

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Ma  
weisen (↑ R 10)



**Netz-Weise**  
Lernen von den Besten.

# Windows Gruppenrichtlinien

Einrichten, Verwalten und  
Fehlersuche

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
weisen (↑ R 10)



**Netz-Weise**  
Lernen von den Besten.

**Netz-Weise**  
**Holger Voges**  
**Freundallee 13a**  
**30173 Hannover**  
**holger.voges@netz-weise.de**

**© 2008, 2013**



## Agenda

- Gruppenrichtlinien – eine Definition
- Einrichten von Richtlinien
- Richtlinien-Einstellungen: Wer, Was, Wo?
- Verwalten mit der GruRiLi Verwaltungskonsole
- Erweitern von Richtlinien mit administrativen Vorlagen
- Tools und Tipps

## Was sind Gruppenrichtlinien?

- Gruppenrichtlinien sind mit Windows 2000 eingeführt worden
- Gruppenrichtlinien ersetzen die NT4 Policies
- Grundlage ist Active Directory!
- Clientgrundlage ist ein NT-basiertes OS > NT4
- Mit jedem Servicepack und Windows Release wachsen die Funktionen von Gruppenrichtlinien
- Gruppenrichtlinien sind ein extrem mächtiges Werkzeug zur Konfiguration von Clients und Benutzerumgebungen



## Das können Gruppenrichtlinien

- Softwareverteilung
- Login- / Logoff-Scripte, Startup- und Shutdown-Scripte
- Zertifikatsverteilung
- Konto-Richtlinien
- Sicherheitseinstellungen
- Ordnerumleitungen
- Software-Einschränkungen
- Registry- und NTFS-Berechtigungen
- ...

## NT4 Policies

- Ursprung der Gruppenrichtlinien
- Einstellungen werden über `ntconfig.pol` auf dem DC verteilt
- Kompliziert zu konfigurieren
- Schwierig zu verteilen
- Problem des Tattooing



## Lokale Sicherheitsrichtlinien

- legen lokale Sicherheitseinstellungen fest
- Werden durch die Einstellungen der Domänen-Richtlinien überschrieben
- Beinhalten Benutzer-Rechte, Überwachungsrichtlinien und Sicherheitseinstellungen

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 105)



**Netz-Weise**  
Lernen von den Besten.

# Die lokalen Sicherheitsrichtlinien

Richtlinie	Sicherheitseinstell...
Kennwort muss Komplexitätsvo...	Aktiviert
Kennwortchronik erzwingen	24 gespeicherte Ke...
Kennwörter mit umkehrbarer V...	Deaktiviert
Maximales Kennwortalter	42 Tage
Minimale Kennwortlänge	7 Zeichen
Minimales Kennwortalter	1 Tage



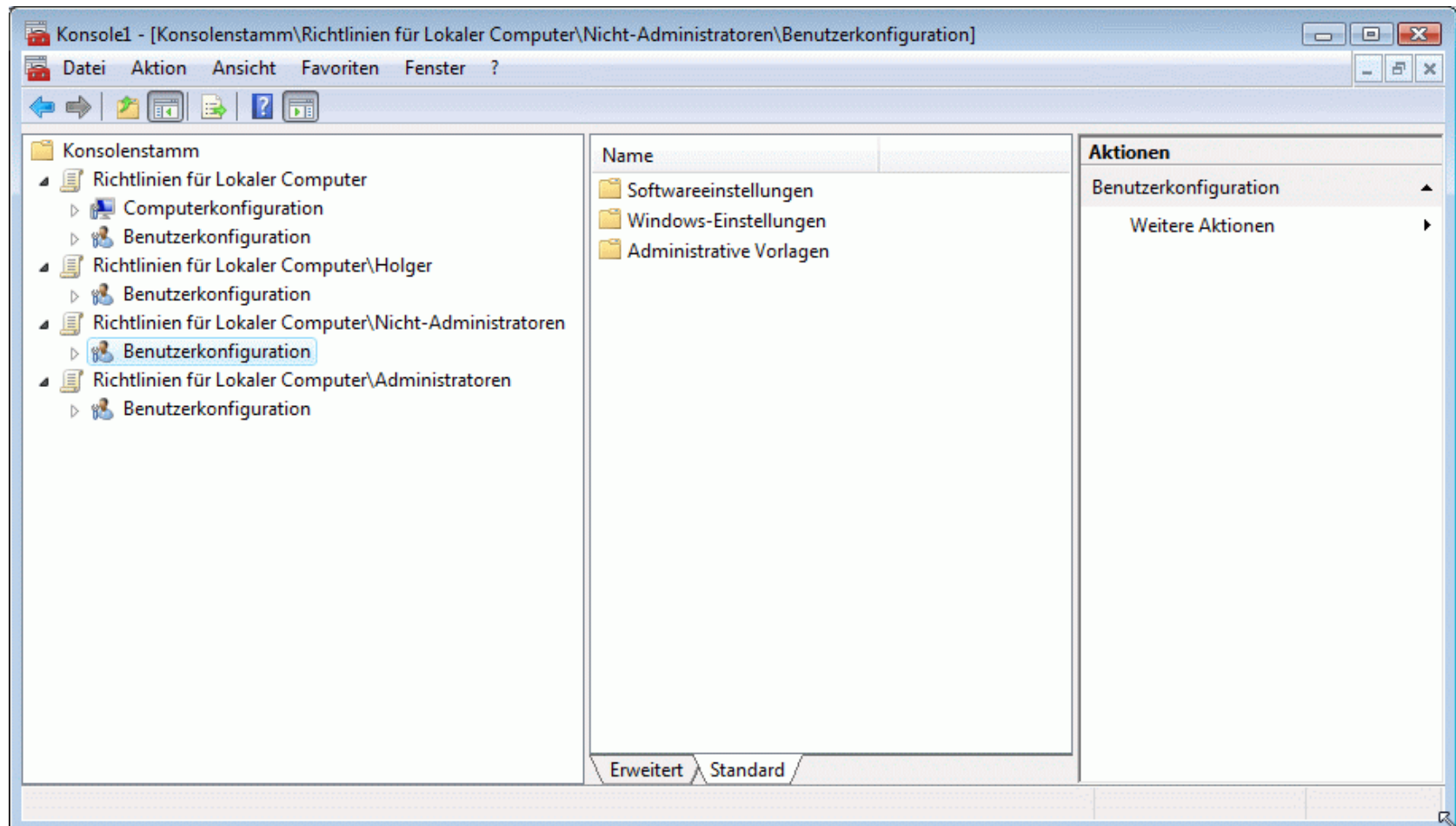


## Lokale Richtlinien

- implementieren die Einstellungen von Gruppenrichtlinien ohne Domäne
- werden im Windows-Ordner abgelegt
- Windows Vista kann mehrere lokale Richtlinien verwalten, Windows XP nur eine



# Konfigurieren lokaler Richtlinien



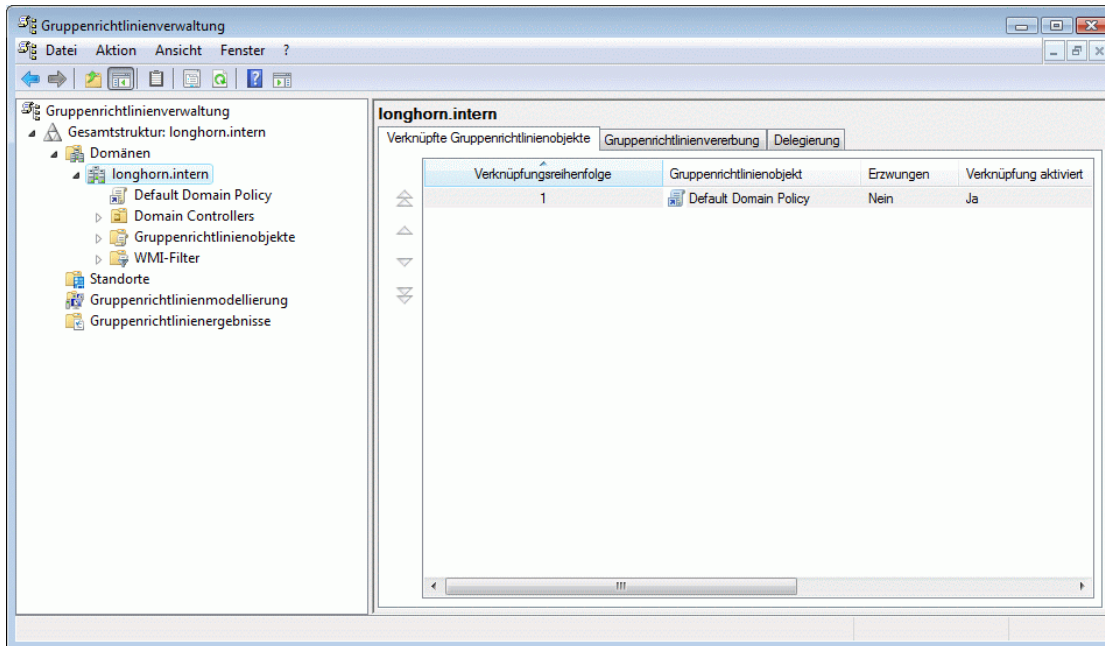
## Domänenrichtlinien

- Benötigen eine AD-Infrastruktur
- Zentrale Konfiguration von Benutzern und Computern
- Einstellungen der Lokalen Sicherheitsrichtlinie plus Lokale Richtlinien plus weitere Funktionen
- Pro Benutzer oder Pro Computer konfigurierbar
- Max. 999 Richtlinien pro Objekt – sind auf ein Objekt mehr Richtlinien angewendet, werden keine Richtlinien angewandt!

## Verwaltung von Gruppenrichtlinien

- Microsoft stellt seit Windows XP die Gruppenrichtlinienverwaltungskonsole zur Verfügung
- Voraussetzungen:
  - Windows XP SP1
  - .NET-Framework 1.1
  - Active Directory Domäne ab Windows 2000
- In Vista „ab Werk“ mitgeliefert
- MMC-Snap-In

# Group Policy Management Console



Auf der Abbildung sieht man im Strukturfenster links die einzelnen Objekte, auf die Gruppenrichtlinien vergeben werden können:

- Standorte
- Domänen
- Organisationseinheiten

In der GPMC ist außerdem ein weiterer Ordner Gruppenrichtlinienobjekte enthalten, der alle Gruppenrichtlinienobjekte anzeigt.

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

## Gruppenrichtlinien

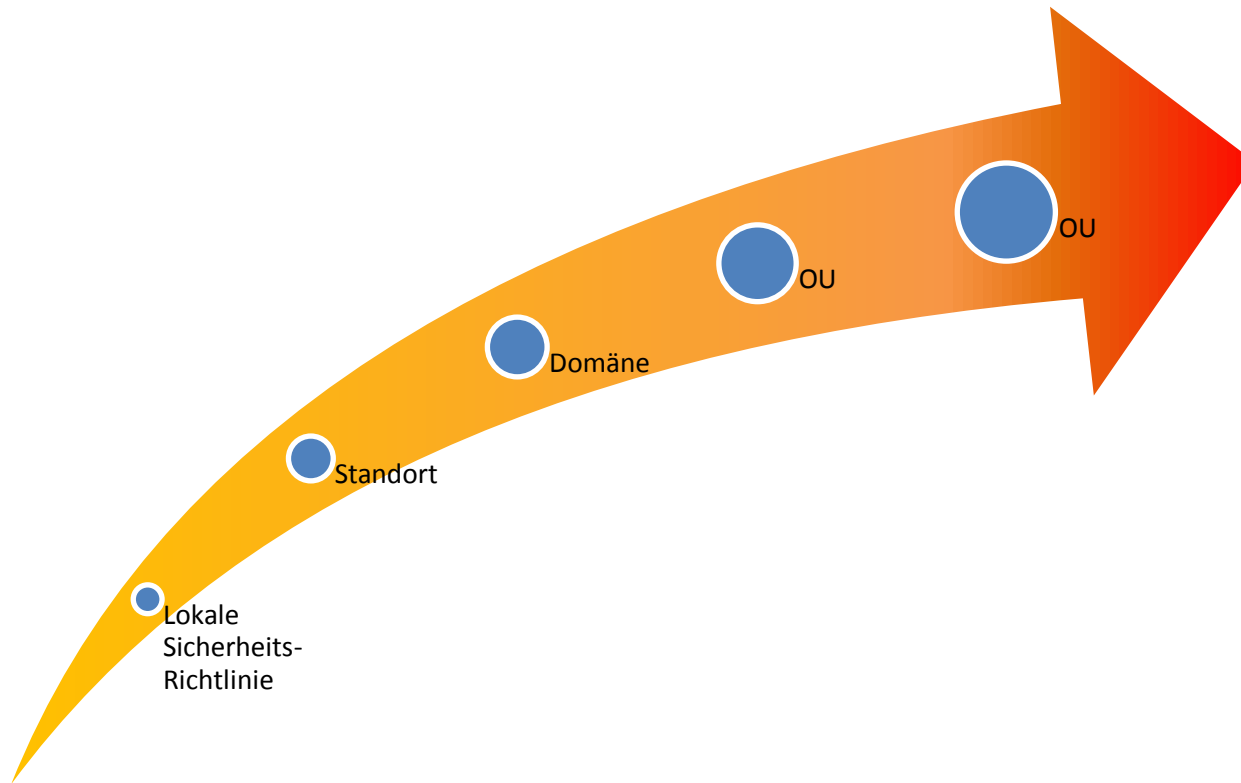
- Werden auf Benutzer- und Computer-Objekte angewendet
- Werden NICHT auf Gruppen angewendet (entgegen dem Namen)

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
weisen (↑ R 108)

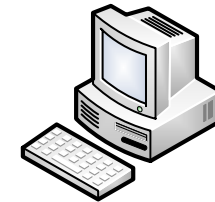


**Netz-Weise**  
Lernen von den Besten.

# Anwendungsreihenfolge und Priorität



Benutzer



Computer



# Gruppenrichtlinien-Einstellungen(1)

- Softwareverteilung
- Kontorichtlinien
- Lokale Richtlinien
- Eingeschränkte Gruppen
- Systemdienste / Registry / Dateisystem
- WLAN-Richtlinien
- Verkabelte Netze (Vista)
- Windows Firewall mit erweiterter Sicherheit (Vista)

Eine gute Zusammenfassung findet sich unter

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/de/library/ServerHelp/0bc86771-025a-46bf-b493-1cf262c17227.mspx?mfr=true>

Weiterführende Infos zu Vista finden sich unter

<http://technet2.microsoft.com/WindowsVista/en/library/02633470-396c-4e34-971a-0c5b090dc4fd1033.mspx?mfr=true>



## Gruppenrichtlinien-Einstellungen(2)

- Softwareeinschränkungen
- Network Access Protection (Vista)
- IP-SEC
- Automatische Scriptausführung
- Druckerbereitstellung (Standortbasiert nur Vista)
- Richtlinienbasierter Quality of Service (Vista)
- Remoteinstallationsdienste
- Ordnerumleitungen
- Internet-Explorer
- Administrative Vorlagen

# Softwareverteilung

- Softwareverteilung erlaubt das automatische Installieren von Software
- Die Softwareverteilung kann pro Benutzer oder pro Computer stattfinden
- 2 Installationsmodi
  - Veröffentlicht (Installation bei Bedarf)
  - Zugewiesen
- Eine Veröffentlichte Installation kann nur für Benutzer erzeugt werden
- Die zu verteilende Software muß als msi-Paket vorliegen

Genau genommen muss die Software nicht als msi-Paket vorliegen, sondern kann auch mit einer sogenannten .zap-Datei bereitgestellt werden. Eine .zap-Datei ist eine Textdatei, die Informationen über die Installation mitgibt. Leider ist diese Installationsvariante aber nur veröffentlichten Installationen (also Benutzerspezifisch) vorbehalten, und der Benutzer, der das Paket installieren möchte, braucht auf dem zu installierenden Rechner administrative Rechte.

## Vorbereiten der Softwareverteilung

- Erzeugen einer Freigabe auf einem Fileserver
- Berechtigungen für zu installierende Konten auf „Lesen“
- Installationsdaten (msi-Pakete) in der Freigabe bereitstellen

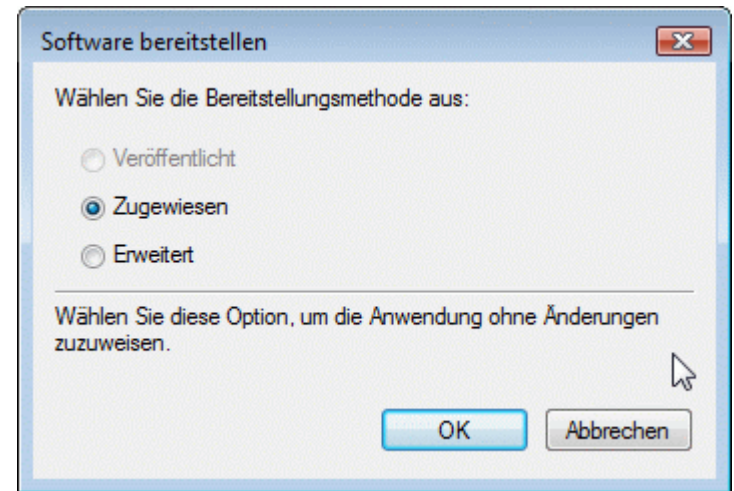
Best Practice:

Die sicherste Möglichkeit zur Softwareverteilung besteht darin, Software nur für Computer zu verteilen, nicht für Benutzer. Dann benötigen Sie auf der Freigabe nur für „Domänencomputer“ Leserechte. Ein normaler Benutzer kann die Verteilungsfreigabe dann nicht sehen und sich folglich auch keine Installationsdaten aus der Freigabe kopieren.

weise (klug); Weise, (kluger Mann)  
-n, -n; ↑ R 5 ff. (kluger Mann)  
weisen (↑ R 105)

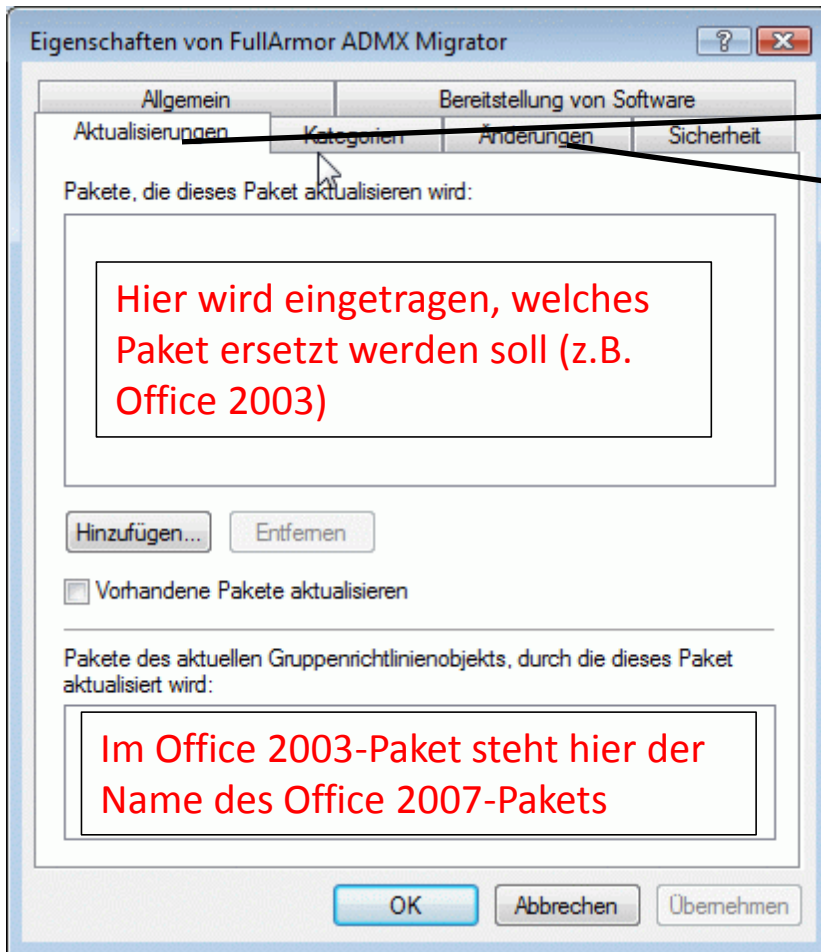
## Erzeugen eines Verteilungspakets

1. Eine neue oder bestehende Richtlinie öffnen
2. Den Knoten Computerkonfiguration / Softwareeinstellungen / Softwareinstallation öffnen
3. Mit der rechten Maustaste ein neues Paket erstellen
4. Paketpfad auswählen (Pfad zur Freigabe)
5. Installationstyp auswählen



wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Men  
weisen (↑ R 10)

# Erweiterte Funktionen



Aktualisierungen wird verwendet, wenn eine alte Softwareversion durch eine neue ersetzt werden soll (z.B. Office 2003 durch Office 2007)

Änderungen sind Anpassungen mit Hilfe von mst-Dateien. Mst-Dateien können nur beim Erzeugen des Pakets hinzugefügt werden, indem man statt veröffentlicht oder zugewiesen „Erweitert“ auswählt

Eine gute Einführung finden Sie auch hier:

[http://www.windowsnetworking.com/articles\\_tutorials/Best-Practices-Group-Policy-Based-Application-Deployment.html](http://www.windowsnetworking.com/articles_tutorials/Best-Practices-Group-Policy-Based-Application-Deployment.html)

Installation von Office 2007 mit Gruppenrichtlinien:

<http://technet2.microsoft.com/Office/en-us/library/efd0ee45-9605-42d3-9798-3b698fff3e081033.mspx?mfr=true>

Achtung! Die Installation von Office 2007 ist leider nicht ganz trivial, da das Office-Entwicklerteam die Installation per Gruppenrichtlinien bei der Entwicklung nur stiefmütterlich behandelt hat. Die Konfiguration findet nicht mehr, wie üblich, über mst-Dateien statt, sondern über eine XML-Datei, was das Standard-Richtlinienverfahren stark einschränkt. Weitere Informationen findet man in der Mailingliste des gpoguy ([www.gpoguy.com](http://www.gpoguy.com)).

