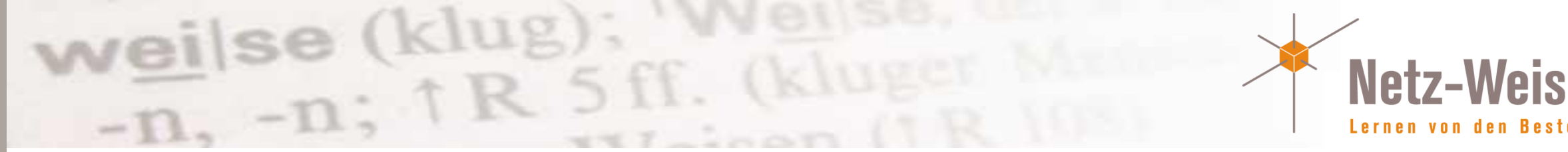


Gruppenrichtlinien

Best-Practices und Troubleshooting

Netz-Weise
Lernen von den Besten.

Holger Voges

CCA,MCSE, MCDBA, MCT, MCITP DB Administrator / DB Developer, MCTIP Enterprise Administrator, MCSE Windows Server 2012

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

Agenda

Netz-Weise
Lernen von den Besten.

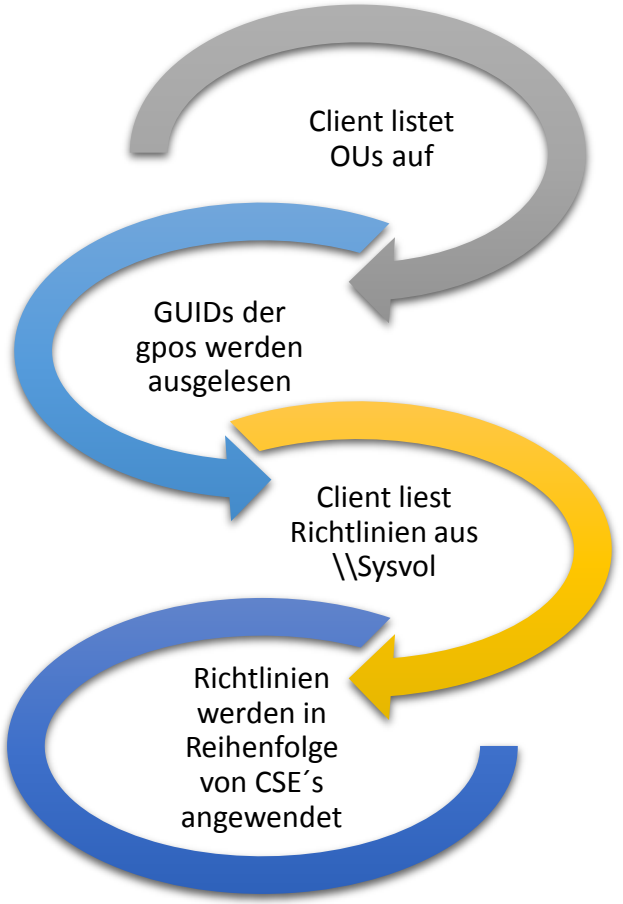
- Funktionsweise von Gruppenrichtlinien
- Best-Practices
- Troubleshooting Advanced

