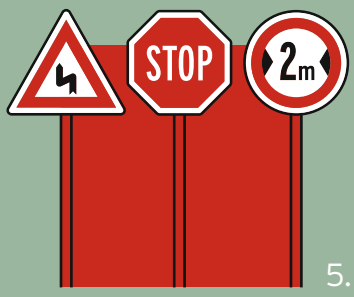
holger VOGES



5. Auflage

VERWALTUNG VON WINDOWS 10

mit Gruppenrichtlinien und Intune

Ein praktischer Leitfaden

Für Windows-Server und -Clients

HANSER

Voges

Verwaltung von Windows 10
mit Gruppenrichtlinien und Intune

Holger Voges

Verwaltung von Windows 10 mit Gruppenrichtlinien und Intune

Ein praktischer Leitfaden

5., aktualisierte und erweiterte Auflage

HANSER

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Sylvia Hasselbach
Copy editing: Sandra Gottmann, Wasserburg
Herstellung: Irene Weilhart
Umschlagdesign: Marc Müller-Bremer, München, www.rebranding.de
Umschlagrealisation: Max Kostopoulos
Titelmotiv: © Max Kostopoulos
Gesamtherstellung: Eberl & Kœsel, Krugzell
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702
Printed in Germany

Print-ISBN: 978-3-446-46389-9
E-Book-ISBN: 978-3-446-46772-9
E-ePub-ISBN: 978-3-446-46773-6

Inhalt

Vorwort

Liebe LeserInnen,

Sie halten die inzwischen 5. Auflage dieses Buches in der Hand, das im Laufe von über 10 Jahren nicht nur zwei verschiedene Autoren, sondern auch mehrere Titelwechsel erlebt hat. Der Titel dieser Ausgabe soll widerspiegeln, dass der Fokus nicht mehr allein auf der Konfiguration von Gruppenrichtlinien liegt, sondern auch das Thema Microsoft PowerShell streift und Microsoft Intune sowie die Verwaltung von Windows-Ereignisprotokollen behandelt. Speziell Intune und Ereignisprotokolle sind in der Vorauflage erwähnt, jedoch aus Zeit- und Platzgründen nicht behandelt worden. Aber Platz ist ja in der kleinsten Hütte, und für die Zeit hat im Jahr 2020 COVID-19 gesorgt. So entsteht aus schlechten Dingen manchmal auch Gutes.

Neben einigen Fehlerkorrekturen, die ich vor allem Ihrem Feedback verdanke, habe ich in dieser Ausgabe das Kapitel über die Änderungen in Windows 10 auf den neuesten Stand gebracht. Wesentliche Änderungen haben sich vor allem im Windows-Servicemodell ergeben, die auch eine Reihe von neuen Gruppenrichtlinien mit sich bringen. Außerdem darf natürlich der neue, Chromium-basierte Edge-Browser nicht fehlen.

Dem Thema Windows-Ereignisanzeige habe ich aufgrund der Komplexität ein komplettes Kapitel gewidmet. Es behandelt die Konfiguration nicht nur aus Gruppenrichtliniensicht, sondern beschreibt ausführlich, wie das Ereignisprotokoll funktioniert und wie Sie es mit Bordmitteln zentral speichern können (Ereignisprotokoll-Weiterleitung).

Die mit Abstand umfangreichste Neuerung betrifft Microsoft Intune. Intune ist ein von Microsoft gehosteter Dienst, der es Ihnen erlaubt, Ihre Clients immer und zu jeder Zeit aus dem Internet heraus zu verwalten, ohne dafür eine eigene Server-Infrastruktur zur Verfügung zu stellen. Das Buch geht dabei vor allem auf die Ähnlichkeiten zu Gruppenrichtlinien ein, ohne das Thema vollständig behandeln zu wollen. Die komplette Thematik würde ein eigenes Buch erfordern. Trotzdem werden Sie im deutschsprachigen Raum aktuell nichts finden, das die Thematik ähnlich umfangreich abdeckt.

Entfernt wurde hingegen das Kapitel über Desired State Configuration (DSC). Das Thema ist nach wie vor interessant, sein Haupteinsatzweck liegt aber im Cloud Deployment. Die großen Schatten, die es im Bereich der Konfigurationsverwaltung vorauswarf, gehörten dann doch eher einem Scheinriesen[1].

[1] *https://de.wikipedia.org/wiki/Scheinriese*

Wenn Sie trotz ausgiebiger Kontrolle meinerseits Fehler in diesem Buch finden, schicken Sie mir bitte eine Mail an *holger.voges@netz-weise.de*. Ich werde Korrekturen als Errata unter *https://Gruppenrichtlinien.training* zur Verfügung stellen.

Wie immer an dieser Stelle ein Dank an meine Partnerin, die nicht nur als Corona-Heldin hilft, das System am Laufen zu halten, sondern mich seelisch und moralisch aufgebaut hat, wenn mich Intune wieder an den Rand eines Nervenzusammenbruchs gebracht hat.

Und nun viel Spaß beim Lesen.

Holger Voges

Wissenswertes zu diesem Buch

Diese kurze Einleitung enthält wichtige Informationen zum Inhalt des Buches und weiterführende Quellen. Auch wenn Sie niemals Vorworte lesen, sollten Sie dieses Kapitel nicht überspringen – es ist kein Vorwort!

Inhalt

Dieses Buch ist in 20 Kapitel gegliedert. Die Kapitel bauen zum Teil aufeinander auf, müssen aber nicht unbedingt in der vorgegebenen Reihenfolge gelesen werden.

- *Kapitel 1* gibt Ihnen einen Überblick darüber, was man unter Gruppenrichtlinien versteht.
- In *Kapitel 2* finden Sie eine Beschreibung der wichtigsten Funktionen der Gruppenrichtlinien-Verwaltungskonsole (GPMC). Außerdem erfahren Sie, wie Sie Gruppenrichtlinienobjekte anlegen und verwalten können.
- *Kapitel 3* behandelt die Verarbeitungsreihenfolge von Gruppenrichtlinienobjekten (GPOs). Das Verständnis der Verarbeitungsreihenfolge ist enorm wichtig, da alle GPOs von den gleichen Vorlagen abgeleitet sind und Einstellungen sich daher gegenseitig überschreiben können.
- In *Kapitel 4* erfahren Sie, wie Sie die Anwendung von GPOs auf bestimmte Benutzer oder Computer einschränken können, indem Sie Filter verwenden.
- *Kapitel 5* widmet sich der Planung von GPOs und den Aspekten, die man beim AD-Design beachten sollte, um Gruppenrichtlinien effizient anwenden zu können.
- In *Kapitel 6* werden die Grundlagen der Softwareverteilung mit Gruppenrichtlinien-Bordmitteln vermittelt. Da die Fähigkeiten von Windows hier sehr eingeschränkt sind, wird danach die Erweiterung von GPOs am Beispiel von „Specops Deploy/App“ gezeigt, einem Fremdherstellertool, das die Softwareverteilung stark erweitert bzw. ersetzt.
- *Kapitel 7* zeigt die Sicherheitseinstellungen, die Sie für Computer per Gruppenrichtlinien konfigurieren können. Das Kapitel geht nicht auf alle Details ein, verschafft Ihnen aber einen guten Überblick über die Möglichkeiten, Sicherheitseinstellungen zentral vorzunehmen.
- *Kapitel 8* geht am Beispiel einzelner administrativer Vorlagen auf die Möglichkeiten ein, Computer und Benutzer zu konfigurieren.

- In *Kapitel 9* erfahren Sie, wie Gruppenrichtlinien-Vorlagen funktionieren und wie Sie sie nutzen können, um GPOs für Ihre eigenen Zwecke zu erweitern.
- In *Kapitel 10* werden Funktionen wie Ordnerumleitung gezeigt, die im Knoten „Windows-Einstellungen" im Benutzer-Teil der Gruppenrichtlinien zu finden sind.
- Mit Windows Vista haben die Gruppenrichtlinieneinstellungen in Windows Einzug gehalten. Gruppenrichtlinieneinstellungen können Login-Skripte fast vollständig ersetzen. In *Kapitel 11* finden Sie eine ausführliche Beschreibung der Funktionsweise.
- *Kapitel 12* befasst sich mit Windows 10, den einzelnen Features-Releases und neuen Funktionen, die mit Windows 10 zum ersten Mal eingeführt worden sind.
- *Kapitel 13* ist ein Kapitel für Fortgeschrittene. Es zeigt, was bei der Verarbeitung von Gruppenrichtlinien auf Client und Server passiert. Wenn es Sie nicht interessiert, wie Windows Gruppenrichtlinien anwendet, können Sie dieses Kapitel überspringen.
- *Kapitel 14*, Verwalten von GPOs, geht auf die Verwaltungsaufgaben wie das Sichern und die Wiederherstellung von GPOs ein.
- *Kapitel 15* zeigt Ihnen, wie Sie vorgehen können, wenn Ihre Gruppenrichtlinien sich nicht so verhalten, wie Sie das erwarten. Anhand von verschiedenen Werkzeugen wird gezeigt, wie Sie Fehler aufspüren und beheben können.
- *Kapitel 16*, Advanced Group Policy Management (AGPM), behandelt die Bearbeitung von Gruppenrichtlinien im Team. Sie benötigen dafür aber eine Zusatzsoftware, die bei Microsoft lizenziert werden muss.
- *Kapitel 17* stellt eine Einführung in die Clientverwaltung mit Microsoft Intune dar. Außerdem erfahren Sie hier, wie Sie ein Intune-Konto anlegen können, um die Beispiele selber anwenden zu können.
- *Kapitel 18*, Clientverwaltung mit Intune, zeigt an einer Reihe von Beispielen, wie Sie Clients konfigurieren, Software verteilen und Reports über die Clientkonfiguration erstellen können.
- *Kapitel 19* befasst sich mit dem Überwachen von Windows mit Hilfe von Ereignisprotokollen. Sie erfahren, wie Sie Ereignisprotokolle zentral anpassen und sammeln können, um auf Bedrohungen frühzeitig zu reagieren.
- *Kapitel 20* fasst alle Themenbereiche rund um das Skripting zusammen. Sie erfahren, wie Sie mit Gruppenrichtlinien Start- und Anmeldeskripte ausführen können, wie Sie mithilfe von PowerShell viele Verwaltungsaufgaben automatisieren und auf welche Weise Sie mit AppLocker die Ausführung von PowerShell einschränken oder verhindern können.

PowerShell-Skripte

In einigen Kapiteln dieses Buches werden verschiedene hilfreiche PowerShell-Skripte beschrieben, welche die Verwaltung von Gruppenrichtlinien vereinfachen. Sie finden alle Codeschnipsel in erweiterter Form als PowerShell-Modul auf der Website zum Buch, *www.gruppenrlinien.training* sowie in der PowerShell-Gallery von Microsoft. Um es zu installieren, entpacken Sie das Modul in einen der Pfade, die in der Umgebungsvariablen `%PSModulePath%` hinterlegt sind. Die Datei muss vorher entblockt werden (s. Bild 1). Alternativ können Sie es über die PowerShell-Gallery über den Befehl `Install-Module -Name`

`GroupPolicyHelper` installieren. Das Modul wird ständig erweitert. Mehr Informationen zu PowerShell-Modulen finden Sie in Abschnitt 17.4 im Kasten „PowerShell-Module“.

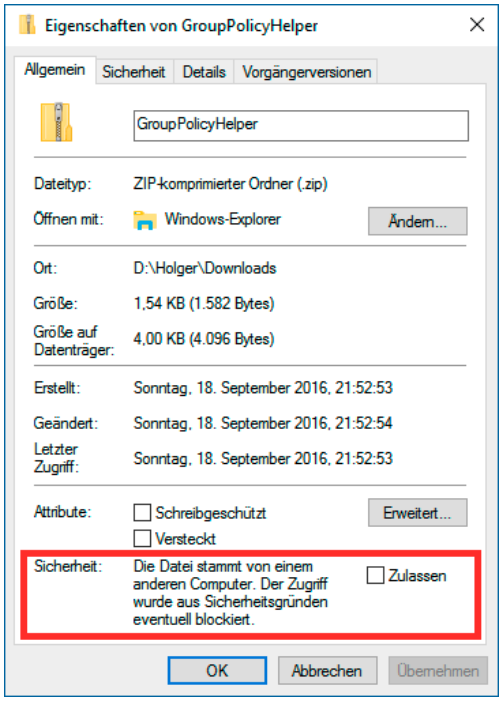


Bild 1
Aus dem Internet heruntergeladene Dateien müssen zugelassen werden.

Linkkürzungen

Ich habe versucht, Ihnen das Eingeben von Links so einfach wie möglich zu machen. Dafür finden Sie hinter allen komplizieren Links eine Kurzform, die den Bitly.com-Dienst nutzt. Der Kurzlink wird eingeführt über „oder kurz“ und startet mit *https://bit.ly/*.

Videos

Da ein Bild mehr als 1000 Worte sagt und ein Video aus vielen Bildern besteht, habe ich einige der hier im Buch behandelten Themen auch als Video veröffentlicht. Dafür habe ich den YouTube-Channel „Gruppenrichtlinien in Windows Server" eingerichtet. Sie finden ihn unter *https://www.youtube.com/channel/UCmV-KA9FZaanVcIY72wIkbw* oder kurz *https://bit.ly/2uMpuY7*.

Aktualisierungen

Administrative Vorlagen sind im Buch in zwei Kapiteln besprochen, aber trotzdem ist es nicht möglich, alle durchzugehen. Daher habe ich mich dazu entschlossen, das auch für Windows 10 nicht zu tun, zumal mit Windows as a Service sowieso ständig mit neuen Gruppenrichtlinien zu rechnen ist. Stattdessen finden Sie unter *https://www.netz-weise.de/weisheiten/doku.html* eine Reihe von Dokumenten zur Verwaltung von Gruppenrichtlinien.

Nutzen Sie auch meinen Blog als Informationsquelle. Unter *https://www.Netz-Weise-it.training/weisheiten/tipps.html* schreibe ich regelmäßig über verschiedene IT-Themen, die mich beschäftigen. Sie finden hier einige Informationen zum Thema Gruppenrichtlinien. Wenn Sie sich für Hyper-V, SQL Server, Windows oder PowerShell interessieren, ist vielleicht auch das eine oder andere für Sie dabei. Außerdem ist der Blog von Mark Heitbrink sehr empfehlenswert, der unter *http://www.gruppenrichtlinien.de/* einen reichhaltigen Fundus an Informationen zur Verfügung stellt.

Nomenklatur

Im Umfeld von Gruppenrichtlinien gibt es eine Reihe von Fachbegriffen, die z. T. nicht ganz einfach zu unterscheiden sind. Das Ganze wird durch schlechte englische Übersetzungen nicht einfacher gemacht. Es folgt eine kleine Definition der wichtigsten Begriffe und Abkürzungen. Ich fürchte, dass auch in diesem Buch durch die Arbeit von ursprünglich zwei Autoren die Benennung trotz aller Anstrengungen nicht immer konsistent ist.

Begriff	Erläuterung
Gruppenrichtlinie	Eine einzelne Einstellung, die auf einen Computer oder Benutzer angewendet werden kann
Gruppenrichtlinienobjekt (GPO)	Gruppenrichtlinien werden in Gruppenrichtlinienobjekten zusammengefasst. Ein GPO ist keine Gruppenrichtlinie! Die Definition wird aber trotzdem oft synonym verwendet.
Gruppenrichtlinien-Vorlage (GPT)	Die Gruppenrichtlinien-Vorlage bezeichnet den Ordner im Dateisystem, in dem die meisten der Gruppenrichtlinien abgelegt sind.
Gruppenrichtlinien-Container (GPC)	Das Objekt, das im AD angelegt wird, wenn man ein neues GPO erstellt, wird auch als Group Policy Container bezeichnet.
Gruppenrichtlinieneinstellungen	Microsoft hat mit Windows Vista neue Einstellungsmöglichkeiten eingeführt, die im Englischen als „Group Policy Preferences“ bezeichnet werden. Im Deutschen wurde das zu „Gruppenrichtlinieneinstellungen“ übersetzt, was sehr missverständlich ist, weil es sich eben nicht um einen Oberbegriff für alle Einstellungen handelt (der Oberbegriff ist Gruppenrichtlinie), sondern um eine ganz spezielle Gruppe von Einstellungen.
Gruppenrichtlinien-Verwaltungskonsole (GPMC)	Das Werkzeug zur Verwaltung von GPOs
Gruppenrichtlinien-Editor	Das Werkzeug zum Bearbeiten eines GPO und zum Setzen von einzelnen Gruppenrichtlinien

Windows 10

Microsoft hat angekündigt, dass Windows 10 das letzte Windows Client-Betriebssystem sein wird, das sie veröffentlichen. Statt alle paar Jahre eine neue Windows-Version herauszubringen, erhält man Windows as a Service, was nichts weiter bedeutet, als dass man im Zeitraum von sechs Monaten Upgrades erhält, die neue Funktionen nachrüsten. Unternehmen können das verhindern, indem sie die LTSC-Version von Windows 10 nutzen – der sogenannte Long Term Servicing Channel. Die LTSC-Version steht aber nur für Windows 10 Enterprise Edition zur Verfügung.

Wenn Sie die Professional Version von Windows 10 einsetzen, müssen Sie damit rechnen, dass Sie in Zukunft nicht mehr alle Gruppenrichtlinien verwenden können. Microsoft hat sich dazu entschieden, nur die Enterprise Edition vollständig zu unterstützen. Eine Liste aller Gruppenrichtlinien, die seit der Version 1607 von Windows 10 nicht mehr unterstützt werden, finden Sie unter *https://docs.microsoft.com/de-de/windows/client-management/group-policies-for-enterprise-and-education-editions* oder kurz *https://bit.ly/2CfO2yM*.

1 Einleitung

In diesem Kapitel werden folgende Fragen beantwortet:

- Was sind Gruppenrichtlinien?
- Mit Gruppenrichtlinien arbeiten
- Welche technische Ausstattung benötigen Sie, um die im Buch beschriebenen Aufgaben nachvollziehen zu können?

1.1 Was sind Gruppenrichtlinien?

Gruppenrichtlinien sind Benutzer- oder Computereinstellungen, die zentral konfiguriert und abgelegt sind und auf einen oder eine Gruppe von Computern oder Benutzern angewendet werden können. Gruppenrichtlinien werden in Sammlungen, sogenannten Group Policy Objects (GPO), zusammengefasst – merken Sie sich diesen Begriff, es ist das meistverwendete Kürzel in diesem Buch. Viele dieser Einstellungen werden dabei in der Systemregistrierung vorgenommen, einige Einstellungen liegen aber auch außerhalb der Systemregistrierung in Form von Dateien oder im Active Directory vor. Mehr zur Funktionsweise erfahren Sie in Kapitel 13, „Funktionsweise von Gruppenrichtlinien“.

Mit Gruppenrichtlinien kann man eine rudimentäre Form der Softwareverteilung durchführen, Sicherheitseinstellungen auf Computern zentral vorgeben und erzwingen, Dienste konfigurieren, Datei- und Registry-Einstellungen setzen, An- und Abmeldeskripte konfigurieren, die Oberfläche des Benutzers umkonfigurieren, Funktionen an- oder abschalten sowie konfigurieren, Zertifikate verteilen und noch vieles mehr.