## Specops Deploy

- Specops Deploy ist eine Erweiterung der AD-Software-Bereitstellung
- Specops Deploy integriert sich nahtlos in den Grup Policy Editor
- Mit Specops-Deploy ist ein zeitgesteuertes Bereitstellen von Software möglich
- Das Gruppieren von Software-Paketen mit einer Installations-Rangfolge wird möglich
- Mit Abhängigkeiten können Abhängigkeiten von Programmen bestimmt werden (GPMC benötigt .NET-Framework usw)
- <http://www.specopssoft.com/products/specopsdeploy/Default.asp>

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 10)



**Netz-Weise**  
Lernen von den Besten.

## Kennwort-Richtlinien



Domänen-Richtlinie -  
1x pro Domäne



Fine Grained Password  
Policies –  
Kennwort-Richtlinien  
per Windows-Gruppe



# Kennwortrichtlinien

- Legen Regeln für Kennwörter fest
- Es gibt bis W2k3 pro Domäne nur 1 gültige Kennwortrichtlinie! Diese wird auf Domänenebene festgelegt.
- Die Standardregeln für Kennwörter sind in der Default Domain Policy definiert
- Die Default Domain Policy wird nie bearbeitet!
- Verschiedene Hersteller bieten Tools, um mehrere Kontorichtlinien pro Domäne zu implementieren
- Ab Windows Server 2008 gibt es mit den Fine Grained Password-Policies die Möglichkeit, zusätzlichen Kennwortrichtlinien zu definieren

Tatsächlich kann man die Default Domain Policy natürlich bearbeiten, aber es absolut davon abzuraten. Alle Einstellungen der Default Domain Policy können überschrieben werden, indem man eine neue Richtlinie auf Domänenebene definiert und in dieser die Einstellungen vornimmt, die anders als die Standard-Einstellungen sein sollen. Hat man die Default-Richtlinien doch mal geändert, hilft „dcpofix.exe“ weiter. Dieses Tool stellt die Standard-Richtlinien wieder her. Bei Windows Server 2003 ist das Tool bereits im System vorhanden, für Windows 2000 kann man es bei Microsoft herunterladen.

<http://www.microsoft.com/downloads/details.aspx?FamilyID=b5b685ae-b7dd-4bb5-ab2a-976d6873129d&DisplayLang=en>

Weiterführende Informationen zu Kennwortrichtlinien-Tools:

[http://www.gruppenrichtlinien.de/Software/6.Specops\\_Password\\_Policy.htm](http://www.gruppenrichtlinien.de/Software/6.Specops_Password_Policy.htm)

[http://www.gruppenrichtlinien.de/Software/7.Altus\\_Passfiltpro.htm](http://www.gruppenrichtlinien.de/Software/7.Altus_Passfiltpro.htm)

Weiterführende Informationen zu mehreren Kennwortrichtlinien unter Windows Server 2008 finden Sie hier:

<http://msmvps.com/blogs/ulfbbsimonweidner/archive/2007/03/12/windows-server-quot-longhorn-quot-granular-password-settings.aspx>

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Mann)  
Weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

# Kennwortrichtlinien

Gruppenrichtlinienobjekt-Editor

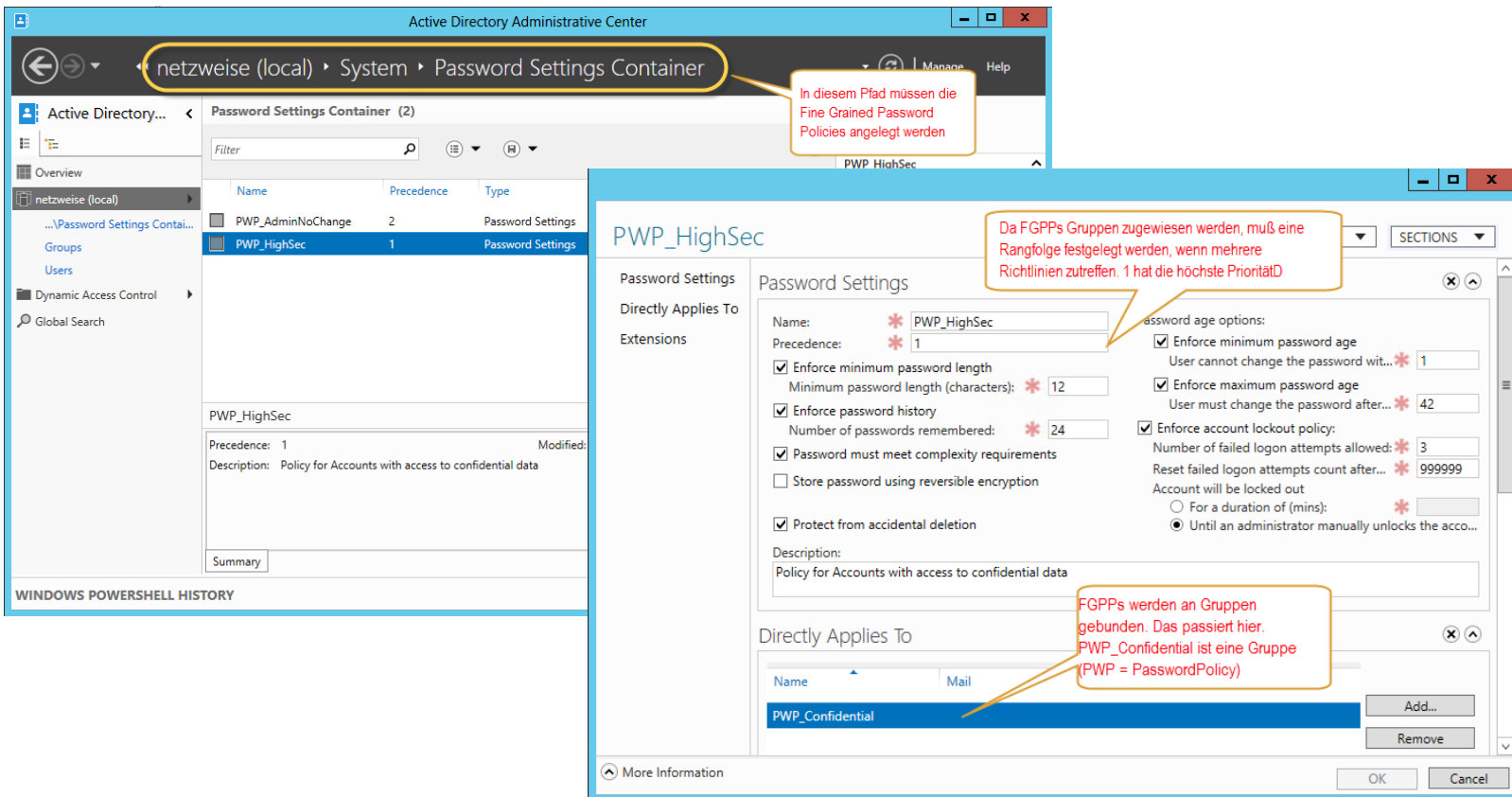
Default Domain Policy [Cowboy.longhorn.inter]

- Computerkonfiguration
  - Softwareeinstellungen
  - Windows-Einstellungen
    - Skripts (Start/Herunterfahren)
    - Bereitgestellte Drucker
    - Sicherheitseinstellungen
      - Kontorichtlinien
        - Kennwortrichtlinien**
        - Kontosperrungsrichtlinien
        - Kerberos-Richtlinie
      - Lokale Richtlinien
      - Ereignisprotokoll
      - Eingeschränkte Gruppen
      - Systemdienste
      - Registrierung
      - Dateisystem
      - Richtlinien für verkabelte Netzwe
      - Windows-Einstellungen mit zusätzl...

Richtlinie	Richtlinieneinstellung
Kennwort muss Komplexitätsvoraussetzu...	Aktiviert
Kennwortchronik erzwingen	24 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsse...	Deaktiviert
Maximales Kennwortalter	42 Tage
Minimale Kennwortlänge	7 Zeichen
Minimales Kennwortalter	1 Taae

Richtlinie	Richtlinieneinstellung
Kontensperrungsschwelle	0 ungültigen Anmeldeversuchen
Kontosperrdauer	Nicht definiert
Zurücksetzungsdauer des Kontosperrung...	Nicht definiert

# Fine Grained Password Policy



Active Directory Administrative Center

netzweise (local) > System > Password Settings Container

Active Directory... < Password Settings Container (2)

Name	Precedence	Type
PWP_AdminNoChange	2	Password Settings
PWP_HighSec	1	Password Settings

PWP\_HighSec

Precedence: 1  
Description: Policy for Accounts with access to confidential data

Summary

WINDOWS POWERSHELL HISTORY

PWP\_HighSec

Password Settings

Directly Applies To

Extensions

Name: PWP\_HighSec

Precedence: 1

Enforce minimum password length  
Minimum password length (characters): 12

Enforce password history  
Number of passwords remembered: 24

Password must meet complexity requirements

Store password using reversible encryption

Protect from accidental deletion

Description: Policy for Accounts with access to confidential data

Password age options:

Enforce minimum password age  
User cannot change the password with... 1

Enforce maximum password age  
User must change the password after... 42

Enforce account lockout policy:  
Number of failed logon attempts allowed: 3  
Reset failed logon attempts count after... 999999  
Account will be locked out  
 For a duration of (mins):  
 Until an administrator manually unlocks the acco...

Directly Applies To

Name	Mail
PWP_Confidential	

Add...  
Remove

More Information

OK Cancel

In diesem Pfad müssen die Fine Grained Password Policies angelegt werden

Da FGPPs Gruppen zugewiesen werden, muß eine Rangfolge festgelegt werden, wenn mehrere Richtlinien zutreffen. 1 hat die höchste Priorität

FGPPs werden an Gruppen gebunden. Das passiert hier. PWP\_Confidential ist eine Gruppe (PWP = PasswordPolicy)

Einrichten von Fine Grained Password Policies unter Windows 2008 / 2008 R2 (keine GUI!): **Appendix A: Fine-Grained Password and Account Lockout Policy Review**

<http://technet.microsoft.com/en-us/library/cc754544%28v=ws.10%29.aspx>



## Lokale Richtlinien

- Lokale Richtlinien aus Domänenrichtlinien überschreiben die lokalen Einstellungen
- Konfigurationsmöglichkeiten:
  - Überwachungseinstellungen
  - Benutzerrechte
  - Sicherheitseinstellungen

weise (klug); Weisheit, Weisheit (kluger Mensch)  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisheit (R 10)



**Netz-Weise**  
Lernen von den Besten.

# Lokale Richtlinien

Richtlinie	Richtlinie
Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrie...	Nicht def...
Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigun...	Nicht def...
Benutzerkontensteuerung: Anwendungsinformationen erkennen und erhöhte...	Nicht def...
Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten...	Nicht def...
Benutzerkontensteuerung: Datei- und Registrierungsfehler an Einzelb...	Nicht def...
Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signier...	Nicht def...
Benutzerkontensteuerung: Nur erhöhte Rechte für UIAccess-Anwendungen, ...	Nicht def...
Benutzerkontensteuerung: Verhalten der Anhebungsaufforderung für Standa...	Nicht def...
Benutzerkontensteuerung: Verhalten der Benutzeraufforderung mit erhöhten...	Nicht def...
DCOM: Computerstarteinschränkungen in Security Descriptor Definition Lan...	Nicht def...
DCOM: Computerzugriffseinschränkungen in Security Descriptor Definition ...	Nicht def...
Domänencontroller: Änderungen von Computerkontenkennwörtern verweig...	Nicht def...
Domänencontroller: Serveroperatoren das Einrichten von geplanten Tasks erl...	Nicht def...
Domänencontroller: Signaturanforderungen für LDAP-Server	Nicht def...
Domänenmitglied: Änderungen von Computerkontenkennwörtern deaktivie...	Nicht def...
Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglic)	Nicht def...
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn m...	Nicht def...
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signi...	Nicht def...
Domänenmitglied: Maximalalter von Computerkontenkennwörtern	Nicht def...
Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Windows 2000 ode...	Nicht def...
Geräte: Anwendern das Installieren von Drucktreibern nicht erlauben	Nicht def...
Geräte: Entfernen ohne vorherige Anmeldung erlauben	Nicht def...
Geräte: Formatieren und Auswerfen von Wechselmedien zulassen	Nicht def...
Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer besch...	Nicht def...
Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer besch...	Nicht def...
Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeichers löschen	Nicht def...
Herunterfahren: Herunterfahren des Systems ohne Anmeldung zulassen	Nicht def...
Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum Ändern de...	Nicht def...
Interaktive Anmeldung: Anzahl zwischenspeicherter vorheriger Anmelde...	Nicht def...
Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben...	Nicht def...
Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich	Nicht def...
Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen	Nicht def...
Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen	Nicht def...
Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden wol...	Nicht def...
Interaktive Anmeldung: Smartcard erforderlich	Nicht def...
Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards	Nicht def...

Sicherheitseinstellungen

Richtlinie	Richtlinieneinstellung
Anmelden über Terminaldienste zulassen	Nicht definiert
Annehmen der Clientidentität nach Auth...	Nicht definiert
Anpassen von Speicherkontingenten für ...	Nicht definiert
Arbeitssatz eines Prozesses vergrößern	Nicht definiert
Auf Anmeldeinformations-Manager als v...	Nicht definiert
Auf diesen Computer vom Netzwerk aus ...	Nicht definiert
Auslassen der durchsuchenden Überprüf...	Nicht definiert
Debuggen von Programmen	Nicht definiert
Durchführen von Volumewartungsaufga...	Nicht definiert
Einsetzen als Teil des Betriebssystems	Nicht definiert
Entfernen des Computers von der Dockin...	Nicht definiert
Ermöglichen, dass Computer- und Benut...	Nicht definiert
Ersetzen eines Tokens auf Prozessebene	Nicht definiert
Erstellen einer Auslagerungsdatei	Nicht definiert
Erstellen eines Profils der Systemleistung	Nicht definiert
Erstellen eines Profils für einen Einzelpro...	Nicht definiert
Erstellen eines Tokenobjekts	Nicht definiert
Erstellen globaler Objekte	Nicht definiert
Erstellen symbolischer Verknüpfungen	Nicht definiert
Erstellen von dauerhaft freigegebenen O...	Nicht definiert
Erzwingen des Herunterfahrens von eine...	Nicht definiert
Generieren von Sicherheitsüberwachungen	Nicht definiert
Herunterfahren des Systems	Nicht definiert
Hinzufügen von Arbeitsstationen zur Do...	Nicht definiert
Laden und Entfernen von Gerätetreibern	Nicht definiert
Lokal anmelden verweigern	Nicht definiert
Lokal anmelden zulassen	Nicht definiert
Sichern von Dateien und Verzeichnissen	Nicht definiert
Sperren von Seiten im Speicher	Nicht definiert
Synchronisieren von Verzeichnisdienstda...	Nicht definiert
Übernehmen des Besitzes von Dateien un...	Nicht definiert
Verändern der Firmwareumgebungsvaria...	Nicht definiert
Verändern einer Objektbezeichnung	Nicht definiert
Verwalten von Überwachungs- und Siche...	Nicht definiert
Wiederherstellen von Dateien und Verzei...	Nicht definiert
Zuariff vom Netzwerk auf diesen Comou...	Nicht definiert

Benutzerrechte

Richtlinie	Richtlinieneinstellung
Anmeldeereignisse überwachen	Nicht definiert
Anmeldeversuche überwachen	Nicht definiert
Kontenverwaltung überwachen	Nicht definiert
Objektzugriffsversuche überwachen	Nicht definiert
Prozessverfolgung überwachen	Nicht definiert
Rechteverwendung überwachen	Nicht definiert
Richtlinienänderungen überwachen	Nicht definiert
Systemereignisse überwachen	Nicht definiert
Verzeichnisdienstzugriff überwachen	Nicht definiert

Überwachung

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Men  
weisen (↑ R 10)

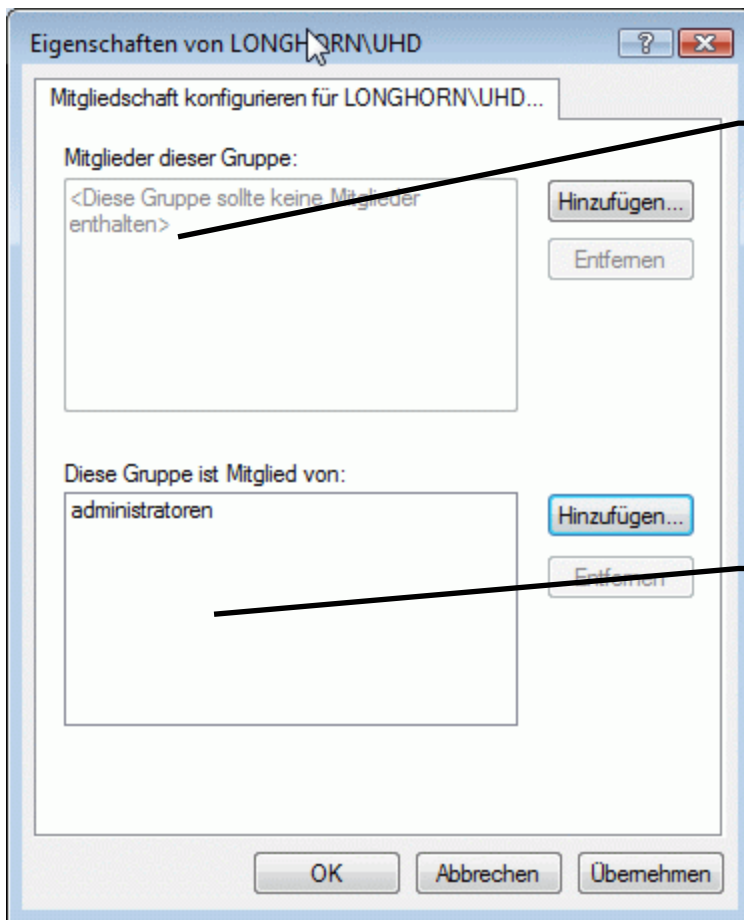
Die Überwachungsrichtlinien legen fest, welche Ereignisse auf den jeweiligen Rechnern protokolliert werden sollen.

Objektzugriffsversuche sind Zugriffe auf das Dateisystem und Drucker. Damit der Objektzugriff protokolliert wird, muss zusätzlich für die zu überwachenden Objekte die Überwachung eingestellt sein. Dies geschieht über den Reiter Sicherheit in den Eigenschaften des Objekts -> Erweitert -> Reiter Überwachung. Hier wird für jeden einzelnen Objektzugriff definiert, welche Zugriffe protokolliert werden sollen und welche nicht.

Die Überwachungsprotokolle werden im Ereignisprotokoll „Sicherheit“ gespeichert. Auf dieses Protokoll haben standardmäßig nur Administratoren Zugriff. In der Default Domain Controllers-Policy ist die Anmeldeüberwachung eingeschaltet, so dass auf allen Domänencontrollern jeder Anmeldevorgang protokolliert wird. Dieser Vorgang führt zu einem starken Anwachsen des Sicherheitsprotokolls. Dieser Vorgang ist beabsichtigt und kein Fehler!

weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
weisen (↑ R 10)

# Eingeschränkte Gruppen



Erzwingt in der angegebenen Gruppe genau diese Mitglieder. Die Standard-Konfiguration der Gruppe wird überschrieben. Wird normalerweise für lokale Gruppen verwendet.

Alle Computer, für die diese Richtlinie gültig wird, nehmen die Gruppe Longhorn\UHD in die Gruppe Administratoren auf.



# Systemdienste / Registry / Dateisystem

- Erlaubt das Vergeben von Berechtigungen auf Registry und Dateisystem
- Es können hier weder Registry-Schlüssel angelegt noch Dateien kopiert werden!
- Systemdienste legen fest, welche Dienste gestartet werden

Achtung! Das Deaktivieren von Diensten kann böse Konsequenzen nach sich ziehen. Das Deaktivieren des Server-Dienstes auf Domänenebene schaltet beispielsweise auch auf allen Servern den Server-Dienst aus, inklusive der Domänen-Controller, die dann nicht mehr starten.

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Mann)  
weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

Messenger, Bittorrent, Regedit, Licht...

...sind für meine User nicht!