Anlegen einer neuen Richtlinie

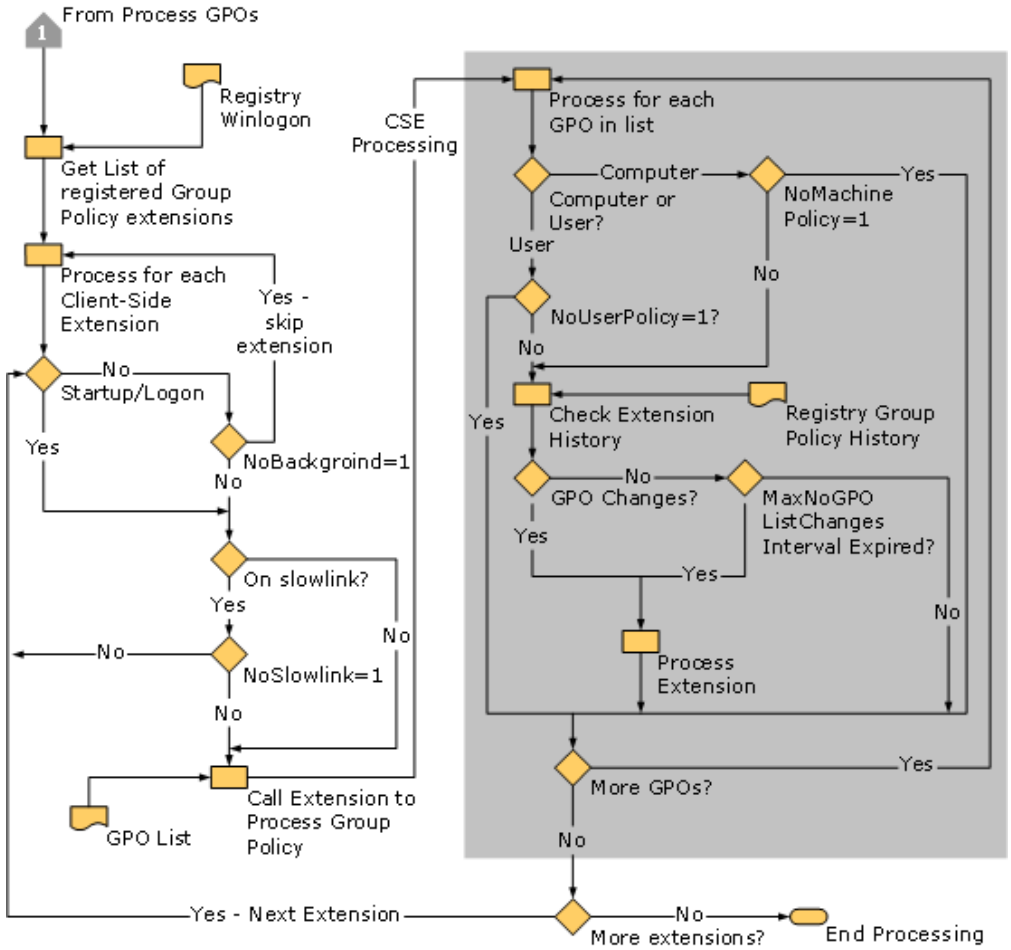
Netz-Weise
Lernen von den Besten.

Der Anmeldeprozess

Netz-Weise
Lernen von den Besten.

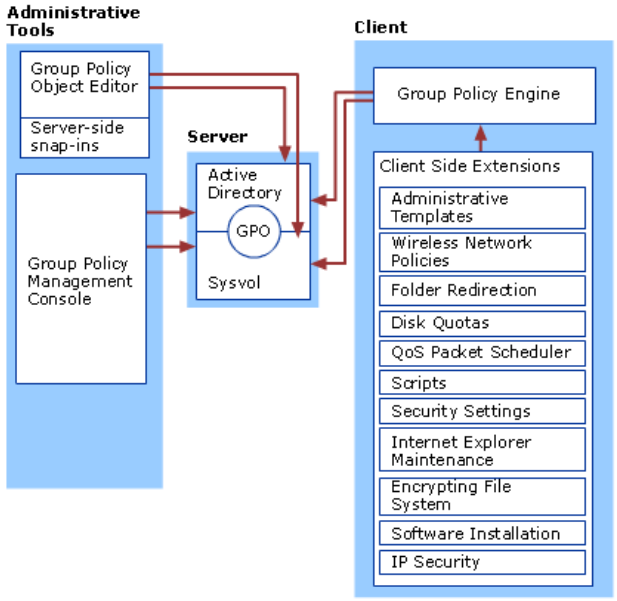


Ablauf einer Anmeldung



Client Side Extensions

- Client Side Extensions (CSE´s) werden beim Start vom Gruppenrichtliniendienst / Netlogon geladen
- 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?

Netz-Weise
Lernen von den Besten.