Zusätzlich zu den Richtlinien wurden mit Server 2008 die Einstellungen eingeführt – eine nicht besonders gelungene Übersetzung aus dem Englischen, wo diese Erweiterung Preferences heißt, was so viel wie Vorzüge oder Vorteile bedeutet. Einstellungen erlauben es,

klassische Anmeldeskriptaufgaben wie das Verbinden von Netzlaufwerken oder Druckern auszuführen oder Dateien auf den Zielrechner zu kopieren. Mehr hierzu erfahren Sie in Kapitel 11, „Gruppenrichtlinien-Einstellungen“.

1.2 Auf welche Objekte wirken Gruppenrichtlinien?

Gruppenrichtlinien haben mit Gruppen nur wenig zu tun, auch wenn der Name dies suggeriert. Zwar kann man auch über Gruppenzugehörigkeiten steuern, ob eine Gruppenrichtlinie auf einen Benutzer oder Computer angewendet werden darf – mehr hierzu in Kapitel 4, „Gruppenrichtlinien filtern“ –, aber Anwendung finden Gruppenrichtlinien nur auf Benutzer- oder Computerkonten. Gruppenrichtlinien wirken niemals auf Gruppen, und das ist auch gut so, denn sonst würden Gruppenrichtlinien sich nicht mehr verwalten lassen.

Welche Gruppenrichtlinien auf ein Benutzer- oder Computerobjekt wirken, hängt einzig vom Speicherort des Kontos im AD ab. Gruppenrichtlinien werden im AD mit drei Typen von Objekten verknüpft, mit Standorten, der Domäne und Organisationseinheiten unterhalb des Domänenobjekts. Ein Konto, das sich „unterhalb“ einer Gruppenrichtlinie befindet, also in einer OU (Organisational Unit), die von einer Gruppenrichtlinie betroffen ist, wird auch durch die Gruppenrichtlinie konfiguriert. Gruppenrichtlinieneinstellungen sind dabei additiv. Liegt ein Konto also im Einflussbereich mehrerer Richtlinien, so werden die Einstellungen aller Richtlinien addiert angewendet.

1.3 Wann werden Gruppenrichtlinien verarbeitet?

Gruppenrichtlinien werden bei der Anmeldung und dem Systemstart verarbeitet. Außerdem findet eine regelmäßige Hintergrundaktualisierung statt. Alle 90 Minuten mit einer zufälligen Abweichung von +30 Minuten gleicht ein Computer seine Einstellungen mit denen der Domäne ab[1]. Bei Domänencontrollern liegt das Standardintervall bei fünf Minuten. Die zufälligen Abweichungen werden eingesetzt, damit nicht alle Computer gleichzeitig die Richtlinien abfragen und das Netzwerk und die Server überlasten.

[1] Genau genommen passiert dies sogar noch häufiger, da der Computer die Einstellungen des Computers und die des Benutzers unabhängig voneinander konfiguriert.

PRAXISTIPP: Sie können diese Werte auch ändern – in einer Gruppenrichtlinie! Sehr kurze Aktualisierungsintervalle sind aber nicht zu empfehlen, da sie das System und das Netzwerk belasten. Zu seltene Hintergrundaktualisierungen können hingegen dazu führen, dass wichtige Änderungen nicht in einer akzeptablen Zeit übernommen werden. Daher sollten Sie in der Regel die Standardwerte beibehalten.

1.4 Wie viele Gruppenrichtlinien sollte man verwenden?

Generell gilt, dass die Verarbeitung von Gruppenrichtlinien den Start- und Anmeldevorgang erheblich verzögern kann. Wenn Sie die Einstellungen auf viele GPOs verteilen, kann dies zulasten der Performance gehen. Daher kann es, wenn Sie sehr viele Gruppenrichtlinien konfigurieren, durchaus sinnvoll sein, viele Einstellungen auf wenige GPOs zu verteilen. Außerdem kann man Gruppenrichtlinien in Bereichen deaktivieren, da Sie aus einem Computer- und einem Benutzeranteil bestehen, die getrennt verarbeitet werden.

Eine genauere Betrachtung der Auswirkungen auf die Anmeldeperformance und wie Sie diese prüfen können, finden Sie in Kapitel 15, „Fehlersuche und Problembehandlung“.

Gruppenrichtlinien sind ein mächtiges Werkzeug, mit dem eine Fülle von Einstellungen und Anpassungen möglich ist. In der Praxis werden Sie jedoch nur die Anpassungen vornehmen wollen, die für Ihr Netzwerk wichtig sind. Bei deutlich über 3000 Richtlinien ohne zusätzliche Vorlagen verlieren sonst auch erfahrene Administratoren den Überblick.

Die wichtigsten Bereiche der Gruppenrichtlinien lernen Sie in den folgenden Kapiteln kennen und sehen dabei viele Beispiele für den Einsatz in der Praxis.

1.5 Worauf muss man beim Ändern von Einstellungen achten?

Gruppenrichtlinien wirken, sobald eine Einstellung übernommen wurde. Wenn Sie Einstellungen vorgenommen haben, in denen Sie z. B. der Systemgruppe „Jeder“ das Recht zum lokalen Anmelden verweigern, ist diese Einstellung ab dem Zeitpunkt aktiv, in dem Sie OK klicken. Sobald ein Client diese Einstellung zieht, ist sie auf dem Client wirksam. Aber auch durch versehentliche Fehlkonfigurationen kommt es immer wieder zu Problemen mit Richtlinien. Darum werden Sie in diesem Buch exemplarische Vorgehensweisen finden, die Ihnen einen sicheren Umgang mit den Gruppenrichtlinien vermitteln. Für häufige Probleme werden auch Lösungen bereitgestellt.

1.6 Was Sie brauchen, um die Aufgaben nachvollziehen zu können

Die Verwaltung von Gruppenrichtlinien sollten Sie immer in einer abgesicherten Testumgebung ausprobieren, bevor Sie beginnen, damit in der Praxis zu arbeiten. Um die Beispiele dieses Buches nachvollziehen zu können, empfehle ich Ihnen mindestens eine virtuelle Maschine mit Windows Server 2016 und eine Reihe von Testclients mit Windows 7, Windows 8.1 und Windows 10 oder zumindest den Betriebssystemen zu installieren, die bei Ihnen im Unternehmen zum Einsatz kommen. Achten Sie darauf, dass Sie für Domänenumgebungen mindestens die Professional-Varianten des Client-Betriebssystems benötigen, für manche Funktionen auch die Enterprise-Variante.

Die virtuellen Maschinen müssen über das Netzwerk miteinander kommunizieren können, Internetzugang wird hingegen keiner benötigt. Ab Windows 8 Professional bietet es sich an, Hyper-V einzusetzen, das als Bestandteil des Betriebssystems mitgeliefert wird. Auf Windows 7 empfiehlt sich das kostenlose Virtual Box.

Richten Sie eine Domäne ein, und nehmen Sie Clients in die Domäne auf. Sie können nun eine Umgebung errichten, die in etwa dem Firmenumfeld, in dem Sie arbeiten, entspricht (typische OU-Struktur, Standorte, Gruppen, Beispielbenutzer etc.), oder Sie warten damit, bis Sie in Kapitel 4 etwas über typische OU-Strukturen für die Arbeit mit Gruppenrichtlinien erfahren haben.

Wenn Sie keine eigene Testumgebung zur Verfügung haben, können Sie auch auf Windows Azure zurückgreifen oder sich eine Testumgebung erstellen. Für dieses Buch können Sie Beispielskripte von der Website *www.gruppenrichtlinien.training* herunterladen.

2 Die Gruppenrichtlinien-verwaltung

In diesem Kapitel werden folgende Themen behandelt:

- Die Gruppenrichtlinienverwaltung hinzufügen
- Mit der Gruppenrichtlinienverwaltung arbeiten
- Gruppenrichtlinienobjekte im Detail
- Gruppenrichtlinienobjekte erstellen
- Gruppenrichtlinienobjekte verknüpfen

2.1 Einführung

Für die Verwaltung von GPOs stellt Microsoft seit Windows Server 2003 die Gruppenrichtlinienverwaltungskonsole (GPMC, Group Policy Management Console) zur Verfügung.

Diese wird automatisch installiert, wenn Sie einen Server zum Domänencontroller machen. Da Sie eine Domäne niemals direkt vom Domänencontroller aus verwalten sollten, können Sie die GPMC auch auf einem anderen Server oder besser noch auf einem administrativen Client installieren.

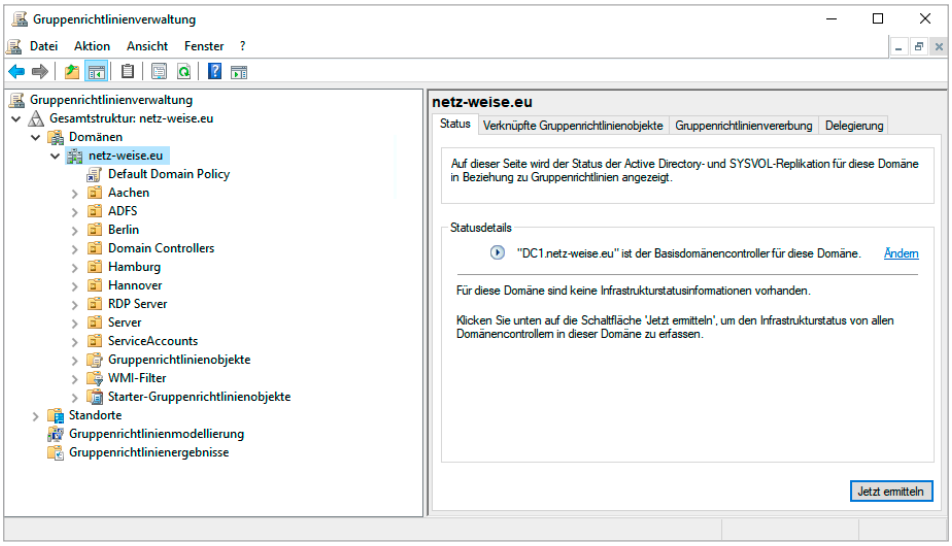


Bild 2.1 Die Gruppenrichtlinienverwaltungskonsole

2.2 Gruppenrichtlinienverwaltung auf einem Server installieren

Die GPMC steht bei Windows Server als installierbares Feature zur Verfügung. Sie müssen sie nur über den Server-Manager oder das Windows Admin Center aktivieren.

Unter Windows Server

Öffnen Sie den Server-Manager und klicken Sie unter **Verwaltung** auf **Rollen und Features hinzufügen**.

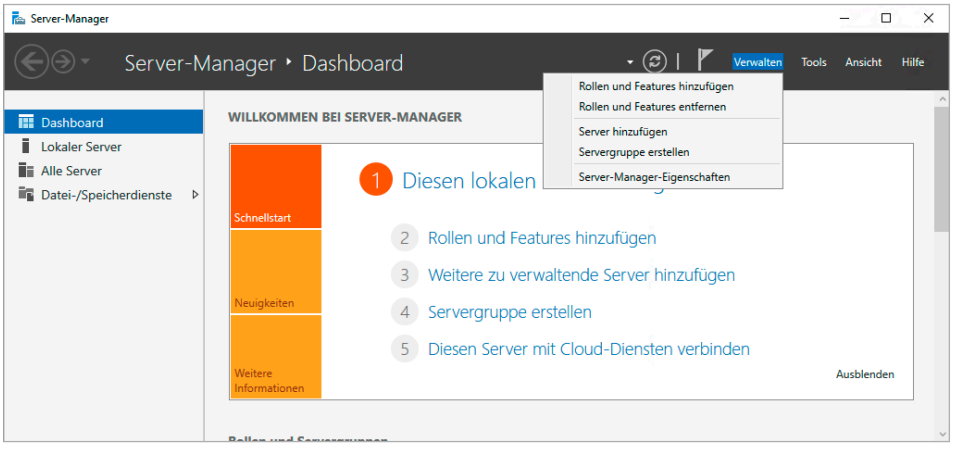


Bild 2.2 Features hinzufügen

Übernehmen Sie im Assistenten die Standardeinstellungen, und wählen Sie dann im Fenster **Features** die Checkbox **Gruppenrichtlinienverwaltung**.

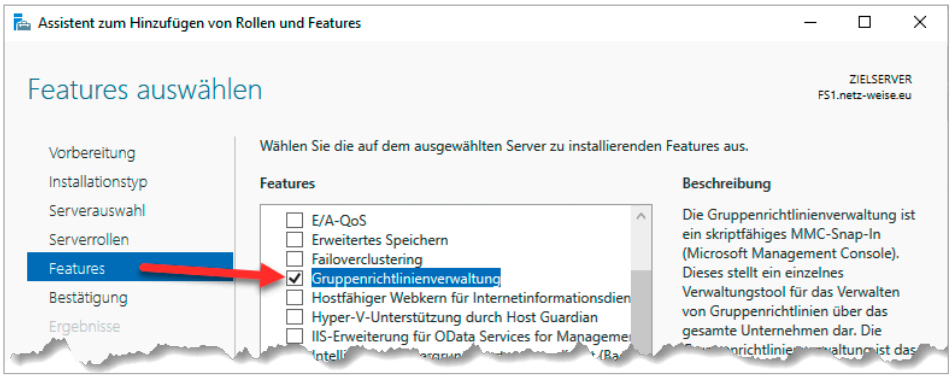


Bild 2.3 Feature Gruppenrichtlinienverwaltung auswählen

Klicken Sie nun **Weiter** und zum Abschluss auf **Installieren**.

Alternativ können Sie die GPMC auch über Windows PowerShell nachinstallieren, indem Sie in einer administrativen PowerShell-Konsole den Befehl `Install-WindowsFeature -Name GPMC` aufrufen.

Auf einem Windows Client

Am empfehlenswertesten ist es, die Administration von einem Client aus auszuführen. Auf dem Client müssen die Administrationswerkzeuge allerdings noch nachinstalliert werden. Sie bekommen den kompletten Satz unter dem Namen „Remote Server Administration Tools“ inklusive des Servers Managers bei Microsoft zum Download. Suchen Sie dafür bei der Suchmaschine Ihres Vertrauens nach „Windows RSAT Tools“. Sie müssen lediglich beachten, dass die RSAT-Tools nicht zwischen den Client-Betriebssystemen kompatibel sind. Wenn Sie die Tools also auf einem älteren Client (Windows 7) installieren, bekommen Sie auch eine alte Version der GPMC. Am besten verwenden Sie immer die aktuellste Windows-Version.

Die RSAT-Tools kommen in Form eines Windows Update-Pakets. Die Installation kann mit einem Doppelklick gestartet werden und benötigt nur ein Akzeptieren der Lizenzbedingungen. Sie brauchen hinterher nichts mehr zu aktivieren, die Tools sind sofort gebrauchsfertig auf dem Client. Ab Windows 10 FR 1809 können Sie die GPMC direkt als optionales Feature aus dem Internet nachinstallieren. Verwenden Sie dafür folgenden PowerShell-Befehl:

```
Add-WindowsCapability -Name Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0 -Online
```

2.3 Gruppenrichtlinienverwaltung erkunden

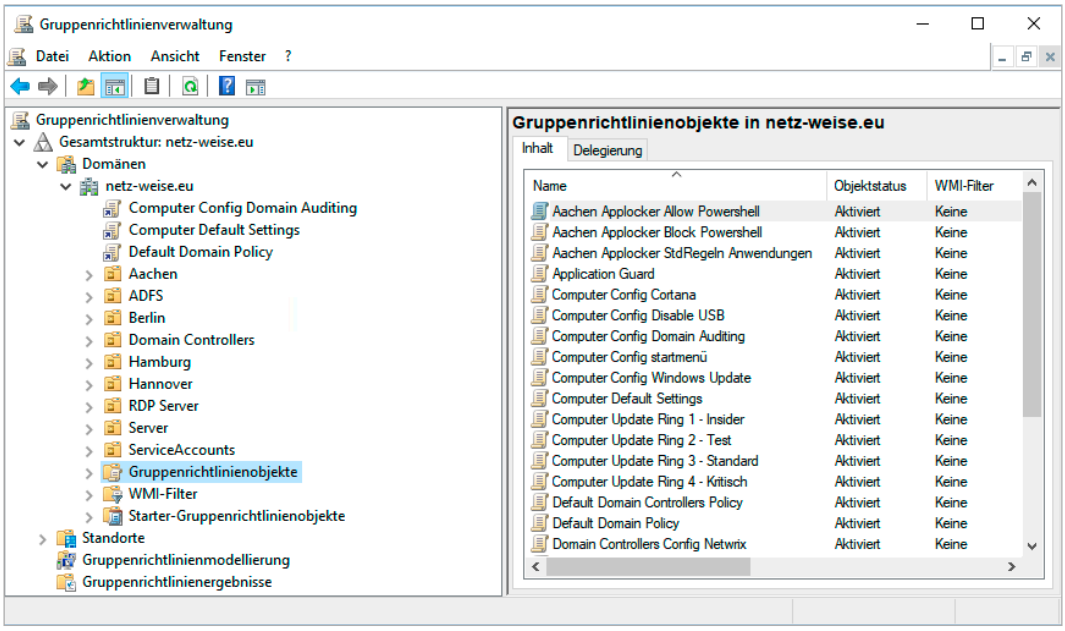


Bild 2.4 Gruppenrichtlinienverwaltung erkunden

Im linken Bereich der GPMC finden Sie die Baumansicht der Gesamtstruktur mit allen Ihren Domänen und Standorten. Öffnen Sie den Knoten „Gruppenrichtlinienobjekte“ unterhalb der Domäne. Hier finden Sie die Gruppenrichtlinienobjekte (GPOs).

PRAXISTIPP: Am schnellsten starten Sie die GPMC über den Ausführen-Befehl. Drücken Sie hierzu gleichzeitig **Windows+R**. Im Ausführen-Fenster, das sich nun öffnet, geben Sie gpmc.msc an und bestätigen mit **Enter**.

2.4 Gruppenrichtlinienverknüpfungen und -objekte

Im Gegensatz zum Symbol des GPO „Default Domain Policy“ im Container Gruppenrichtlinienobjekte trägt das Symbol der „Default Domain Policy“ unterhalb des Domänennamens einen kleinen Pfeil – es handelt sich um eine Verknüpfung.

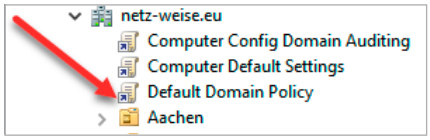


Bild 2.5
GPOs werden im AD erstellt und dann mit OUs verknüpft.

GPOs können auf der Domäne, den Organisationseinheiten und auf Standorten verknüpft werden, gespeichert werden sie aber stets im Container „Gruppenrichtlinienobjekte“.