## Softwareeinschränkungen

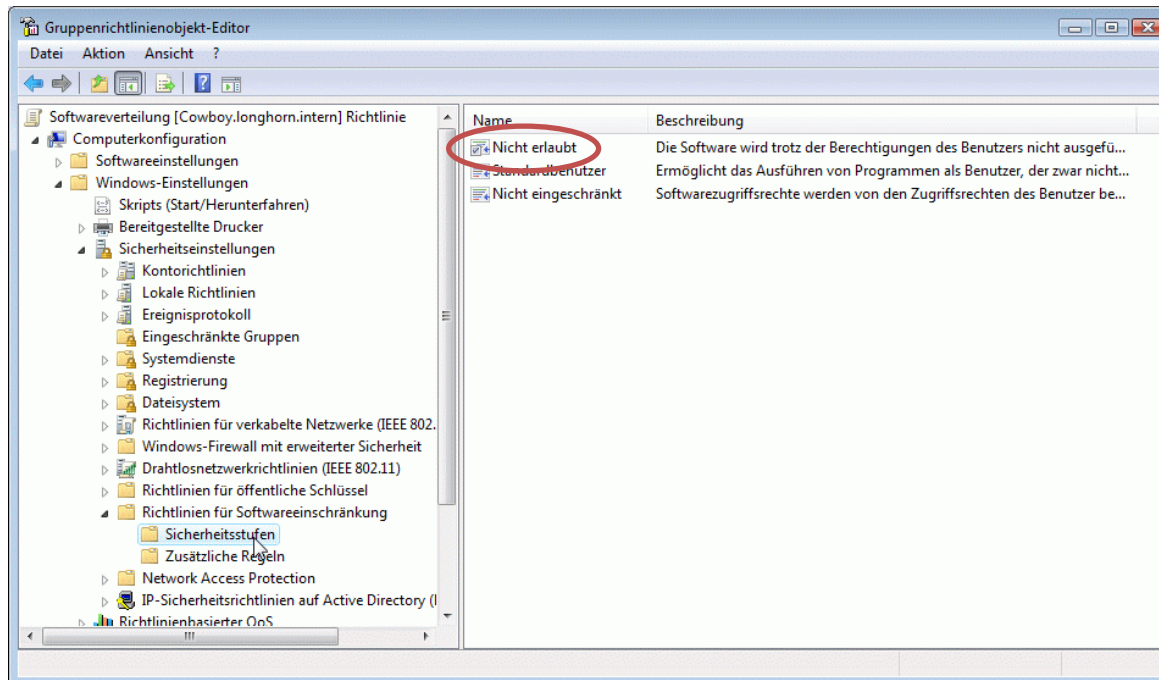
- Softwareeinschränkungen konfigurieren, welche Programme gestartet werden können
- Einstellungen pro Computer oder pro Benutzer
- Die Standardregeln sorgen dafür, dass der Computer immer starten kann

Softwareeinschränkungen sind eine wunderbare Lösung für Terminal-Server. Alternativ können Sie auch den Applocker einsetzen (nächste Folien).

weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 10)

# Softwareeinschränkungen konfigurieren

- Im 1. Schritt muss eine neue Regel definiert werden
- Im 2. Schritt wird festgelegt, ob standardmäßig alle Programme erlaubt oder verboten sind



# Regeln definieren

- Windows unterstützt 4 Regeln:
  1. Hash-Regeln erzeugen Datei-Hashs über Programm-Dateien
  2. Zertifikat-Regeln definieren signierte Dateien, die erlaubt sind
  3. Pfadregeln definieren anhand des Pfades die Programme
  4. Netzwerkzonen-Regeln (Internetzonen) legen anhand der Herkunft fest, welche Programm gestartet werden dürfen
- Diese Reihenfolge entspricht auch der Priorität der Regeln

Die Priorität bezieht sich darauf, dass ein Programm durch mehrere Regeln betroffen sein kann. Wird einem Programm per Hash die Ausführung erlaubt, aber per Pfadregel verboten, so kann das Programm trotzdem ausgeführt werden.

## **Precedence of software restriction policies rules**

<http://technet2.microsoft.com/WindowsServer/en/library/86aaca03-a242-4874-864c-87e1e38d5da51033.aspx?mfr=true>

weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mann)  
Weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

# Die Regeln

Gruppenrichtlinienobjekt-Editor

Softwareverteilung [Cowboy.longhorn.intern] Richtlinie

- Computerkonfiguration
  - Softwareeinstellungen
  - Windows-Einstellungen
    - Skripts (Start/Herunterfahren)
    - Bereitgestellte Drucker
    - Sicherheitseinstellungen
      - Kontorichtlinien
      - Lokale Richtlinien
      - Ereignisprotokoll
      - Eingeschränkte Gruppen
      - Systemdienste
      - Registrierung
      - Dateisystem
      - Richtlinien für verkabelte Netzwerke (IEEE 802.11)
      - Windows-Firewall mit erweiterter Sicherheit
      - Drahtlosnetzwerkrichtlinien (IEEE 802.11)
      - Richtlinien für öffentliche Schlüssel
      - Richtlinien für Softwareeinschränkung
        - Sicherheitsstufen
        - Zusätzliche Regeln
      - Network Access Protection
      - IP-Sicherheit
      - Richtlinienbasierter Schutz

Name	Typ	Sicherheitsstufe	Beschreibung
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Pfad	Nicht eingesch...	
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Pfad	Nicht eingesch...	

Fügt Zertifikatregel hinzu.

# Pfadregeln

- definieren einmal einen Dateisystempfad (legt fest, welche Pfade erlaubt oder verboten sind)
- Können auch Registry-Pfade definieren -> Werte in der Registry, die auf erlaubte oder verbotene Pfade verweisen
- Die 2 Standard-Regeln erlauben alle Programme, die im Ordner Programme und Windows liegen

Durch die Standard-Regeln wird sichergestellt, dass Windows funktioniert. Mit den Standard-Einstellungen kann ein Benutzer nur Programme starten, die im Programme-Ordner liegen. Dieser wiederum ist für Benutzer nur lesend verwendbar, so dass im Endeffekt nur Programme gestartet werden können, die von einem Administrator im Standard-Pfad installiert worden sind.

## Applocker

- Applocker ist ab Windows Server 2008R2/Win7 verfügbar
- Im Gegensatz zu SRS können Regeln auf Gruppen und Benutzer angewandt werden
- Deny-Regeln überschreiben immer Allow!
- Verfügbar mit Windows Server Standard / Win 7 Enterprise / Win 8 Pro
- Application Information / Anwendungsidentitäts-Dienst muß auf zu verwaltendem Client gestartet sein



wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man...  
Weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

# Applocker

The screenshot shows the Group Policy Management Editor window. The left pane displays a tree view of Group Policy Objects, with 'AppLocker' expanded under 'Application Control Policies'. The right pane shows a table of Executable Rules.

Action	User	Name	Condition	Exception
✓ Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
✓ Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
✓ Allow	BUILTIN\Administrators	All files	Path	
⊘ Deny	Everyone	%OSDRIVE%\tools\*	Path	

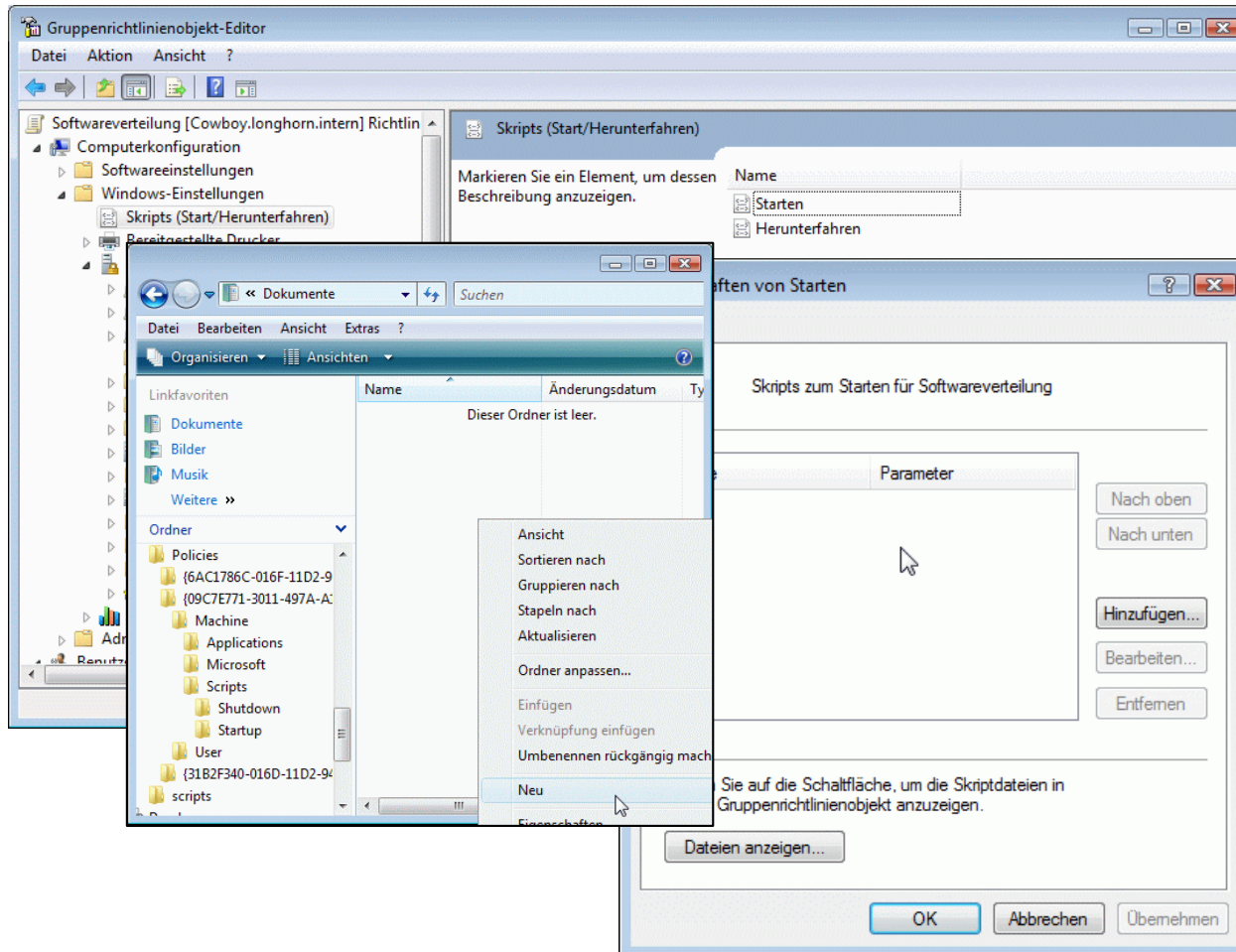


# Automatische Scriptausführung

- Richtlinien erlauben das Ausführen beim:
  - Starten des Rechners
  - Herunterfahren des Rechners
  - Login eines Benutzers
  - Logoff eines Benutzers
- Scripte für den Rechner werden im System-Kontext ausgeführt (administrative Rechte)
- Benutzer-Scripte haben nur die Rechte des Benutzers
- Seit Windows Server 2008 R2 können auch Powershell-Scripte genutzt werden

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
Weisen (↑ R 10)

# Ein Script hinzufügen



The screenshot shows the 'Gruppenrichtlinienobjekt-Editor' (Group Policy Object Editor) window. The left pane shows the tree structure with 'Skripts (Start/Herunterfahren)' selected. The right pane shows the 'Skripts (Start/Herunterfahren)' configuration page. A 'Skripten von Starten' dialog box is open, displaying a list of scripts to start for software distribution. The 'Parameter' field is empty. A context menu is open over the 'scripts' folder in the left pane, with the 'Neu' (New) option selected.

Gruppenrichtlinienobjekt-Editor

Skripts (Start/Herunterfahren)

Markieren Sie ein Element, um dessen Beschreibung anzuzeigen.

Name

Starten

Herunterfahren

Skripten von Starten

Skripts zum Starten für Softwareverteilung

Parameter

Nach oben

Nach unten

Hinzufügen...

Bearbeiten...

Entfernen

Sie auf die Schaltfläche, um die Skriptdateien in Gruppenrichtlinienobjekt anzuzeigen.

Dateien anzeigen...

OK Abbrechen Übernehmen

weise (klug); Weisheit, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 10)

Das Hinzufügen eines Scripts ist ein wenig kryptisch. Das Anmeldescript muss in der Gruppenrichtlinie hinterlegt sein. Daher gilt:

1. In der Richtlinie in Windows-Einstellungen das Script (anmelden/abmelden/starten/herunterfahren) auswählen.
2. Im folgenden Fenster Dateien anzeigen wählen.
3. Das folgende Fenster öffnet sich direkt im Pfad der Richtlinie. Kopieren Sie in diesen Pfad das Script hinein.
4. Schließen Sie das Explorer-Fenster und klicken Sie in der Richtlinie auf „Hinzufügen“. Klicken Sie anschließend auf Durchsuchen.
5. Hier sehen Sie jetzt das kopierte Script. Wählen Sie es aus.
6. Das wars. Seltsam? Aber so steht es geschrieben.

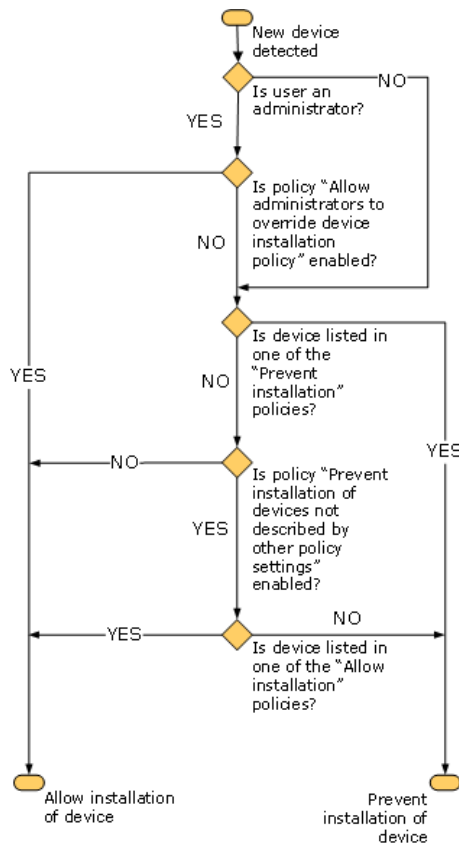


## Anmeldescripte erzeugen

- Group Policy Preferences statt Login-Scripts nutzen
- Mit der Kommandozeile
- Mit Powershell

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 10)

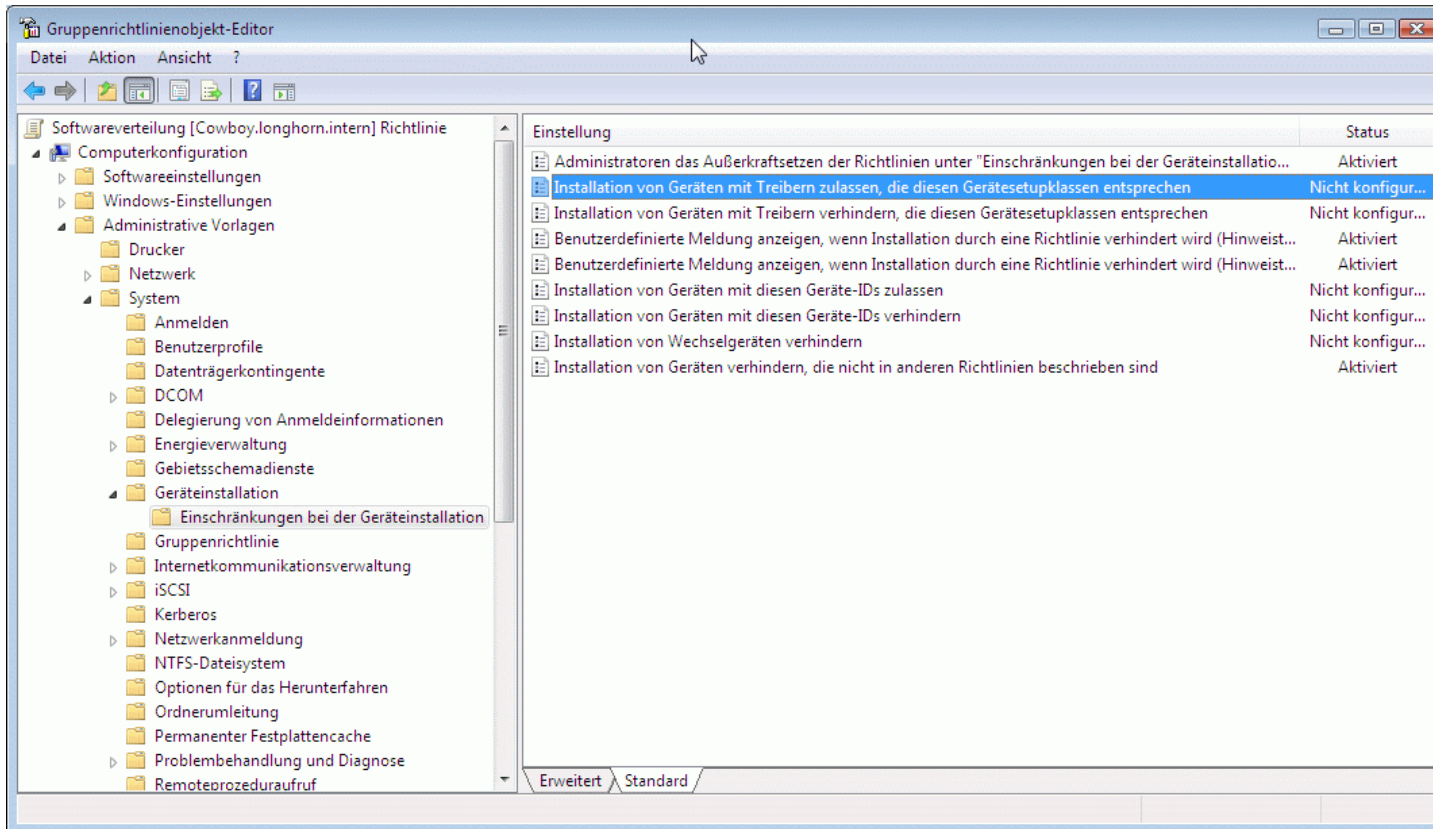
# Treiberinstallation blockieren



- Vista kann Geräte blockieren
- Die Geräte werden anhand Ihrer Geräte-ID erkannt
- Die Konfiguration wird pro Computer vorgenommen
- Administratoren können ausgenommen werden

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 105)

# Computerrichtlinien

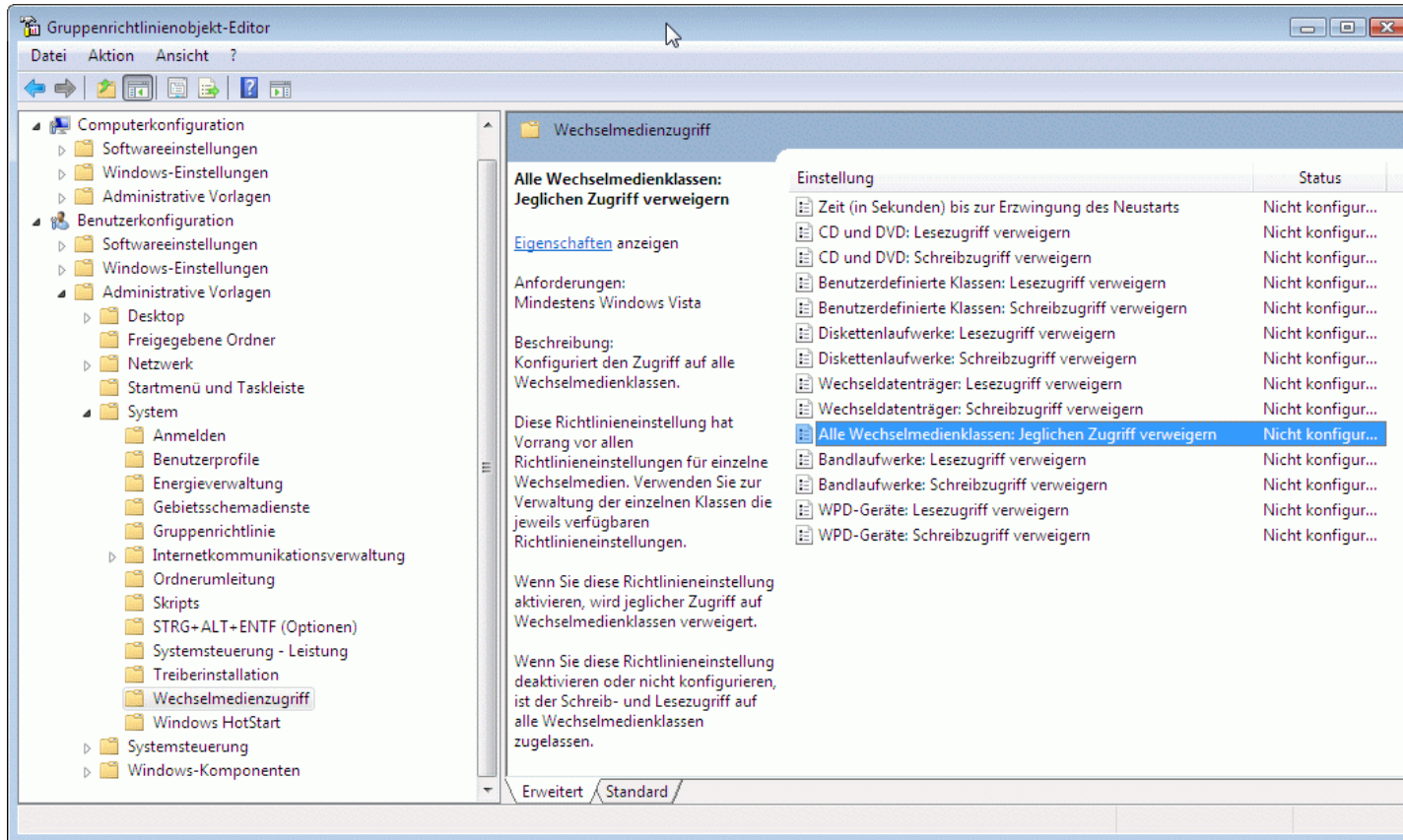


The screenshot shows the Group Policy Editor window. The left pane displays a tree view of policy categories, with 'Einschränkungen bei der Geräteinstallation' selected. The right pane shows a list of policies with their status. The policy 'Installation von Geräten mit Treibern zulassen, die diesen Gerätesetupklassen entsprechen' is highlighted in blue and has a status of 'Nicht konfigur...'.

Einstellung	Status
Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallatio...	Aktiviert
<b>Installation von Geräten mit Treibern zulassen, die diesen Gerätesetupklassen entsprechen</b>	<b>Nicht konfigur...</b>
Installation von Geräten mit Treibern verhindern, die diesen Gerätesetupklassen entsprechen	Nicht konfigur...
Benutzerdefinierte Meldung anzeigen, wenn Installation durch eine Richtlinie verhindert wird (Hinweist...	Aktiviert
Benutzerdefinierte Meldung anzeigen, wenn Installation durch eine Richtlinie verhindert wird (Hinweist...	Aktiviert
Installation von Geräten mit diesen Geräte-IDs zulassen	Nicht konfigur...
Installation von Geräten mit diesen Geräte-IDs verhindern	Nicht konfigur...
Installation von Wechselgeräten verhindern	Nicht konfigur...
Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind	Aktiviert

In dieser Richtlinie kann die Installation aller Treiber oder bestimmter Geräteklassen für alle Benutzer dieses Rechners (!) deaktiviert werden. Als einzige Ausnahme kann man den Administrator angeben.

# Medienzugriff sperren



In der Benutzerkonfiguration kann der lesende und schreibende Zugriff auf Gerätetypen blockiert werden.