- 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

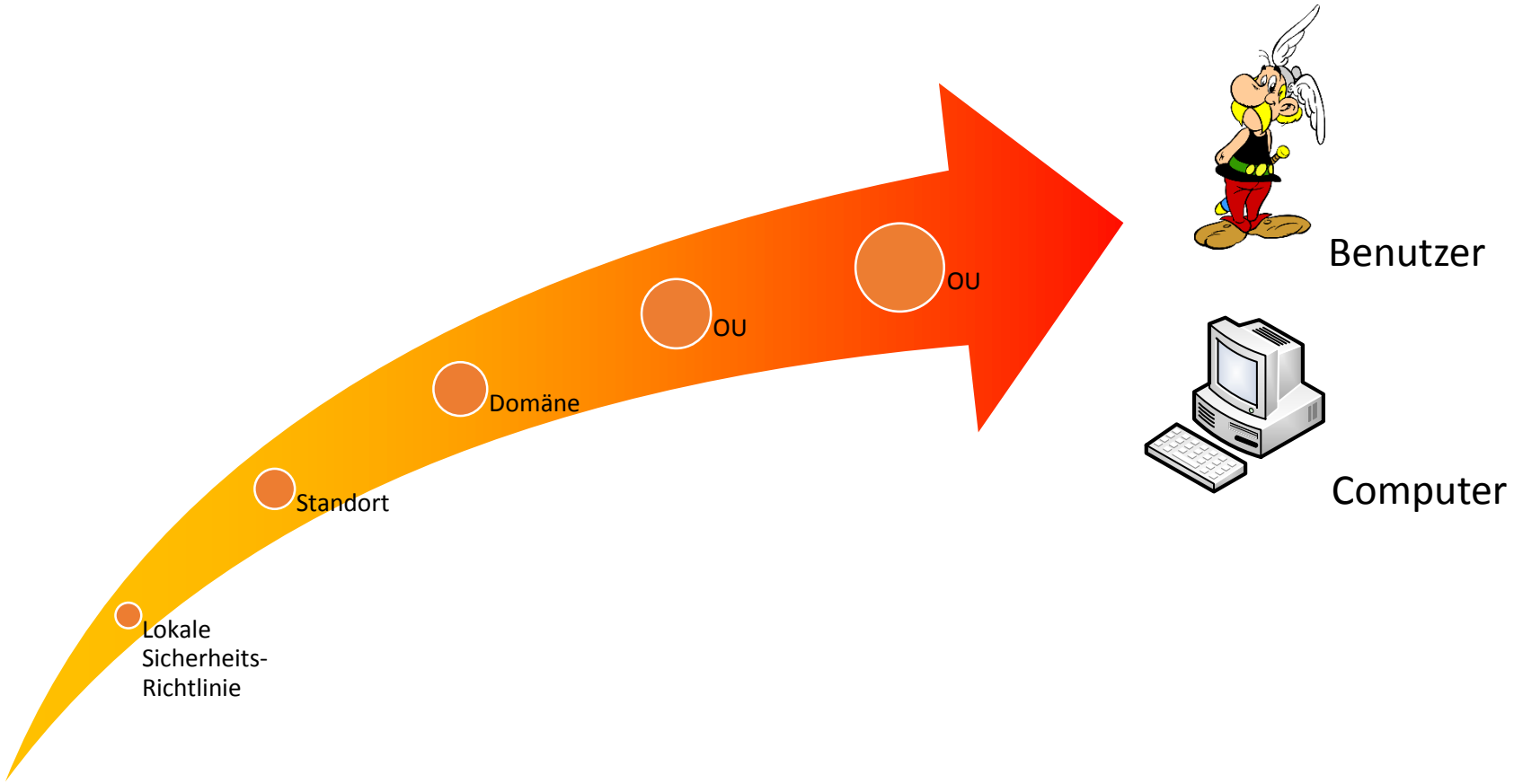
Aktualisieren der Richtlinien

Netz-Weise
Lernen von den Besten.

- GPupdate erzwingt das Überprüfen auf neue Richtlinien
- GPupdate /force aktualisiert alle Richtlinieneinstellungen. Sonst werden nur neue oder geänderte Richtlinien angewendet.
- Ab Windows Server 2012 kann über die GPMC auf OUs das Update erzwungen werden
- Mit Powershell ist ein Remote-Update möglich:

```
Get-ADComputer –filter * -Searchbase "cn=computers,
dc=Contoso,dc=com" | foreach{ Invoke-GPUpdate –computer
$_.name -force}
```

Anwendungsreihenfolge und Priorität



Erzwingen von Richtlinien

Netz-Weise
Lernen von den Besten.

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

Langsame Netzwerkverbindungen

Netz-Weise
Lernen von den Besten.

- 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
- Kann über Gruppenrichtlinien konfiguriert werden

Planen der Implentierung

Netz-Weise
Lernen von den Besten.

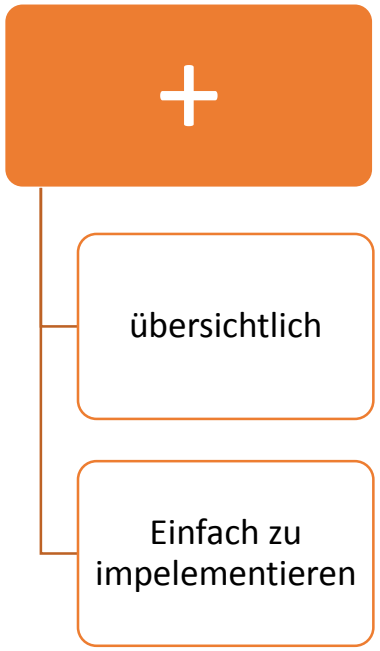
OU-Basiert

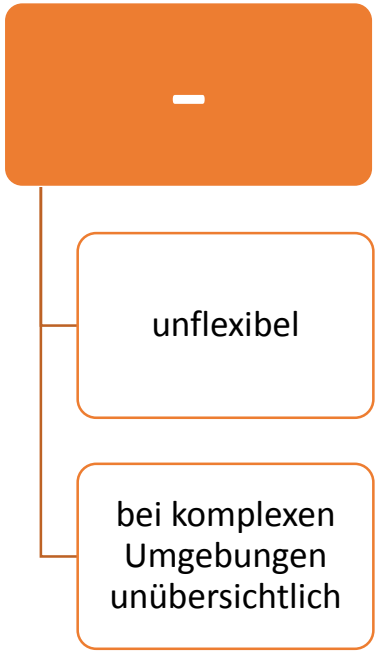
Gruppen-Basiert

OU-basierte Implementierung

Netz-Weise
Lernen von den Besten.