Sie können ein GPO auch mehrfach verknüpfen und z. B. eine Richtlinie für Benutzer mit den Organisationseinheiten `OU=Benutzer,OU=Hannover,DC=Netz-Weise,DC=eu` und `OU=Benutzer,OU=Hamburg,DC=Netz-Weise,DC=eu` verknüpfen.

2.5 Gruppenrichtlinienobjekte im Detail

Erweitern Sie nun den Knoten „Gruppenrichtlinienobjekte“ und wählen Sie in der Konsolenstruktur die Default Domain Policy.

2.5.1 Register Bereich einer Gruppenrichtlinie

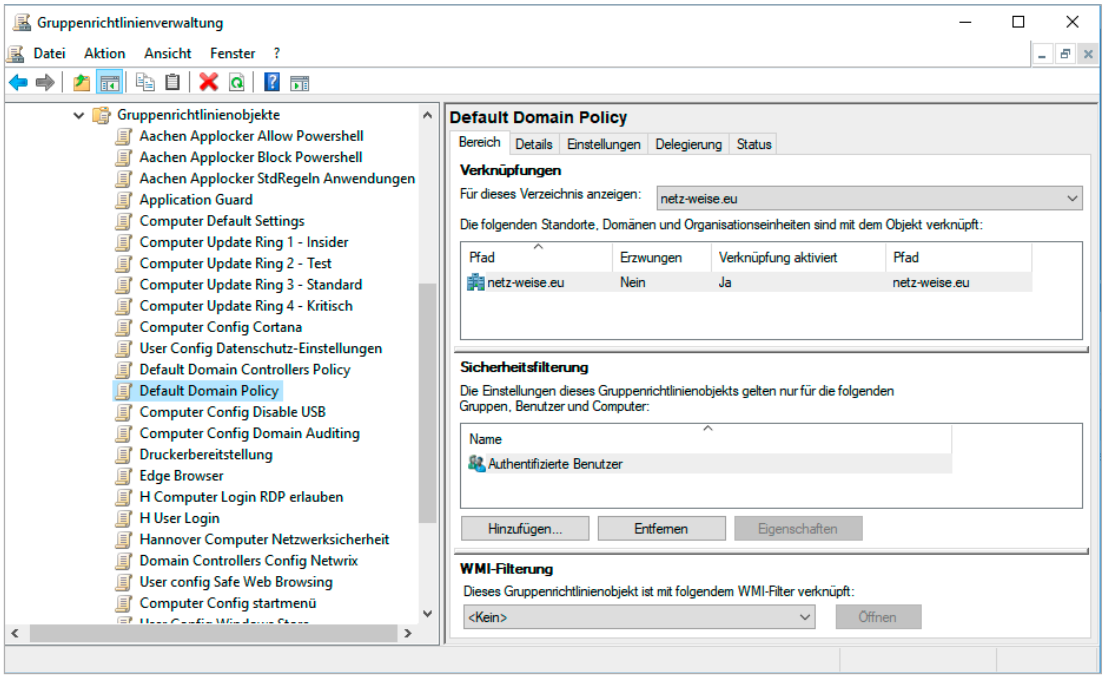


Bild 2.6 Register **Bereich** der Default Domain Policy

Im Register **Bereich** sehen Sie oben „Verknüpfungen“. Hier sind unter „Pfad“ die Domänen und Organisationseinheiten aufgeführt, mit denen das GPO verknüpft ist.

Daneben ist vermerkt, ob die Richtlinie erzwungen wird. Erzwingen bedeutet, dass diese Richtlinien immer Vorrang haben, wenn es zu Konflikten zwischen den Einstellungen unterschiedlicher GPOs kommt. Näheres dazu erfahren Sie in Abschnitt 3.4.4 – „Erzwingen von GPOs“, und in Kapitel 13, „Funktionsweise von Gruppenrichtlinien“.

Verknüpfungen können deaktiviert werden, ohne sie zu löschen. So können Sie GPOs zeitweise unwirksam machen.

In der Mitte des Fensters sind Sicherheitsfilterungen aufgezeigt. Über die Sicherheitsfilterung können Sie festlegen, für welche Benutzer und Computer eine Gruppenrichtlinie gültig wird. Standardmäßig ist stets die Gruppe „Authentifizierte Benutzer“ eingetragen. Zu dieser gehören alle Benutzer und Computer, die sich in der Domäne angemeldet haben.

Sie können die authentifizierten Benutzer entfernen und stattdessen andere Gruppen berechtigen. Dadurch schränken Sie den Kreis der Konten, die von dem GPO betroffen werden, ein. In Abschnitt 4.2.1 – „Sicherheitsfilterung anwenden“, erhalten Sie mehr Details zur Wirkweise der Sicherheitsfilterung.

WMI-Filterung stellt eine Möglichkeit dar, die Wirkung eines GPO auf bestimmte Computer zu beschränken. Allerdings werden für WMI-Filter keine Gruppen verwendet, sondern Hard- oder Softwareeigenschaften eines Rechners abgefragt, anhand derer dann entschieden wird, ob ein GPO angewendet wird oder nicht. WMI-Filter werden ebenfalls in Kapitel 4 behandelt.

2.5.2 Register Details eines GPO

Wählen Sie nun das Register **Details**.

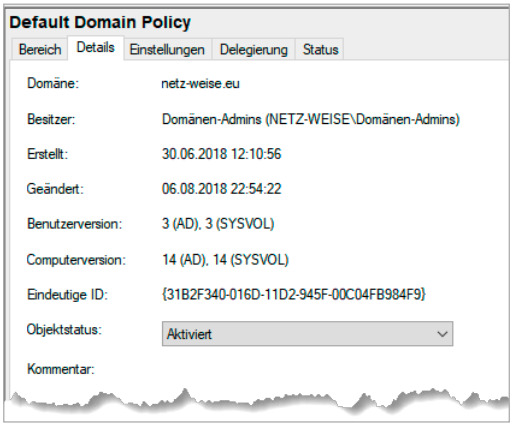


Bild 2.7
Register **Details** der Default Domain Policy

Unter **Details** ist aufgeführt, wer der Besitzer des GPO ist, wann diese erstellt und wann zuletzt geändert wurde, welche Version der Benutzer- und Computereinstellungen vorliegt – mehr hierzu später – und wie die eindeutige ID der Richtlinie lautet. Über „Objektstatus“ können Sie das GPO hier ganz oder teilweise deaktivieren.

2.5.3 Register Einstellungen eines GPO

In der Registerkarte **Einstellungen** finden Sie einen Report über alle aktiven Einstellungen eines GPO. Diese Report ist vor allem dann wichtig, wenn Sie die Einstellungen eines GPO überprüfen wollen. Im Group Policy Editor, der Konsole zum Bearbeiten eines GPO, ist das Suchen nach gesetzten oder nicht gesetzten Einstellungen ein bisschen wie die Suche nach der Nadel im Heuhaufen.

Klicken Sie zum Überprüfen der Einstellungen auf das Register **Einstellungen** und dann im rechten Bereich des Fensters auf **Computerkonfiguration** – **Richtlinien** – **Windows-Einstellungen** – **Sicherheitseinstellungen** – **Kontorichtlinien/Kennwortrichtlinien**. Sie können hier die einzelnen Einstellungen sehen, die im Knoten „Kennwortrichtlinien“ vorgenommen wurden. Was diese Einstellungen bedeuten, erfahren Sie in Kapitel 7, „Sicherheitseinstellungen“.

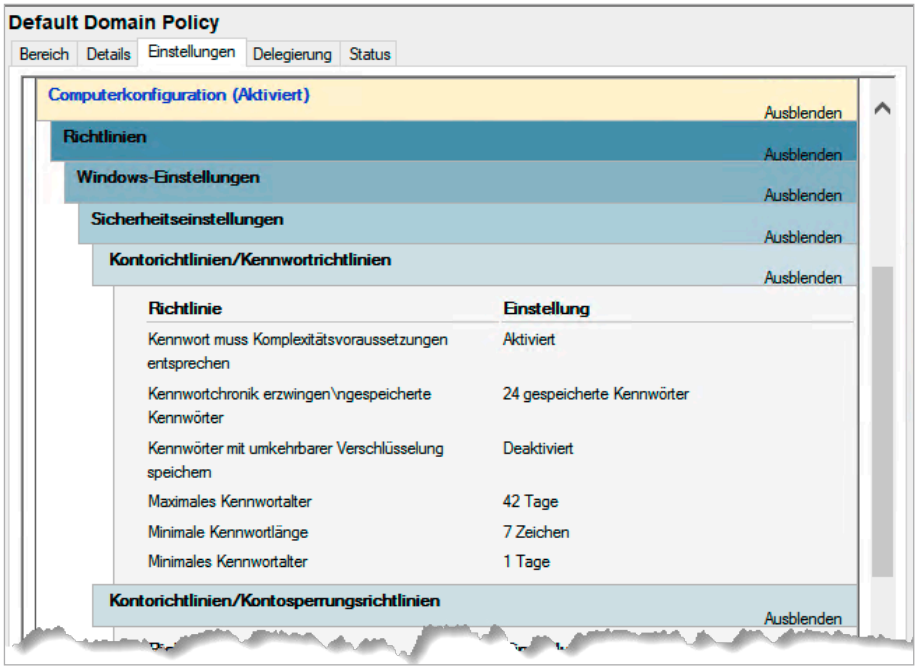


Bild 2.8 Register **Einstellungen** der Default Domain Policy

2.5.4 Register Delegierung eines GPO

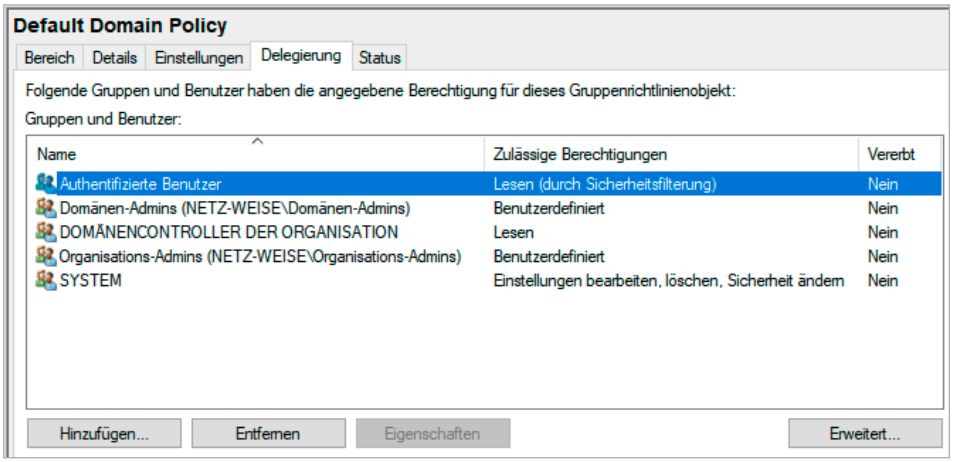


Bild 2.9 Register **Delegierung** der Default Domain Policy

Unter dem Register **Delegierung** sind die einzelnen Gruppen und deren Berechtigungen auf das Gruppenrichtlinienobjekt differenziert aufgeführt. Die Sicherheitsfilterung, die Sie bereits unter **Bereich** konfigurieren konnten, wird tatsächlich hier angewendet. Über die Delegierung können aber auch administrative Einstellungen auf ein GPO angepasst werden. Zudem können Sie den Zugriff auf ein GPO hier komplett verweigern, was z. B. genutzt werden kann, um Administratoren von den Wirkungen der Gruppenrichtlinien auszunehmen.

2.5.5 Register Status eines GPO

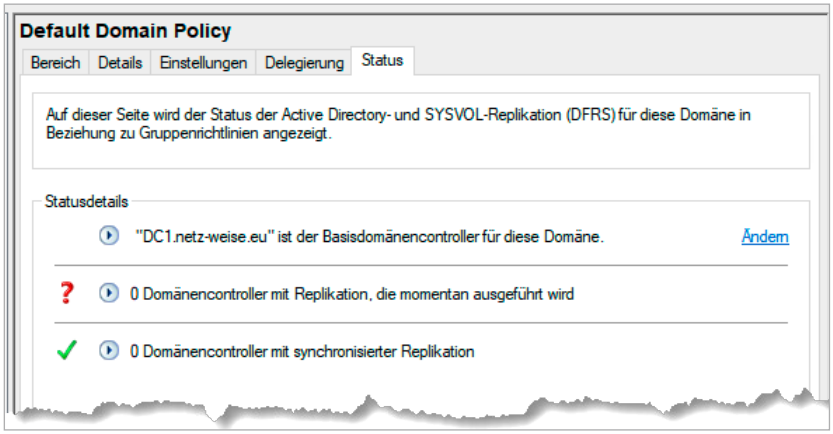


Bild 2.10 Register **Status** der Default Domain Policy

Unter **Status** können Sie ab Windows Server 2012 den Replikationsstatus eines GPO prüfen. Die Replikation eines GPO wird über zwei verschiedene Systeme gesteuert, das Active Directory und das Dateisystem. Hier können Sie sehen, ob beide Systeme synchron sind. Den Status können Sie nur direkt auf dem GPO im Container „Gruppenrichtlinienobjekte“ sehen, auf einer Verknüpfung wird er nicht angezeigt.

2.6 Standorte und Gruppenrichtlinien

Gruppenrichtlinien können auch mit AD-Standorten verknüpft werden. Sie benötigen hierfür allerdings Organisations-Admin-Rechte.

Standorte werden standardmäßig nicht angezeigt. Um Ihre Standorte einzublenden, wählen Sie aus dem Kontextmenü von **Standorte** den Eintrag **Standorte anzeigen** aus.

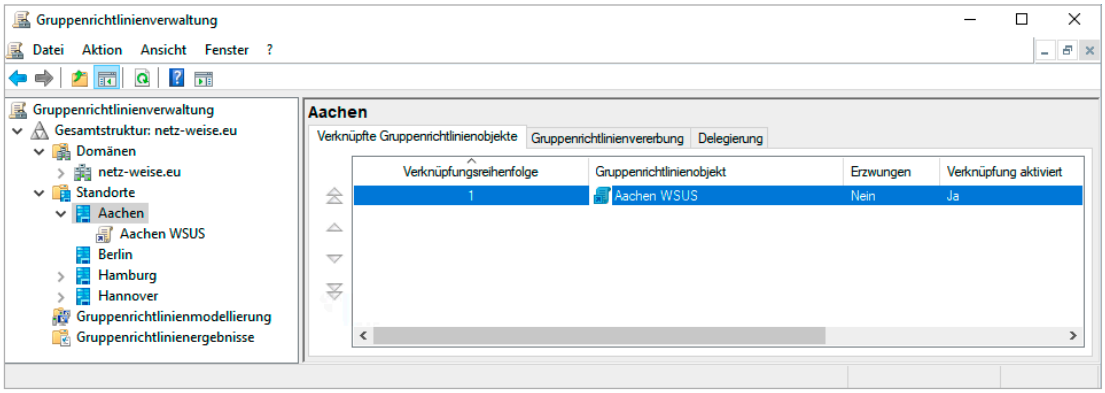


Bild 2.11 Standorte müssen explizit eingeblendet werden.

Standortverknüpfungen sind die einzige Möglichkeit, GPOs auch domänenübergreifend zu konfigurieren, und sollten mit sehr viel Fingerspitzengefühl eingesetzt werden. Mehr dazu finden Sie in Abschnitt 13.3, „Gruppenrichtlinien auf Standorten“.

PRAXISTIPP: Indem Sie die Richtlinien für WSUS und Softwareverteilung mit einem Standort statt einer den Standort repräsentierenden Organisationseinheit verknüpfen, stellen Sie sicher, dass mobile Geräte stets die lokale Quelle für Updates und Software verwenden. Das Computerkonto des Notebooks eines Berliner Vertriebsmitarbeiters ist stets in der OU Vertrieb. Für die Ermittlung des Standortes wird das Subnetz des Computers ausgewertet. Da das Notebook seine IP-Konfiguration von einem lokalen DHCP-Server (z. B. in Hannover) erhält, erkennt das System den aktuellen Standort und kann den Verkehr lokal halten, ohne dass ein Administrator ständig die Computerkonten verschieben müsste.

2.7 Weitere Elemente der Gruppenrichtlinienverwaltung

Sie sehen in der Konsolenstruktur des Weiteren die Elemente WMI-Filter, Starter-Gruppenrichtlinienobjekte, Gruppenrichtlinienmodellierung und Gruppenrichtlinienergebnisse. Auf diese gehen wir in späteren Kapiteln ausgiebig ein. An dieser Stelle bleibt es bei einer groben Übersicht, welche Sie der Tabelle 2.1 entnehmen können.

Tabelle 2.1 Übersicht über zusätzliche Elemente der Gruppenrichtlinienverwaltung

Element	Aufgabe
WMI-Filter	Dient der Verwaltung von WMI-Filtern. Mit WMI-Filtern ist es möglich, GPOs anhand von Client-Eigenschaften dynamisch anzuwenden. WMI-Filter müssen immer in diesem Knoten erstellt werden und können dann mit einem GPO verknüpft werden.
Starter-Gruppenrichtlinienobjekte	Hierbei handelt es sich um Vorlagensammlungen, die verwendet werden können, um ein neues GPO mit Standardeinstellungen auszustatten. Die Vorlagen werden unter Starter-Gruppenrichtlinienobjekte gespeichert und verwaltet, müssen aber vor der ersten Verwendung erst importiert werden.
Gruppenrichtlinienmodellierung	Die Gruppenrichtlinienmodellierung dient dazu, Auswirkungen von Gruppenrichtlinienverknüpfungen im Vorfeld zu testen.
Gruppenrichtlinienergebnisse	Mit Gruppenrichtlinienergebnissen lässt sich nachvollziehen, welche Einstellungen für Benutzer und Computer aus welchen GPOs gekommen sind und wie diese verarbeitet wurden.

2.8 Gruppenrichtlinie erstellen

Erstellen Sie nun ein neues GPO im Knoten „Gruppenrichtlinienobjekte“. Klicken Sie dazu auf den Knoten und wählen Sie im Kontextmenü den Befehl **Neu**. Geben Sie einen sprechenden Namen für das GPO ein – das Thema Benennungskonventionen wird in einem späteren Kapitel noch ausführlich behandelt. Starter-Gruppenrichtlinienobjekte stehen erst nach der Aktivierung zur Verfügung und sind in fast allen Fällen auch sinnlos und veraltet.

2.9 Gruppenrichtlinie verknüpfen

Nachdem Sie das GPO erstellt haben, müssen Sie es verknüpfen, damit es zur Anwendung kommt. Wählen Sie dazu eine Test-Organisationseinheit aus, mit der Sie die neue Gruppenrichtlinie verknüpfen. Wenn Sie noch keine Test-OU erstellt haben, können Sie auch aus dem Kontextmenü mit **Neue Organisationseinheit** eine Organisationseinheit erstellen.