# Internet-Explorer-Einstellungen

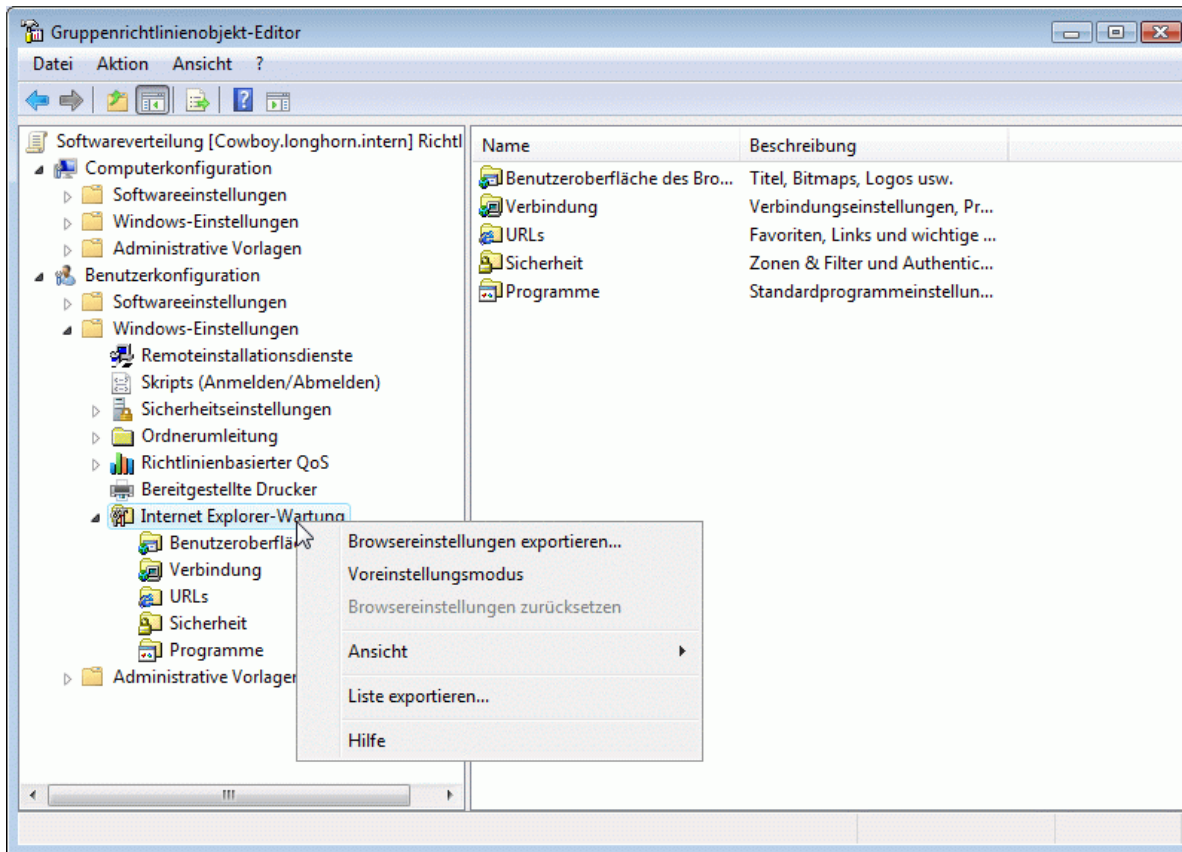
- Der IE kann über die Benutzer-Einstellungen konfiguriert werden
- Mit dem Voreinstellungs-Modus (Rechtsklick auf Internet Explorer Wartung) können weitere Einstellungen vorgenommen werden
- Bis Win XP muß man für umfangreichere Einstellungen das IEAK installieren
- Seit Vista ist das IEAK vollständig implementiert
- **Mit IE 10 wird die Internet-Explorer Wartung komplett deaktiviert. IE-Einstellungen sind dann nur noch über Group Policy Preferences möglich!**

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
weisen (↑ R 103)



**Netz-Weise**  
Lernen von den Besten.

# IE-Wartung im den Richtlinien



## Administrative Vorlagen

- Administrative Vorlagen stellen eine Unmenge an Einstellungen zur Verfügung
- Die Administrativen Vorlagen sind durchweg Registry-Werte, die auf dem Client angewendet werden
- Achtung! In den Einstellungen der Vorlagen kommt häufig eine doppelte Verneinung vor!



## Einstellungen suchen und finden

- Microsoft stellt für jedes Betriebssystem eine Excel-Datei mit den Richtlinien-Einstellungen zur Verfügung
- Durch die Excel-Datei kann per Stichwort nach Einstellungen gesucht werden
- “Group Policy Settings Reference” als Download bei Microsoft
- GPSearch-Website bei Windows Azure

Group Policy Settings Reference for Windows and Windows Server  
<http://www.microsoft.com/en-us/download/details.aspx?id=25250>

weise (klug); Weisse, wei  
-n, -n; ↑ R 5 ff. (kluger Me  
weisen



**Netz-Weise**  
Lernen von den Besten.

# Group Policy Search



Tree Filter Copy Misc printer Deutschland (Deutsch)

### Policy Tree

- Neue Drucker automatisch in Active Directory veröffentlichen
- Nicht wieder veröffentlichte Drucker löschen
- Nur Point-and-Print für Pakete verwenden
- Point-and-Print für Pakete - Genehmigte Server
- Point-and-Print-Einschränkungen
- Point-and-Print-Verbindung auf die Suche in Windows Update ausdehnen
- Veröffentlichungsstatus überprüfen
- Verzeichnislöschintervall
- Verzeichnislöschpriorität
- Verzeichnislöschwiederholungen
- Verzeichnislöschwiederholungsversuche protokollieren
- Vom Druckertreiber gemeldete Kompatibilitätseinstellung zur Ausführung des Druckertreibers außer Kr
- Webbasiertes Drucken**
- Freigegebene Ordner
- Microsoft Office
- Netzwerk
- Startmenü und Taskleiste
- System
- Systemsteuerung
- Windows-Komponenten

### Search results

- Webbasiertes Drucken
- Neue Drucker automatisch in Active Directory veröffentlichen
- Benutzerdefinierte Support-URL im linken Fensterbereich des Ordners
- Druckerinstallations-Assistent - Netzwerksuchseite (Verwaltetes Netzwerk)
- Netzwerk nach Druckern durchsuchen
- Druckaufträge auf dem Server immer wiedergeben
- Löschen von öffentlichen Druckern zulassen
- Websites nach Druckern durchsuchen
- Installation von Druckern, die Kernelmodultreiber verwenden, nicht
- Hinzufügen von Druckern verhindern
- Löschen von Druckern verhindern
- Druckerinstallations-Assistent - Netzwerksuchseite (Nicht verwaltetes
- Nur Point-and-Print für Pakete verwenden
- Point-and-Print für Pakete - Genehmigte Server
- Nur Point-and-Print für Pakete verwenden
- Point-and-Print für Pakete - Genehmigte Server
- Computerstandort
- Druckerstandortsuchtext im Vorhinein ausfüllen
- Point-and-Print-Einschränkungen
- Point-and-Print-Einschränkungen
- Standardpfad in Active Directory für die Suche nach Druckern
- Nach Druckern suchen

### Details

Policy	Webbasiertes Drucken
Category Path	Computer Configuration\Administrative Templates\Drucker\
Supported On	Microsoft Windows 2000 only
Registry Key	HKLM\Software\Policies\Microsoft\Windows NT\printer
Value	DisableWebPrinting

### Explanation

Bestimmt, ob Internetdrucken auf diesem Server aktiviert ist.

Internetdrucken ermöglicht die Anzeige von Druckern auf Webseiten, sodass Drucker über das Internet oder ein Intranet angezeigt, verwaltet und verwendet werden können.

Internetdrucken ist eine Erweiterung der Internetinformationsdienste (IIS). Damit Internetdrucken verwendet werden kann, muss IIS installiert sein und müssen Druckunterstützung sowie diese Einstellung aktiviert sein.

Hinweis: Diese Einstellung gilt nur für das serverseitige Internetdrucken. Die Einstellung verhindert nicht, dass auf dem Druckclient auf dem Computer über das Internet gedruckt wird.

Weitere Informationen finden Sie unter der Einstellung "Benutzerdefinierte Support-URL im linken Fensterbereich des Ordners 'Drucker'" in diesem Ordner und unter der Einstellung "Websites nach Druckern durchsuchen" unter "Benutzerkonfiguration\Administrative Vorlagen\Systemsteuerung\Drucker".

<http://gpsearch.azurewebsites.net/>



# GPO Settings Reference

**Sicherheitswarnung** Datenverbindungen wurden deaktiviert. Optionen...

A1 Group Policy Settings Reference

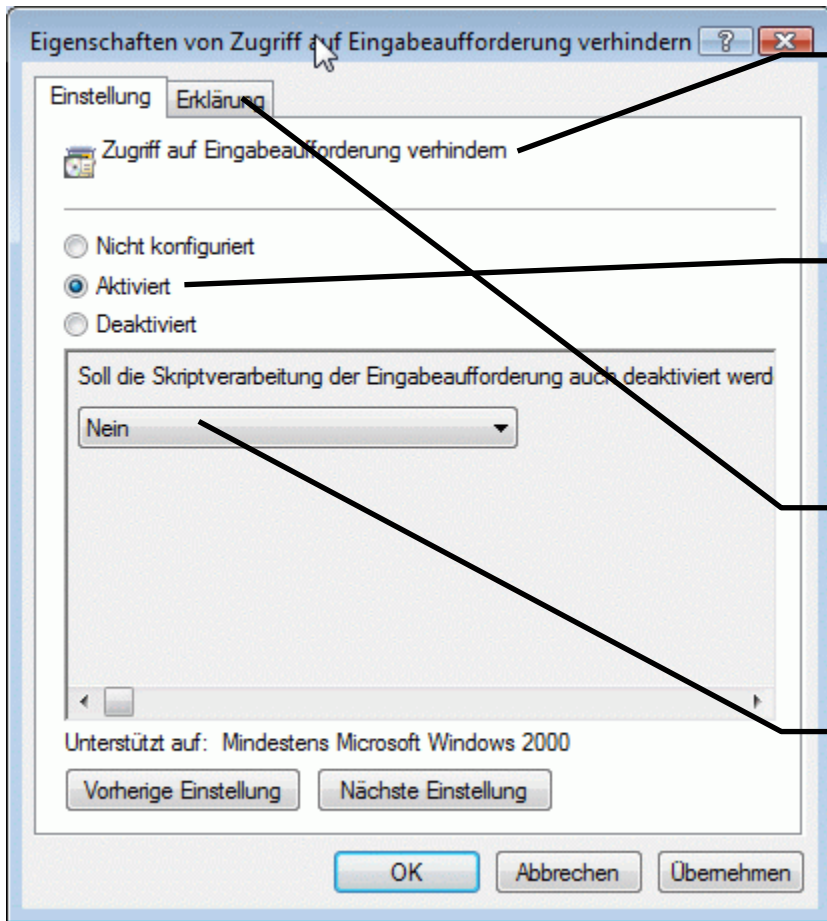
	A	B	C
1	<b>Group Policy Settings Reference</b>		
2	<b>Version 1.3 Windows Server 2003 Service Pack 1</b>		
3			
4	This spreadsheet lists the policy settings for computer and user configurations included in the Administrative Template (.adm) files delivered with		
5	<b>Windows Server 2003 Service Pack 1</b> . The policy settings included cover Windows Server 2003, Windows XP Professional,		
6	and Windows 2000. These .adm files are used to expose policy settings when you edit Group Policy objects		
7	(GPOs) in the Group Policy Object Editor (also known as GPEdit).		
8			
9	The Security Settings worksheet includes information about Account Policies (Password Policy, Account Lockout Policy, and Kerberos Policy), Local Policies (Audit Policy, User		
10	Rights Assignment, and Security Options), Event Log, Restricted Groups, System Services, Registry, and File System policy settings. Note: This does not include security settings		
11	that exist outside of the Security Settings extension (scecli.dll), such as Wireless Network extension, Public Key Policies, or Software Restriction Policies.		
12			
13	Each .adm file is represented by a single worksheet within this spreadsheet. In addition, a worksheet containing all policy settings, called <b>All</b> , is provided for ease		
14	of reference. By using the ADM Parser utility (admx.msi, available from the Microsoft Web site), you can import		
15	custom .adm files into the spreadsheet to reflect your specific environment. For more information, see the ADM Parser utility Help.		
16			
17	You can use the filtering capabilities included in this spreadsheet to view a specific subset of data based on one or a combination of		
18	values available in one or more of the columns. In addition, you can select <b>Custom</b> in the drop-down list of any of the column		
19	headings to add additional filtering criteria within that column. To view a specific subset of data, click the drop-down arrow in the		
20	column heading cells that contain the value, or combination of values, on which you want to filter, and then click the desired value in the		
21	drop-down list. For example, to view a subset of policy settings that are available through the Inetres.adm template and viewed under the		
22	Computer Configuration node, in the <b>All</b> worksheet, click <b>.adm File</b> , click <b>Inetres.adm</b> , and then, in <b>Computer/User Node</b> , click <b>MACHINE</b> .		
23			
24	<b>Legal Notice</b>		
25	The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication.		
26	Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot		
27	guarantee the accuracy of any information presented after the date of publication.		
28	The information contained in this document relates to pre-release software product, which may be substantially modified before its first commercial release.		
29	Accordingly, the information may not accurately describe or reflect the software product when first commercially released.		
30	This document is provided for informational purposes only, and Microsoft makes no warranties, express or implied, with respect to this document or the information contained in it.		
31	This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.		
32	This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.		
33	Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in		
	or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for		
	any purpose, without the express written permission of Microsoft Corp.		

Instructions All System.adm Inetres.adm conf.adm Wuau.adm Wmplayer.adm Update History Security Settings WinXP; W\$

Bereit 100%

weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 10)

# Administrative Vorlagen konfigurieren



Diese Richtlinie verbietet das Benutzen der Eingabeaufforderung

Ist die Richtlinie **aktiviert**, wird der Zugriff auf die Eingabeaufforderung verhindert (Doppelte Verneinung!)

Hier steht bei allen vordefinierten Richtlinien eine Erklärung der Funktion

Hier können zusätzliche Einstellungen stehen. In diesem Fall: Batch-Dateien (und Login-Scripte) werden nicht verhindert



# Gruppenrichtlinien-Funktionen

- Filtern mit Berechtigungen
- WMI-Filter (ab XP)
- Resultant Set of Policies (ab XP)
- Richtlinien-Vererbung
- Erzwingen von Richtlinien (No Override)





## Filtern mit Berechtigungen

- Die Berechtigung „Gruppenrichtlinie übernehmen“ steuert, auf wenn eine Richtlinie angewendet wird
- „Authentifizierte Benutzer“ haben das Recht standardmäßig
- Erlaubt das Ausnehmen von Admins
- Gut zur Softwareverteilung nutzbar
- Sollte mit Vorsicht genossen werden

## WMI-Filter

```
Select * from Win32_ComputerSystem where manufacturer = "Toshiba" and  
Model = "Tecra 800" OR Model = "Tecra 810"
```

- Erlauben anhand von WMI-Queries das Anwenden von Richtlinien
- WMI-Queries ähneln SQL-Abfragen und fragen Hardware-Informationen des Rechners ab
- Ergibt eine WMI-Abfrage „true“, wird die Richtlinie angewendet
- WMI-Filter werden erst ab XP unterstützt

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

Da Windows 2000 keine WMI-Filter unterstützt, werden Richtlinien mit WMI-Filter auf Windows 2000 Betriebssystemen immer angewendet, unerheblich davon, ob die WMI-Abfrage für den Rechner wahr oder falsch ist.

Weiterführende Informationen und Beispiele:

GPMC und WMI-Filter

<http://technet2.microsoft.com/WindowsServer/en/library/6237b9b2-4a21-425e-8976-2065d28b31471033.mspx?mfr=true>

WMI Administrative Tools enthält den WMI-Event-Browser, mit dem man sich alle in WMI enthaltenen Objekte und Informationen ansehen kann:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=6430f853-1120-48db-8cc5-f2abdc3ed314&DisplayLang=en>



## Resultant Set of Policies (RSOP)

- Zeigt die auf einem Client tatsächlich angewendeten Richtlinien an
- Steht als MMC-Snap-In zur Verfügung
- Kann über die GPMC verwaltet werden
- Wird auch von gpresult.exe ab Windows XP genutzt : „gpresult /H Results.htm“
- Wird erst seit Windows XP unterstützt

## Richtlinien-Vererbung

- Gruppenrichtlinien verbreiten sich über alle untergeordneten OUs
- Dabei sind die Richtlinieneinstellungen additiv
- Geraten 2 Richtlinien in Konflikt, hat normalerweise die Richtlinie Priorität, die näher am Objekt ist (s. Eingangsfolie 14/15)
- Mit der Vererbungsblockierung können alle übergeordneten Richtlinien geblockt werden

wei|se (klug); 'Weise, die  
-n, -n; ↑ R 5 ff. (kluger Mann  
Weisen (↑ R 108)



**Gruppenrichtlinienverwaltung**

Verknüpfte Gruppenrichtlinienobjekte Gruppenrichtlinienvererbung Delegation

Die Liste enthält keine mit Standorten verknüpften Gruppenrichtlinienobjekte. Weitere Informationen erhalten Sie in der Hilfe.

Rangfolge	Gruppenrichtlinienobjekt	Speicherort	Objektstatus	WMI-Filter
1	UC_HR_Default	HR	Aktiviert	Keine

## Erzwingen von Richtlinien

- Erzwingen (in Windows 2000 fälschlich als „Kein Vorrang“ übersetzt) erhöht die Priorität einer Richtlinie
- Eine erzwingen Richtlinie überschreibt Einstellungen aller untergeordneten konkurrierenden Richtlinien
- Erzwangene Richtlinien ignorieren die Vererbungsblockierung
- Erzwangene Richtlinie sollten **mit Vorsicht** eingesetzt werden!

wei|se (klug); Weisheit, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 105)



**Netz-Weise**  
Lernen von den Besten.

Tatsächlich werden Richtlinien nacheinander abgearbeitet, beginnend beim Standard über die Domänenrichtlinie zu den Richtlinien auf Organisationseinheiten. Eine Richtlinie, die später angewendet wird, überschreibt eventuell konkurrierende Einstellungen. Wird eine Richtlinie erzwungen, wird diese schlicht immer als Letzte abgearbeitet.

Werden Richtlinien erzwungen, obwohl dies nicht unbedingt notwendig ist, führt dies früher oder später zum Chaos. Daher sind erzwungen Richtlinien im Normalfall zu meiden.

Ein sinnvoller Einsatzzweck von Richtlinien wäre dann gegeben, wenn eine Firmenvorschrift eine bestimmte Einstellung AUF JEDEN FALL erfordert. Dann kann eine Richtlinie auf Domänenebene erzwungen werden, die auch nicht versehentlich überschrieben werden kann.



weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man...  
Weisen (↑ R 105)



**Netz-Weise**  
Lernen von den Besten.

# Durchbrechen der Vererbung...

Rangfolge	Gruppenrichtlinienobjekt	Speicherort	Objektstatus	WMI-Filter
1 (Erzungen)	Firewall	Netzweise.com	Aktiviert	Keine
2	UC_HR_Default	HR	Aktiviert	Keine

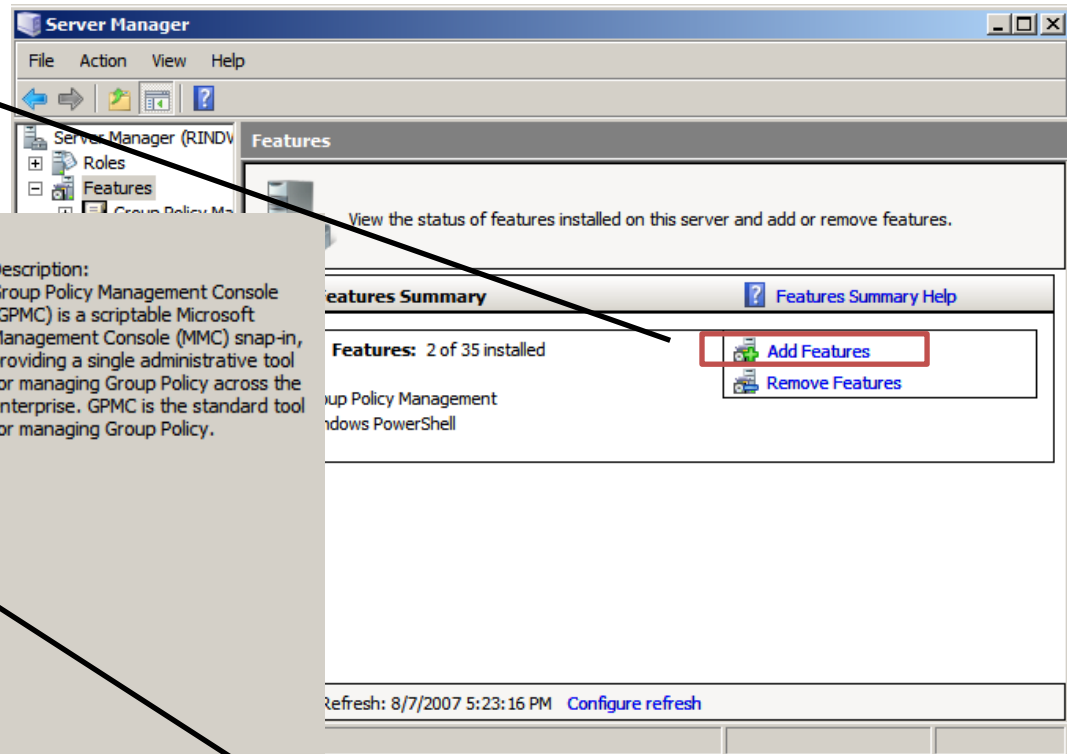


## Verwaltungsfunktionen der GPMC

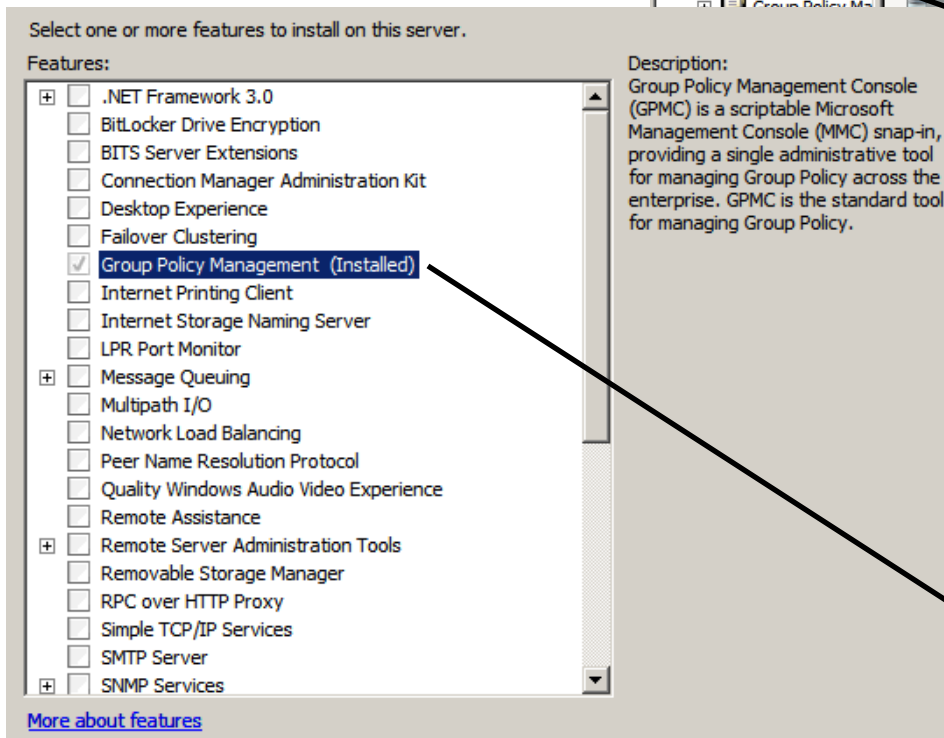
- Richtlinien-Berichte
- Sicherheitsfilterung und Delegation
- WMI-Filter
- Sichern und Wiederherstellen von Richtlinien
- Import von Richtlinieneinstellungen
- Gruppenrichtlinienmodellierung
- Resultant Set of Policies
- Gruppenrichtlinien-Scripting

