 Minuten ein gefundenes Fressen.

Wo werden die Kennwortrichtlinien gesetzt?

Oft kann man lesen, die Kennwortrichtlinien müssten in der Default Domain Policy gesetzt werden. Das ist völliger Unfug. Die Einstellungen müssen nur auf einer Richtlinie auf Domänenebene gesetzt werden. Die Einstellungen werden dann auf dem Domänen-Objekt im AD gesetzt. Das kann man sehen, wenn z.B. ADSIEdit oder LDP bemüht:

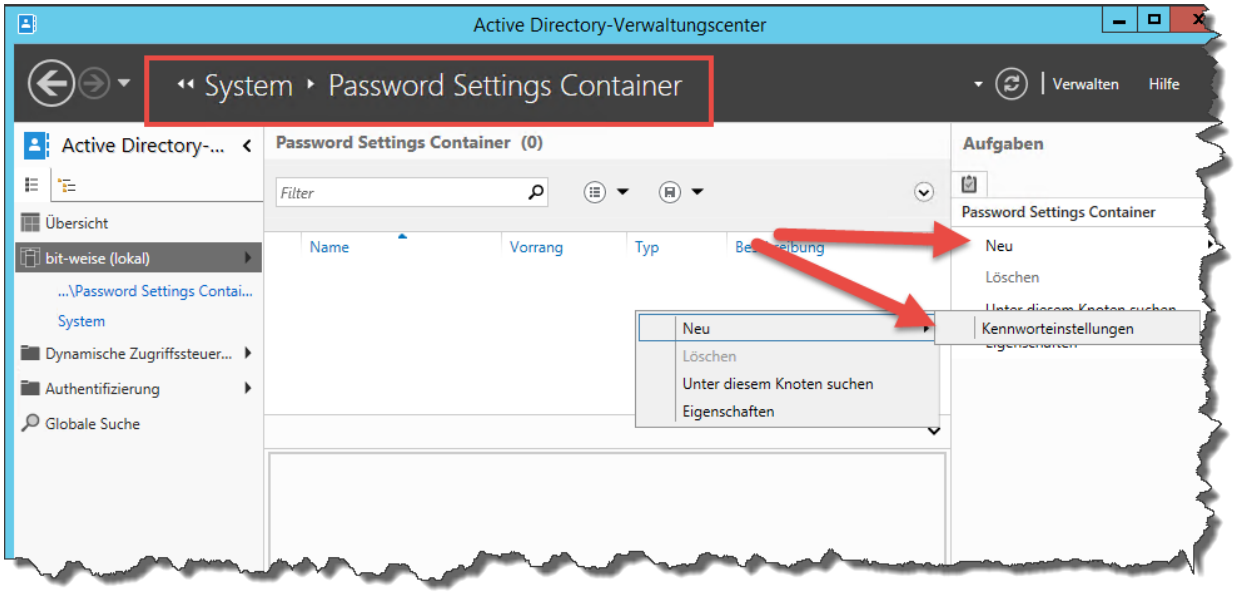


Sie können Kennwortrichtlinien auch auf OU-Ebene definieren. Diese Einstellungen scheinen wirkungslos zu sein, aber das sind sie gar nicht. Die Einstellungen hier wirken sich aber nicht auf die Domäne aus, sondern auf die lokalen Sicherheitsrichtlinien. Diese Einstellungen gelten für alle lokalen Benutzerkonten, während Domänenbenutzer die Einstellungen der Domäne verwenden.

Fine Grained Password Policies (Granulare Kennwortrichtlinien)

Granulare Kennwortrichtlinien hat Microsoft mit Windows Server 2008 eingeführt. Sie ermöglichen es jetzt endlich, innerhalb einer Domänen unterschiedliche Vorgaben für Benutzerkennwörter zu erzwingen, da die Einstellungen auf der Domäne letztendlich nur eine Einstellung zuließen. Sie arbeiten aber von der Konfiguration nach einem ganz anderen Prinzip als die Domänenrichtlinien – auf Benutzer- bzw. Gruppenebene.

Eine granulare Kennwortrichtline besteht aus einem Kennwortrichtlinienobjekt, dass die Einstellungen festlegt. Die Einstellungen entsprechen denen der Domänen-Kennwortrichtlinien. Die Zuordnung zu Benutzern findet jetzt allerdings statt, indem der Benutzer oder die Gruppe direkt der Richtlinie zugewiesen wird. Während das bis Windows Server 2008 R2 nur mit Hilfe von Powershell ging, steht mit dem Active Directory Verwaltungscenter unter Windows Server 2012 nun auch eine grafische Oberfläche zur Verfügung. Starten Sie hierzu das Verwaltungscenter, wählen Sie Ihre Domäne und navigieren Sie in den Container System -> Password Settings Container.