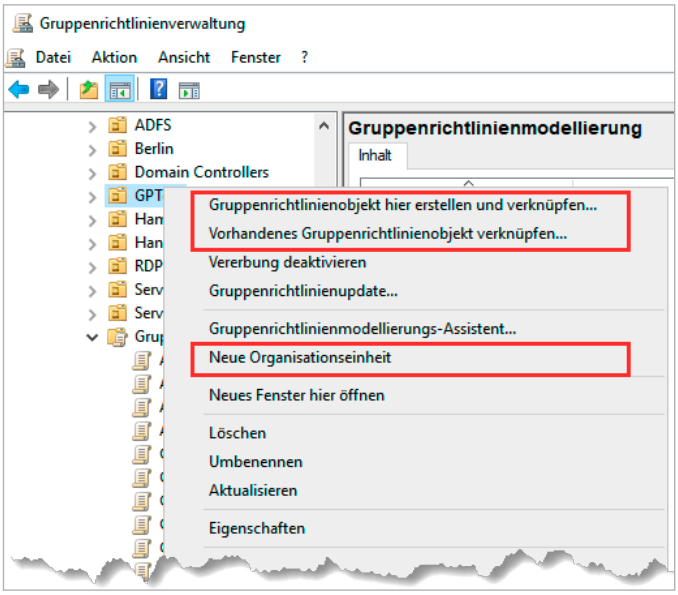


Bild 2.12 Über das Kontextmenü einer OU können Sie ein vorhandenes GPO verknüpfen, aber auch erstellen.

Markieren Sie die Organisationseinheit und klicken Sie im Kontextmenü auf **Vorhandenes Gruppenrichtlinienobjekt verknüpfen**. Wählen Sie nun im Fenster **Gruppenrichtlinienobjekt auswählen** das GPO aus, das Sie hier verknüpfen möchten.

Sie können alternativ auch ein GPO auf einer Organisationseinheit in einem Schritt erstellen und verknüpfen. Wählen Sie dazu im Kontextmenü der OU den Befehl **Gruppenrichtlinienobjekt hier erstellen und verknüpfen**.

PRAXISTIPP: In einer Produktivumgebung ist es nicht empfehlenswert, Gruppenrichtlinienobjekte direkt zu erstellen. Sie sollten diese erst erstellen und konfigurieren, anschließend mit einer Test-OU verknüpfen, Testbenutzer und -Computer der OU hinzufügen und sich mit diesen anmelden. Erst wenn Sie sicher sind, dass das GPO keinen Schaden anrichtet, sollte es mit einer produktiven OU verknüpft werden.

2.10 Gruppenrichtlinie bearbeiten

Um die Konfiguration eines GPO anzupassen, wählen Sie aus seiner Verknüpfung oder dem Objekt selber im Kontextmenü **Bearbeiten** aus. Die Bearbeitung des GPO findet in einem eigenen Werkzeug statt, dem Gruppenrichtlinien-Editor.

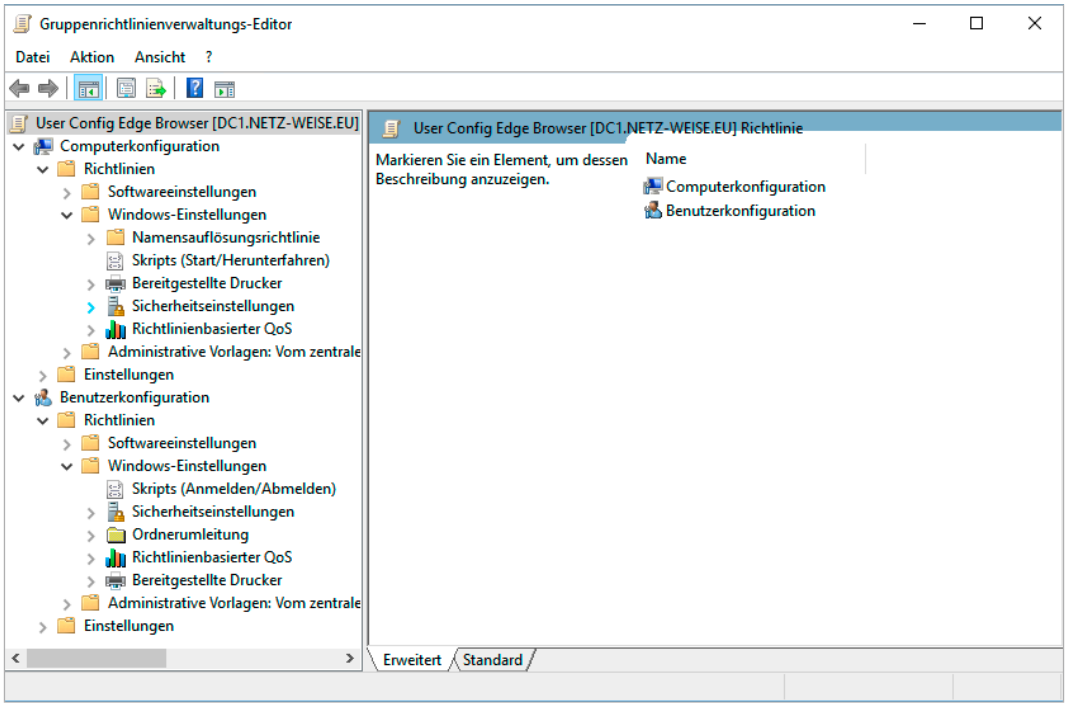


Bild 2.13 Der Gruppenrichtlinien-Editor mit einer teilweise geöffneten Konfiguration eines GPO

Der Gruppenrichtlinien-Editor ist untergliedert in die Bereiche „Computerkonfiguration“ und „Benutzerkonfiguration“, die sich aus den Richtlinien und den Einstellungen zusammensetzen.

Der Bereich „Richtlinien“ besteht aus den drei Bereichen „Softwareeinstellungen“, „Windows-Einstellungen“ und „Administrative Vorlagen“.

Zu den einzelnen Richtlinien, und was sie bedeuten, erfahren Sie in den nächsten Kapiteln mehr.

3 Verarbeitungsreihenfolge von Gruppenrichtlinien

Dieses Kapitel behandelt folgende Themen:

- In welcher Reihenfolge werden Gruppenrichtlinienobjekte verarbeitet?
- Wie wird die Verarbeitungsreihenfolge durch **erzwungen** und **Vererbung deaktivieren** beeinflusst?
- Was ist der Loopback-Verarbeitungsmodus?
- Gruppenrichtlinienobjekte teilweise oder ganz deaktivieren

3.1 Einführung

In diesem Kapitel erfahren Sie, wie Sie die Verarbeitung der GPOs über die Group Policy Management Console (GPMC) verwalten können. Einen tieferen Einblick in die Vorgänge, die während der Gruppenrichtlinienverarbeitung ablaufen, erhalten Sie in Kapitel 13, „Funktionsweise von Gruppenrichtlinien“.

3.2 Grundlagen der Gruppenrichtlinienverarbeitung

Gruppenrichtlinien werden von Windows seit Vista mithilfe eines eigenständigen Dienstes, des Gruppenrichtlinienclients, verarbeitet. Er ist dafür verantwortlich, die GPOs aus der Domäne zu verarbeiten und Computer- bzw. Benutzereinstellungen anzuwenden.

Der Gruppenrichtlinienclient startet die Gruppenrichtlinienverarbeitung automatisch beim Systemstart, bei jeder Benutzeranmeldung und zeitgesteuert alle 90 bis 120 Minuten. Die Verarbeitung erfolgt dabei für Computer und Benutzer unabhängig.

Es werden nur Einstellungen verarbeitet, die auch tatsächlich konfiguriert sind. Das klingt trivial, ist es aber nicht. Denn Sie haben speziell in den administrativen Vorlagen der GPOs immer die Möglichkeit, eine Einstellung auf „Aktiviert", „Deaktiviert" oder „Nicht konfiguriert" zu setzen. „Nicht konfiguriert" bedeutet, dass die Gruppenrichtlinie nicht angepasst wird, also weder ein- noch ausgeschaltet ist. „Deaktiviert" dagegen bedeutet, dass eine Einstellung explizit ausgeschaltet wird.

3.3 Verarbeitungsreihenfolge in der Gruppenrichtlinienverarbeitung

Ein GPO besteht immer aus zwei Einstellungsknoten – einer Computerkonfiguration und einer Benutzerkonfiguration. Eigentlich haben wir es hier nicht mit einer, sondern mit zwei GPOs zu tun, da die Computereinstellungen und die Benutzereinstellungen nicht gleichzeitig angewendet werden!

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

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

Ein kleines Beispiel zur Verdeutlichung:

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

1. Default Domain Policy
2. HH Deploy Tools User
3. HH Config Base User

an.

Bild 3.1 Computer- und Benutzerkonfiguration werden getrennt verarbeitet.

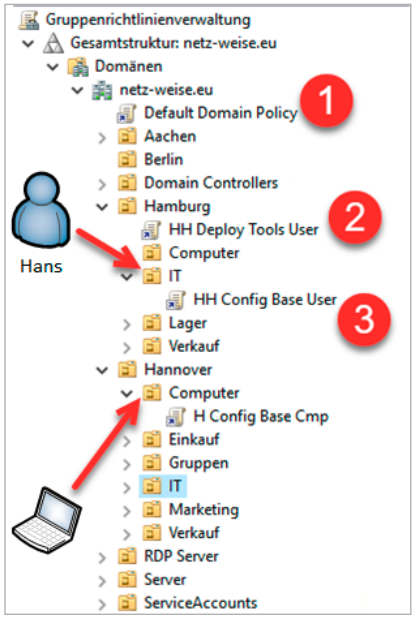


Bild 3.2
Der Benutzer kommt aus Hamburg, der Computer aus Hannover.

Wenn sich in der Richtlinie „H Config Base Cmp“ die Einstellung aus der unten stehenden Abbildung befindet, wirkt sich diese Einstellung auf den Benutzer aus?

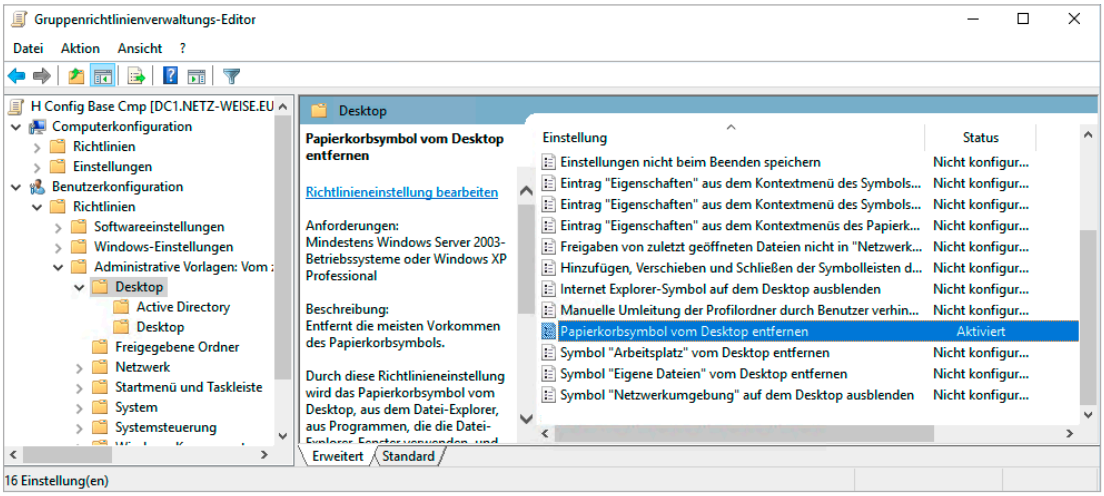


Bild 3.3 In dem GPO wird der Papierkorb für Benutzer vom Desktop ausgeblendet.

Die Antwort lautet Nein, da sie zwar in der Benutzerkonfiguration gesetzt ist, aber in einem GPO, das nur für den Computer angewendet wird, und die wird für den Benutzer nicht gültig!

3.4 Anpassungen der Verarbeitungsreihenfolge von GPOs

Sie können die Verarbeitungsreihenfolge von GPOs beeinflussen. So können etwa Einstellungen erzwungen und die Vererbung von übergeordneten Richtlinien abgelehnt werden, die Bereiche „Computerkonfiguration“ oder „Benutzerkonfiguration“ lassen sich deaktivieren, und die Übernahme von Richtlinien kann durch Gruppenzugehörigkeiten gefiltert werden. Im Folgenden werden die einzelnen Funktionen kurz erläutert.

3.4.1 Bereiche von GPOs deaktivieren

Sie können in einem GPO festlegen, dass nur der Teilbereich Benutzerkonfiguration aktiviert sein soll, der Teilbereich Computerkonfiguration oder beide. Im letzten Fall ist das gesamte GPO außer Funktion. Dies kann etwa sinnvoll sein, wenn ein GPO deaktiviert, aber nicht gelöscht werden soll.

HINWEIS: Der Objektstatus einer Gruppenrichtlinie ist nicht auf eine Verknüpfung beschränkt. Wenn ein Teilbereich deaktiviert ist, wirkt sich das auf alle Verknüpfungen des GPO aus!

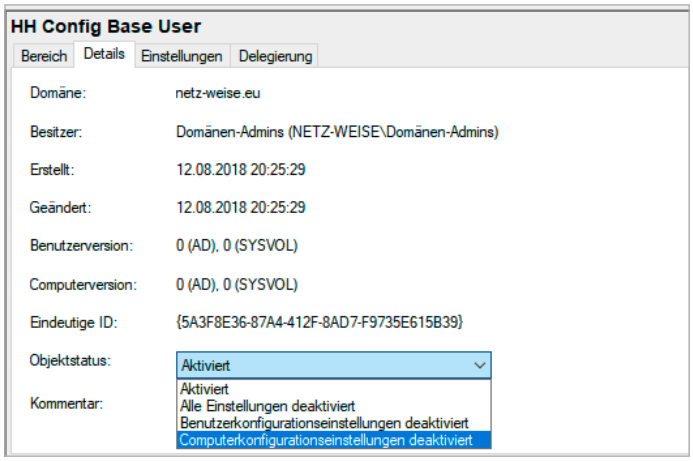


Bild 3.4 Bereiche eines GPO deaktivieren

Um Bereiche einer Gruppenrichtlinie zu deaktivieren, gehen Sie folgendermaßen vor:

Navigieren Sie in der Gruppenrichtlinienverwaltungskonsole auf die Gruppenrichtlinienverknüpfung oder das Gruppenrichtlinienobjekt, das Sie bearbeiten möchten, und wählen Sie im rechten Fenster das Register **Details**. Dann können Sie im Rollfeld **Objektstatus** die entsprechende Einstellung auswählen.

Um zu überprüfen, welche Gruppenrichtlinien in welchen Bereichen aktiv sind, können Sie in der Gruppenrichtlinienverwaltungskonsole auf die Organisationseinheit navigieren, mit der die GPOs verknüpft sind. Im rechten Fenster können Sie dann die Spalte **Objektstatus** überprüfen.

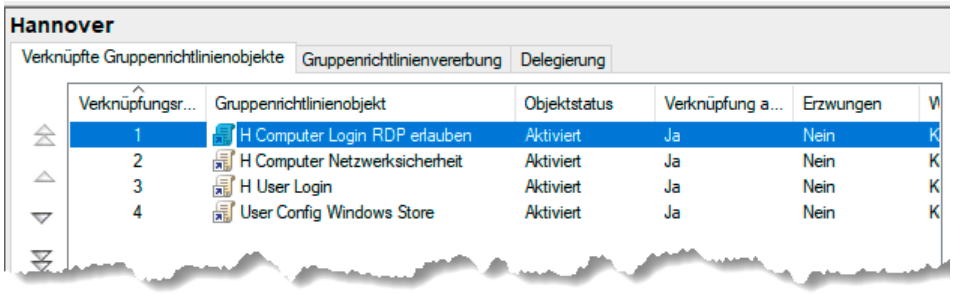


Bild 3.5 Objektstatus von GPOs prüfen

3.4.2 Verknüpfungen aktivieren/deaktivieren

Sie können auch eine einzelne Verknüpfung einer Gruppenrichtlinie mit einer Organisationseinheit deaktivieren oder aktivieren. Dies gilt aber stets für alle Bereiche der GPO.

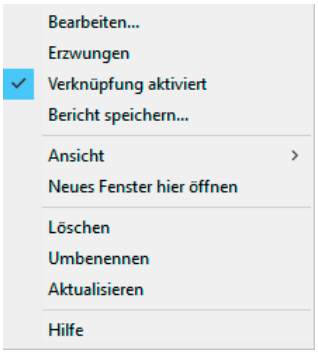


Bild 3.6
Verknüpfungseigenschaften bearbeiten

Öffnen Sie das Kontextmenü einer Gruppenrichtlinienverknüpfung, um diese zu deaktivieren oder zu aktivieren.

Den Status einer Gruppenrichtlinienverknüpfung können Sie überprüfen, indem Sie die zugehörige Organisationseinheit in der Gruppenrichtlinienverwaltungskonsole aufrufen. Deaktivierte Verknüpfungen sind heller dargestellt und im rechten Fenster ist der Verknüpfungsstatus mit Ja/Nein gekennzeichnet.

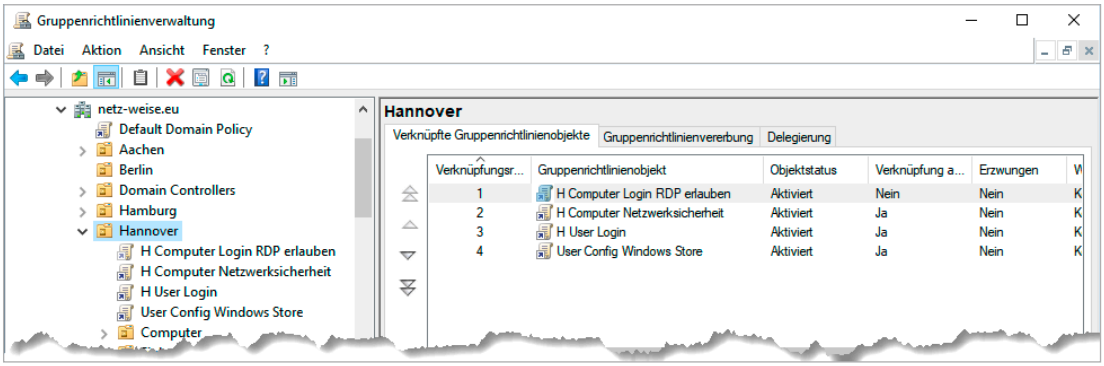


Bild 3.7 Verknüpfungsstatus überprüfen

3.4.3 Vererbung deaktivieren

Sie können für eine Organisationseinheit festlegen, dass diese keine übergeordneten Richtlinien übernehmen soll. Dies bezeichnet man als **Vererbung deaktivieren**, obwohl die Vererbung eigentlich gar nicht deaktiviert, sondern nur die Vererbung von übergeordneten GPOs blockiert wird. Untergeordnete Organisationseinheiten erben auch weiterhin die Gruppenrichtlinien einer Organisationseinheit mit deaktivierter Vererbung!