# GPMC unter Server 2008 installieren

(1) Im Server-Manager  
„Add Feature“ wählen



(2) Im Add-Feature-Wizard  
GPMC auswählen



## Richtlinien-Berichte

- Richtlinien-Berichte zeigen nur die tatsächlich vorgenommen Einstellungen an
- Berichte lassen sich als Dokumentation im Format HTML oder XML speichern
- Ein Bericht sollte nach jeder Änderung einer Richtlinie erstellt und zentral gespeichert werden

# Sicherheitsfilterung und Delegation

- Filterung erlaubt das Anwenden auf bestimmte Gruppen
- Es gibt Konzepte, die Gruppenrichtlinien auf Domänenebene verwalten und die Richtlinien per Domänen-Gruppe zuweisen
- Mit der Filterung ist es möglich, die Admins aus Richtlinien zu entfernen
- Gutes Konzept für Softwareverteilung

Die Kombination, Richtlinien mit OU-Strukturen zu verwalten und zusätzlich mit Sicherheitsfiltern zu versehen, ist aus meiner Erfahrung grundsätzlich problematisch. Die Übersicht geht bei einer Kombination beider Systeme verloren, es sei denn, man hat eine strikte Trennung nach Funktionen.

weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mann)  
Weisen (↑ R 105)



## Filtern, sieben und aussortieren

**Group Policy Management**

File Action View Window Help

Domains

- Netzweise.com
  - Default Domain Po
  - Firewall
  - SD-SpecopsGPE
  - specops
- Domain Controller
- Service Accounts
- Group Policy Object
- Starter GPOs
- Sites

**specops**

Scope: Details Settings Delegation

**Links**

Display links in this location: Netzweise.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Netzweise.com	No	Yes	Netzweise.co

**Security Filtering**

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

**WMI Filtering**

This GPO is linked to the following WMI filter:

WMI Filter
<none>
Win7
Win8





## Backup / Restore von Richtlinien

- Mit der GPMC können Sicherungen von Gruppenrichtlinien angelegt werden
- Das Backup enthält alle Daten aus dem Sysvol-Ordner und zusätzliche Verwaltungsinformationen in Form von XML-Dateien
- Mit einer Richtliniensicherung können zerstörte Richtlinien und alte Stände wiederhergestellt werden
- Eine Sicherung kann auch zum Richtlinienexport genutzt werden
- Nicht gesichert werden IPSEC-Einstellungen und WMI-Filter (liegen im AD)



## Backup / Restore mit Powershell

- Windows Powershell hat ein Modul „GroupPolicy“ mit cmdlets zur Richtlinienverwaltung
- „Get-gpo -All“ zeigt alle Richtlinien an
- „Backup-gpo -Path Pfad“ sichert Richtlinien
- „Get-gpo -ALL | Backup-gpo -Path Pfad“ sichert alle Richtlinien



# Import von Richtlinienereinstellungen

- Die GPMC erlaubt den Import von Richtlinien
- Der Import erfolgt immer in eine bestehende Richtlinie
- Die Vorlage für den Import ist die Sicherung einer bestehenden Richtlinie
- Beim Import werden Daten in eine neue Richtlinie geladen. Evtl. Bestehende Einstellungen werden dabei überschrieben
- Importtabellen unterstützen den Import von Berechtigungen, indem die SID's der Original-Domäne in die SID's der Zieldomäne übersetzt werden

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 103)



**Netz-Weise**  
Lernen von den Besten.

# Sichern und Importieren

The screenshot shows the Group Policy Management console with the 'Firewall-Konfiguration' window open. The left pane shows the tree structure under 'nwtraders.net'. The right pane shows the configuration for 'Workstations'. A context menu is open over the 'Firewall-Konfiguration' object, with 'Sichern...' and 'Einstellungen importieren...' highlighted in red.

**Firewall-Konfiguration**

Bereich Details Einstellungen Delegierung

**Verknüpfungen**

Für dieses Verzeichnis anzeigen: nwtraders.net

Die folgenden Standorte, Domänen und Organisationseinheiten sind mit dem Objekt verknüpft:

Pfad	Erzungen	Verknüpfung aktiviert	Pfad
Workstations	Nein	Ja	nwtraders.net/Braunschweig/Workstations

Context menu options:

- Bearbeiten...
- Status der Gruppenrichtlinie
- Sichern...**
- Von Sicherung wiederherstellen...
- Einstellungen importieren...**
- Bericht speichern...
- Ansicht
- Neues Fenster
- Kopieren
- Löschen
- Umbenennen
- Aktualisieren
- Hilfe

Buttons: Entfernen, Eigenschaften, Öffnen

Status bar: **Sichert das Gruppenrichtlinienobjekt.**



# Gruppenrichtlinienmodellierung

## Gruppenrichtlinienmodellierung...

- ähnelt von der Funktionalität RSOP
- vereinfacht das Planen von Richtlinien
- benötigt einen Domänencontroller mit W2k3
- simuliert die Abarbeitung der Richtlinien auf dem Client
- kann auch zum Troubleshooting für W2k verwendet werden

weise (klug); Weise, Weisheit  
 -n, -n; ↑ R 5 ff. (kluger Mensch)  
 Weisheit (R 10)



**Netz-Weise**  
 Lernen von den Besten.

# Resultant Set of Policies

**hvoges auf VS2005**  
 Daten ermittelt am: 22.03.2006 13:49:58

**Zusammenfassung der Computerkonfiguration**

**Allgemein**

Computername	NWTRADERS\VS2005
Domäne	nwtraders.net
Standort	Standardname-des-ersten-Standorts
Gruppenrichtlinie zuletzt verarbeitet am	22.03.2006 13:32:09

**Gruppenrichtlinienobjekte**

**Angewendete Gruppenrichtlinienobjekte**

Name	Verknüpfungsstandort	Revision
Default Domain Policy	nwtraders.net	AD (3), Sysvol (3)
Firewall-Konfiguration	nwtraders.net/Braunschweig/Workstations	AD (2), Sysvol (2)
Windows Update	nwtraders.net/Braunschweig/Workstations	AD (8), Sysvol (8)

**Abgelehnte Gruppenrichtlinienobjekte**

Name	Verknüpfungsstandort	Grund: abgelehnt
Richtlinien der lokalen Gruppe	Local	Leer

**Sicherheitsgruppenmitgliedschaft bei Anwendung der Gruppenrichtlinie**

- VORDEFINIERT\Administratoren
- Jeder
- VORDEFINIERT\Benutzer
- NWTRADERS\VS2005\$
- NWTRADERS\Domänencomputer
- NT-AUTORITÄT\NETZWERK
- NT-AUTORITÄT\Authentifizierte Benutzer

**WMI-Filter**

Name	Wert	Gruppenrichtlinienobjekt-Referenz
nur XP SP2	Wahr	Firewall-Konfiguration

**Komponentenstatus**

Komponentenname	Status	Letzter Prozess am
Gruppenrichtlinieninfrastruktur	Erfolgreich	22.03.2006 13:32:17
EFS recovery	Erfolgreich (keine Daten)	27.02.2006 14:21:05
Registrierung	Erfolgreich	22.03.2006 13:32:17
Security	Erfolgreich	27.02.2006 14:21:05

**Zusammenfassung der Benutzerkonfiguration**

**Allgemein**

**Gruppenrichtlinienobjekte**

**Windows Update**  
 Daten ermittelt am: 22.03.2006 12:43:48

**Administrative Vorlagen**

**Windows-Komponenten/Windows Update**

Richtlinie	Einstellung
Automatische Updates sofort installieren	Deaktiviert
Clientseitige Zielzuordnung aktivieren	Aktiviert
Zielgruppenname für diesen Computer	Server
Erneut zu einem Neustart für geplante Installationen auffordern	Aktiviert
Folgendes Zeitraum (in Minuten) warten, bevor zu einem Neustart aufgefordert wird.	10
Internen Pfad für den Microsoft Updatedienst angeben	Aktiviert
Interner Updatedienst zum Ermitteln von Updates:	http://wvusserver1
Intranetserver für die Statistiken (Beispiel: http://Intranet/Upd01)	http://wvusserver1
Neustart für geplante Installationen verzögern	Aktiviert
Folgendes Zeitraum (in Minuten) warten, bevor ein geplanter Neustart ausgelöst wird.	5
Nicht-Administratoren gestatten, Updatebenachrichtigungen zu erhalten	Deaktiviert
Zeitplan für geplante Installationen neu erstellen	Aktiviert
Wartezeit nach Systemstart (Minuten):	1

**Benutzerkonfiguration (Aktiviert)**

Keine Einstellungen definiert

weise (klug); Weise, -n; ↑ R 5 ff. (kluger Mensch); weisen (↑ R 10 ff.)



# Powershell-gpo-Commandlets

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> get-command -Module GroupPolicy

CommandType      Name                                     ModuleName
-----
Alias             Get-GPPermissions                      GroupPolicy
Alias             Set-GPPermissions                      GroupPolicy
Cmdlet            Backup-GPO                             GroupPolicy
Cmdlet            Copy-GPO                               GroupPolicy
Cmdlet            Get-GPInheritance                      GroupPolicy
Cmdlet            Get-GPO                                GroupPolicy
Cmdlet            Get-GPOReport                          GroupPolicy
Cmdlet            Get-GPPermission                       GroupPolicy
Cmdlet            Get-GPPrefRegistryValue                GroupPolicy
Cmdlet            Get-GPRegistryValue                    GroupPolicy
Cmdlet            Get-GPResultantSetOfPolicy             GroupPolicy
Cmdlet            Get-GPStarterGPO                       GroupPolicy
Cmdlet            Import-GPO                              GroupPolicy
Cmdlet            Invoke-GPUpdate                         GroupPolicy
Cmdlet            New-GPLink                              GroupPolicy
Cmdlet            New-GPO                                 GroupPolicy
Cmdlet            New-GPStarterGPO                       GroupPolicy
Cmdlet            Remove-GPLink                           GroupPolicy
Cmdlet            Remove-GPO                              GroupPolicy
Cmdlet            Remove-GPPrefRegistryValue             GroupPolicy
Cmdlet            Remove-GPRegistryValue                 GroupPolicy
Cmdlet            Rename-GPO                              GroupPolicy
Cmdlet            Restore-GPO                             GroupPolicy
Cmdlet            Set-GPInheritance                      GroupPolicy
Cmdlet            Set-GPLink                              GroupPolicy
Cmdlet            Set-GPPermission                       GroupPolicy
Cmdlet            Set-GPPrefRegistryValue                GroupPolicy
Cmdlet            Set-GPRegistryValue                    GroupPolicy

PS C:\Users\Administrator> _
```

## Funktionsweise (DC)

- Richtlinien werden auf dem Server im Ordner %Systemroot%\sysvol\sysvol\`“Domäne“\Policies` abgelegt
- Jede Policy wird über eine GUID referenziert
- In jeder Policy ist ein Ordner Machine (Computerrichtlinien) und ein Ordner User (Benutzerrichtlinien) angelegt
- Die Datei gpt.ini im Stamm der Policy enthält die Versionsnummer der Richtlinie
- Der Ordner Sysvol wird zwischen den DC per FRS bzw. DFS-Replikation (Server 2008) repliziert



## Funktionsweise (AD)

- Für jede Policy ist im Container System\Policies ein Objekt angelegt
- Jede OU und jedes Domänen-Objekt besitzt ein Attribut gPLink, das den LDAP-Pfad zu allen verknüpften Policies beinhaltet

## Funktionsweise (Client)

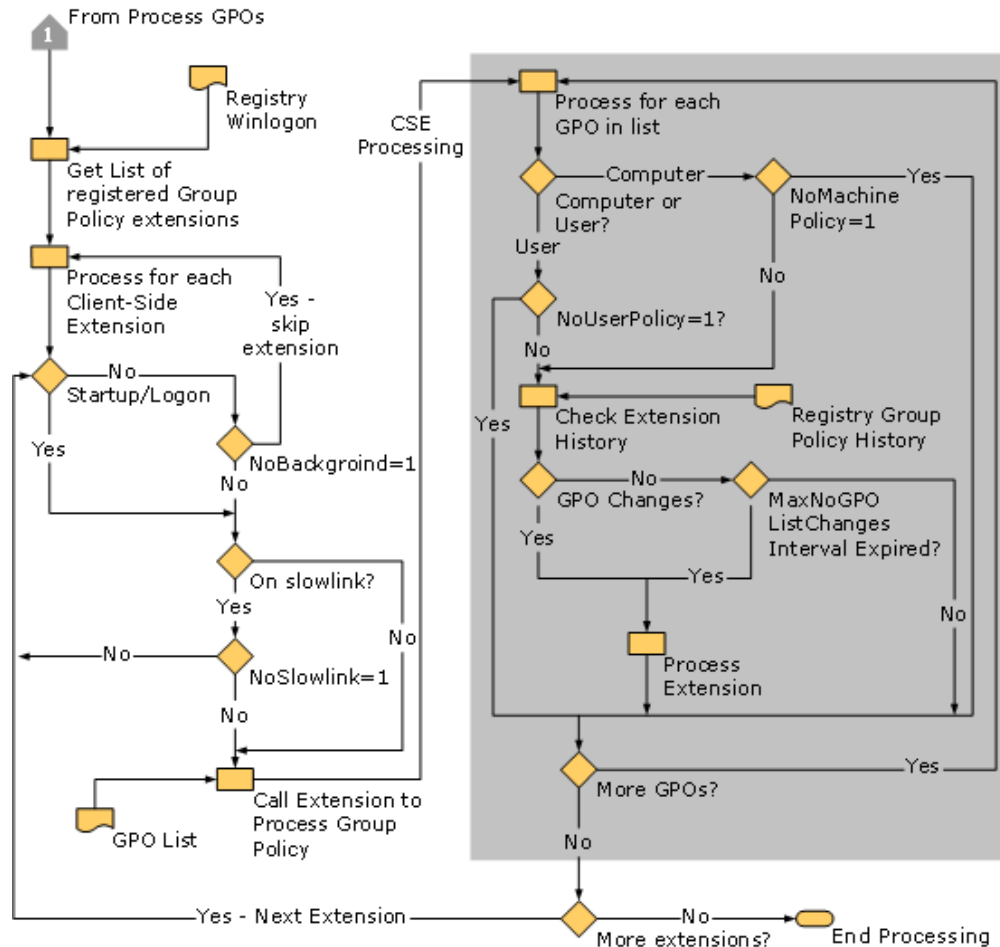
- Bei der Anmeldung fragt der Client alle Richtlinien vom AD ab, die für den Benutzer / Computer angewendet werden müssen
- Der Computer lädt die Richtlinien vom Anmeldeserver aus der Freigabe sysvol herunter
- Die Anmeldedienst (Win 2000 / XP) bzw. Gruppenrichtliniendienst (ab Vista) wendet die Richtlinieneinstellungen ab
- Das Ausführen der Änderungen findet über Client Side Extensions statt



weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mann)  
Weisen (↑ R 108)



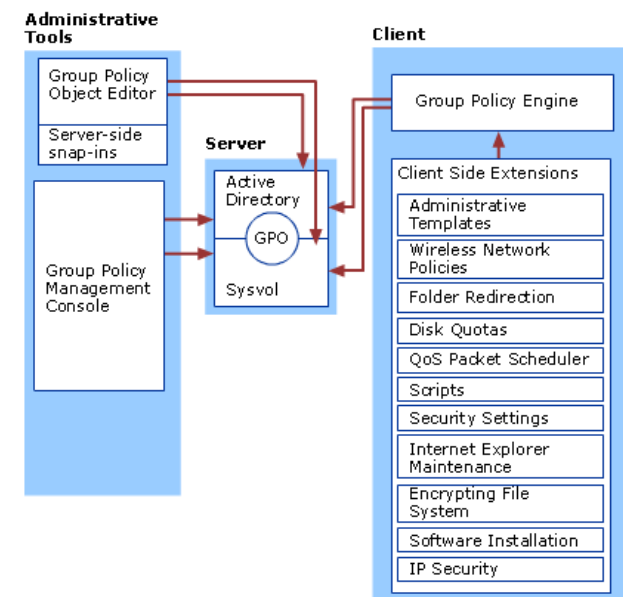
# Ablauf einer Anmeldung





## Client Side Extensions

- Client Side Extensions (CSE's) werden beim Start vom Gruppenrichtliniendienst / Netlogon geladen werden
- Die installierten CSE stehen in der Registry:  
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions
- Die CSE's werden in der Reihenfolge aufgerufen, in der Sie in der Registry aufgelistet sind



## Was passiert auf dem Client?

- Gruppenrichtlinien werden zeitgesteuert angewendet
- Welche Richtlinien angewendet werden, hängt von der Netzwerkanbindung ab
- Ein Großteil der Richtlinien wird in der Registry hinterlegt
- Seit Windows 2000 gibt es spezielle Schlüssel für Policies

## Aktualisieren der Richtlinien

- GPupdate erzwingt unter Windows XP das Überprüfen auf neue Richtlinien
- GPupdate /force aktualisiert alle Richtlinieneinstellungen. Sonst werden nur nur neue oder geänderte Richtlinien angewendet.
- Ab Windows Server 2012 kann über die GPMC auf OUs das Update erzwungen werden
- Specops GPUpdate ermöglicht eine Aktualisierung der Gruppenrichtlinien auf allen Clients zu erzwingen
- Specops GPUpdate ist kostenlos!
- **Download:** <http://www.specopssoft.com/products/specopsgpupdate/default.asp>

## Langsame Netzwerkverbindungen

- Windows kann anhand der Geschwindigkeit der Netzwerkverbindung einzelne Funktionen deaktivieren
- Die Netzwerkgeschwindigkeit wird bis Windows XP mit einem Ping bestimmt
- Seit Windows Vista kommt der Network Location Awareness Dienst zum Einsatz

# Erkennung mit ICMP (Ping)

1. Ping the server with 0 bytes of data and time the number of milliseconds. This value is time#1. If it is less than 10 ms, exit (assume a fast link).
2. Ping the server with 2 KB of uncompressible data, and time the number of milliseconds. This value is time#2. The algorithm uses a compressed .jpg file for this
3.  $\text{DELTA} = \text{time\#2} - \text{time\#1}$ . This removes the overhead of session setup, with the result being equal to the time to move 2 KB of data
4. Calculate Delta three times, adding to TOTAL each DELTA value.
5.  $\text{TOTAL}/3 = \text{Average of DELTA, in milliseconds.}$
6.  $2 * (2 \text{ KB}) * (1000 \text{ millisec/sec}) / \text{DELTA Average millisec} = X$
7.  $X = (4000 \text{ KB/sec}) / \text{DELTA Average}$
8.  $Z \text{ Kilobits per second (Kbps)} = (4000 \text{ KB/sec}) / \text{DELTA Average} * (8 \text{ bits/byte})$
9.  $Z \text{ Kbps} = 32000 \text{ kbps/Delta Avg.}$

Eine genaue Beschreibung des Anmeldeprozesses findet sich hier:

<http://technet2.microsoft.com/WindowsServer/en/library/89d7ec5f-a909-4f61-aded-c5b69f5f730b1033.msp?mfr=true>

## Network Location Awareness

- Network Location Awareness erlaubt Zugriff auf Ressourcen-Verfügbarkeit und Betriebssystem-Ereignisse:
  - Aufwachen aus Ruhezustand oder Standby
  - Aufbau einer VPN-Verbindung
  - Verbindungsaufbau mit WLANs
  - Wiederverfügbarkeit von Netzwerkverbindungen
- Unabhängig von der Verfügbarkeit des ICPM-Protokolls

## Richtlinien für Richtlinien

- Ändern Sie niemals die Standardrichtlinien
- Versuchen Sie, das Erzwingen von Richtlinien zu vermeiden
- Nutzen Sie die GPMC, um alle Richtlinien zu dokumentieren
- Planen Sie den Einsatz im Vorfeld gründlich!
- Testen Sie alle Richtlinien vor der Implementierung
- Legen Sie Namenskonventionen fest
- Entscheiden Sie sich für eine Richtlinienkonfiguration per Organisationseinheiten oder Berechtigungs-Filtern
- Anzahl der Richtlinien klein halten (Anmeldezeit!)
- Richtlinien immer mit dem neuesten OS im Einsatz bearbeiten
- Sichern Sie ihre Richtlinien regelmässig



## Erweitern Administrativer Vorlagen

- Sie können Gruppenrichtlinien mit ADM- und ADMX-Dateien selbständig erweitern
- ADM-Dateien legen Registry-Werte fest, die von Richtlinien angewendet werden
- Registry-Werte, die nicht im dafür vorgesehenen Policy-Key abgelegt werden, „tätowieren sich“ in die Registry
- Eine Reihe von Programmen bringen bereits erweiterte ADM-Dateien mit

## ADM-Dateien

- ADM-Dateien sind die Konfigurationsdateien für den Knoten „Administrative Vorlagen“
- Sie beinhalten Einstellungen, die auf dem Client über Registry-Keys angepasst werden
- Sie können manuell erzeugt werden
- Sie werden vom Gruppenrichtlinieneditor gpedit.msc geladen
- Sie werden standardmäßig in Sysvol abgelegt
- Sie sind für die Konfiguration des Clients nicht notwendig

## Funktionsweise von ADMs

- Es gibt 5 Standard-ADM-Dateien:
  - Conf.amd, inetres.adm, system.adm, Wmplayer.adm, Wuau.adm
  - Die Original-ADMs sollten niemals editiert werden!
- ADM-Vorlagen zur Konfiguration von MS Office stehen im Office Resource Kit zur Verfügung
- Viele ADM-Vorlagen sind im Internet verfügbar
- Tattooing bezeichnet den Vorgang, bei dem Registry-Einstellungen aus Richtlinien nach dem Entfernen der Richtlinie in der Registry verbleiben



# Aufbau einer ADM-Datei