- OU-Struktur bildet die Gruppenrichtlinienprozesse ab
- Für neue Anforderungen neue OUs
- Eine Planung der Anwendungsreihenfolge ist extrem wichtig!

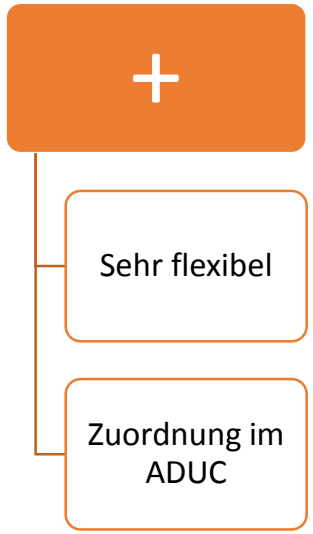


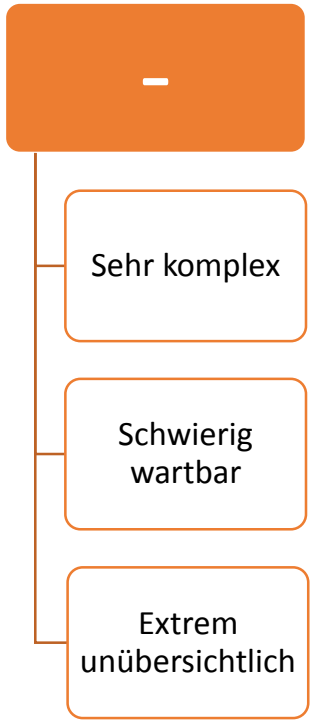


Gruppenbasierte Implementierung

Netz-Weise
Lernen von den Besten.

- Richtlinienvergabe kann auf Gruppen erfolgen
- Unabhängig von OUs
- Wird über AD-Berechtiungen gesetzt



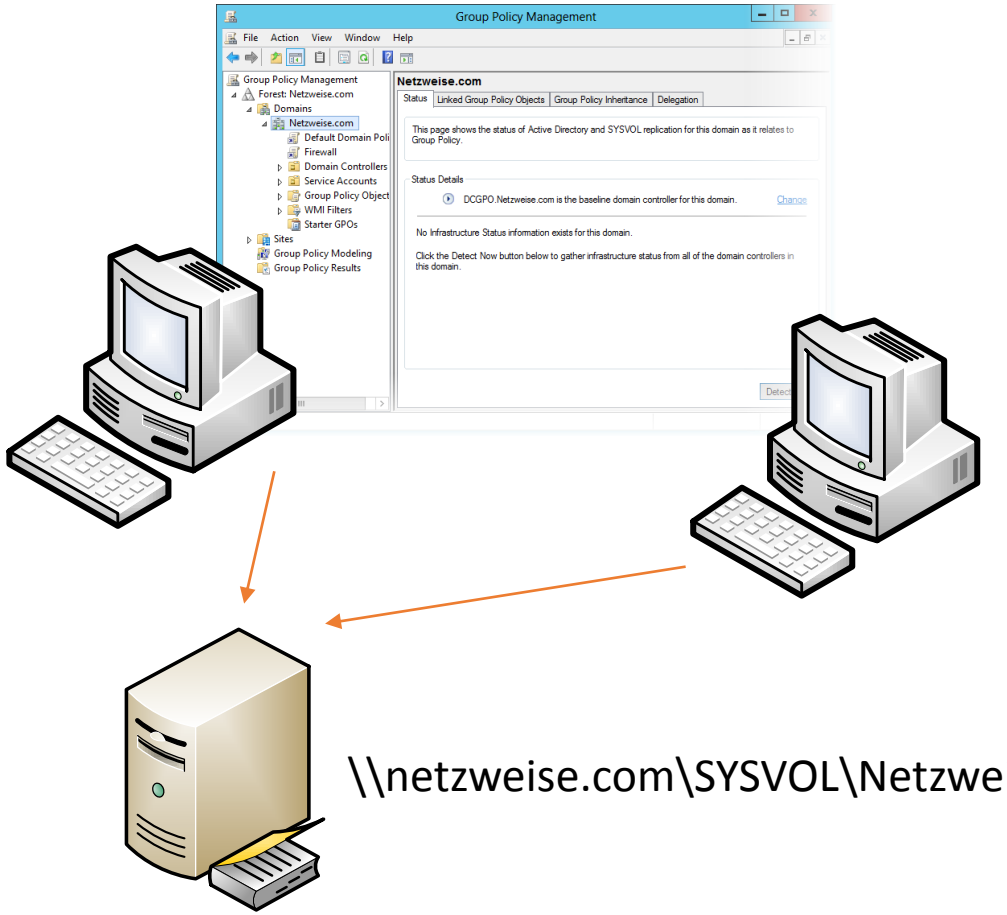


Wie viele Richtlinien sind zu viel?