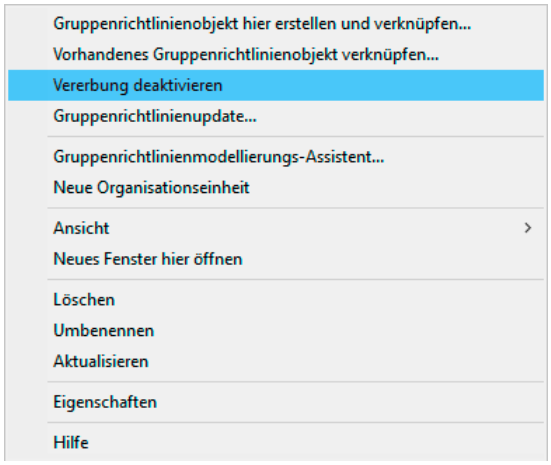


Bild 3.8
Vererbung deaktivieren

Um die Vererbung von Gruppenrichtlinien für eine Organisationseinheit zu deaktivieren, öffnen Sie ihr Kontextmenü und klicken Sie auf **Vererbung deaktivieren**. Die Organisationseinheit ist nun mit einem Ausrufezeichen in einem blauen Kreis gekennzeichnet.

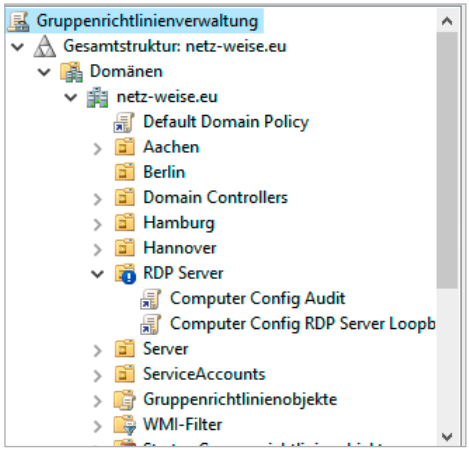


Bild 3.9
Organisationseinheit mit deaktivierter Vererbung

3.4.4 Erzwingen von GPOs

Wenn Sie sicherstellen möchten, dass die Einstellungen eines GPO nicht überschrieben werden, können Sie diese mit einem Schreibschutz versehen. Klicken Sie hierzu mit der rechten Maustaste auf die Gruppenrichtlinienverknüpfung und aktivieren Sie im Kontextmenü den Befehl **Erzwungen** (s. Bild 3.6).

Erzwungene GPOs lassen sich durch nachfolgende GPOs nicht mehr überschreiben. Außerdem durchbricht ein erzwungenes GPO die Vererbungsblockierung – es ist also immer gültig. Dies wird in der Konsolenstruktur durch ein Vorhängeschloss auf der Gruppenrichtlinienverknüpfung markiert. Effektiv wird eine erzwungene Richtlinie einfach in der

Verarbeitungsreihenfolge an das Ende verschoben, was man auch sehr gut auf der Registerkarte „Gruppenrichtlinienvererbung einer OU“ sehen kann.

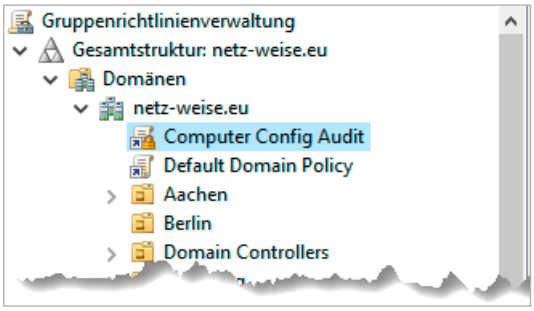


Bild 3.10
Erzwungene GPOs tragen ein Schloss auf dem Icon.

HINWEIS: Das Erzwingen sollten Sie meiden wie der Teufel das Weihwasser, auch wenn es Ihnen im Notfall gerade sinnvoll erscheint, mal schnell die Einstellung zu erzwingen, die aus unerfindlichen Gründen nicht angewendet wird – Sie vergessen hinterher (ich wette um eine Kiste Bier), die Einstellung wieder rückgängig zu machen, und beim nächsten Mal müssen Sie ein weiteres GPO erzwingen, weil Ihre Verarbeitung einfach nicht funktionieren will …

Der Sinn von Erzwingen ist es, Sicherheitseinstellungen, die z. B. aufgrund von Sicherheitsrichtlinien immer auf allen Computer gesetzt sein müssen, gegen alle Widerstände durchzusetzen. Nur hierfür sollte diese Option auch eingesetzt werden.

3.5 Loopbackverarbeitungsmodus

Auf bestimmten Computersystemen ist es von Vorteil, wenn die Benutzereinstellungen nicht übernommen werden, sondern stattdessen eine computerspezifische Benutzerkonfiguration erzwungen werden kann. Das sind meistens Computer, die besonders geschützt werden müssen, weil mehrere Benutzer mit dem gleichen Gerät arbeiten. Klassische Beispiele dafür sind sogenannte Kiosk-PCs, die allgemein zugänglich z. B. in Bibliotheken oder Empfangsbereichen stehen, oder RDP-Server, auf denen viele Benutzer gleichzeitig arbeiten. Im folgenden Beispiel wird hierfür ein GPO im Loopbackverarbeitungsmodus konfiguriert. Der Loopbackverarbeitungsmodus sagt dem Gruppenrichtlinienclient, der für das Anwenden der Gruppenrichtlinien zuständig ist, dass die Einstellungen der Benutzerkonfiguration des Computers beim Anmelden eines Benutzers auch ausgewertet werden sollen. Das hat effektiv zur Folge, dass Sie über die Computerrichtlinien steuern können, welche Benutzereinstellungen beim Anmelden verarbeitet werden, und zwar unabhängig vom Benutzer, der sich anmeldet.

Hierzu ein praktisches Beispiel: Sie konfigurieren einen Computer, der in der Lobby Ihrer Firma allen Gästen kostenlos zur Verfügung stehen soll. Gäste sollen an dem Computer aber nichts anderes machen können als einen Webbrowser starten und im Internet surfen. Auch wenn ein Kollege aus dem Unternehmen sich an dem PC anmeldet, soll er nur den Webbrowser sehen, um zu verhindern, dass er Daten auf dem Client zurücklässt, oder noch schlimmer, dass er sich nicht abmeldet und damit den Netzwerkzugriff für alle Gäste ermöglicht.

Der schwierige Teil der Aufgabe ist es, Ihren Benutzern den Zugriff zu sperren. Für Gastbenutzer könnten Sie einfach ein Gastkonto anlegen, mit dem Gäste angemeldet werden. Das verhindert aber nicht, dass ein Kollege sein Benutzerkonto verwendet, um sich anzumelden und den entsperrten Unternehmensdesktop mit allen Vorzügen, die Sie in den GPOs konfiguriert haben, zu nutzen.

Eine Lösung ist es, ein GPO auf der Organisationseinheit des Lobby-PCs anzulegen und den Loopbackmodus zu aktivieren. Anschließend können Sie in den Benutzereinstellungen des GPO festlegen, dass Benutzer eine definierte Shell (also ein Startprogramm) anstatt des Desktops bekommen sollen, und welche Schikanen Ihnen auch immer einfallen, um den Benutzern des Lobby-PC möglichst wenige Möglichkeiten zu geben, neben dem Webbrowsen Arbeitstätigkeiten nachzugehen.

PRAXISTIPP: Windows 10 bringt übrigens für genau dieses Szenario eine Reihe von Optionen mit, die keine Gruppenrichtlinien benötigen. Mehr Informationen finden Sie im technischen Newsletter von Netz-Weise in der Februar- und April-Ausgabe von 2018. Sie können die Newsletter unter *https://www.netz-weise-it.training/weisheiten/newsletter2.html* herunterladen.

3.5.1 Loopbackverarbeitungsmodus einrichten

Am besten legen Sie für den Kiosk-PC zuerst eine eigene Organisationseinheit an, da der Loopbackmodus natürlich für alle Computerkonten angewendet wird, die von dem GPO betroffen sind. Anschließend legen Sie ein neues GPO an und öffnen es zur Bearbeitung. Das Beispiel-GPO soll **H Computer Kiosk Loopback** heißen – der Name spiegelt die wesentlichen Informationen wider.

Die Einstellung **Loopbackverarbeitungsmodus für Benutzerrichtlinien** finden Sie unter **Computerkonfiguration – Richtlinien – Administrative Vorlagen – System – Gruppenrichtlinie**. Da in dieser Kategorie sehr viele Einstellungen zu finden sind, ist es hilfreich, die hier gesammelten Gruppenrichtlinien alphabetisch zu ordnen. Klicken Sie hierfür auf den Spaltennamen **Einstellung**.

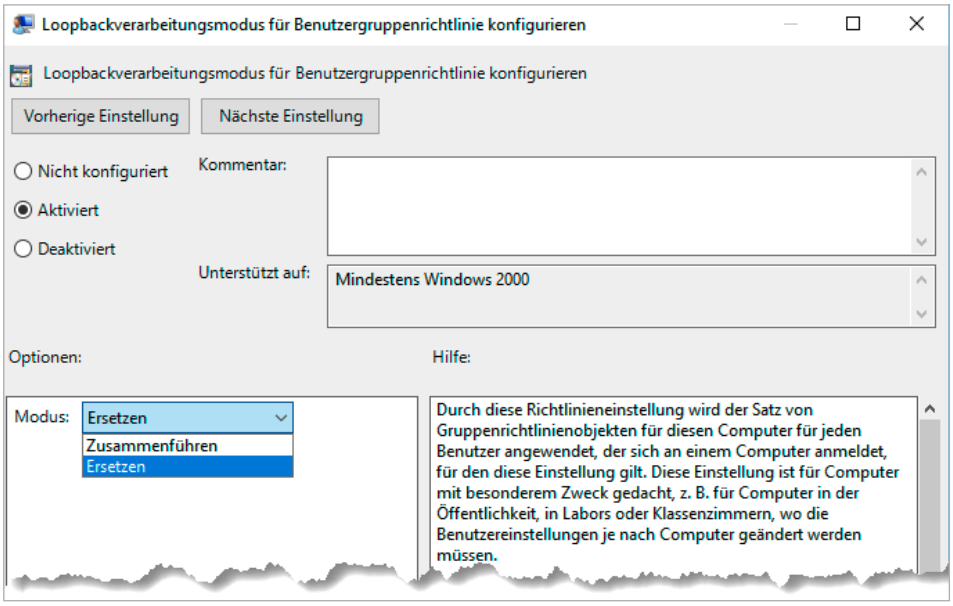


Bild 3.11 Der Loopbackverarbeitungsmodus kennt auch noch einmal Modi.

In der Richtlinie stehen Ihnen drei Konfigurationsoptionen zur Verfügung: „Nicht konfiguriert“, „Aktiviert“ und „Deaktiviert“. Es handelt sich um eine typische administrative Vorlage; mehr dazu in Kapitel 8, „Administrative Vorlagen“. Die Standardeinstellung, „Nicht aktiviert“, besagt, dass diese Gruppenrichtlinie keine Aussage zu der Einstellung trifft – sie ist neutral. Das ist ein wichtiger Punkt, da Gruppenrichtlinien additiv sind. Ein anderes GPO, das diese Gruppenrichtlinie konfiguriert, kann also nicht kollidieren.

Wenn Sie die Einstellung auf „Deaktiviert“ setzen, schalten Sie den Loopbackverarbeitungsmodus explizit aus. Einstellungen aus einem anderen GPO, das früher angewendet wurde, werden durch diese Einstellung unwirksam gemacht.

„Aktiviert“ schaltet den Loopbackverarbeitungsmodus ein. Sie müssen sich jetzt entscheiden, wie mit den Benutzereinstellungen umgegangen werden soll, die der Benutzer aus seinen eigenen GPOs mitbringt. Wählen Sie „Zusammenführen“, um die Benutzereinstellungen der Computerrichtlinie mit denen des Benutzer zu vereinen. Für den Kiosk-PC wählen Sie aber „Ersetzen“, denn die Benutzereinstellungen sollen hier nicht angewendet werden. Um eine alternative Shell zu starten, können Sie die Gruppenrichtlinie **Richtlinien – Administrative Vorlagen – System – Benutzerdefinierte Benutzeroberfläche** der Benutzerkonfiguration verwenden. Denken Sie daran, sie in der GPO des Computers zu aktivieren! Sie können hier einen Dateipfad eintragen, z. B. `%Windir%\Notepad.exe`.

Nachdem Sie den Gruppenrichtlinieneditor geschlossen haben, können Sie die Konfiguration mit der Gruppenrichtlinienverwaltungskonsole überprüfen. Öffnen Sie dazu im Detailfenster rechts das Register **Einstellungen** und öffnen Sie die Computer- bzw. Benutzerkonfiguration, die Sie angelegt haben.

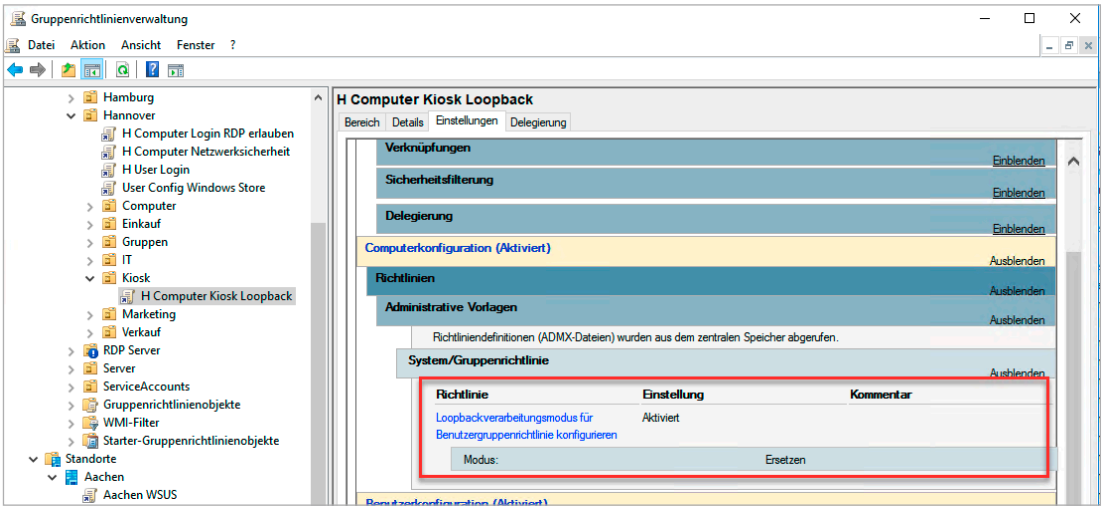


Bild 3.12 Loopbackverarbeitung überprüfen

Wenn ein Benutzer sich am Kiosk-PC anmeldet, bekommt er nicht mehr den Desktop, sondern nur noch das Notepad zu sehen. Wenn der Benutzer allerdings **Strg+Alt+Entf** drückt, kann er den Taskmanager starten und von da aus den Explorer. Es gibt also wohl noch das eine oder andere Sicherheitsloch in der Konfiguration …

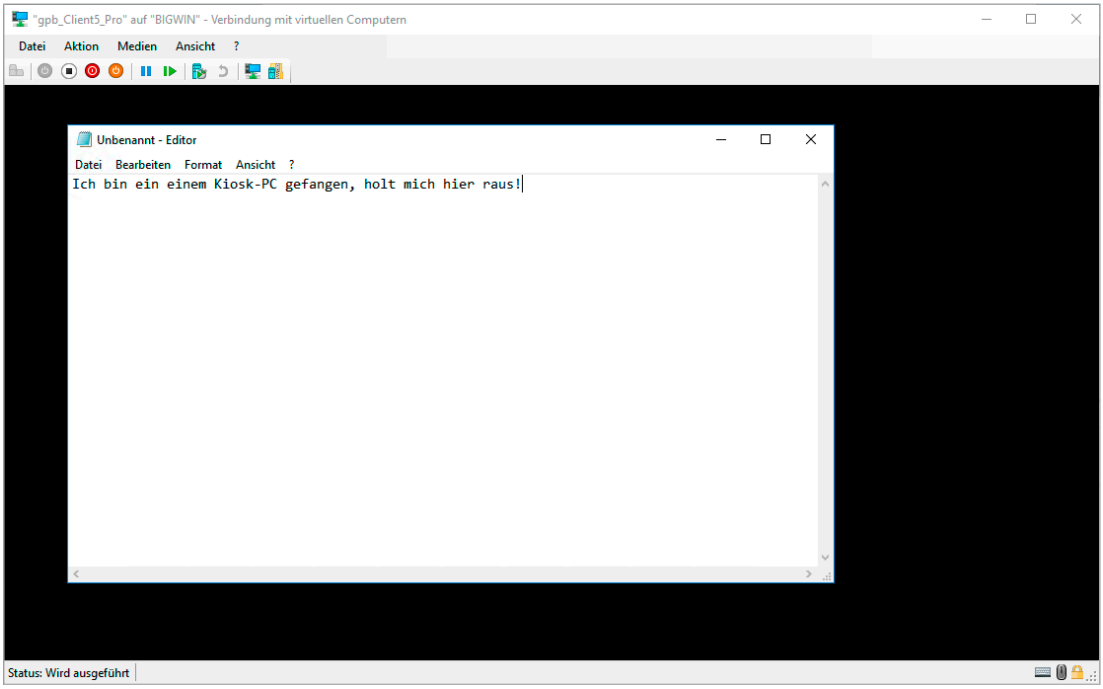


Bild 3.13 Nach der Anmeldung gibt es nur noch das Notepad zu sehen.

4 Gruppenrichtlinien filtern

In diesem Kapitel werden folgende Themen behandelt:

- Wann bietet sich welche Art von Gruppenrichtlinienfilterung an?
- Sicherheitsfilterungen auf GPOs anwenden
- Wie verwende ich Berechtigungen, um Benutzer vor Gruppenrichtlinienobjekten zu schützen?
- Zwischen verschiedenen Rechnern unterscheiden: mit WMI-Filtern Hardware- und Softwareeigenschaften abfragen

4.1 Einführung

Ein GPO wird mit Standorten, Domänen oder Organisationseinheiten verknüpft und wirkt auf alle Benutzer, die sich unterhalb des GPO befinden. Man kann also sagen, dass das GPO auf alle Konten wirkt, die sich innerhalb des Containers befinden, auf die das GPO wirkt. Hiervon gibt es nur zwei Ausnahmen. Sie haben auf einer Organisationseinheit die Richtlinienvererbung deaktiviert (siehe Kapitel 3), oder Sie haben einen Gruppenrichtlinienfilter angewendet. Zum Filtern stehen Ihnen drei Methoden zur Verfügung.

1. Erlauben Sie nur einer eingeschränkten Gruppe das Anwenden der Gruppenrichtlinien (positive Sicherheitsfilterung).
2. Verweigern Sie einzelnen Benutzern oder Computern das Recht, die Gruppenrichtlinie anzuwenden (negative Sicherheitsfilterung).
3. Bestimmen Sie über eine WMI-Abfrage, ob eine Gruppenrichtlinie angewendet werden soll (WMI-Filter).