```
CATEGORY !!AdministrativeServices

POLICY !!DisableCMD
    KEYNAME "Software\Policies\Microsoft\Windows\System"
    #if version >= 4
    SUPPORTED !!SUPPORTED_Win2k
    #endif

    EXPLAIN !!DisableCMD_Help

    PART !!DisableCMDScripts      DROPDOWNLIST  NOSORT
        VALUENAME "DisableCMD"
        ITEMLIST
            NAME !!DisableCMD_YES      VALUE NUMERIC 1
            NAME !!DisableCMD_NO      VALUE NUMERIC 2 DEFAULT
        END ITEMLIST
    END PART
END POLICY
END CATEGORY ; AdministrativeServices
```

Die Keys in der Registry und die Anzeige in gpedit

Textvariablen aus dem oberen Bereich werden hier definiert

```
[strings] ←
DisableCMD_Help="Verhindert, dass Benutzer die interaktive [...] werden.."
```



## Tools zum Bearbeiten von ADMs

- ADMX aus den Support-Tools
- Reg2ADM speichert Registry Keys als ADM-Dateien
- Editoren zum einfachen Erstellen von ADM-Dateien:
  - ADM Template Editor von Syprosoft
  - Policy Template File Editor
  - ADM Utils (Perl-Scripte)

## ADMX-Dateien

- ADMX-Dateien ersetzen ADM-Dateien
- ADMX-Dateien sind im XML-Format abgelegt
- ADMX-Dateien sind Sprachneutral
- ADML-Dateien sind sprachspezifisch
- ADMX-Dateien können parallel mit ADM-Dateien benutzt werden
- Pfad: %windir%\policyDefinitions\[*MUIculture*]
- Zum Bearbeiten wird OS ab Vista gebraucht



## Bearbeiten von ADMX-Dateien

- ADMX-Dateien sind XML-Dateien und können mit jedem Text-Editor bearbeitet werden
- MS stellt den ADMX-Migrator von Full Armor kostenlos zur Verfügung
- ADMX-Migrator kann ADM-Dateien migrieren
- ADMS-Migrator beinhaltet auch einen ADMX-Editor



Auf der MS-Website finden Sie eine Reihe von Informationen zu ADMX-Files:

Group-Policy Sample ADMX-Files

<http://www.microsoft.com/downloads/details.aspx?FamilyId=3D7975FF-1242-4C94-93D3-B3091067071A&displaylang=en>

Group Policy ADMX Schema files

<http://www.microsoft.com/downloads/details.aspx?FamilyId=B4CB0039-E091-4EE8-9EC0-2BBCE56C539E&displaylang=en>

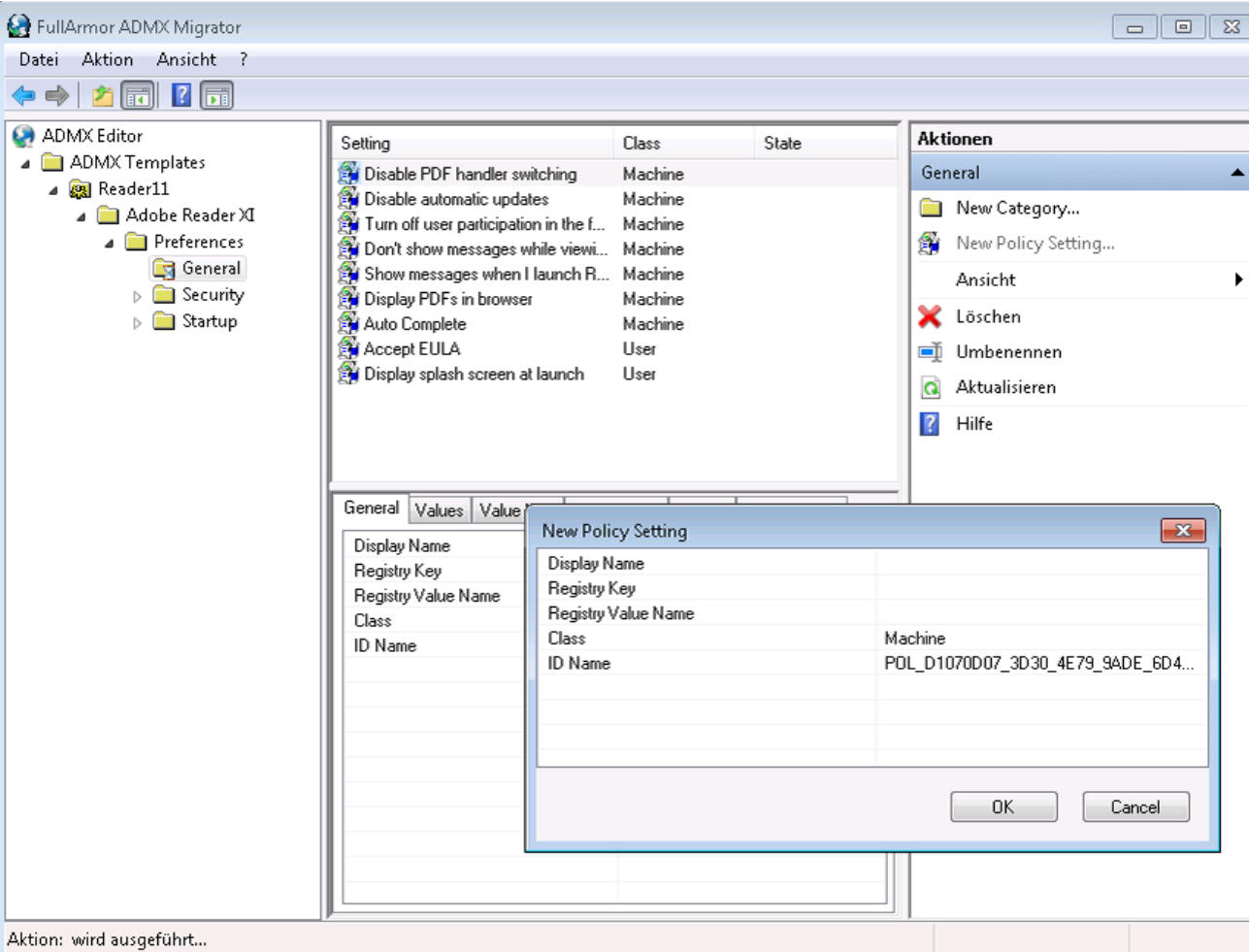
Group Policy ADMX Syntax Reference Guide

<http://technet2.microsoft.com/windowsserver2008/en/library/1db6fd85-d682-4d7d-9223-6b8dfafddc1c1033.msp?mfr=true>



wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man...  
Weisen (↑ R 105)

# Bring your own Policy (ByoP)



The screenshot shows the FullArmor ADMX Migrator application. The main window is titled 'FullArmor ADMX Migrator' and contains an 'ADMX Editor' pane on the left with a tree view showing 'Reader11' > 'Adobe Reader XI' > 'Preferences' > 'General'. The central pane displays a table of settings:

Setting	Class	State
Disable PDF handler switching	Machine	
Disable automatic updates	Machine	
Turn off user participation in the f...	Machine	
Don't show messages while viewi...	Machine	
Show messages when I launch R...	Machine	
Display PDFs in browser	Machine	
Auto Complete	Machine	
Accept EULA	User	
Display splash screen at launch	User	

Below the table is a 'General' tab with fields for 'Display Name', 'Registry Key', 'Registry Value Name', 'Class', and 'ID Name'. A 'New Policy Setting' dialog box is open over this area, with the following fields filled:

Field	Value
Display Name	
Registry Key	
Registry Value Name	
Class	Machine
ID Name	POL_D1070D07_3D30_4E79_9ADE_6D4...

The dialog box has 'OK' and 'Cancel' buttons at the bottom. At the bottom of the main window, a status bar shows 'Aktion: wird ausgeführt...'. The right-hand pane contains an 'Aktionen' (Actions) menu with options like 'New Category...', 'New Policy Setting...', 'Löschen', 'Umbenennen', 'Aktualisieren', and 'Hilfe'.

## ADM /ADMX auf dem Server

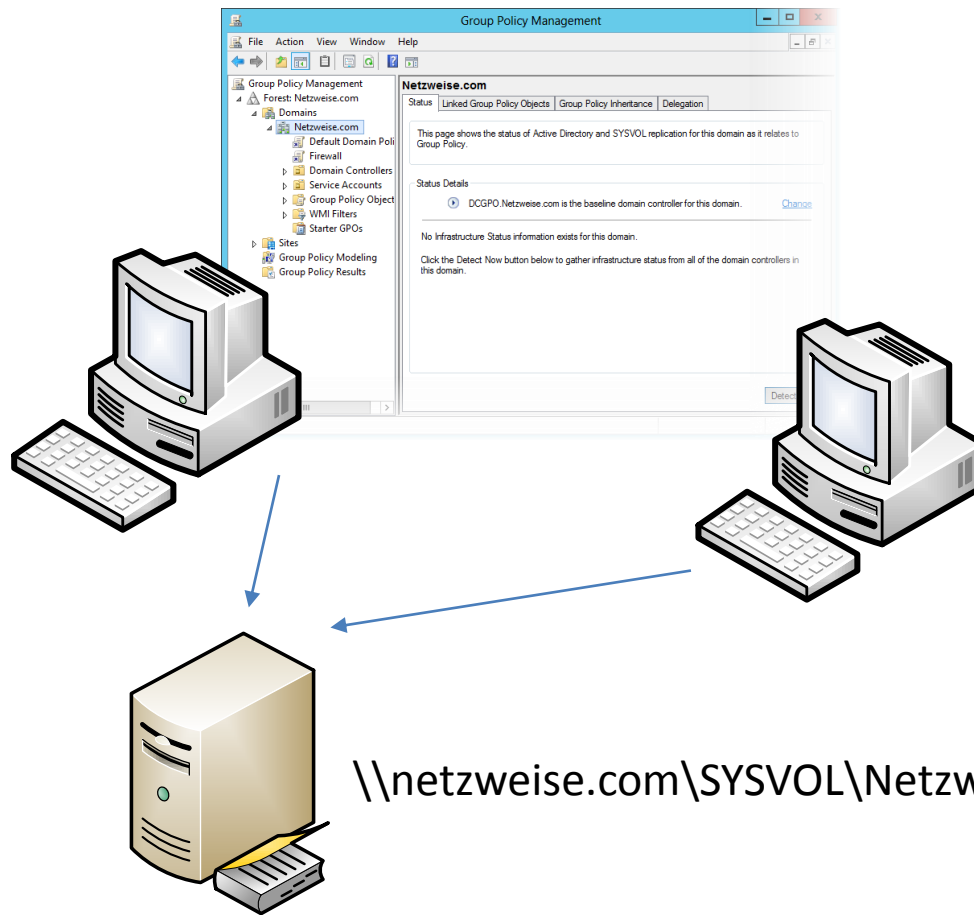
- Beim Anlegen einer Richtlinie werden die ADM-Dateien in die SYSVOL-Freigabe geladen
- Jede Richtlinie legt Ihre ADM-Dateien neu ab
- Dadurch braucht jede Richtlinie ca. 4 MB -> hoher Replikationsverkehr
- ADMX-Dateien können zentral in einem Ordner gespeichert werden (muß manuell angelegt werden , benötigt Longhorn als DC)
- Ab Windows Server 2008 wird DFS-Replikation für SYSVOL-Replikation verwenden

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 105)



**Netz-Weise**  
Lernen von den Besten.

# Ein Speicherort, sie zu knechten

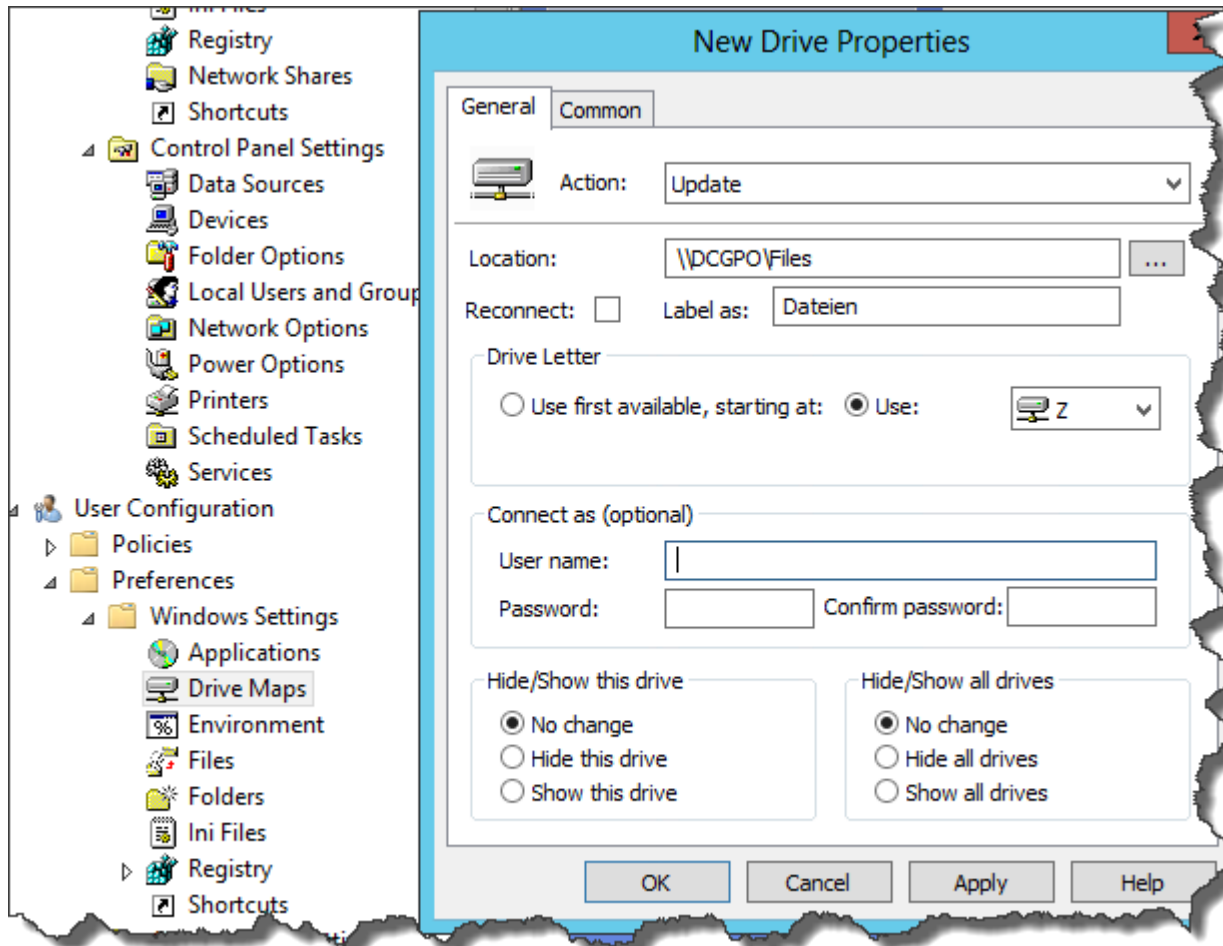


`\\netzweise.com\SYSTEM\Netzweise.com\Policies\PolicyDefinitions`

## Group Policy Preferences

- Seit Windows Server 2008 Bestandteil von Windows
- Zum Einrichten der Client-Umgebung, wie Laufwerk-und Druckermapping, Dateien kopieren, Registry-Einträge anlegen...
- Mit Targetting kann man einschränken, auf welchen Rechnern eine Policy Preference eingerichtet werden soll (wie WMI-Filter)

# Group Policy Preferences



weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 105)



**Netz-Weise**  
Lernen von den Besten.

# Group Policy Preferences - Targetting

**New Drive Properties**

General Common

Options common to all items

- Stop processing items in this extension if an error occurs
- Run in logged-on user's security context (user policy option)
- Remove this item when it is no longer applied
- Apply once and do not reapply
- Item-level targeting

Targetting...

Description

OK Cancel Apply Help

**Targetting Editor**

New Item Add Collection Item Options Delete Help

- Batt New Item
- Computer Name
- CPU Speed
- Date Match
- Disk Space
- Domain
- Environment Variable
- File Match
- IP Address Range
- Language
- LDAP Query
- MAC Address Range
- MSI Query
- Network Connection
- Operating System
- Organizational Unit
- PCMCIA Present
- Portable Computer
- Processing Mode
- RAM
- Registry Match
- Security Group
- Site
- Terminal Session

\*PC.netzweise.com

192.168.2.50 - 192.168.2.99

Synchronous, Asynchronous, Background, Slow link

Additional Information...

OK Cancel



# Troubleshooting-Tools

- GPO Logging ADM Template
- Registry.pol Viewer
- gpupdate
- Command Line GPO Refresh
- GPDisable
- Killpol
- Gptime
- Group Policy Health Reporter
- RSOP
- Gpotool
- DCDiag
- GPResult
- Group Policy Monitor
- Policy Reporter
- GP Inventory
- Windows Hilfe
- Policyspy

[www.gpoguy.com](http://www.gpoguy.com)

<http://sdmsoftware.com/group-policy-management-products/freeware-group-policy-tools-utilities/>

## Troubleshooting mit RSOP's

- GPRresult, Group Policy Monitor, GPMC, Policyspy und die Windows Hilfe nutzen RSOP
- GPRresult muss bei W2k noch installiert werden (Windows Support Tools)
- Der Group Policy Monitor soll die Gruppenrichtlinienverarbeitung protokollieren. Leider ist er auf deutschen Systemen nicht sauber lauffähig
- Policyspy ist ebenfalls ein Reskit-Tool und kann RSOP's und andere Daten Fernabfragen

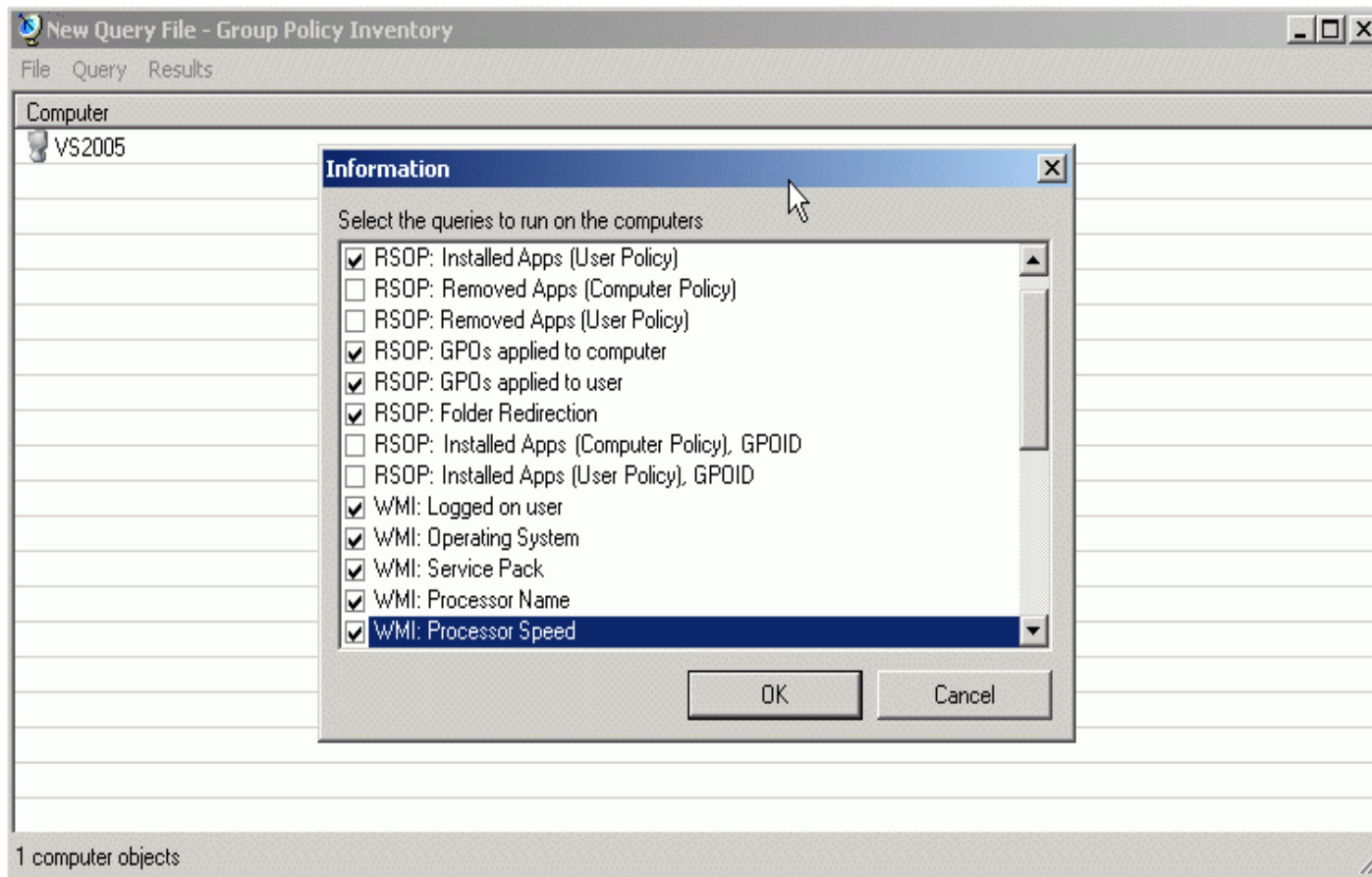


wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mann)  
Weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

# Policspy



Das Abfragefenster von Policspy



## Gpotool

- GPOtool ist Teil des Windows Resource Kits
- Gpotool
  - überprüft die Richtlinien-Konsistenz
  - überprüft die Richtlinien-Replikation
  - zeigt Informationen über die einzelnen Gruppenrichtlinien-Objekte an
  - startet mit dem Parameter /v im ausführlichen Modus

weise (klug); Weise,  
-n, -n; ↑ R 5 ff. (kluger Me  
weisen (R 10)



**Netz-Weise**  
Lernen von den Besten.

# Gpresult und gpoutil

```
cmd.exe
An 22.03.2006 um 17:06:05 erstellt

RSOP-Ergebnisse für NUTRADERS\huges auf US2005 : Protokollierungsmodus

Betriebssystemtyp: Microsoft Windows XP Professional
Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Betriebssystemversion: 5.1.2600
Domänenname: NUTRADERS
Domänentyp: Windows 2000
Standortname: Standardname-des-ersten-Standorts
Zwischengespeichertes Profil: C:\Dokumente und Einstellungen\HUGES
Lokales Profil:
Langsame Verbindung? Nein

COMPUTEREINSTELLUNGEN

CN=US2005,OU=Workstations,OU=Braunschweig,DC=nutraders,DC=net
Zeit der letzten Gruppenrichtlinienanwendung: 22.03.2006 at 17:05:18
Gruppenrichtlinie wurde angewendet von: dci.nutraders.net
Gruppenrichtlinienschwellexwert Für langsame Verbindung: 500 kbps

Angewendete Gruppenrichtlinienobjekte

Windows Update
Firewall-Konfiguration
Default Domain Policy

Die folgenden Gruppenrichtlinie werden nicht angewendet, da sie herausgefiltert
ert wurden.