Netz-Weise
Lernen von den Besten.

- Jede Richtlinie verlängert den Anmeldeprozess
- Viele Einstellungen in einer Richtlinie sind schneller verarbeitet als die gleiche Anzahl Einstellungen in vielen Richtlinien
- Synchrone vs. asynchrone Bearbeitung

Ein Speicherort, sie zu knechten

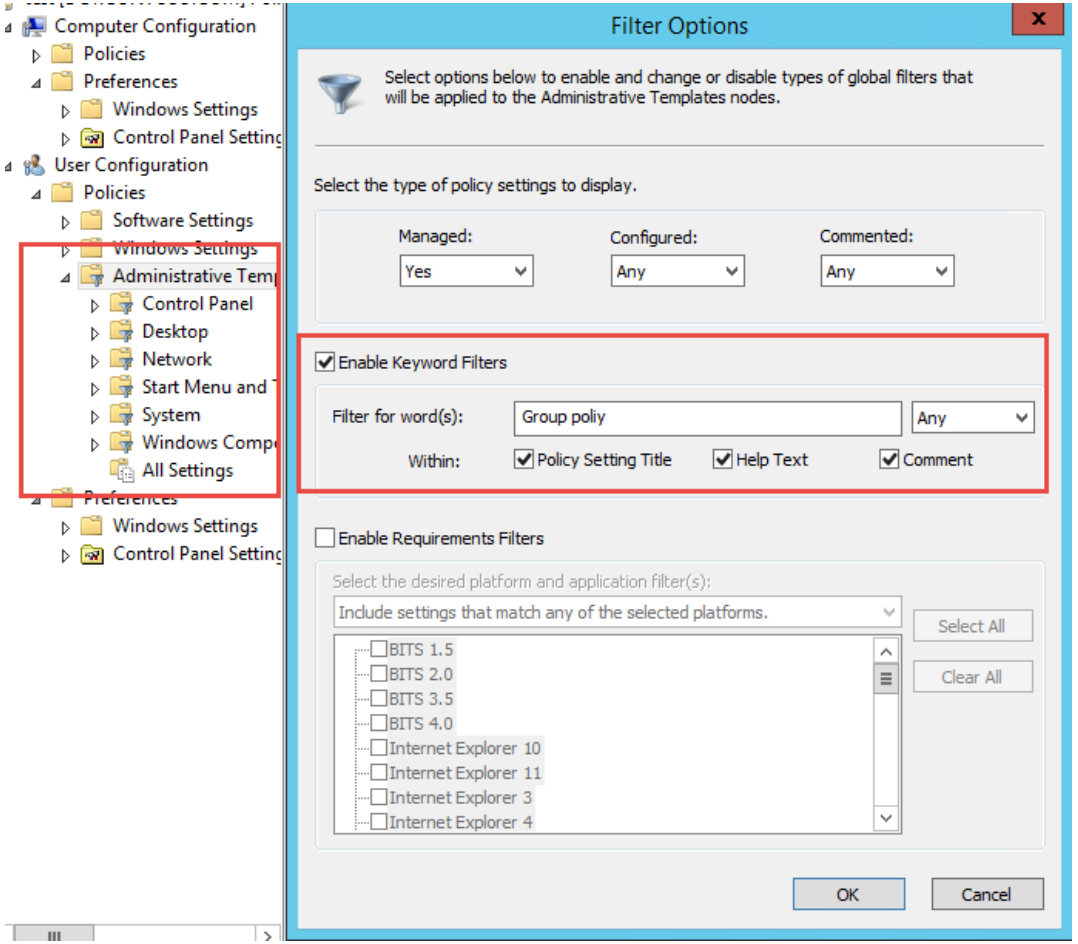


\\netzweise.com\SYSVOL\Netzweise.com\Policies**PolicyDefinitions**

Administrative Einstellungen filtern

Netz-Weise
Lernen von den Besten.

- Im Gruppenrichtlinienfilter wurde mit Windows Server 2008 eine Filterfunktion eingebaut
- Hier kann man nach Stichworten im Namen und der Beschreibung einer Richtlinie suchen



WMI-Filter

Netz-Weise
Lernen von den Besten.