Sicherheitsfilterung bietet sich immer dann an, wenn nur eine Gruppe von Benutzern oder Computern über ein GPO Einstellungen erhalten soll. Wenn ein GPO für bestimmte Benutzer oder Gruppen nicht gelten soll, wie z. B. Admins, verweigern Sie Ihre Anwendung. WMI-Filter werden in der Regel verwendet, wenn zwischen den Eigenschaften der verschiedenen Rechner unterschieden werden muss, z. B. zwischen mobilen Systemen und Desktop-PCs oder zwischen verschiedenen Betriebssystemen.

4.2 Filtern über Gruppenzugehörigkeiten

4.2.1 Sicherheitsfilterung verwenden

Im Register **Bereich** eines GPO können Sie unter Sicherheitsfilterung sehen, für welche Benutzer diese wirksam ist. Standardmäßig steht hier die Gruppe der authentifizierten Benutzer, die alle Benutzer und Computer umfasst, die sich irgendwo in Ihrem Forst angemeldet haben – faktisch also jeder.

Um das GPO nur auf bestimmte Benutzer oder Sicherheitsgruppen anzuwenden, müssen Sie die Gruppe der authentifizierten Benutzer entfernen. Markieren Sie die Gruppe hierfür im Feld „Sicherheitsfilterung“ und wählen Sie **Entfernen**. Anschließend können Sie über **Hinzufügen** die Gruppen oder die Benutzer auswählen, für die das GPO angewendet werden soll.

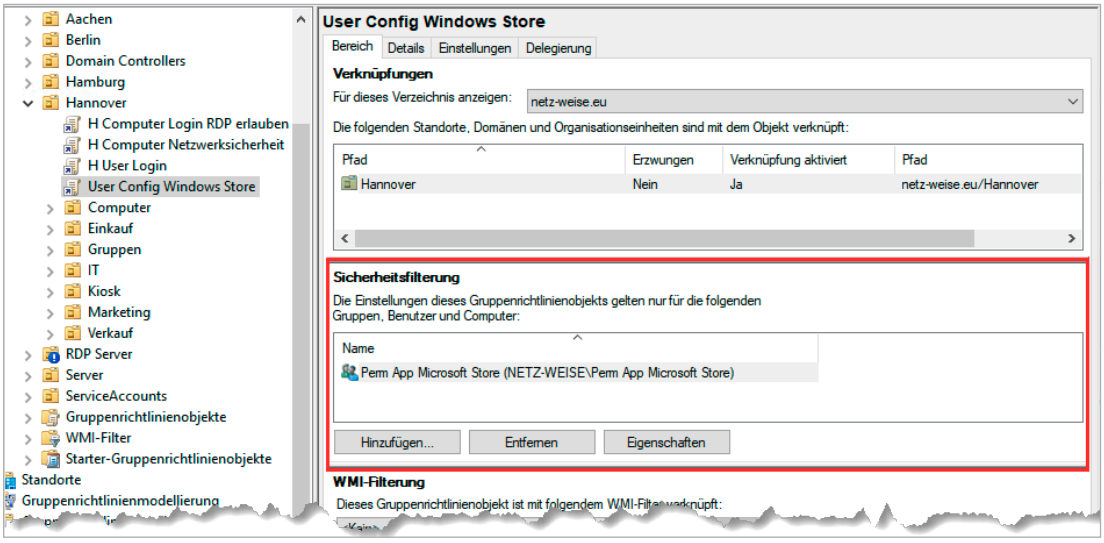


Bild 4.1 Die authentifizierten Benutzer wurden ausgetauscht. Das GPO wird nur auf die neue Gruppe angewendet.

Wenn Sie die Berechtigungen entfernen, warnt Sie die GPMC, dass die Computerkonten Leseberechtigungen für das GPO brauchen.

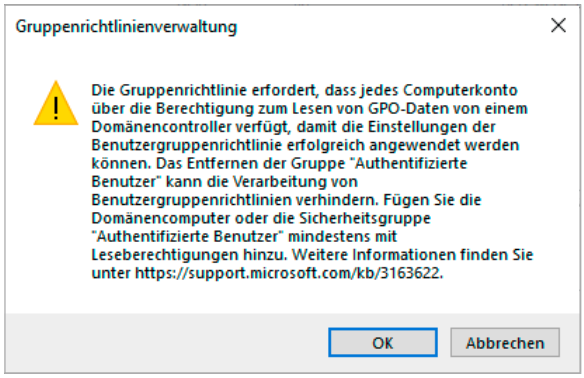


Bild 4.2
Windows warnt, dass das Computerkonto Leseberechtigungen benötigt.

Diese Warnung wird angezeigt, weil der Gruppenrichtlinien-Client jedes Computers zumindest das Recht braucht, ein GPO zu lesen. Bis Juni 2016 hat Windows das dadurch gelöst, dass der Client die GPO-Informationen unter dem Kontext des Benutzers gelesen hat, oder anders gesagt: Er hat die Identität des Benutzers angenommen. Mit dem Patch MS16-072 hat Microsoft dieses Verhalten aus Sicherheitsgründen geändert, und der Gruppenrichtlinienclient muss die Konfiguration des GPO nun unter seinem eigenen Kontext abfragen. Ist in der Gruppe, die Sie statt der authentifizierten Benutzer hinzufügen, also nicht auch das Computerkonto enthalten, an dem der Benutzer sich anmeldet, kann dieser die User-Richtlinien nicht lesen, und sie werden nicht angewendet.

Der Computer braucht aber nicht das Recht, die GPOs auszuführen, sondern nur dasjenige, sie zu lesen. Und diese – und weitere – Berechtigungen können Sie auf der Registerkarte „Delegierung“ einrichten.

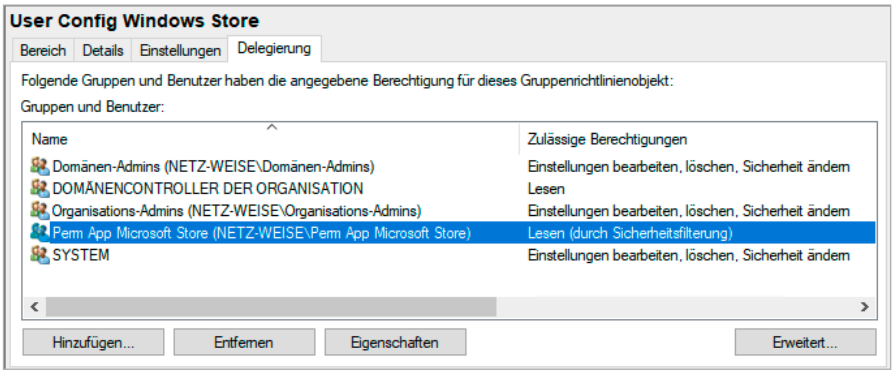


Bild 4.3 Die Registerkarte „Delegierung“ erlaubt die direkte Berechtigungsvergabe.

Fügen Sie hierfür die Gruppe der Domänencomputer der Liste hinzu, indem Sie **Hinzufügen** auswählen, im Auswahlfenster „Domänen“ eingeben und sich die Gruppe über **Namen überprüfen** auflösen lassen. Im nun erscheinenden Fenster können Sie die Berechtigung auswählen, die die Domänencomputer haben sollen.

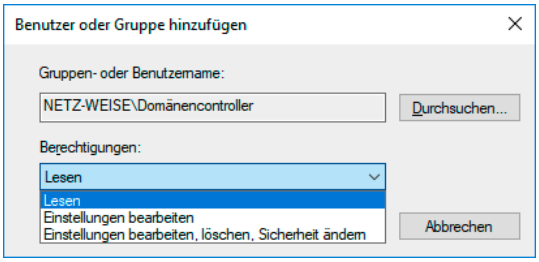


Bild 4.4
Wählen Sie „Lesen“ aus, damit der Computer das GPO abrufen kann.

Die Lesen-Berechtigung erlaubt das Lesen eines GPO, ohne es anwenden zu dürfen. Die beiden anderen Berechtigungen sind administrativ und erlauben das Bearbeiten des GPO sowie das Verändern der Berechtigungen und Löschen.

Nachdem Sie die Domänencomputer mit Lesen-Berechtigungen hinzugefügt haben, funktioniert der Sicherheitsfilter. Da das manuelle Hinzufügen der Domänencomputer ziemlich aufwendig und fehlerträchtig ist, können Sie eine Anpassung im AD-Schema vornehmen – es handelt sich nicht um eine Schema-Erweiterung, sie ist also jederzeit reversibel –, damit die Gruppe der Domänencomputer beim Anlegen einer neuen GPO immer Lesen-Berechtigung bekommt. Das Cmdlet **Add-GphDefaultPermissions** aus dem PowerShell-Modul „GrouppolicyHelper“ zum Buch erledigt das für Sie. Rufen Sie es einfach ohne Parameter auf – Sie benötigen allerdings Schema-Administrator-Rechte. Alternativ können Sie die Änderung auch von Hand durchführen. Mark Heitbrink beschreibt den Vorgang ausführlich unter *https://www.gruppenrichtlinien.de/artikel/gpo-admin-einrichten-gruppenrichtlinien-delegation/* oder kurz *https://bit.ly/2vPocvN*.

4.2.2 Berechtigungen verweigern

Wenn Sie einzelne Benutzer, Computer oder Gruppen von den Auswirkungen eines GPO ausnehmen wollen, können Sie das Recht zum Übernehmen der Einstellungen verweigern. Sie nutzen hierzu den gleichen Effekt wie eben für Domänencomputer beschrieben – Sie verhindern, dass ein Konto ein GPO anwenden kann. Wechseln Sie hierzu von dem GPO, das Sie verweigern wollen, wieder auf die Registerkarte **Delegierung**, wählen aber den Button **Erweitert**. Es öffnet sich ein Fenster mit den Sicherheitseinstellungen für das GPO. Sie können hier die einzelnen Berechtigungen sehen, die auf dem Group Policy Container im AD vergeben sind – mehr zu den Details finden Sie in Kapitel 13, „Funktionsweise von Gruppenrichtlinien“. Wenn das Konto oder die Gruppe, die Sie von der Wirkung des GPO ausnehmen wollen, noch nicht in der Liste enthalten ist, fügen Sie es oder sie hinzu, ansonsten wählen Sie den Eintrag, den Sie bearbeiten möchten, direkt aus. Im folgenden Beispiel soll die Gruppe der Domänen-Admins von der GPO „H User Login“ ausgenommen werden.

In der Liste der verfügbaren Berechtigungen gibt es die Berechtigung **Gruppenrichtlinie übernehmen**, die benötigt wird, um ein GPO anzuwenden. Setzen Sie bei der Gruppe „Domänen-Admins“ einen Haken in der Spalte „Verweigern“. Die Verweigern-Berechtigung spielt eine ganz besondere Rolle, denn sie wird beim Prüfvorgang vor allen Zulassen-Berechtigungen abgefragt. Ist eine Berechtigung verweigert, bricht der Computer die weitere Prüfung für diese Berechtigung ab. Verweigern hat also Vorrang vor Erteilen-Berechtigungen. So

kann den Domänen-Admins die Berechtigung „Gruppenrichtlinie übernehmen“ verweigert werden, auch wenn sie z. B. über die Gruppe „Authentifizierte Benutzer“, in der auch jeder Domänen-Administrator immer Mitglied ist, das Recht hätten, die GPO anzuwenden.

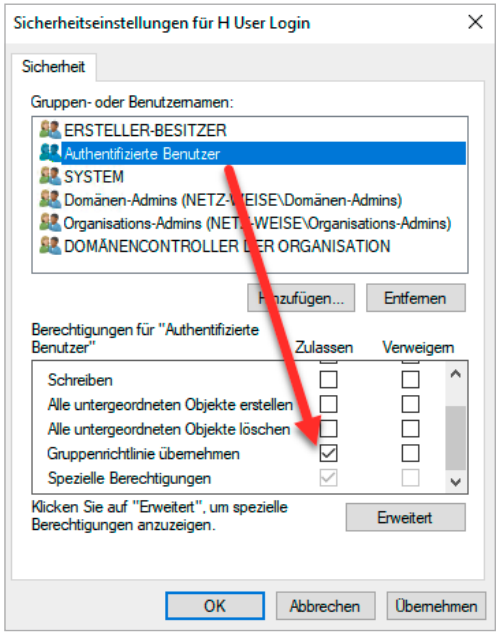


Bild 4.5
Die Gruppe „Authentifizierte Benutzer“, in der alle Konten enthalten sind, darf die Gruppenrichtlinie übernehmen.

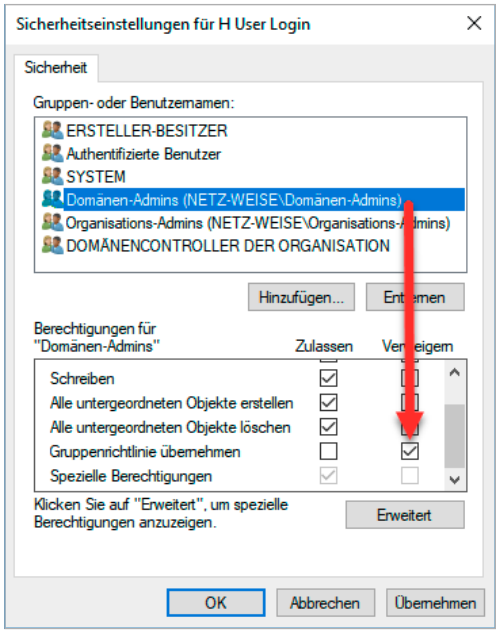


Bild 4.6
„Verweigern“ verhindert, dass die Berechtigung „Gruppenrichtlinie übernehmen“ zugelassen werden kann.

4.3 WMI-Filter

Mit Windows XP hat Microsoft neben der Sicherheitsfilterung eine zusätzliche Funktion zur Steuerung von Gruppenrichtlinien eingeführt, die WMI-Filter. Der Gruppenrichtlinienclient nutzt WMI-Filter, um den Computer auf bestimmte Eigenschaften wie z. B. die Betriebssystemversion zu prüfen, bevor er ein GPO anwendet. Das kann z. B. bei Softwareverteilungsrichtlinien Sinn machen (siehe Kapitel 6), um sicherzustellen, dass der Computer überhaupt das minimal notwendige Betriebssystem besitzt. Oder man kann prüfen, ob ausreichend Festplattenplatz zur Verfügung steht, um eine Anwendung zu installieren. Zusammenfassend kann man sagen, dass WMI-Filter es erlauben, abhängig von den Gegebenheiten des Zielcomputers eine Gruppenrichtlinie anzuwenden.

4.3.1 Einführung in WMI

WMI (Windows Management Instrumentation) ist die Microsoft-Implementierung von WBEM (Web-Based Enterprise Management), einer Initiative mehrerer Hersteller, die Ende der 1990er-Jahre das Ziel hatte, eine einheitliche Verwaltungsplattform ähnlich SNMP (Simple Network Management Protocol) zu schaffen, mit der es möglich sein sollte, Netzwerkgeräte und Computer zentral zu verwalten. Das hat zwar bisher nicht geklappt, u. a. weil Microsoft mit WMI wieder einmal eigene Wege eingeschlagen hat, aber WMI ist zumindest auf jedem Windows-System seit Windows 2000 verfügbar und stellt eine Unmenge von Informationen über den Computer bereit.

WMI teilt die Verwaltungsinformationen in WMI-Klassen ein, die in Form einer Baumstruktur hierarchisch miteinander verbunden sind. Im WMI-Namensraum gibt es jede Menge Zweige, aber für die Verwaltung der Windows-Systeme ist vor allem ein Zweig vorgesehen: ROOT\CIMV2. CIM steht dabei für Common Infrastructure Model, den allgemeinen Standard, von dem WMI abgeleitet ist (mehr Hintergrund zu WMI finden Sie in der englischen Wikipedia: *https://en.wikipedia.org/wiki/Windows_Management_Instrumentation* oder kurz *https://bit.ly/2MVJw9e*).

Im Namensraum (sagen wir der Verständlichkeit halber einfach Ordner) ROOT\CIMV2 finden Sie eine Reihe von Klassen. Diese Klassen haben alle Namen, und alle interessanten Klassen beginnen mit dem Namen Win32_. Die Win32-WMI-Klassen sind der Ort, an dem die interessanten Informationen über Ihre Computer in Form von Eigenschaften gespeichert sind – ganz korrekt ist das eigentlich nicht, da die Informationen nicht in den Klassen stehen, sondern in den von ihnen abgeleiteten Instanzen, aber die schmutzigen Details sind an dieser Stelle für das weitere Verständnis nicht relevant.

In den Klassen sind schier unerschöpfliche Informationen gespeichert. Um die Daten aus den Klassen abfragen zu können, stellt Microsoft die WQL (WMI Query Language) zur Verfügung. Sie brauchen jetzt keine Angst davor zu haben, eine neue Programmiersprache lernen zu müssen, denn WQL ist zum einen fast identisch mit SQL, zum anderen brauchen Sie nur eine simple Select-Abfrage, die Sie einfach variieren können.

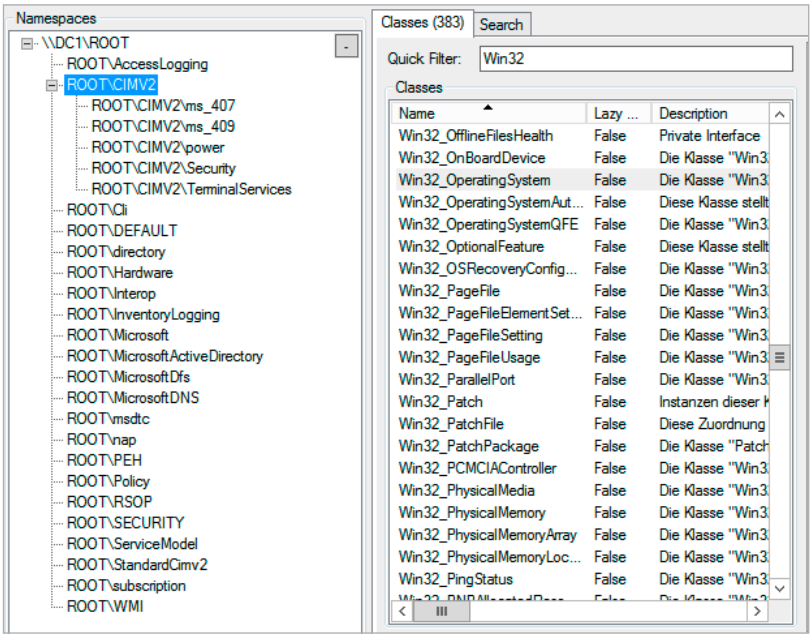


Bild 4.7 Der WMI-Namensraum hat eine Baumstruktur.

Eine WQL-Abfrage hat folgende Form:

Listing 4.1 Die Klasse Win32_OperatingSystem

```
Select * from Win32_OperatingSystem
```

Select * **from** besagt, dass Sie alle Eigenschaften der Klasse abfragen möchten, die hinter dem FROM steht.

Diese Abfrage können Sie einfach mit PowerShell nachvollziehen, indem Sie das Cmdlet `Get-WMIObject` verwenden (siehe Listing 4.2).