Richtlinien der lokalen Gruppe
Filterung: Nicht angewendet (Leer)

Der Computer ist Mitglied der folgenden Sicherheitsgruppen:

Administratoren
Jeder
Benutzer
US2005$
Domänencomputer
NETZERN
Authentifizierte Benutzer

BENUTZEREINSTELLUNGEN

CN=Holger Voges,OU=Benutzer,OU=Braunschweig,DC=nutraders,DC=net
Zeit der letzten Gruppenrichtlinienanwendung: 22.03.2006 at 16:19:19
Gruppenrichtlinie wurde angewendet von: dci.nutraders.net
Gruppenrichtlinienschwellexwert Für langsame Verbindung: 500 kbps

Angewendete Gruppenrichtlinienobjekte

Default Domain Policy

Die folgenden Gruppenrichtlinie werden nicht angewendet, da sie herausgefiltert
ert wurden.

Richtlinien der lokalen Gruppe
Filterung: Nicht angewendet (Leer)

Der Benutzer ist Mitglied der folgenden Sicherheitsgruppen:

Domänen-Benutzer
Jeder
Benutzer
Administratoren
INTERNETIÜ
Authentifizierte Benutzer
LOKAL
Domänen-Admins
```

```
Command Shell

C:\Programme\Windows Resource Kits\Tools>gpoutil /v
Validating DCs...
Available DCs:
dci.nutraders.net
Searching for policies...
Found 5 policies

=====
Policy {09F72725-FD85-4C8D-83B4-344C0575BFEE}
Friendly name: [Checked Out] Firewall-Konfiguration
Policy OK
=====
Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Policy
Policy OK
=====
Policy {525AF7C4-CB8E-49AE-A0CF-3F7884F28752}
Friendly name: Firewall-Konfiguration
Policy OK
=====
Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Controllers Policy
Policy OK
=====
Policy {70754213-E6C1-4E90-8DD6-45B86563DDC6}
Friendly name: Windows Update
Policy OK
=====
Policies OK

C:\Programme\Windows Resource Kits\Tools>
```

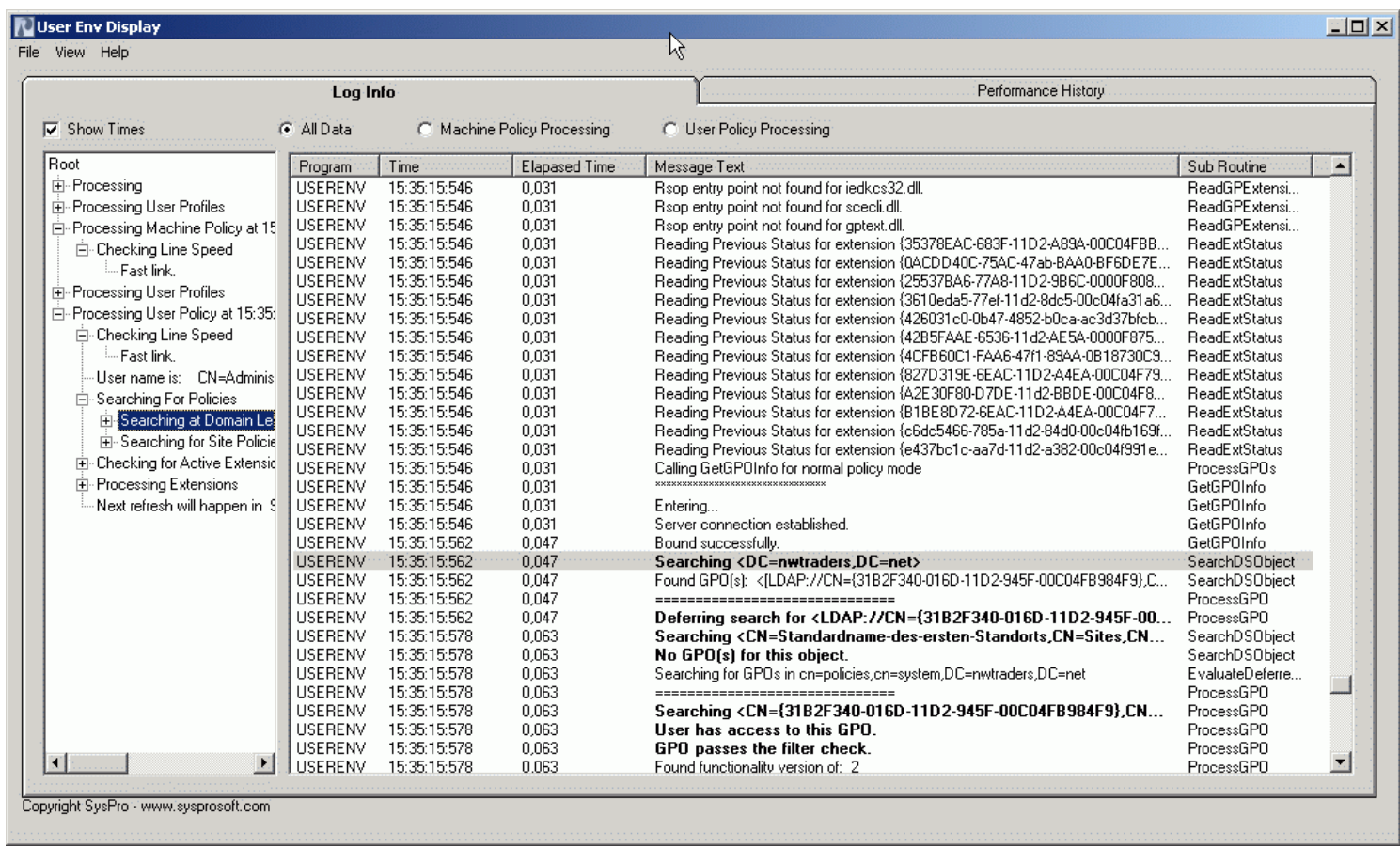
# Troubleshooting mit Logfiles

- Bis Server 2003 / Win XP können Logfiles erzeugt werden
- Die Protokollierung der Gpo-Verarbeitung kann in der Registry aktiviert werden
- Policy Reporter formatiert die Log-Datei userenv.log lesbar
- Das GPO Logging Template aktiviert Protokollierung per gpo

Gruppenrichtlinien-Kern und Registry CSE	%windir%\debug\usermode\userenv.log
Sicherheit CSE	%windir%\security\logs\winlogon.log
Ordnerumleitung	%windir%\debug\usermode\fddeploy.log
Software-Verteilung	%windir%\debug\usermode\apppgmt.log
Windows Installer (Softwareverteilung)	%windir%\temp\msi*.log
Windows Installer (benutzerinitiiert)	%temp%\msi*.log

weise (klug); Weise, -n;  
-n; -n; ↑ R 5 ff. (kluger Me  
Weisen (R 19)

# Policy Log Analyzer



**User Env Display**  
File View Help

**Log Info** Performance History

Show Times     All Data     Machine Policy Processing     User Policy Processing

Program	Time	Elapsed Time	Message Text	Sub Routine
USERENV	15:35:15:546	0,031	Rsop entry point not found for iedkcs32.dll.	ReadGPExtensi...
USERENV	15:35:15:546	0,031	Rsop entry point not found for scecli.dll.	ReadGPExtensi...
USERENV	15:35:15:546	0,031	Rsop entry point not found for gptext.dll.	ReadGPExtensi...
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {35378EAC-683F-11D2-A89A-00C04FB...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {0ACDD40C-75AC-47ab-BAA0-BF6DE7E...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {25537BA6-77A8-11D2-9B6C-0000F808...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {3610eda5-77ef-11d2-8dc5-00c04fa31a6...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {426031c0-0b47-4852-b0ca-ac3d37fbc...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {42B5FAAE-6536-11d2-AE5A-0000F875...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {4CFB60C1-FAA6-47f1-89AA-0B18730C9...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {827D319E-6EAC-11D2-A4EA-00C04F79...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {A2E30F80-D7DE-11d2-8BDE-00C04F8...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {B1BE8D72-6EAC-11D2-A4EA-00C04F7...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {c6dc5466-785a-11d2-84d0-00c04fb169f...	ReadExtStatus
USERENV	15:35:15:546	0,031	Reading Previous Status for extension {e437bc1c-aa7d-11d2-a382-00c04f991e...	ReadExtStatus
USERENV	15:35:15:546	0,031	Calling GetGPOInfo for normal policy mode	ProcessGPOs
USERENV	15:35:15:546	0,031	*****	GetGPOInfo
USERENV	15:35:15:546	0,031	Entering...	GetGPOInfo
USERENV	15:35:15:546	0,031	Server connection established.	GetGPOInfo
USERENV	15:35:15:562	0,047	Bound successfully.	GetGPOInfo
USERENV	15:35:15:562	0,047	<b>Searching &lt;DC=nwtraders.DC=net&gt;</b>	SearchDSObject
USERENV	15:35:15:562	0,047	Found GPO(s): <LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},C...	SearchDSObject
USERENV	15:35:15:562	0,047	*****	ProcessGPO
USERENV	15:35:15:562	0,047	<b>Deferring search for &lt;LDAP://CN={31B2F340-016D-11D2-945F-00...</b>	ProcessGPO
USERENV	15:35:15:578	0,063	<b>Searching &lt;CN=Standardname-des-ersten-Standorts,CN=Sites,CN...</b>	SearchDSObject
USERENV	15:35:15:578	0,063	<b>No GPO(s) for this object.</b>	SearchDSObject
USERENV	15:35:15:578	0,063	Searching for GPOs in cn=policies,cn=system,DC=nwtraders,DC=net	EvaluateDeferre...
USERENV	15:35:15:578	0,063	*****	ProcessGPO
USERENV	15:35:15:578	0,063	<b>Searching &lt;CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN...</b>	ProcessGPO
USERENV	15:35:15:578	0,063	<b>User has access to this GPO.</b>	ProcessGPO
USERENV	15:35:15:578	0,063	<b>GPO passes the filter check.</b>	ProcessGPO
USERENV	15:35:15:578	0,063	Found functionality version of: 2	ProcessGPO

Copyright SysPro - www.sysprosoft.com

Der Policy Log Reporter von Sysprosoft zeigt die Userenv.log in lesbarer Form an

## Troubleshooting ab Vista

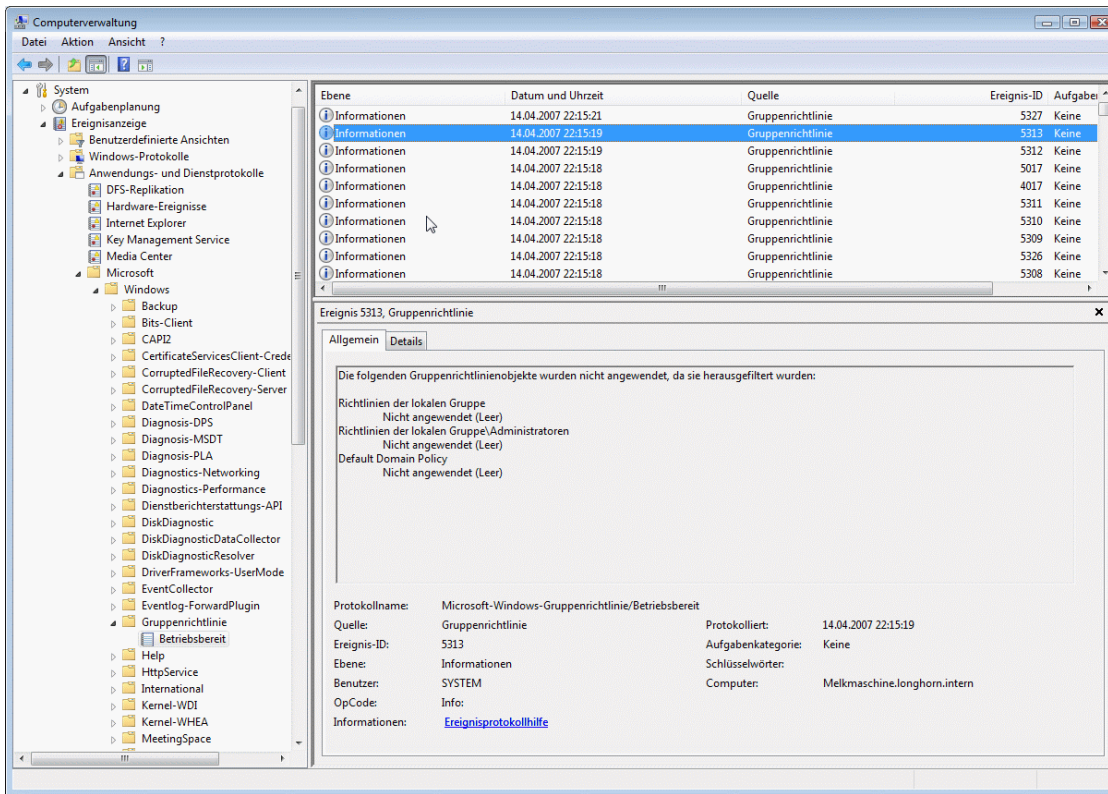
- Der Gruppenrichtliniendienst protokolliert im Ereignisprotokoll
- Microsoft liefert das Log View Tools zur Anzeige von Gruppenrichtlinien-Einträgen als Text-Log
- Das Log View Tool kann man bei Microsoft herunterladen

<http://www.microsoft.com/en-us/download/details.aspx?id=11147>

### **Troubleshooting Group Policy Using Event Logs**

<http://technet2.microsoft.com/WindowsVista/en/library/7e940882-33b7-43db-b097-f3752c84f67f1033.msp?mfr=true>

# Gruppenrichtlinien Ereignisanzeige



Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabe
Informationen	14.04.2007 22:15:21	Gruppenrichtlinie	5327	Keine
Informationen	14.04.2007 22:15:19	Gruppenrichtlinie	5313	Keine
Informationen	14.04.2007 22:15:19	Gruppenrichtlinie	5312	Keine
Informationen	14.04.2007 22:15:18	Gruppenrichtlinie	5017	Keine
Informationen	14.04.2007 22:15:18	Gruppenrichtlinie	4017	Keine
Informationen	14.04.2007 22:15:18	Gruppenrichtlinie	5311	Keine
Informationen	14.04.2007 22:15:18	Gruppenrichtlinie	5310	Keine
Informationen	14.04.2007 22:15:18	Gruppenrichtlinie	5309	Keine
Informationen	14.04.2007 22:15:18	Gruppenrichtlinie	5326	Keine
Informationen	14.04.2007 22:15:18	Gruppenrichtlinie	5308	Keine

**Ereignis 5313, Gruppenrichtlinie**

Allgemein Details

Die folgenden Gruppenrichtlinienobjekte wurden nicht angewendet, da sie herausgefiltert wurden:

- Richtlinien der lokalen Gruppe
  - Nicht angewendet (Leer)
- Richtlinien der lokalen Gruppe\Administratoren
  - Nicht angewendet (Leer)
- Default Domain Policy
  - Nicht angewendet (Leer)

Protokollname: Microsoft-Windows-Gruppenrichtlinie/Betriebsbereit  
 Quelle: Gruppenrichtlinie  
 Ereignis-ID: 5313  
 Ebene: Informationen  
 Benutzer: SYSTEM  
 OpCode: Info  
 Informationen: [Ereignisprotokollhilfe](#)

Protokolliert: 14.04.2007 22:15:19  
 Aufgabenkategorie: Keine  
 Schlüsselwörter:  
 Computer: Melkmaschine.longhorn.intern

Das Log für Gruppenrichtlinienergebnisse findet sich unter  
Ereignisanzeige > Anwendungs- und Dienstprotokolle > Microsoft > Windows > Gruppenrichtlinien

## GPLogView

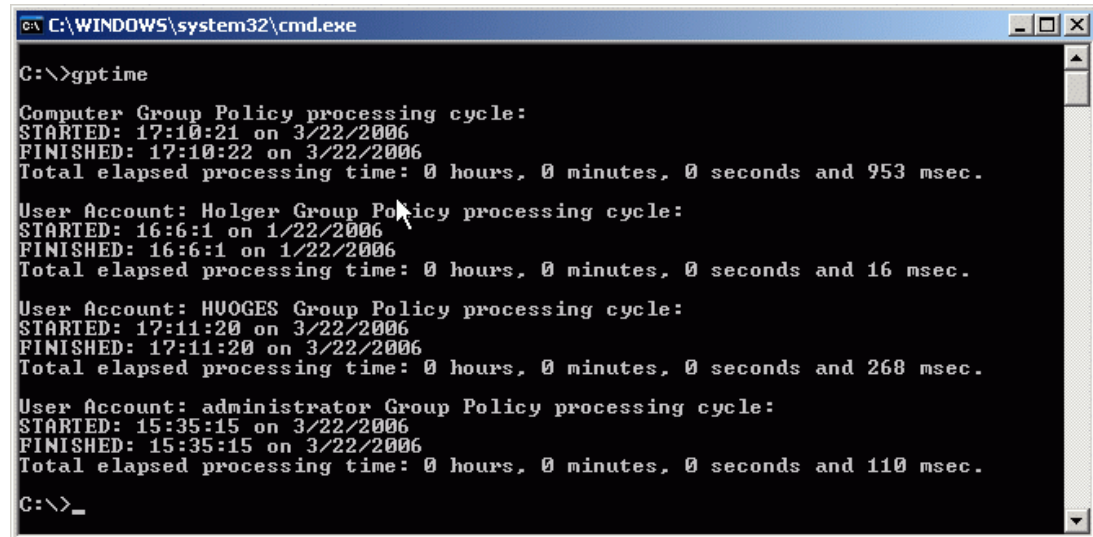
- **Alle Richtlinienereignisse exportieren**  
`gplogview -o c:\ereignisse.txt`
- **Activity-ID filtern und als HTML ausgeben**  
`gplogview -a „ID“ -h -o ereignisse.htm`
- **Monitor-Mode mit XML-Logging**  
`gplogview -x -m`
- **Ein gespeichertes Protokoll als Eingabe**  
`gplogview -i GPO.evtx -o Ereignisse.txt`



# Ablaufzeit-Analyse

- Gptime zeigt die Zeit an, die eine einzelne Gruppenrichtlinie bis zum Beenden der Abarbeitung gebraucht hat
- Mit GPTime kann die Anmeldezeit für Benutzer optimiert werden

<http://www.gpoguy.com>



```
C:\WINDOWS\system32\cmd.exe
C:\>gptime

Computer Group Policy processing cycle:
STARTED: 17:10:21 on 3/22/2006
FINISHED: 17:10:22 on 3/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 953 msec.

User Account: Holger Group Policy processing cycle:
STARTED: 16:6:1 on 1/22/2006
FINISHED: 16:6:1 on 1/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 16 msec.

User Account: HUOGES Group Policy processing cycle:
STARTED: 17:11:20 on 3/22/2006
FINISHED: 17:11:20 on 3/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 268 msec.