- Mit WMI-Filtern kann die Abarbeitung der Richtlinien weiter verfeinert werden
- Eine Richtlinie wird nur dann angewendet, wenn der WMI-Filter True ergibt
- WMI-Filter verlangsamen den Anmeldeprozess weiter

Resulting Set of Policies

Netz-Weise
Lernen von den Besten.

- Zeigt die auf einem Client tatsächlich angewendet 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

Richtlinienbackup

Netz-Weise
Lernen von den Besten.

- 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

Internet-Explorer-Einstellungen

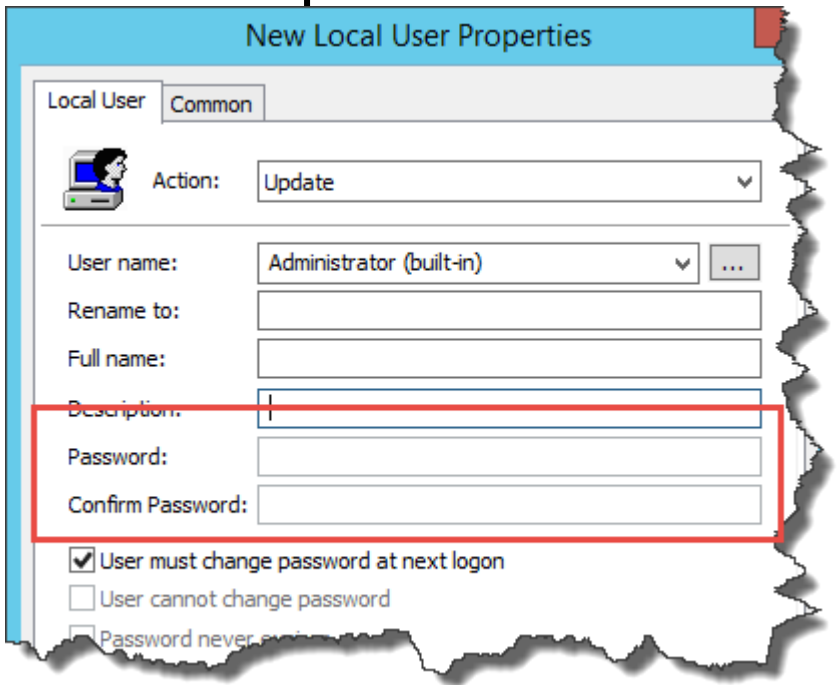
Netz-Weise
Lernen von den Besten.

- 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!

Kennwort ändern per GP-Einstellungen

Netz-Weise
Lernen von den Besten.

- Mit Gruppenrichtlinien-Einstellungen konnten Kennwörter lokaler Benutzer geändert werden
- Die Kennwörter sind nur leicht verschlüsselt im \\SYSVOL abgelegt
- Die Funktion zum Ändern lokaler Benutzerkonten ist seit April 2014 per Update deaktiviert
- Alternativ steht ein Powershell-Script zur Remoteänderung zur Verfügung



JASBUG

Netz-Weise
Lernen von den Besten.