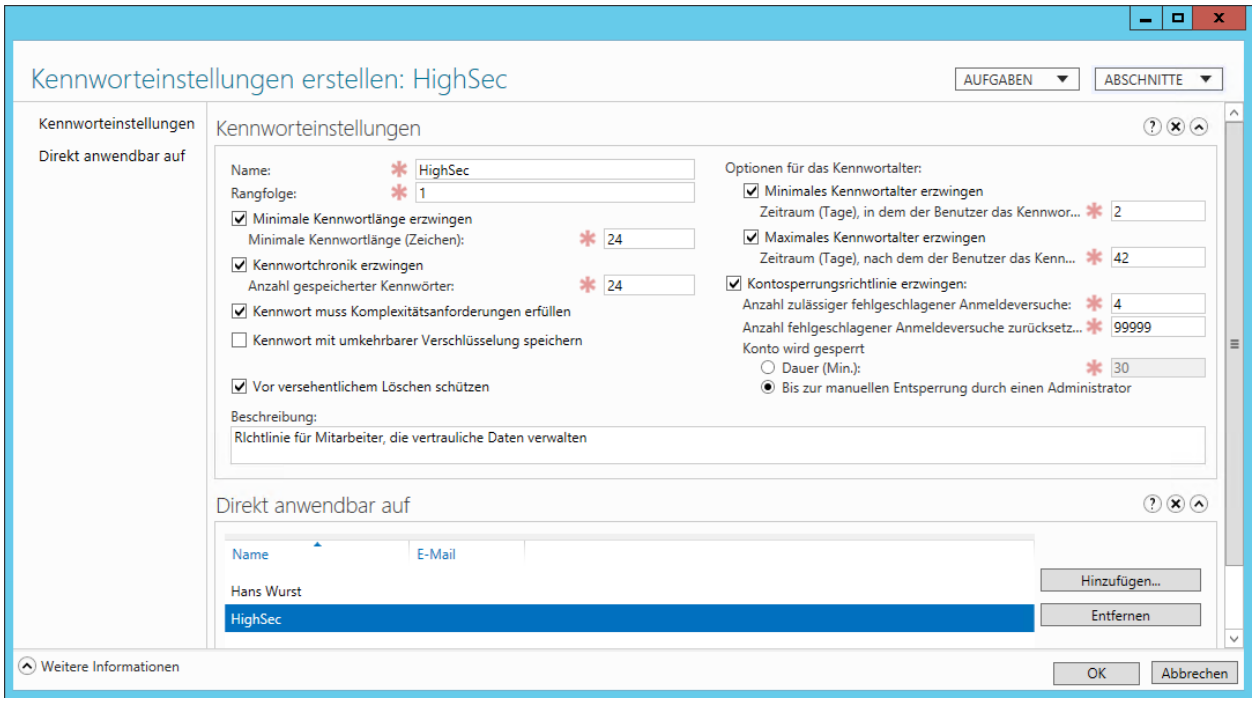
Klicken Sie entweder im Aufgaben-Menü Rechts oder mit Rechtklick im Mittelfenster auf Neu -> Kennwortrichtlinieneinstellungen, um ein neues Richtlinieneinstellungen-Objekt zu erzeugen. Die Einstellungen, die Sie hier vornehmen können, sollten Ihnen bekannt vorkommen. Neu sind hier 3 Einträge:

Name
Da Sie eine beliebige Anzahl von Kennworteinstellungs-Objekten anlegen können, können Sie so die einzelnen Einstellungen voneinander unterscheiden.

Direkt anwendbar auf
Da man irgendwie festlegen muss, für wen eine Richtlinie gelten soll, muss man jetzt über diesen Eintrag die Benutzer oder Gruppen hinzufügen, für die diese Richtlinie gelten soll. Hierbei gilt, dass ein granulares Richtlinienobjekt die Einstellungen aus der Domänenrichtlinie überschreibt. Wenn ein

Benutzer direkt in einer Richtlinie eingetragen wurde (wie Hans Wurst in der Abbildung), dann überschreibt die Einstellung alle weiteren Richtlinien, die für Hans Wurst eventuell noch über Gruppenmitgliedschaften gültig werden könnten. Ist ein Benutzer nicht direkt in einem Richtlinienobjekt eingetragen, aber ist er Mitglied in einer Gruppe, für die ein Richtlinienobjekt definiert wurde, so gilt dieses Objekt für ihn. Aber was passiert, wenn ein Benutzer in mehreren Gruppen ist, für die verschiedene Kennwortrichtlinieneinstellungen gelten?

Rangfolge (precedence)
Dann kommt die Rangfolge ins Spiel. Wenn ein Benutzer z.B. in zwei Gruppen Mitglied ist, für die unterschiedliche Kennworteinstellungen gelten, so wird die Richtlinie mit der geringsten Rangfolge angewendet. Kleine Werte haben also eine höhere Priorität.



Und was passiert, jetzt, wenn 2 Kennwortrichtlinieneinstellungen die gleiche Rangfolge haben? Windows prüft das beim Anlegen nicht. In diesem Fall wird die GUID der Richtlinie zum Vergleich herangezogen, wobei die Richtlinie mit der kleineren GUID gewinnt. Wichtig ist allerdings, dass das letzte Byte des ersten Teils der Richtlinie herangezogen wird. Ein Beispiel:

2 Richtlinien haben die GUIDs
8d1af386-f4ab-4897-a8c3-5674a243e587
und
dc60d50e-b53b-4368-92f4-31b5694214ce

In diesem Fall gewinnt die erste Richtlinie, und zwar, weil 86 größer ist als 0e.