Listing 4.2 Mit PowerShell eine WMI-Abfrage ausführen

```
> Get-WmiObject -Query "Select * from Win32_OperatingSystem"
SystemDirectory : C:\Windows\system32
Organization    :
BuildNumber     : 14393
RegisteredUser  : Windows User
SerialNumber    : 00329-00000-00003-AA690
Version         : 10.0.14393
```

Sie sehen, dass Ihnen die Klasse Win32_OperatingSystem u. a. Informationen darüber gibt, wo Ihr Betriebssystem installiert ist, aber auch über dessen Version. Tatsächlich ist das nur ein Bruchteil der Informationen, die in der Klasse Win32_OperatingSystem stehen, denn PowerShell unterdrückt einen großen Teil der Eigenschaften, um Sie nicht mit Daten zu überfluten. Versuchen Sie spaßeshalber einmal, die Ausgabe des obigen Befehls in ein **Select-Object** * weiterzuleiten (siehe Listing 4.3).

Listing 4.3 Alle Eigenschaften von Win32_OperatingSystem anzeigen

```
> Get-WmiObject -Query "Select * from Win32_OperatingSystem" | select *
```

Ich spare Ihnen an dieser Stelle die komplette Ausgabe, es sind 84 Eigenschaften.

Damit Sie nicht alle Klassen per PowerShell analysieren müssen, verwenden Sie am besten einen grafischen WMI-Browser. Sehr empfehlenswert, weil leistungsfähig und kostenlos, ist z. B. WMI Explorer, den Sie bei Github unter *https://github.com/vinaypamnani/wmie2/releases* oder kurz *https://bit.ly/2nJwgcQ* herunterladen können. Der WMI Explorer ist ein .NET-basiertes Werkzeug und muss nicht installiert werden. Sie brauchen ihn nur zu entpacken und zu starten (siehe Bild 4.8).

Geben Sie zuerst unter (1) den Computer an, mit dem Sie sich verbinden wollen, und klicken Sie auf **Connect**. Für den lokalen Rechner können Sie einfach einen . (Punkt) eingeben. Der WMI Explorer fragt jetzt den Namensraum ab und zeigt ihn unter Namespaces an. Wählen Sie als Nächstes unter Namespaces „ROOT\CIMV2“ aus (2) und geben Sie im Feld „Quick Filter“ (3) Win32 ein. Der WMI Explorer zeigt dann nur noch die Klassen an, die mit Win32 beginnen. Nun haben Sie eine vollständige Auflistung aller Klassen und können drauflos experimentieren. Wählen Sie z. B. Win32_ComputerSystem (4) aus, wird die Auswahl unter „Instances“ aufgelistet und die Eigenschaften der Instanz werden rechts in der Liste angezeigt. Hier finden Sie eine Eigenschaft namens „TotalPhysicalMemory“, die Ihnen den verfügbaren physikalischen Speicher anzeigt. Klicken Sie ruhig mal ein bisschen in den Klassen herum – kaputt machen können Sie nichts, aber es gibt viel Spannendes zu entdecken. Schauen Sie sich z. B. Win32_Bios an. Wenn Sie unter *Classes* die Maus über einer Klasse stehen lassen, wird Ihnen übrigens auch die Beschreibung der Klasse angezeigt (die Sie zudem unter *Description* finden).

WQL erlaubt es auch, WMI-Daten auf bestimmte Bedingungen zu überprüfen. Für die Überprüfung implementiert WQL wieder die SQL-Syntax – wer ein bisschen SQL kann, ist also fein raus. Um bestimmte Datensätze auszufiltern, verwendet SQL die Where-Klausel:

```
Select * from Win32_OperatingSystem
Where OSArchitecture = '64-Bit'
```

Diese Abfrage bedeutet übersetzt: Gib mir alle Eigenschaften von `Win32_OperatingSystem` zurück, wenn (oder wo) die Eigenschaft `OSArchitecture` dem Wert `'64-Bit'` entspricht. Weil der Eintrag `'64-Bit'` ein Text ist, muss er zusätzlich in Anführungszeichen gesetzt werden.

Ist der Computer, auf dem Sie die Abfrage ausführen, mit einem 64-Bit-Windows installiert worden, gibt die Abfrage alle Eigenschaften der Klasse `Win32_OperatingSystem` zurück. Hierfür ist das * hinter dem Select verantwortlich. Ist der Computer ein 32-Bit-System, liefert die Abfrage gar nichts zurück. Mit WQL können Sie aber nicht nur auf Gleichheit prüfen.

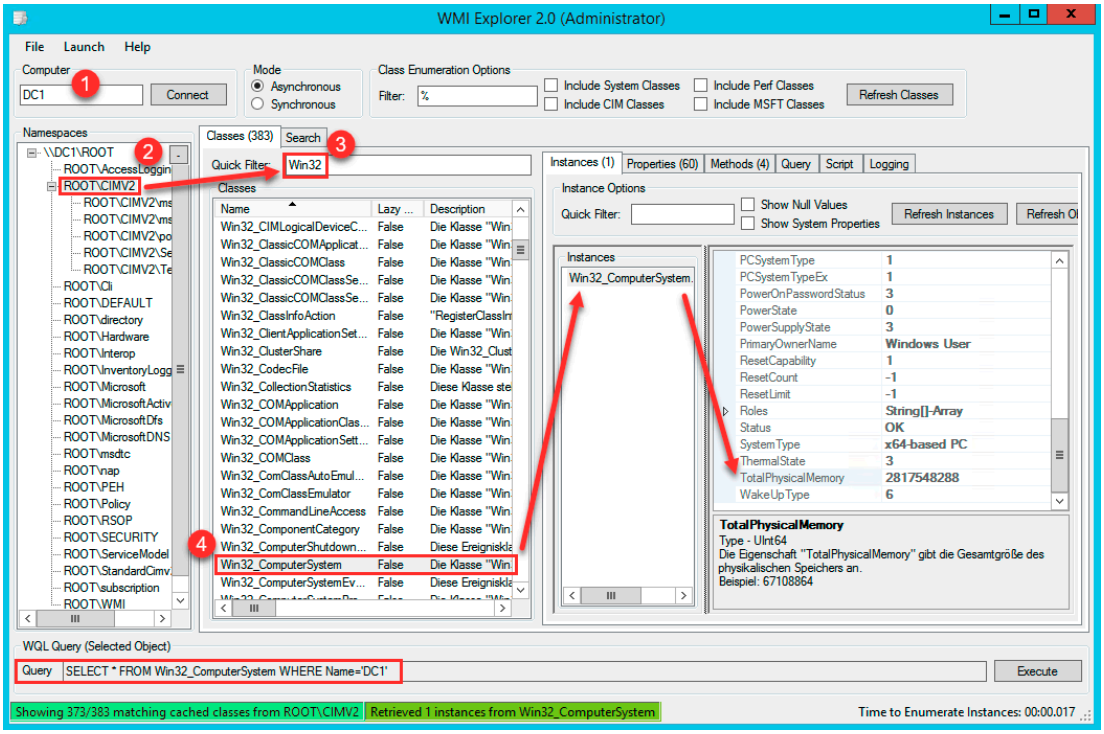


Bild 4.8 WMI Explorer stellt den WMI-Namensraum grafisch dar.

Tabelle 4.1 Die Operatoren mit Beispielen

Operator	Bedeutung	Beispiel
>	Größer	`SELECT * FROM Win32_LogicalDisk WHERE (FreeSpace > 5368709120) and (DeviceID = "C:")`
>=	Größer oder gleich	`Select * from Win32_ComputerSystem Where TotalPhysicalMemory >= 2146451456`
<	Kleiner	
<=	Kleiner oder gleich	
<>	Ungleich	`select * from Win32_OperatingSystem WHERE (ProductType <> "2") AND (ProductType <> "3")`
like	Vergleich mit einem Muster. Als Platzhalter wird % verwendet.	`SELECT * FROM Win32_OperatingSystem where (Version like '10.%') or (Version like '6.3.%')`

Wenn Sie eine WQL-Abfrage erstellt haben, können Sie sie im WMI Explorer auch gleich prüfen, indem Sie eine Klasse auswählen und dann das Register „Query“ öffnen. Geben Sie hier Ihre Abfrage im Textfenster „WQL Query“ ein und wählen Sie die Schaltfläche **Execute**. Ob die Abfrage ein Ergebnis liefert, sehen Sie im Fenster „Results“.

4.3.2 WQL zum Filtern von GPOs

Mit dem Wissen um WMI ist es jetzt einfach, einen WMI-Filter zu schreiben. Ein WMI-Filter ist nämlich nichts anderes als eine im AD hinterlegte WQL-Abfrage, die mit einem GPO verbunden wird. Der WMI-Filter entspricht dabei genau einer WQL-Abfrage. Der Gruppenrichtlinienclient wertet, wenn ein GPO mit einem WMI-Filter verbunden ist, die WQL-Abfrage lokal auf dem Client aus. Wenn die WQL-Abfrage irgendeine Rückgabe liefert, wird das GPO auf dem Client angewendet. Gibt die WQL keinen Wert zurück, wird das GPO übersprungen. Schauen Sie sich dazu noch einmal die WQL-Abfrage an, die den verfügbaren Arbeitsspeicher testet: `Select * from Win32_ComputerSystem Where TotalPhysicalMemory >= 2146451456`. Wenn Sie diese Abfrage auf Ihrem Computer ausführen, gibt die Abfrage alle Eigenschaften der Klasse `Win32_ComputerSystem` zurück (aufgrund des *), wenn Ihr Computer über mindestens 2 GB RAM verfügt. Hat Ihr Computer weniger als 2 GB RAM, liefert die Abfrage kein Ergebnis, denn es konnte ja keine Klasse gefunden werden, auf die die Where-Bedingung zutrifft. Liefert die Abfrage kein Ergebnis zurück, wird das GPO übersprungen.

4.3.3 WMI-Filter erstellen

- Erweitern Sie in der GPMC die Konsolenstruktur und wählen Sie **WMI-Filter**.
- Starten Sie im Kontextmenü den Befehl **Neu**.

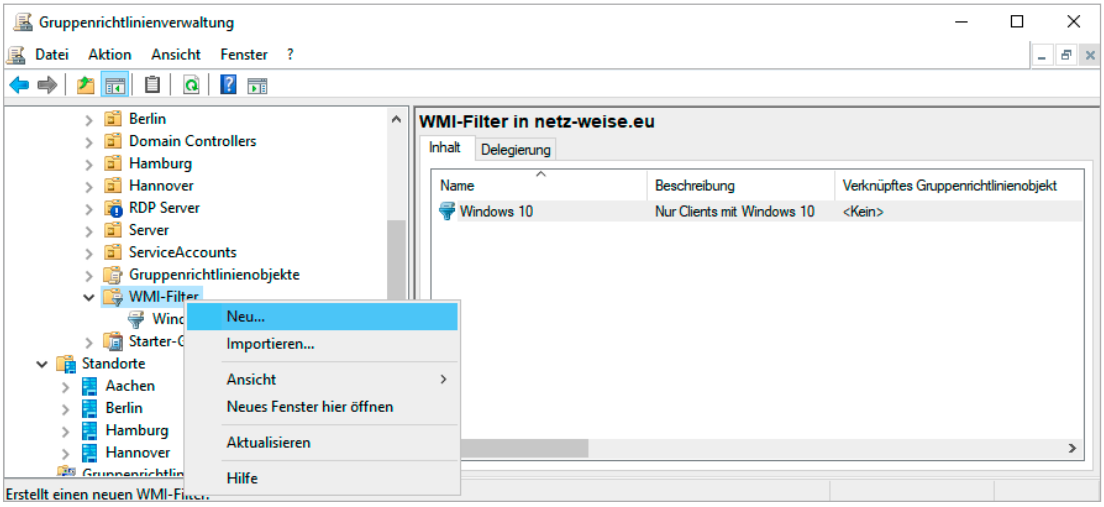


Bild 4.9 Neuen WMI-Filter erstellen

- Geben Sie einen Namen und eine Beschreibung (optional) für den neuen Filter an, z. B. „WMI-Filter für mobile Geräte“.
- Klicken Sie unter „Abfragen“ auf **Hinzufügen**.
- Belassen Sie den Namespace bei `root\CIMv2` und geben Sie bei Abfrage die gewünschte Abfrage ein.

HINWEIS: Im folgenden Beispiel wird eine Abfrage nach dem `PCSystemType` aus der Klasse `Win32_ComputerSystem` verwendet, wobei `'2'` dem Type Mobile entspricht. `PCSystemType` steht allerdings erst ab Vista zur Verfügung. Wenn Sie tatsächlich immer noch ältere Systeme im Einsatz haben sollten, verwenden Sie die Klasse `Win32_SystemEnclosure` und die Eigenschaft `ChassisType`. Eine schöne Auflistung der möglichen Abfragen finden Sie unter *http://woshub.com/sccm-and-wmi-query-to-find-all-laptops-and-desktops/* oder kurz *https://bit.ly/2nHBVjK*.

Listing 4.4 WQL zum Filtern von mobilen Geräten

```
SELECT * FROM Win32_ComputerSystem WHERE PCSystemType = 2
```

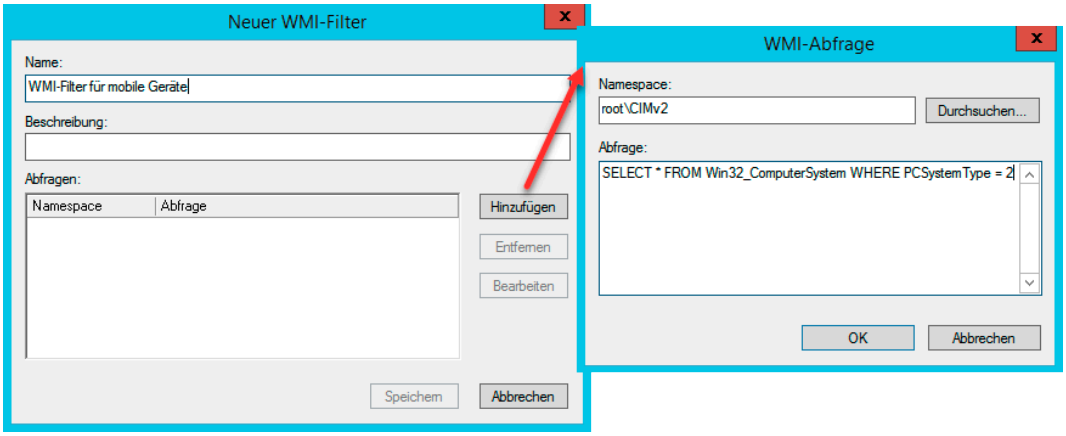


Bild 4.10 WMI-Abfrage definieren

- Bestätigen Sie Ihre Abfragedefinition mit **OK**.

  Wenn Sie an dieser Stelle eine Warnung erhalten, die besagt, dass „der angegebene Namespace kein gültiger Namespace auf dem lokalen Computer ist“, verwenden Sie vermutlich Windows Server 2012 R2. Brechen Sie sicherheitshalber noch einmal ab, und klicken Sie in Ihrer WMI-Abfrage auf **Durchsuchen**. Sie bekommen dann alle WMI-Namensräume angezeigt. Sollte Ihnen in der Liste nicht „root\CIMv2“ angezeigt werden, haben Sie vermutlich tatsächlich ein Problem. Wird der Namensraum aufgelistet, können Sie die Warnung einfach ignorieren. Es handelt sich um einen Bug in Windows Server 2012 R2, der WMI-Filter funktioniert trotzdem einwandfrei. Ab Windows Server 2016 ist der Fehler behoben.

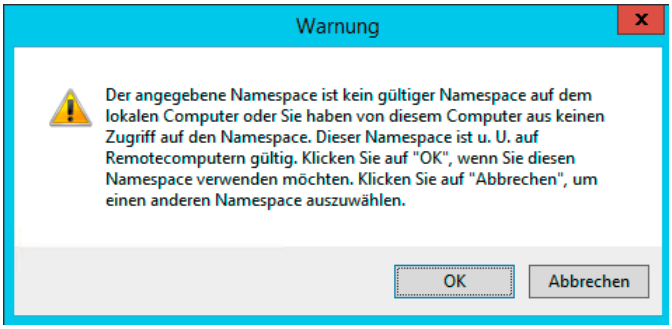


Bild 4.11
Fehlermeldung beim Erstellen eines WMI-Filters

- Sie können auch mehrere WQL-Abfragen in einem Filter zusammenfassen. Klicken Sie hierfür auf **Hinzufügen** und wiederholen die Prozedur. Alle angegebenen Filter werden nacheinander ausgeführt. Die Abfragen sind AND-verknüpft, was bedeutet, dass alle Abfragen ein Ergebnis liefern müssen, damit die GPO angewendet wird. Es gibt keine Möglichkeit, dieses Verhalten zu ändern!
- Wenn Sie **Speichern** auswählen, überprüft das System die WMI-Abfrage. Sollte diese nicht korrekt sein, erhalten Sie eine Fehlermeldung.

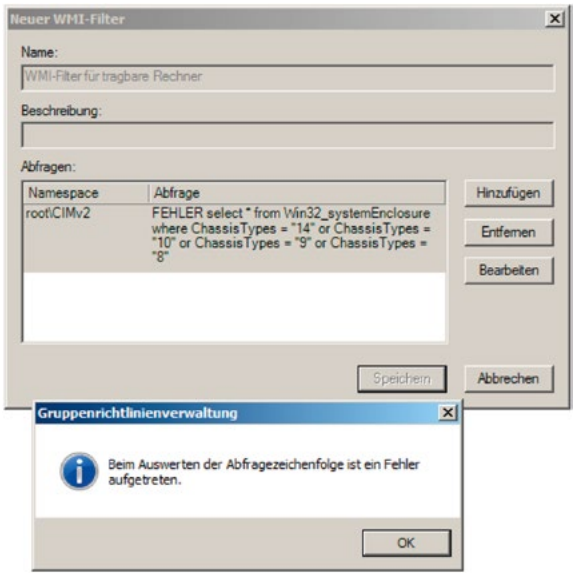


Bild 4.12
Syntaxprüfung

4.3.4 WMI-Filter anwenden

- Markieren Sie das GPO, dem Sie einen WMI-Filter zuweisen möchten, und aktivieren Sie im unteren Fensterbereich unter WMI-Filterung das Drop-down-Menü. Wählen Sie dort den Filter, den Sie verwenden möchten.
- Sie werden gefragt, ob Sie den Filter ändern wollen. Bestätigen Sie mit **Ja**.