User Account: administrator Group Policy processing cycle:
STARTED: 15:35:15 on 3/22/2006
FINISHED: 15:35:15 on 3/22/2006
Total elapsed processing time: 0 hours, 0 minutes, 0 seconds and 110 msec.

C:\>_
```



## Erweiterungen

- Einige Tools zum Erweitern von Gruppenrichtlinien
  - Office Resource Kit (ORK)
  - AGPM (Advanced Group Policy Management)
  - Specops Command

## Office ADMX-Templates

- Das ORK stellt ab Office 2000 ADM-Dateien zur Office-Konfiguration bereit
- Fast alle Office-Einstellungen lassen sich per Richtlinie vorgeben
- Komplette Office-Menüs können vollständig deaktiviert werden

- **Download:**

Office 2010

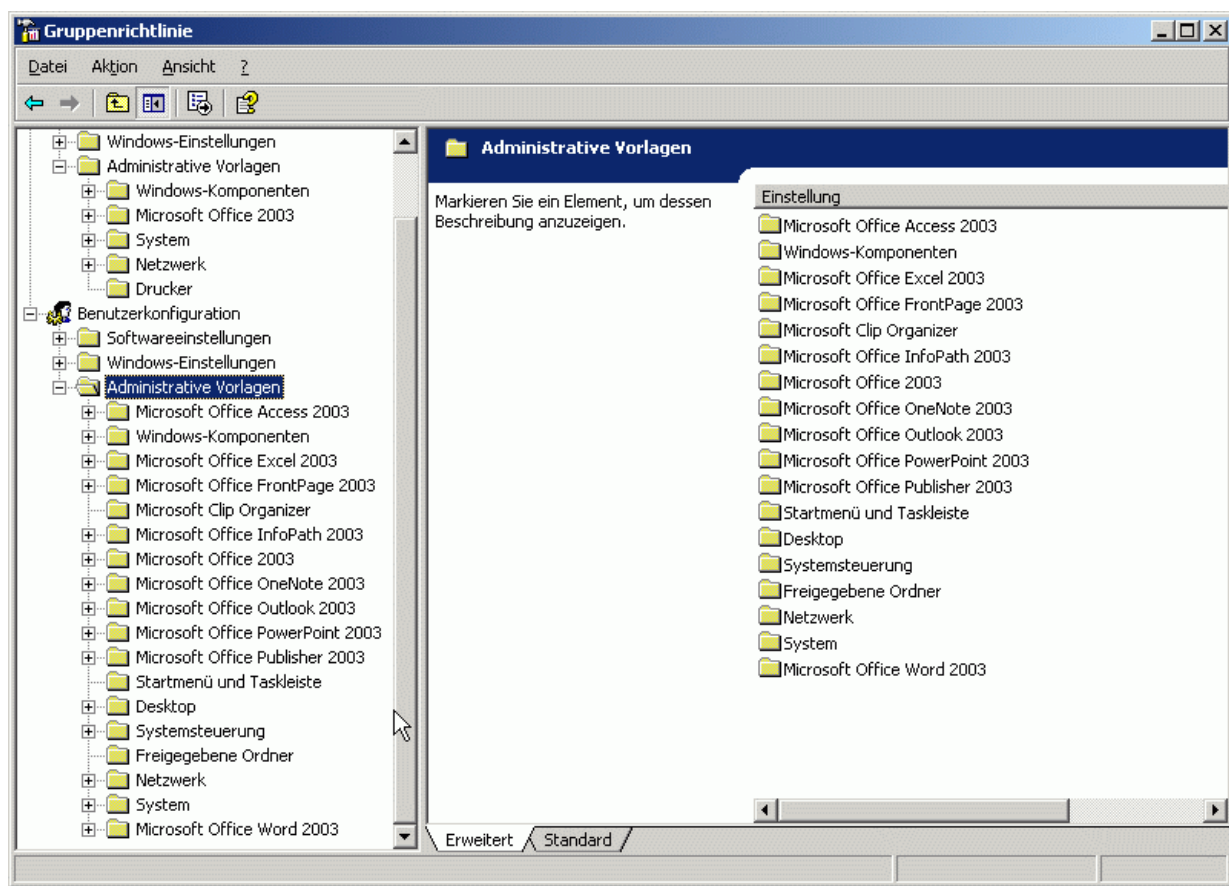
<http://www.microsoft.com/en-us/download/details.aspx?id=18968>

Office 2013

<http://www.microsoft.com/en-us/download/details.aspx?id=35554>

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
Weisen (↑ R 10)

# Die Office Richtlinien



Alle Office-Richtlinien des Benutzers auf einen Blick

# Advance Group Policy Management

- AGPM erweitert die GPMC um Funktionen zur Verwaltung von Gruppenrichtlinien
- AGPM Vault ist Bestandteil des Desktop Optimization Kit
- Funktionalität:
  - Offline-Bearbeitung von Gruppenrichtlinien
  - Versionkontrolle von Gruppenrichtlinien
  - Rollenbasierte Delegation (Enterprise)
  - Check-In und Check-Out von Richtlinien (Enterprise)
  - Differenz-Reporting
  - GPO-Vorlagen

weise (klug); Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 105)



**Netz-Weise**  
Lernen von den Besten.

Gruppenrichtlinienverwaltung

Datei Aktion Ansicht Fenster ?

Gruppenrichtlinienverwaltung

- Gesamtstruktur: Netzweise.com
  - Domänen
    - Netzweise.com
      - Applocker
      - computer und Benutzer
      - Default Domain Policy
      - Firewall
      - specops
      - Computer
      - Domain Controllers
      - Hannover
      - Service Accounts
      - Test
      - Gruppenrichtlinienobjekte
      - WMI-Filter
      - Starter-Gruppenrichtlinienobjekte**
        - Änderungssteuerung**
      - Standorte
      - Gruppenrichtlinienmodellierung
      - Gruppenrichtlinienergebnisse

### Änderungssteuerung für Netzweise.com

Inhalt: Domänendelegation AGPM-Server Produktionsdelegation

Gruppenrichtlinienobjekte suchen

Gesteuert Ungesteuert Ausstehend Vorlagen Papierkorb

Gruppenrichtlinienobjekte:

Name	Status	Geändert von	Änderungsdatum	Kommentar
computer und Benutzer	Eingecheckt	Administrator (NETZWEISE\Administ...	27.08.2013 20:40:31	
Firewall	Eingecheckt	Miraculix (Miraculix@Netzweise.com)	27.08.2013 20:37:35	
specops	Eingecheckt	Administrator (NETZWEISE\Administ...	27.08.2013 16:55:39	

Diese Gruppen und Benutzer verfügen über diese Rollen für das ausgewählte Gruppenrichtlinienobjekt im Archiv:

Name	Rollen	Vererbt
Administrator (NETZWEISE\Administrator)	Vollzugriff	Ja
Asterix (Asterix@Netzweise.com)	Prüfer, Bearbeiter	Ja
Majestix (Majestix@Netzweise.com)	Prüfer, Genehmigende Person	Ja
Miraculix (Miraculix@Netzweise.com)	Prüfer, Bearbeiter	Ja
Obelix (Obelix@Netzweise.com)	Prüfer	Ja
S-1-5-21-535681966-476841327-1696152028...	Prüfer, Bearbeiter	Ja

Hinzufügen... Entfernen Eigenschaften Erweitert...

Änderungssteuerung

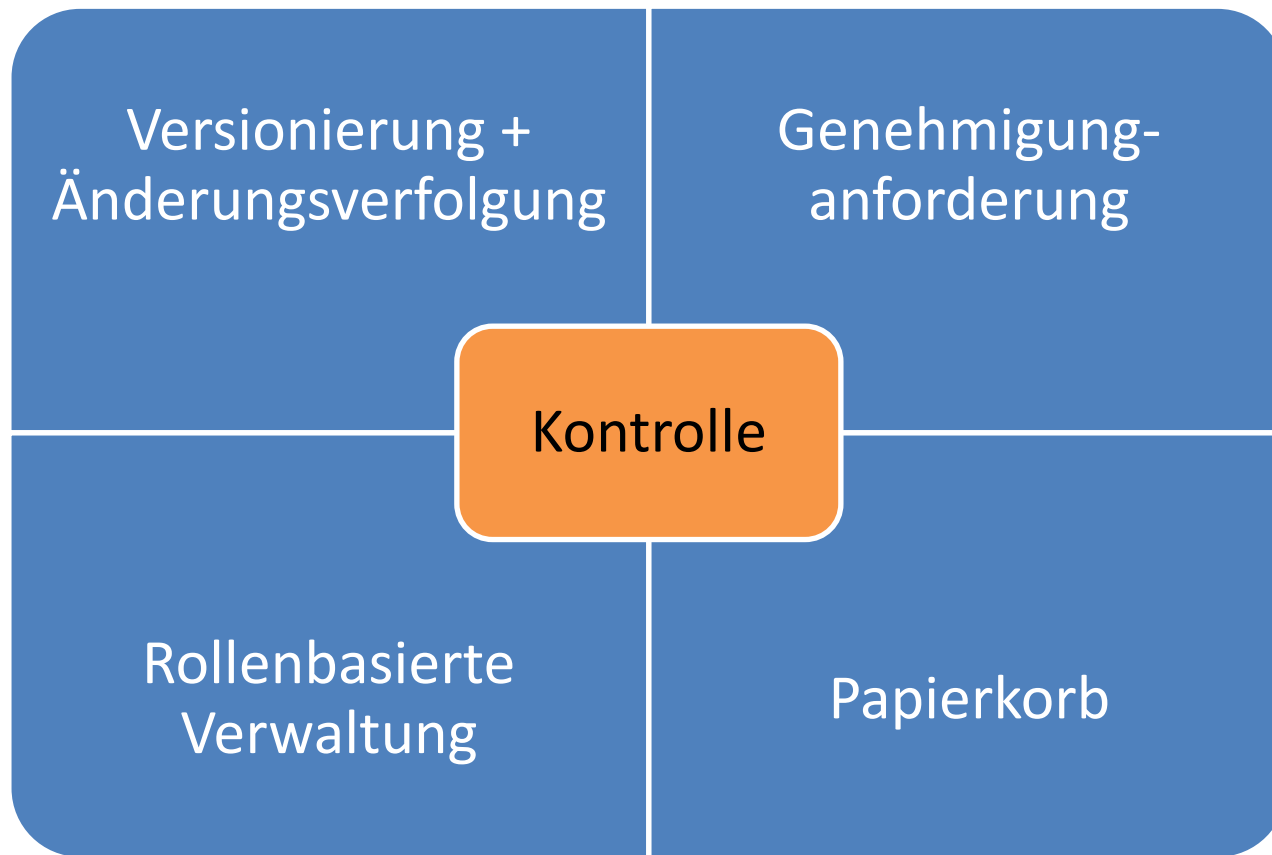
DE 14:48 28.08.2013

wei|se (klug); 'Weise, der  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 105)



**Netz-Weise**  
Lernen von den Besten.

# Advance group policy management



AGMP How to Video bei Youtube

<http://www.youtube.com/watch?v=ifWj9ka3n38>

wei|se (klug); 'Weise, ...  
-n, -n; ↑ R 5 ff. (kluger Man  
weisen (↑ R 10)



**Netz-Weise**  
Lernen von den Besten.

# Rollenbasiertes Delegations-Modell

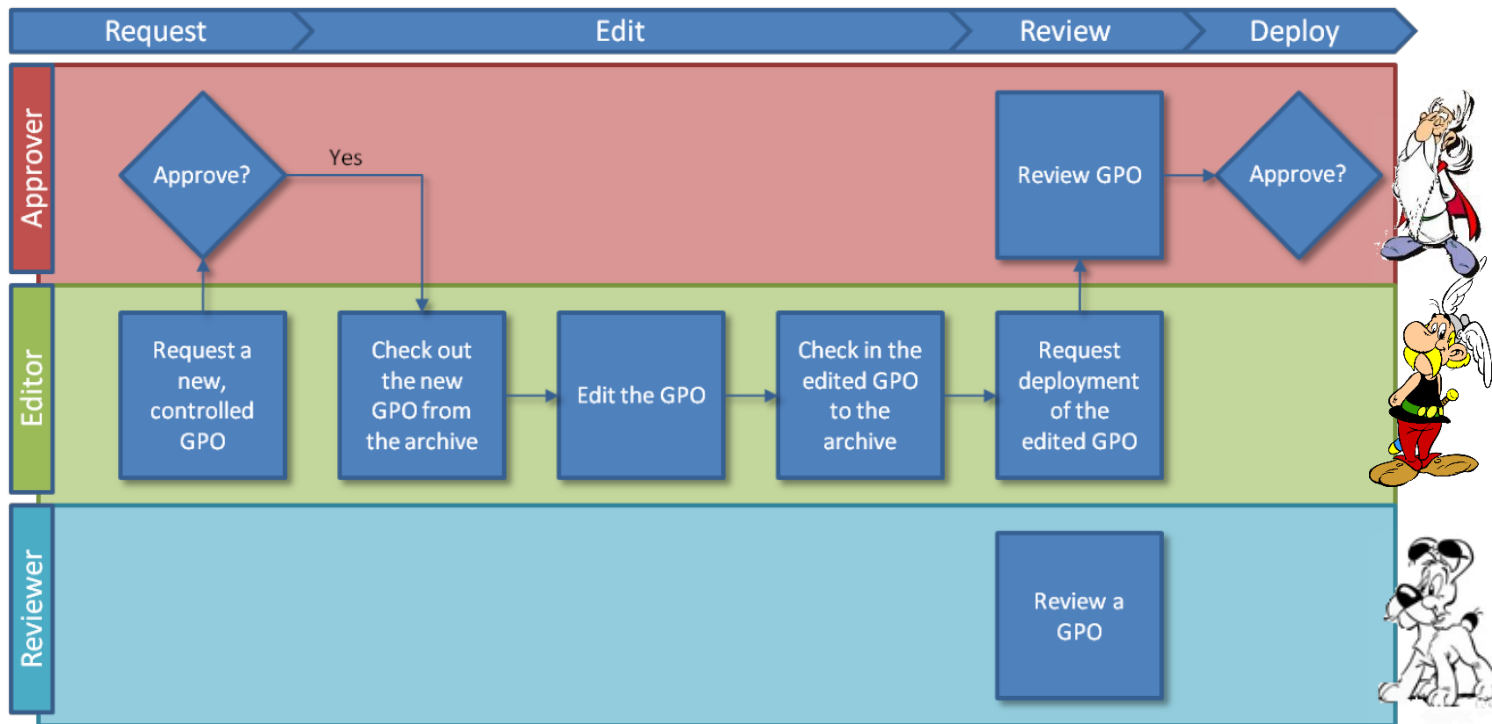


Figure 5. Role-based delegation





## Specops Command

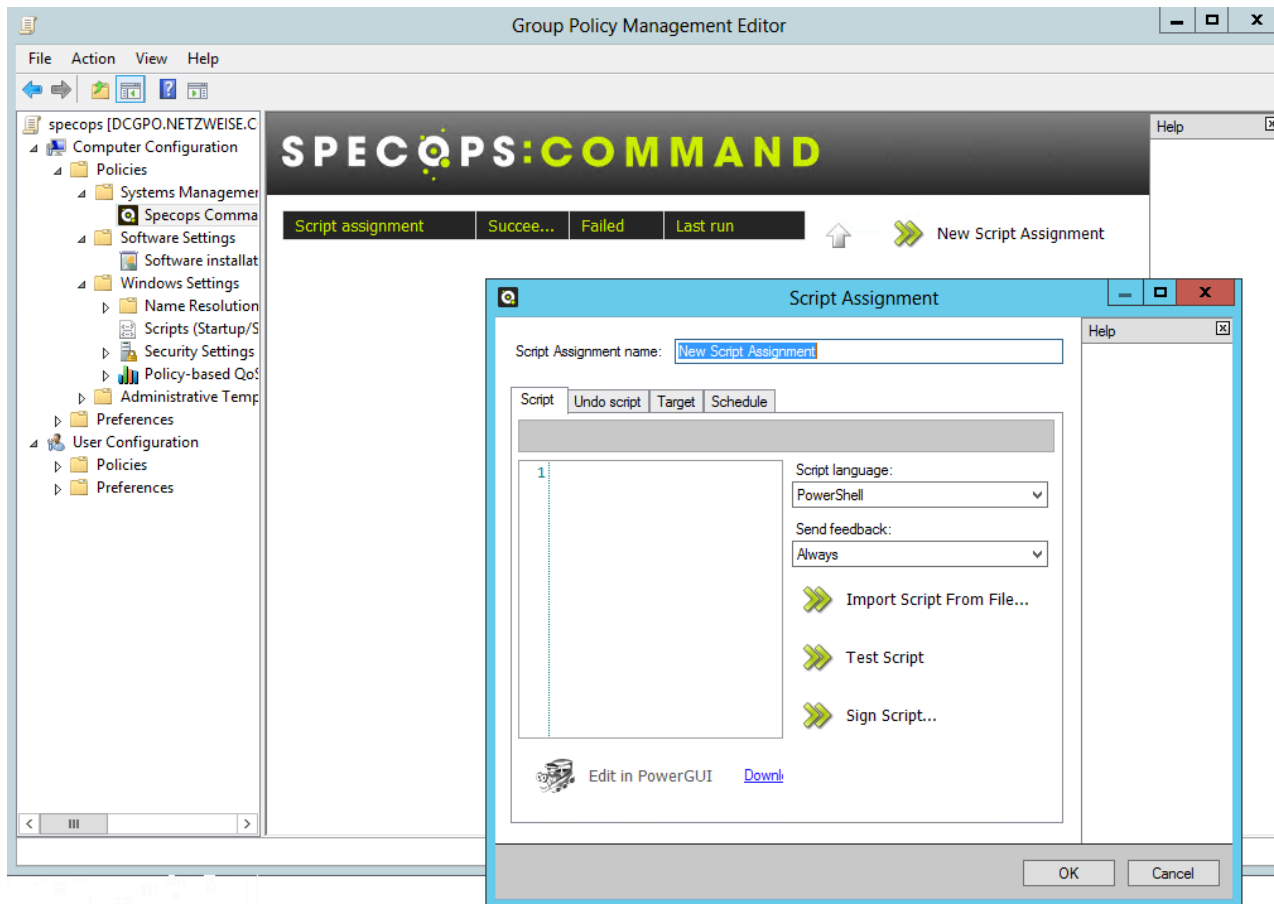
- Kann Scripte unabhängig von Login-Scripten ausführen
- Zeitgesteuert
- Targets können definiert werden
- Undo-script kann hinterlegt werden, um Einstellungen rückgängig zu machen

weise (klug); Weise, Weisheit  
-n, -n; ↑ R 5 ff. (kluger Mensch)  
Weisen (↑ R 108)



**Netz-Weise**  
Lernen von den Besten.

# Script and Run





## Neu in Windows Server 2012

- Remote GPUUpdate
- Replikationsstatus
- Gruppenrichtlinien-Dienst hält nach 10 min Inaktivität automatisch
- Keine Internet Explorer Maintenance mehr!



## Bekannte Probleme

- Fehlermeldung: “The following entry in the [strings] section is too long and has been truncated”  
(<http://support.microsoft.com/default.aspx?kbid=842933> )
- Richtlinien sind deaktivierbar (gpdisable)
- Zu große Sysvol-Ordner können sehr starken Replikationsverkehr erzeugen  
Lösung: Lokales Speichern der ADM's  
(<http://support.microsoft.com/?id=816662#XSLTH4236121121120121120120>)



# Weiterführende Quellen bei MS

- Microsoft Group Policy Website  
<http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/default.aspx>
- Technet Group Policy Center  
<http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.aspx>
- Implementing Common Desktop Management Scenarios with the Group Policy Management Console  
<http://technet2.microsoft.com/WindowsServer/en/Library/7b33dcd6-0ad2-44e8-82f8-962425b6cf8e1033.aspx>
- Enterprise Management with the Group Policy Management Console  
<http://www.microsoft.com/windowsserver2003/gpmc/default.aspx>
- Whitepaper: Introduction to Group Policy in Windows Server 2003  
<http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.aspx>
- Whitepaper: Administering Group Policy with the GPMC  
<http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.aspx>
- MS Technet: Step-by-Step Guide to Understanding the Group Policy Feature Set  
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/gpfeat.aspx>
- Technet – Group Policy Troubleshooting  
<http://technet2.microsoft.com/WindowsServer/en/Library/0c627456-5dfa-44db-b43a-e41c8f4f09231033.aspx>
- TechNet Support WebCast: Behandeln von Problemen mit Gruppenrichtlinien und Profilprobleme in einer Domäne-Umgebung, indem der Protokollierung von Userenv verwendet  
<http://support.microsoft.com/default.aspx?kbid=835302>
- MS KB: Troubleshooting Group Policy application problems  
<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B250842>
- SO WIRD'S GEMACHT: Festlegen erweiterter Einstellungen in Internet Explorer mit Hilfe von Gruppenrichtlinienobjekten  
<http://support.microsoft.com/?kbid=274846>
- Group Policy Settings Reference  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=7821C32F-DA15-438D-8E48-45915CD2BC14&displaylang=en>

## Andere Quellen

- Group Policy Wiki  
<http://grouppolicy.editme.com/>
- GPO-Guy  
<http://www.gpoguy.com/>
- Website von Mark Heitbrink (MVP) zum Thema Gruppenrichtlinien  
[www.gruppenrichtlinien.de](http://www.gruppenrichtlinien.de)
- Marks Sysinternals Blog: Circumventing Group Policy as a Limited User  
<http://www.sysinternals.com/blog/2005/12/circumventing-group-policy-as-limited.html>
- Group Policy Preferences Overview  
<http://www.microsoft.com/en-us/download/details.aspx?id=24449>
- WMI Code Creatore  
<http://www.microsoft.com/en-us/download/details.aspx?id=8572>
- ADMX-Templates für Acrobat 11  
<http://www.404techsupport.com/2012/10/adobe-reader-11-has-landed-with-gpo-adm-templates/>
- Group Policy Best Practices  
<http://windowsitpro.com/group-policy/group-policy-design-best-practices>