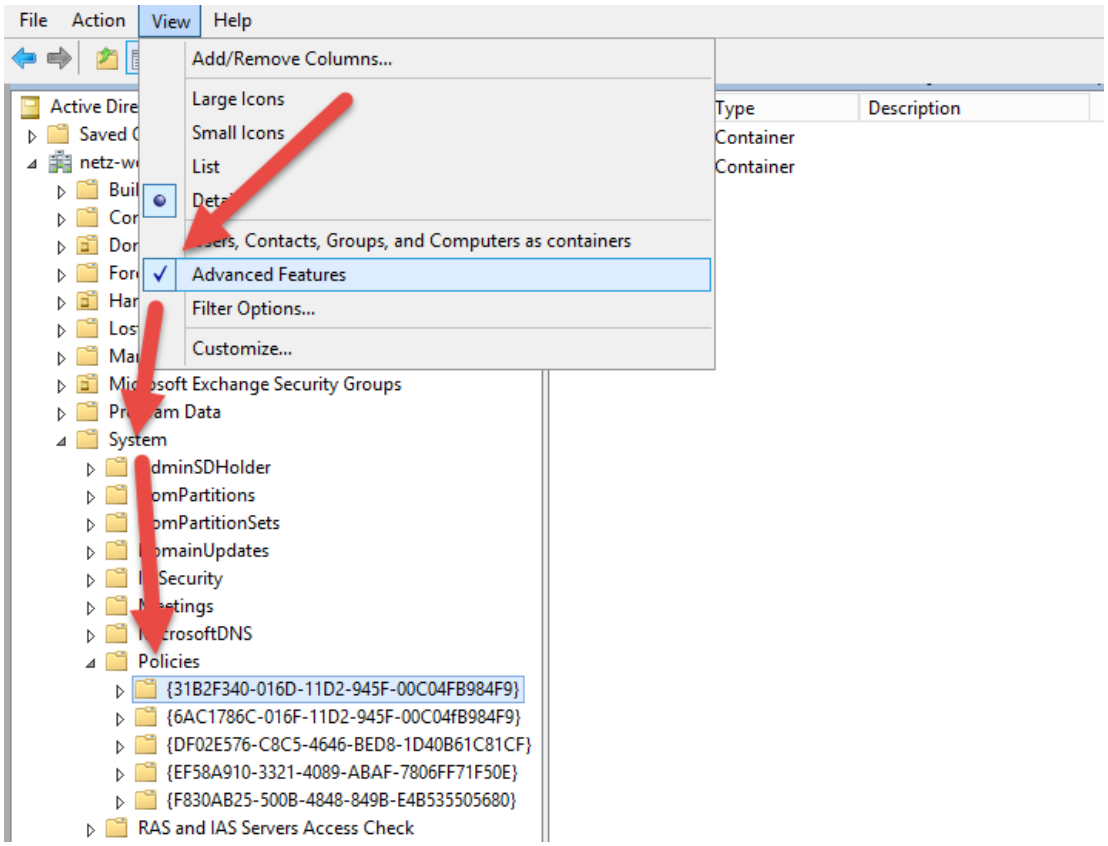
Zusammenspiel Server-Client

Die Kennwortrichtlinien werden zwar auf dem Server eingestellt, aber für die Erzwingung der Kennwortrichtlinien ist der Client zuständig. Hierfür gibt es seit Windows 2000 die Erweiterung Passfilt.dll, die die Kennwörter auf die Komplexitätsanforderungen hin überprüft. Diese Passfilt.dll kann prinzipiell durch eine eigene dll ersetzt werden. Es gibt eine Reihe von Fremdhersteller-Tools, die das

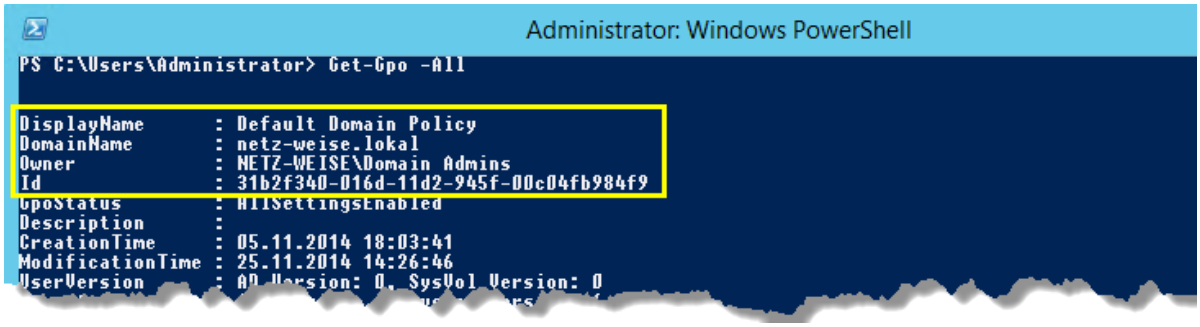
implementieren, da die Windows-eigene Passfilt.dll bestenfalls als rudimentär zu bezeichnen ist. Aktiviert man nämlich die Überprüfung der Komplexitätsrichtlinien für Kennwörter, dann wird neben den oben genannten Kriterien Großschreibung, Kleinschreibung, Sonderzeichen und Zahlen nur noch eins geprüft: Kommt der Benutzername im Kennwort vor. Wenn man das alte Kennwort z.B. einfach mit einer Zahl versieht, so kann man einfach sein Kennwort einfach hochzählen. Es findet keine Überprüfung statt, ob das alte Kennwort im neuen Kennwort vorkommt! Das führt letztlich jede Kennwortrichtlinie ad absurdum.