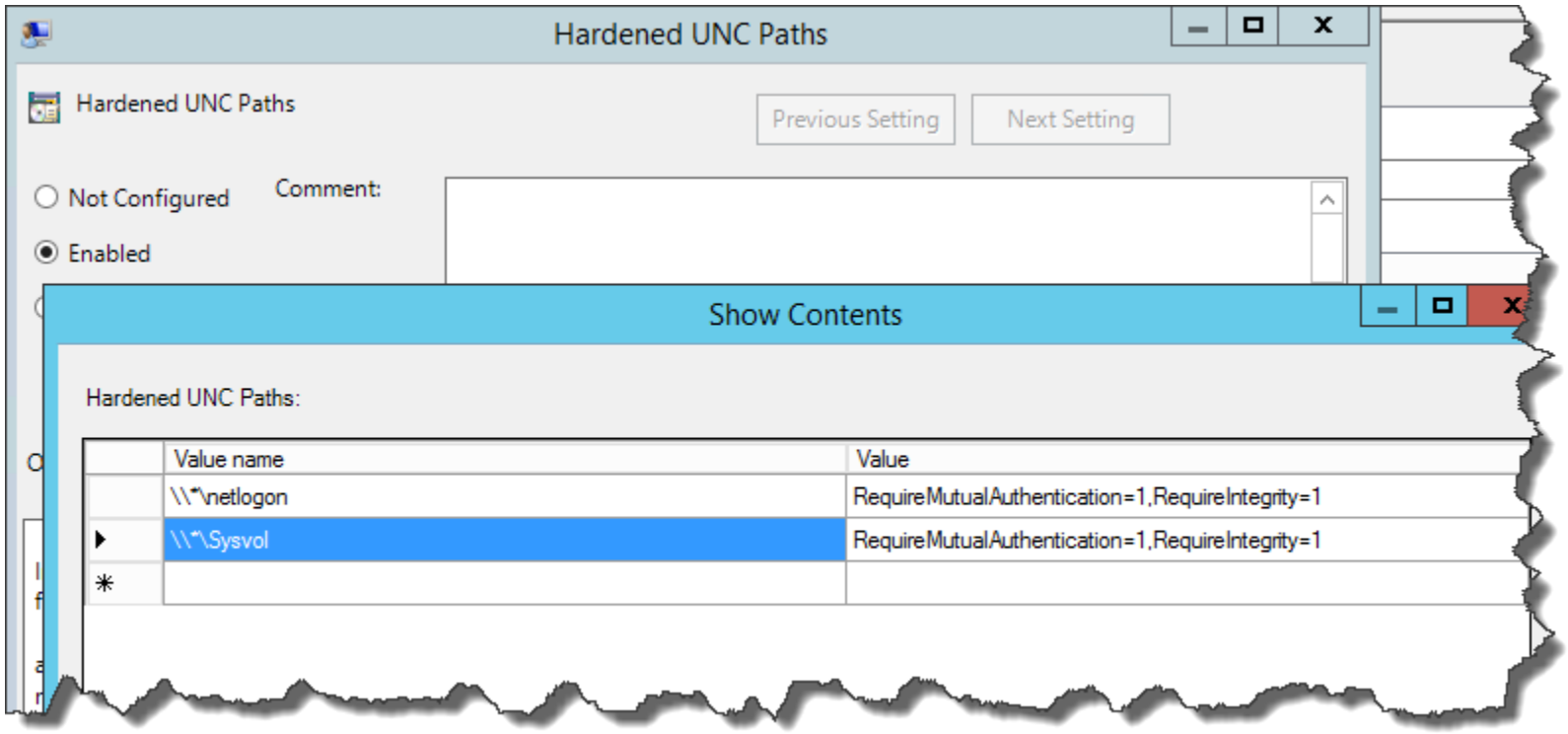
- Ermöglicht das Einschleusen von Gruppenrichtlinien
- Ursache: Der Client prüft beim Download der Richtlinien nicht die Quelle der Richtlinien
- Ein weiterer Bug erlaubt das Zurücksetzen sämtlicher Sicherheitseinstellungen
- Bugfixes:
  MS15-014 >
  MS15-011 > Implementiert SMB-Signaturen, gegenseitige Authentifizierung und optional SMB-Verschlüsselung

Die implementieren Härtungen müssen manuell aktiviert werden!

https://sdmsoftware.com/group-policy-blog/security-related/understanding-jasbug-vulnerability-group-policy/

Härten

Netz-Weise
Lernen von den Besten.