Funktionsweise von Gruppenrichtlinien

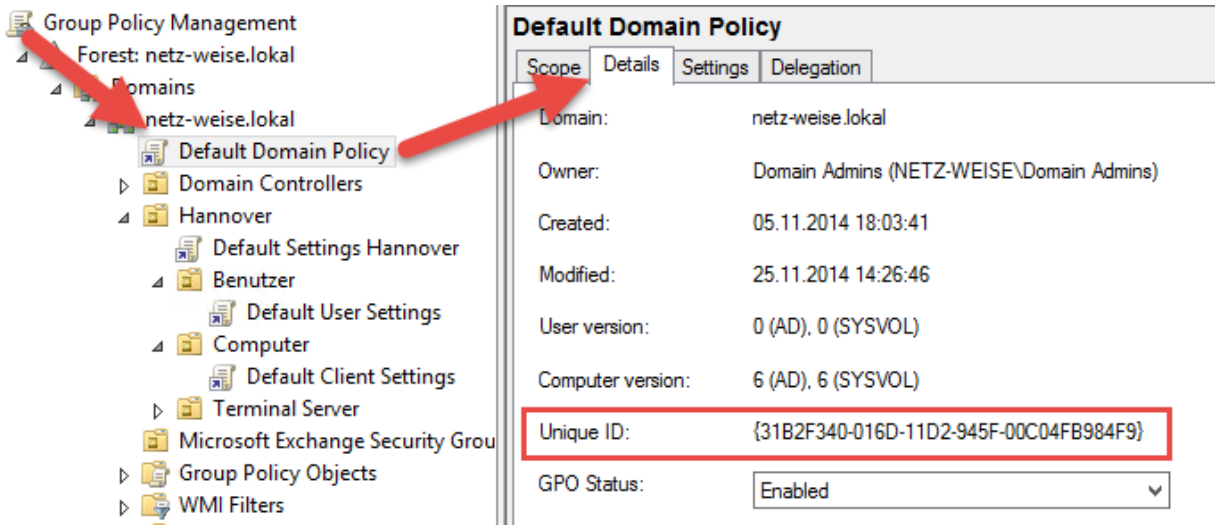
Gruppenrichtlinien basieren auf mehreren Komponenten, die zusammen spielen. Die erste Komponente ist das Active Directory. Im AD wird für jede Gruppenrichtlinie, ein Group Policy Object erstellt (gpo), das im AD im Container system\Policies abgelegt wird. Der Ordner System wird im Active Directory Benutzer und Computer nur in der erweiterten Ansicht angezeigt.



Im Container Policies werden die Policies jedoch nicht im Klartextnamen angezeigt (der sich verändern kann), sondern anhand ihrer eindeutigen, unveränderlichen ID. Um der ID den Namen zuzuordnen, kann man entweder in der Group Policy Management Konsole die Gruppenrichtlinie auswählen und den Reiter Details öffnen, oder man nutzt die Windows Powershell und das Commandlet get-gpo mit dem Parameter –all:

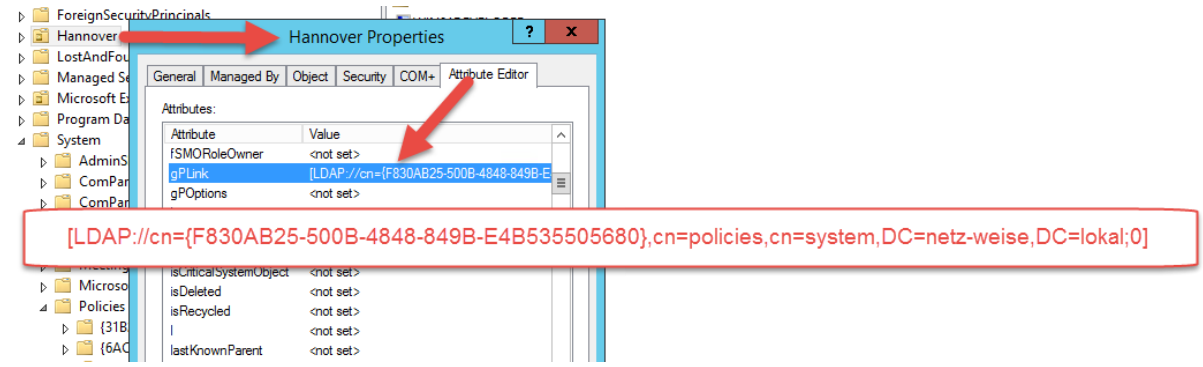


In der Powershell…

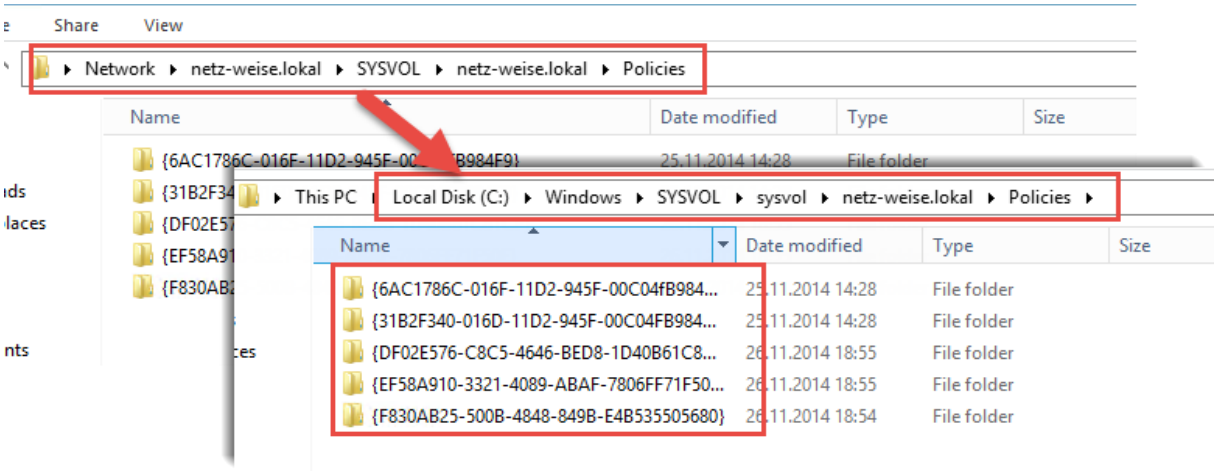


oder in der GPMC

Die Richtlinienobjekte können jetzt einer oder mehreren Organizational Units zugewiesen werden, auf die Sie angewendet werden können. AD-Intern wird hierzu auf der OU im Attribut gplink der Name der Richtlinie eingetragen:



Die eigentlichen Einstellungen befinden sich jedoch auf den Domänencontrollern im Dateisystem im Ordner Sysvol. Der Ablagepfad für den Sysvol-Ordner wird bei der Installation des AD fegelegt (s.o.) und liegt standardmäßig im Windows-Ordner. Der Ordner ist über den Namen Sysvol freigegeben und kann von allen Clients aus über den Freigabenamen *Name der Domäne**Sysvol* erreicht werden. Damit alle Domänencontroller immer die gleichen Gruppenrichtlinien-Einstellungen zur Verfügung stellen, wird der Ordner außerdem über alle Domänencontroller durch DFS-Replikation synchronisiert.



Für jede gpo gibt es einen Ordner im Dateisystem, der über die Freigabe \\domäne\sysvol erreichbar ist

Für die Anwendung bzw. Erzwingung dieser Einstellungen ist aber nicht der Server zuständig, sondern der Gruppenrichtlinien-Dienst auf dem Windows-Client. Dieser Dienst fragt in regelmäßigen Abständen die Gruppenrichtlinien aus dem AD ab, und wendet diese dann der Reihe nach an. Dabei verwendet er folgende Reihenfolge:

+ Priorität -

- Lokale Sicherheitsrichtlinie
- Richtlinien auf Standorten
- Richtlinie auf der Domäne
- Richtlinien auf Organisationseinheiten (beginnend von der Domäne Stufenweise bis zum Objekt)

Da die Richtlinien sich gegenseitig überschreiben, gelten für den Client bzw. Benutzer bei sich widersprechenden Einstellungen immer die, die zuletzt angewandt wurden, also die, die sich näher am Objekt befinden.

Der Gruppenrichtlinien-Dienst arbeitet mit Unterkomponenten, die er aufruft, die sogenannten Client Side Extensions (cse). Jede Extension ist eine DLL, die für die Konfiguration einzelner Komponenten der Gruppenrichtlinien zuständig ist. So gibt es z.B. eine cse für Ordnerumleitungen, eine für Registry-Settings, eine für WLAN-Einstellungen, eine für eingeschränkte Computergruppen usw. Eine vollständige Auflistung aller Extensions und Ihre GUIDs finden Sie hier:

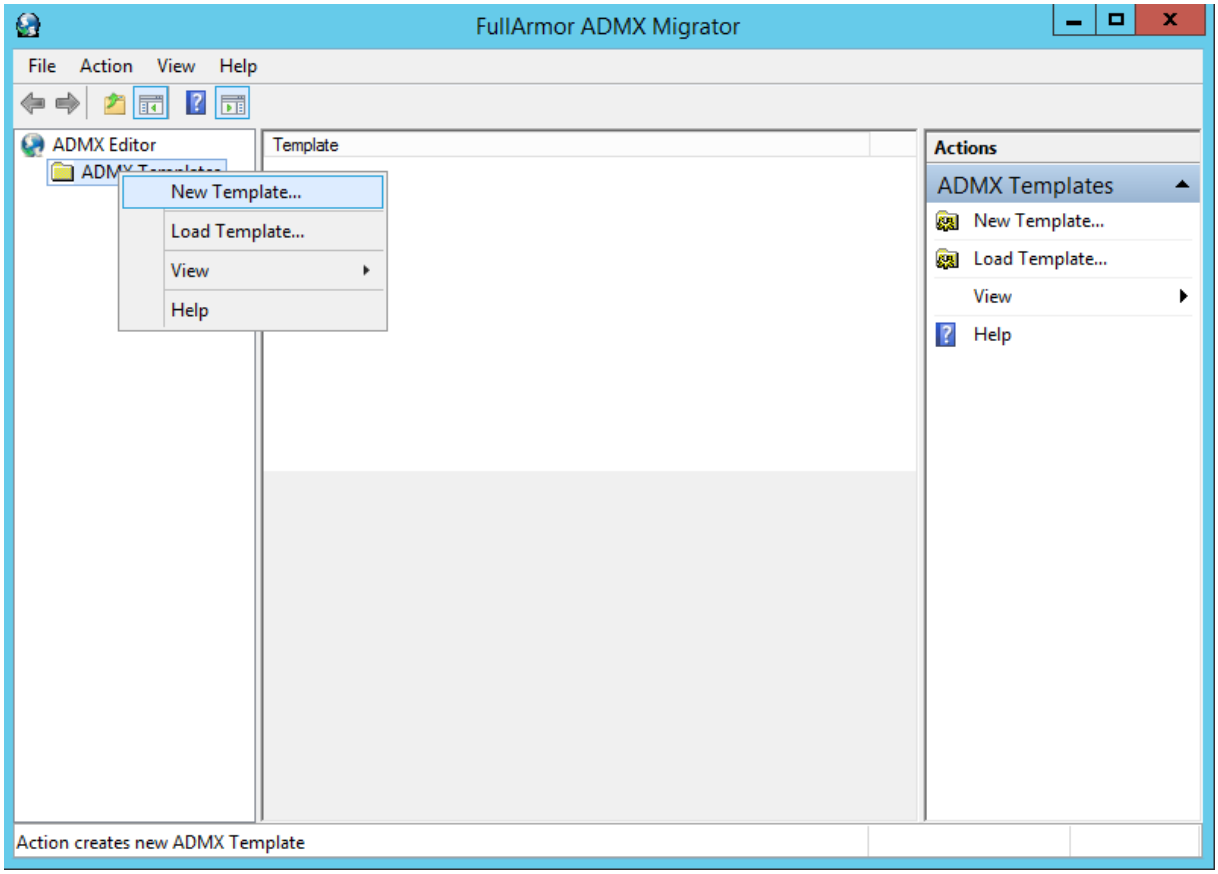
http://blogs.technet.com/b/mempson/archive/2010/12/01/group-policy-client-side-extension-list.aspx

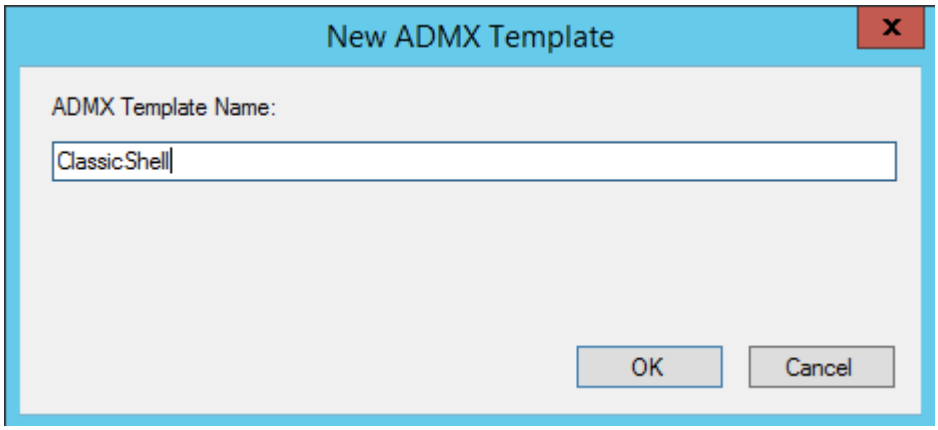
http://www.gruppenrichtlinien.de/artikel/client-side-extensions-cses/

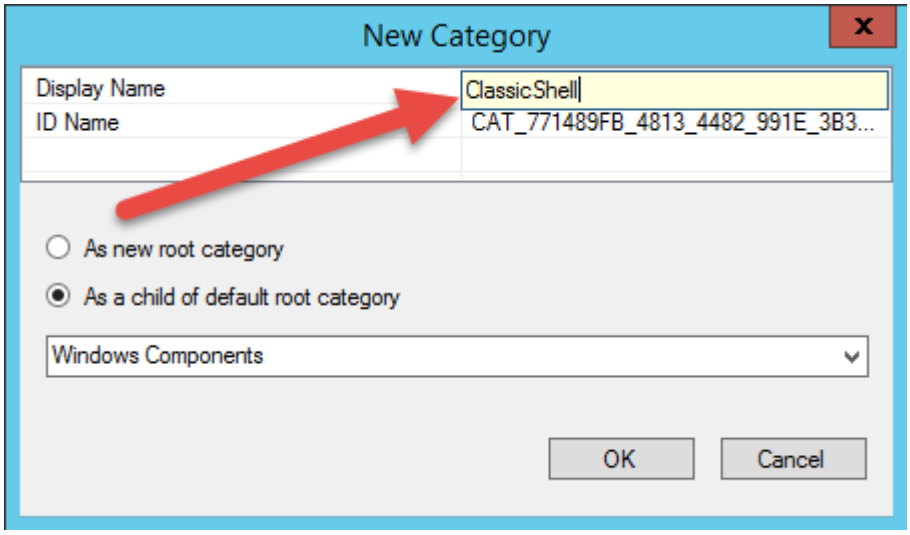
Die CSE werden vom Gruppenrichtlinienclient immer in einer festen Reihenfolge aufgerufen. Die Reihenfolge und die installierten Extensions finden Sie in der Registry im Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions.