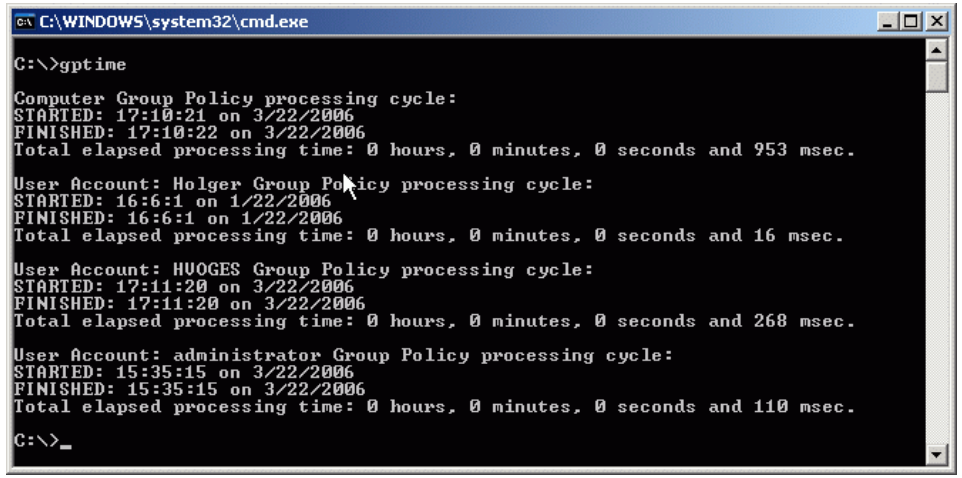


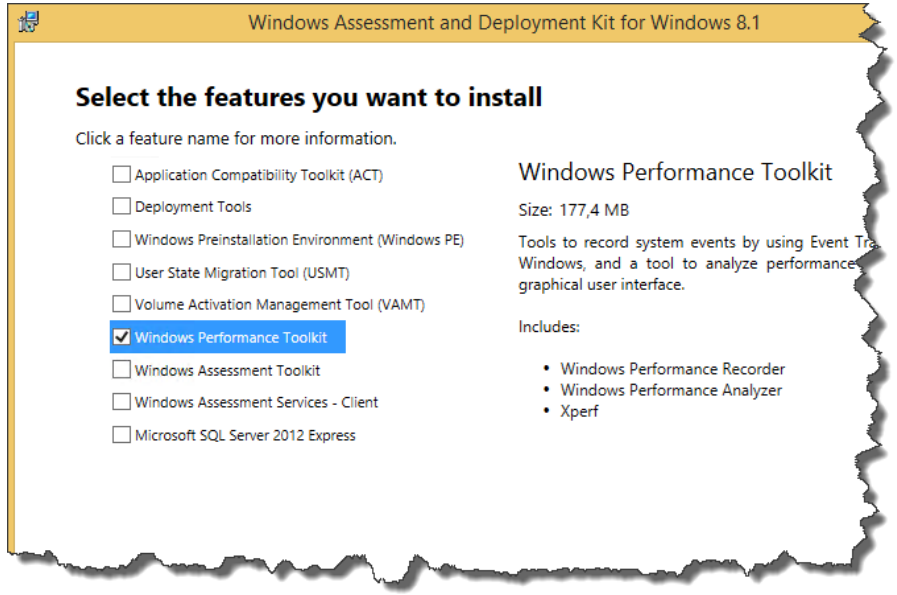
NetworkProvider.ADMX

Den Anmeldevorgang prüfen

Netz-Weise
Lernen von den Besten.

- GPTime zeigt die Zeit an, die eine einzelne Gruppenrichtlinie bis zum Beenden der Abarbeitung gebraucht hat http://www.gpoguy.com
- Procmon kann den Anmeldevorgang protokollieren
- Mit dem Windows-Performance Toolkit kann die Anmeldezeit gemessen werden





Troubleshooting ab Vista

Netz-Weise
Lernen von den Besten.

- 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
- Alternativ kann Powershell oder Logparser verwendet werden

- Troubleshooting Group Policy Event Logs https://technet.microsoft.com/de-DE/library/7e940882-33b7-43db-b097-f3752c84f67f

Event-ID Range

Netz-Weise
Lernen von den Besten.

Range	Description
4000–4007	Group Policy start events: These informational events appear in the event log when an instance of Group Policy processing begins.
4016–4299	Component start events: These informational events appear in the event log when a component of Group Policy processing begins the task described in the event.
5000–5299	Component success events: These informational events appear in the event log when a component of Group Policy processing successfully completes the task described in the event.
5300–5999	Informative events: These informational events appear in the event log during the entire instance of Group Policy processing and provide additional information about the current instance.
6000–6007	Group Policy warning events: These warning events appear in the event log when an instance of Group Policy processing completes with errors.
6017–6299	Component warning events: These warning events appear in the event log when a component of Group Policy processing completes the task described in the event with errors.
6300–6999	Informative warning events: These warning events appear in the event log to provide additional information about possible error conditions with the action described in the event.
7000–7007	Group Policy error events: These error events appear in the event log when the instance of Group Policy processing does not complete.
7017–7299	Component error events: These error events appear in the event log when a component of Group Policy processing does not complete the task described in the event.
7300–7999	Informative error events: These error events appear in the event log to provide additional information about the error condition with the action described in the event.
8000–8007	Group Policy success events: These informational events appear in the event log when the instance of Group Policy completes successfully.

Einfaches zuordnen von Log-Einträgen

Netz-Weise
Lernen von den Besten.

- Im Eventlog wird für jedes Überprüfen der gpo´s eine Activity-ID erzeugt.
- EventID´s: 4000 bis 4007
- Die Activity-ID ist eine Sequenznummer, die alle Ereignisse eines gpo-Refresh zusammenfasst.

GPLogView

Netz-Weise
Lernen von den Besten.

- 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`

Richtlinien dokumentieren

Netz-Weise
Lernen von den Besten.

- Mit GMPC können gpo-Einstellungen exportiert werden (HTML, XML)
- Mit Powershell kann dieser Vorgang automatisiert werden

```
Get-GPOReport -ReportType Html -Path c:\gpbackup\policies.hta –All
```

```
Get-GPO -All | ForEach-Object { Get-GPOReport -ReportType Html -
Path "c:\gpobackup\$($_.displayname).hta" -guid $_.ID }
```

Replikationsstatus in GPMC

Netz-Weise
Lernen von den Besten.

- DFS-Replikation für die Synchronisation des SYSVOL-Ordners
- Der Status der Replikation kann über die GPMC überprüft werden
- Alternativ kann das Powershell-Script get-adgporeplication verwendet werden, um einzelne Richtlinien zu prüfen