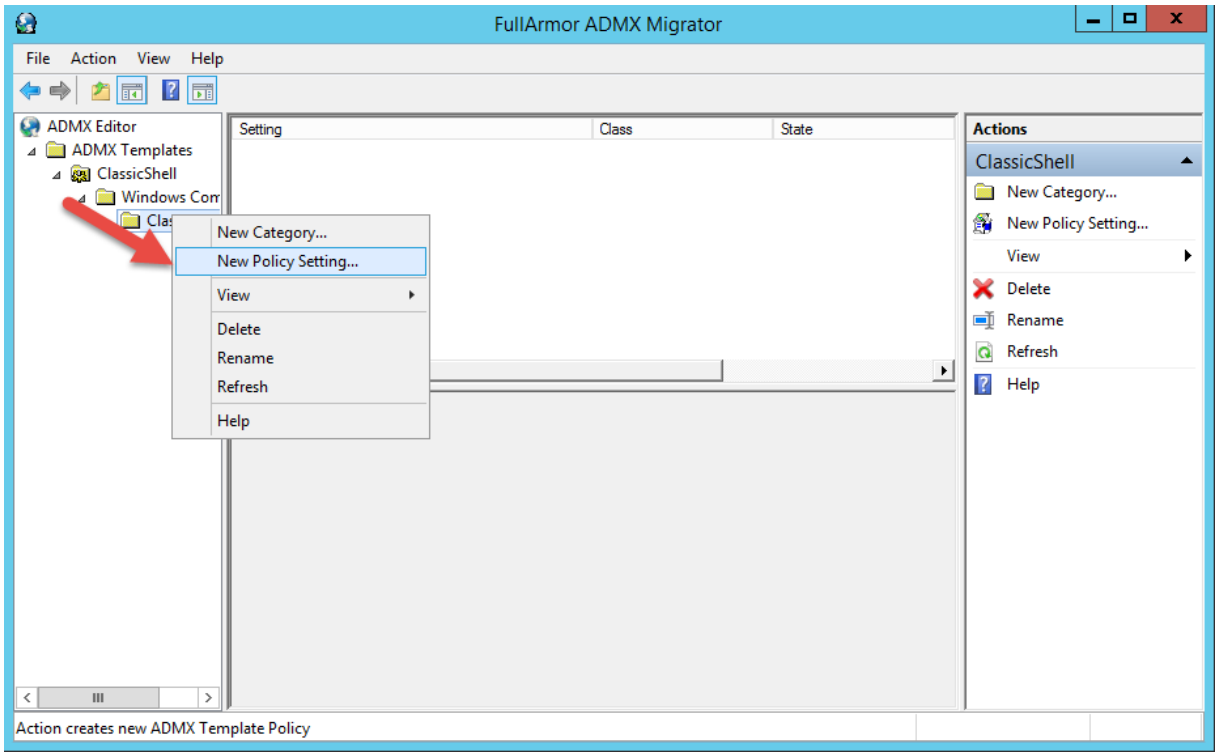
Anhang A

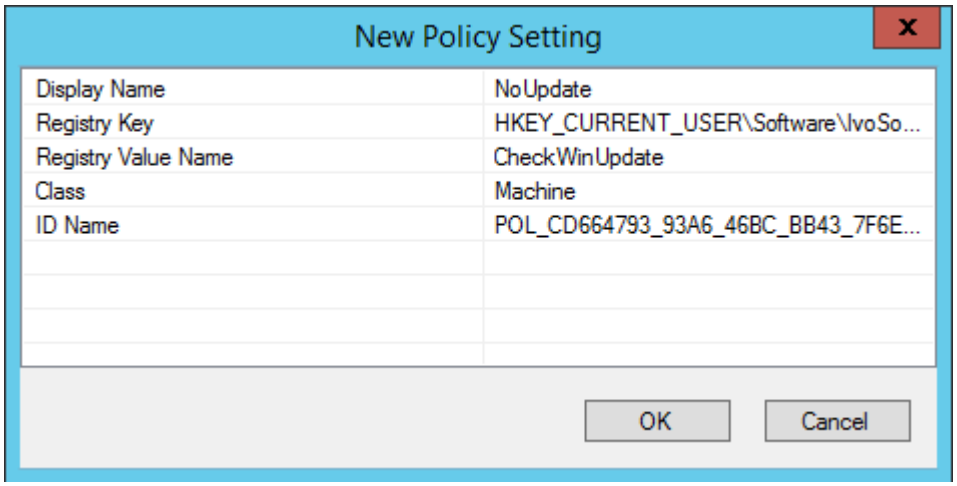
ADMX-Template erstellen mit dem FullArmor ADMX Editor

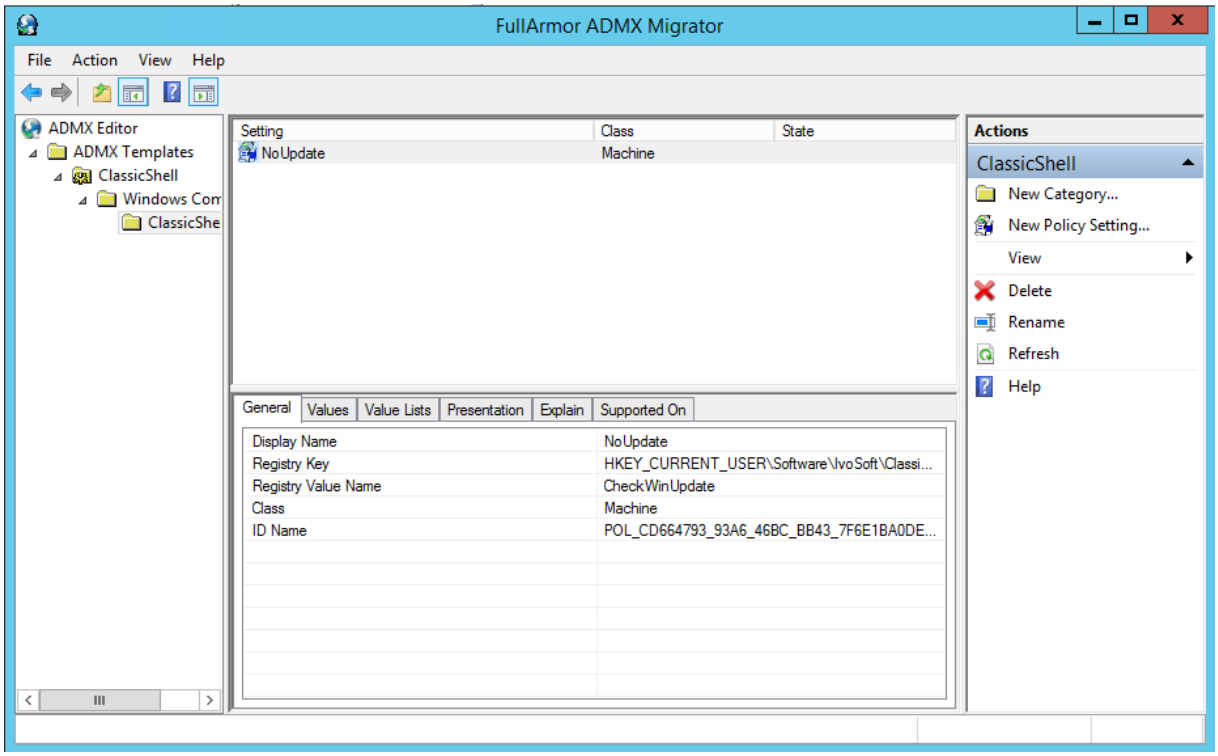


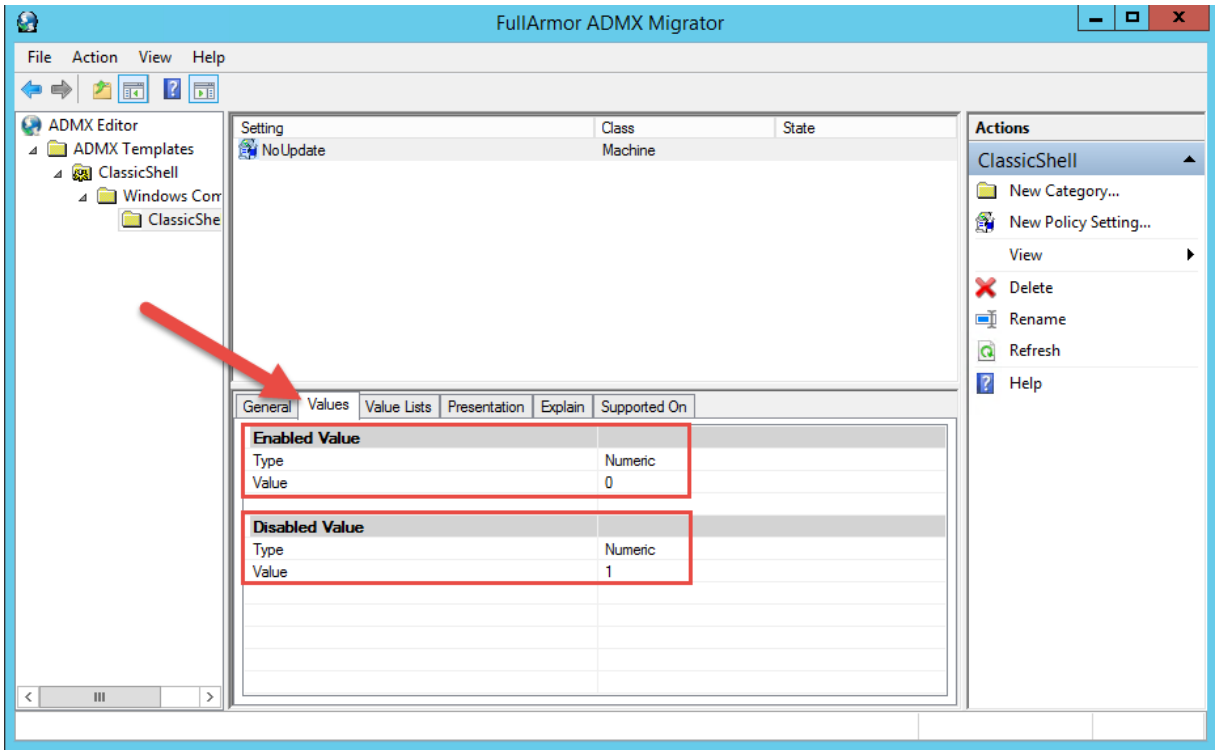



New Category
Display Name
ClassicShell
ID Name
CAT_771489FB_4813_4482_991E_3B3...
As new root category
As a child of default root category
Windows Components
OK
Cancel


FullArmor ADMX Migrator
File
Action
View
Help
ADMX Editor
ADMX Templates
ClassicShell
Windows Com
Setting
Class
State
New Category...
New Policy Setting...
View
Delete
Rename
Refresh
Help
Actions
ClassicShell
New Category...
New Policy Setting...
View
Delete
Rename
Refresh
Help
Action creates new ADMX Template Policy


New Policy Setting
Display Name
NoUpdate
Registry Key
HKEY_CURRENT_USER\Software\IvoSo...
Registry Value Name
CheckWinUpdate
Class
Machine
ID Name
POL_CD664793_93A6_46BC_BB43_7F6E...
OK
Cancel


FullArmor ADMX Migrator
File Action View Help
ADMX Editor
ADMX Templates
ClassicShell
Windows Com
ClassicShe
Setting
Class
State
NoUpdate
Machine
General
Values
Value Lists
Presentation
Explain
Supported On
Display Name
NoUpdate
Registry Key
HKEY_CURRENT_USER\Software\IvoSoft\Classi...
Registry Value Name
CheckWinUpdate
Class
Machine
ID Name
POL_CD664793_93A6_46BC_BB43_7F6E1BA0DE...
Actions
ClassicShell
New Category...
New Policy Setting...
View
Delete
Rename
Refresh
Help


FullArmor ADMX Migrator
File Action View Help
ADMX Editor
ADMX Templates
ClassicShell
Windows Com
ClassicShe
Setting
Class
State
NoUpdate
Machine
General
Values
Value Lists
Presentation
Explain
Supported On
Enabled Value
Type
Numeric
Value
0
Disabled Value
Type
Numeric
Value
1
Actions
ClassicShell
New Category...
New Policy Setting...
View
Delete
Rename
Refresh
Help

Anhang B

Links

Active Directory

Demoting Domain Controllers and Domains
http://technet.microsoft.com/en-us/library/jj574104.aspx

Gruppenrichtlinien

Group Policy Design Guidelines – Part 2
http://www.grouppolicy.biz/2010/07/best-practice-group-policy-design-guidelines-part-2/

Step-By-Step Guide to Controlling Device Installation Using Group Policy
http://msdn.microsoft.com/en-us/library/bb530324.aspx

Advanced Audit Policy Configuration
http://technet.microsoft.com/en-us/library/jj852202(v=ws.10).aspx