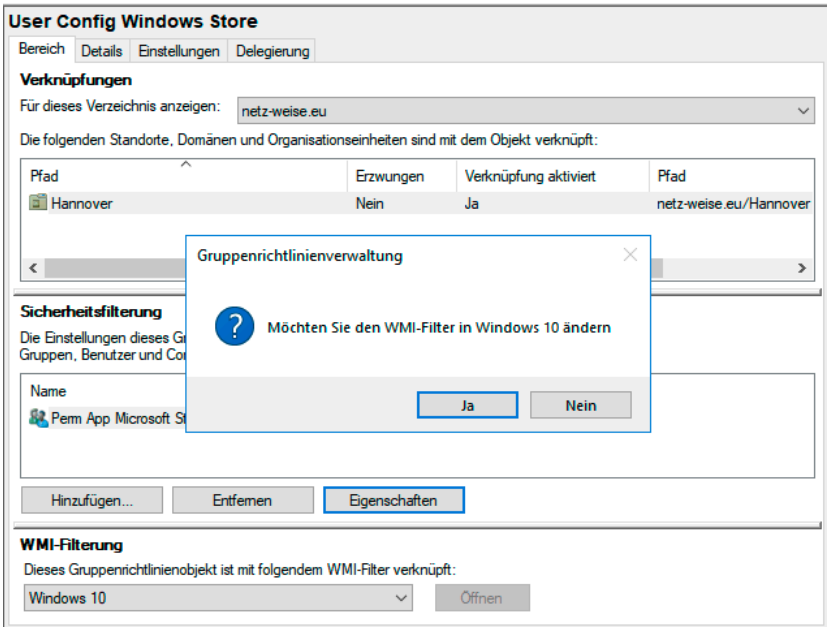


Bild 4.13 WMI-Filter zuweisen

4.3.5 WMI-Filter entfernen

- Markieren Sie das GPO, dem Sie einen WMI-Filter zuweisen möchten, und aktivieren Sie im unteren Fensterbereich unter „WMI-Filterung“ das Drop-down-Menü.
- Wählen Sie dort **<Kein>**, um den Filter zu entfernen. Sie werden gefragt, ob Sie den WMI-Filter entfernen möchten. Bestätigen Sie mit **Ja**.

4.3.6 WMI-Filter exportieren

Sie können WMI-Filter exportieren. Das kann z. B. für das Kopieren eines WMI-Filters aus Ihrer Testumgebung oder für eine Migration sinnvoll sein. Außerdem können Sie über den Export ein Backup Ihrer WMI-Filter erstellen. Wenn Sie viele WMI-Filter haben, können Sie auch PowerShell für den Export verwenden.

- Öffnen Sie den Knoten „WMI-Filter“ in der Konsolenstruktur der GPMC.
- Öffnen Sie das Kontextmenü des WMI-Filters, und wählen Sie „Exportieren“ aus.
- Geben Sie den Zielpfad für den Filter an, und wählen Sie „Speichern“, um den Filter als .mof-Datei zu speichern. Das .mof-Format ist textbasiert, Sie können es also hinterher in einem Texteditor prüfen.

4.3.7 WMI-Filter importieren

- Öffnen Sie das Kontextmenü des Knotens WMI-Filter in der Konsolenstruktur der GPMC und wählen Sie **Importieren**.
- Im Auswahlfenster navigieren Sie zur .MOF-Datei, wählen den Filter und anschließend **Öffnen** aus.
- Im Import-Fenster können Sie den Filter noch einmal prüfen oder anpassen. Mit **Import** wird der Filter erstellt.

4.3.8 Beispiele von WMI-Abfragen für WMI-Filter

WMI-Filter lassen sich für eine schier unerschöpfliche Anzahl von Abfragen verwenden. Sie können z. B. Hardwarekomponenten auslesen, installierte Anwendungen oder Treiber abfragen oder auch den Betriebsstatus von Computern auslesen. Eine englische Dokumentation sämtlicher WMI-Klassen finden Sie im Internet unter *https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/wmi-reference* oder kurz *https://bit.ly/2nJw1Pm*.

Tabelle 4.2 zeigt Ihnen einige WMI-Abfragen, die Sie verwenden können, um Abfragen in Ihrem Netzwerk zu definieren.

Tabelle 4.2 WMI-Abfragen für WMI-Filter

Abfrage, ob das installierte Betriebssystem ein deutschsprachiges Windows 10 ist: `Select Version from Win32_OperatingSystem where Version like "10.0%" and CountryCode="49"`
Abfrage, ob das installierte Betriebssystem Windows 8 oder Windows 10 ist: `Select Version from Win32_OperatingSystem where (Version like "6.3%") or (Version like "10.%")`
Nach einer bestimmten Windows 10 Build-Nummer (Feature Release) suchen: `Select BuildNumber from Win32_Operatingsystem Where Buildnumber = '17134'`
Nach mehreren Build-Nummer suchen geht, indem man mehrere WMI-Abfragen in einem Filter zusammenfasst., oder schneller, indem man eine OR-Verknüpfung verwendet: `Select BuildNumber from Win32_Operatingsystem Where Buildnumber = '17134' or Buildnumber = '16299'`
Abfrage, ob das Rechnermodell ein Laptop FSC Lifebook E8010 mit Intel-Prozessor ist: `Select Model from Win32_ComputerSystem where (manufacturer = "FUJITSU SIEMENS") and (Model = "LIFEBOOK E8010 INT")`
Abfrage, ob Hotfix KB2478063 (Microsoft .NET Framework 4 Platform-Update 1 – Laufzeitupdate) installiert ist: `Select HotFixID from Win32_QuickFixEngineering where HotFixID = "KB2478063"` **ACHTUNG! Diese Abfrage läuft sehr lange und kann die Verarbeitung Ihrer Gruppenrichtlinien deutlich verzögern. Versuchen Sie, das Suchen nach Hotfixes zu vermeiden!**

Abfrage, ob der Firewalldienst läuft:

```
Select State from Win32_service where name='MpsSvc' and State='Running'
```

Abfrage, ob ein Rechner tragbar ist:

```
SELECT PCSystemType FROM Win32_ComputerSystem WHERE PCSystemType = 2
```

Abfrage, ob auf dem Datenträger C: mindestens 5 GB Speicherplatz frei ist:

```
SELECT FreeSpace FROM Win32_LogicalDisk WHERE (FreeSpace > 5368709120)
and (DeviceID = "C:")
```

Abfrage, ob mindestens 2 GB Arbeitsspeicher installiert sind:

```
Select TotalPhysicalMemory from Win32_ComputerSystem Where TotalPhysicalMemory >=
2146451456
```

4.3.9 WMI-Filter optimieren

WMI-Filter sind eine tolle Sache, weil Sie GPOs so anhand der Möglichkeiten der Clients anwenden können. Aber für WMI-Filter gilt wie für alles andere auch: Testen Sie Ihre WMI-Filter, bevor Sie sie anwenden. Ein WMI-Filter funktioniert nämlich nicht unbedingt so, wie Sie es erwarten, und unter Umständen braucht das Abfragen der WMI-Datenbank außerdem auch noch sehr lange. Die meisten WMI-Filter sind zwar in Millisekunden abgearbeitet. Sie können die Verarbeitung sogar noch optimieren, indem Sie in der WQL-Abfrage hinter dem Select nicht * angeben, sondern eine der Eigenschaften der WMI-Klasse. Der WMI-Filter kann dann noch schneller verarbeitet werden. Bei einer einzelnen Abfrage macht das wenig Performancegewinn, muss ein Gruppenrichtlinienclient aber viele WMI-Abfragen verarbeiten, summieren sich auch Millisekunden zu merklichen Zeitspannen.

Es gibt aber einige Klassen, deren Abfragen zu merklichen Verzögerungen führen und die Sie auf jeden Fall meiden sollten. Das ist die im Beispiel oben verwendete Klasse `Win32_QuickFixEngineering`, die Ihnen installierte Updates anzeigt, und die Klasse `Win32_Product`, die Ihnen die auf dem Computer installierten Programme zurückliefert. Beide Klassen rufen die Informationen erst ab, wenn man die WQL-Abfrage startet, und benötigen mehrere Sekunden (!), um die Abfrage zu beenden. Wenn ein Gruppenrichtlinienclient mehrere solcher aufwendigen WQL-Filter auswerten muss, kann sich das schnell zu lähmenden Wartezeiten für den Benutzer addieren.

Um zu testen, wie lange eine WQL-Abfrage benötigt, können Sie das PowerShell-Cmdlet `Measure-Command` einsetzen, das die Laufzeit eines Kommandos bestimmen kann. Rufen Sie dafür die WQL-Abfrage per `Get-WMIObject` auf, und übergeben Sie das Kommando an Measure-Command:

```
> measure-command { Get-WMIObject -Query "Select * from Win32_QuickFixEngineering
where HotFixID = 'KB316 4035'" }

Days              : 0
Hours             : 0
Minutes           : 0
Seconds           : 1
```

```
Milliseconds      : 162
Ticks             : 11627903
TotalDays         : 1,34582210648148E-05
TotalHours        : 0,000322997305555556
TotalMinutes      : 0,0193798383333333
TotalSeconds      : 1,1627903
TotalMilliseconds : 1162,7903
```

Der Abruf der Klasse `Win32_QuickFixEngineering` hat eine Sekunde und 162 Millisekunden gebraucht.

Eine gute Untersuchung des Einflusses von WMI-Filtern auf die Anmeldung finden Sie bei Helge Klein unter *https://helgeklein.com/blog/2016/01/how-group-policy-impacts-logon-performance-3-wmi-filters-ilt/* oder kurz *https://bit.ly/2PeHjHF*.

5 Gruppenrichtlinien-Infrastruktur planen

In diesem Kapitel werden folgende Themen behandelt:

- AD-Design und GPOs
- Benennung von GPOs
- GPOs dokumentieren
- Testen von GPOs
- Empfohlene Vorgehensweisen

5.1 Einführung

Wenn Sie Gruppenrichtlinien zur zentralen Verwaltung Ihrer Benutzer und Computer einsetzen wollen, hat das wesentliche Auswirkungen auf das Design Ihrer AD-Infrastruktur, da Gruppenrichtlinien nur auf Standorte, Domänenobjekte sowie Organizational Units (OUs) angewendet werden können. Sie sollten bei der Planung Ihres OU-Aufbaus also auf jeden Fall schon den Einsatz von Gruppenrichtlinien im Auge haben.

Wenn im Laufe der Zeit die Anzahl der GPOs immer weiterwächst, stellen viele Unternehmen außerdem fest, dass es ihnen immer schwerer fällt, die Einstellungen in ihren GPOs wiederzufinden. Hier hilft eine sinnvolle Benennungsstrategie, die es erlaubt, GPOs und ihre Verursacher leichter zu finden. Außerdem sollte eine Dokumentation nicht fehlen. Glücklicherweise ist es seit Windows Server 2008 möglich, einen großen Teil der Einstellungen direkt in den GPOs zu kommentieren.

Denken Sie außerdem daran, neue GPOs immer zu testen, bevor sie in der Produktion freigegeben werden. GPOs sind ein mächtiges Werkzeug, mit dem man mächtig viel kaputt machen kann.

5.2 AD-Design und GPOs

Mit Active Directory hat Microsoft die Möglichkeit geschaffen, Benutzer- und Computerdaten strukturiert in Containern abzulegen. Das war nicht immer so. Noch bei NT4 waren alle Benutzer, Gruppen und Computer in einer Liste gespeichert. Wenn Sie NT4 nicht mehr kennen, machen Sie doch spaßeshalber einmal die Benutzerverwaltung in der Computerverwaltung auf und versuchen Sie sich vorzustellen, wie sich ein Netzwerk bedient, in dem 5000 Benutzer und 500 Gruppen in einer Liste untereinanderstehen.

Das Active Directory stellt Ihnen eine Struktur zur Verfügung, die einer Ordnerstruktur im Dateisystem ähnelt. Diese Struktur sieht bei einer frisch installierten Domäne aus wie in Bild 5.1.

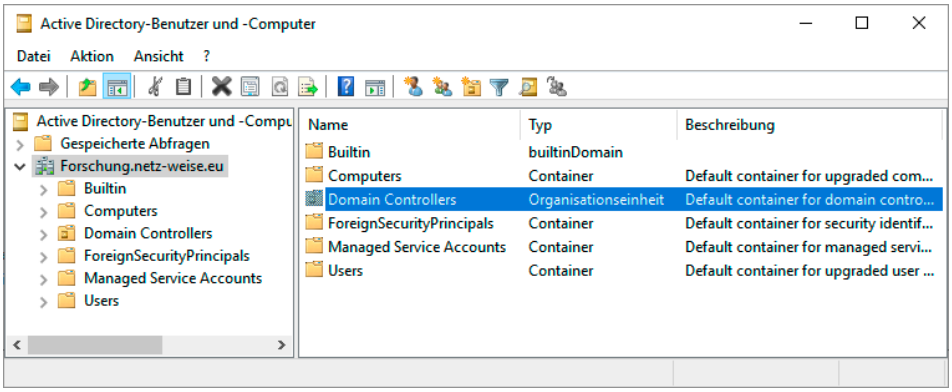


Bild 5.1 Ansicht einer neu installierten Domäne

Sie sehen eine ganze Reihe von Containern sowie eine OU. Rein optisch ist erst einmal kein großer Unterschied zwischen einem Container und einer OU festzustellen. Die OU ist nur daran zu erkennen, dass unter „Typ“ „Organisationseinheit“ angegeben und auf dem Ordner-Symbol eine kleine Schriftrolle erkennbar ist. Auch technisch sind die Unterschiede nur gering, aber mit gewaltigen Auswirkungen; denn Gruppenrichtlinien können auf Containern nicht angelegt werden. Da OUs keine Nachteile gegenüber Containern haben, können Sie in „Active Directory-Benutzer und -Computer“ auch gar keine Container anlegen.

Die einzige OU, die nach der Installation des AD existiert, ist die OU „Domain Controllers“. Auf ihr ist die „Default Domain Controllers Policy“ verknüpft. Die Default Domain Controllers Policy beinhaltet eine ganze Reihe von Einstellungen, die die Sicherheit von Domänencontrollern deutlich erhöhen (siehe Bild 5.2) – Domänencontroller sind das Herz Ihres AD. Bekommt ein unberechtigter Benutzer Zugriff darauf, können Sie faktisch mit einer Neuinstallation beginnen.

Mit der Installation des Active Directory auf einem Server wird dessen Computerkonto in die OU „Domain Controllers“ verschoben und der Computer neu gestartet. Nach dem Neustart verbindet sich der Gruppenrichtlinienclient mit der Domäne, findet die jetzt für ihn gültige Gruppenrichtlinie „Default Domain Controllers“ und wird automatisch gehärtet, ohne dass noch jemand Hand anlegen muss.

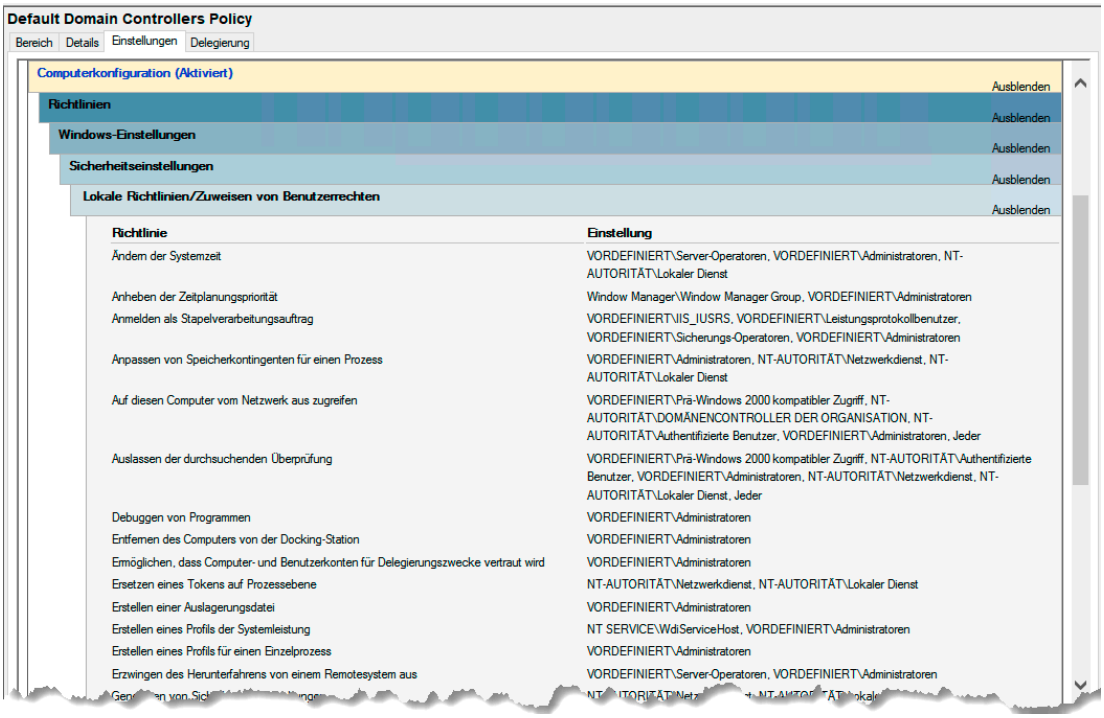


Bild 5.2 Die Default Domain Controllers Policy sichert DCs ab.

Dieses Verhalten zeigt eindrucksvoll, wie viel Arbeit Ihnen Gruppenrichtlinien abnehmen können, wenn Sie Ihre Konten und Ihre Gruppenrichtlinien intelligent platzieren. Installieren Sie einen Computer, legen Sie sein Konto in der richtigen OU an, und schon wird der Computer beim ersten Neustart konfiguriert.

5.2.1 OUs und Gruppenrichtlinien

OUs und Gruppenrichtlinien sind sehr eng miteinander verbunden, denn eigentlich ist der einzige Grund, warum Sie OUs brauchen, die Tatsache, dass OUs mit Gruppenrichtlinien verknüpft werden können. Alle anderen Funktionen könnten Sie genauso gut mit Containern erledigen. Wenn Sie Ihr OU-Design vornehmen, sollten Sie also das Design in erster Linie an den geplanten Gruppenrichtlinien orientieren.

OUs haben grundsätzlich drei Aufgaben im AD. Zum einen sind sie dafür da, Benutzer, Computer und Gruppen in überschaubare Administrationseinheiten zu unterteilen. Unter NT4 war es eine Katastrophe, Benutzerkonten zu verwalten. Mit dem AD haben Sie jetzt die Möglichkeit, Benutzer in gemeinsamen Organisationsstrukturen abzulegen. Das macht das Auffinden von Konten deutlich einfacher.

OUs können aber auch dazu verwendet werden, administrative Berechtigungen im AD zu vergeben. Diese Berechtigungen gelten ausschließlich in der AD-Datenbank – Sie können also Benutzern im AD auf einer OU das Recht geben, die Kennwörter aller Benutzer zurück-

zusetzen oder neue Gruppen anzulegen. Was Sie nicht können, ist, einem Benutzer hier das Recht zu geben, einen PC zu administrieren. Diese Berechtigungen werden ausschließlich lokal auf den Clients verwaltet und können nur über Gruppenmitgliedschaften gesteuert werden. Das geht wohlgemerkt auch im AD, aber eben nicht über die Berechtigungen einer Organisationseinheit.

So können Sie auch Standort-Administratoren definieren, die z. B. in Aachen GPOs verknüpfen können. Wählen Sie hierzu in „Active Directory-Benutzer und -Computer" eine OU und wählen Sie im Kontextmenü „Objektverwaltung zuweisen …" (siehe Bild 5.3 bis Bild 5.5).

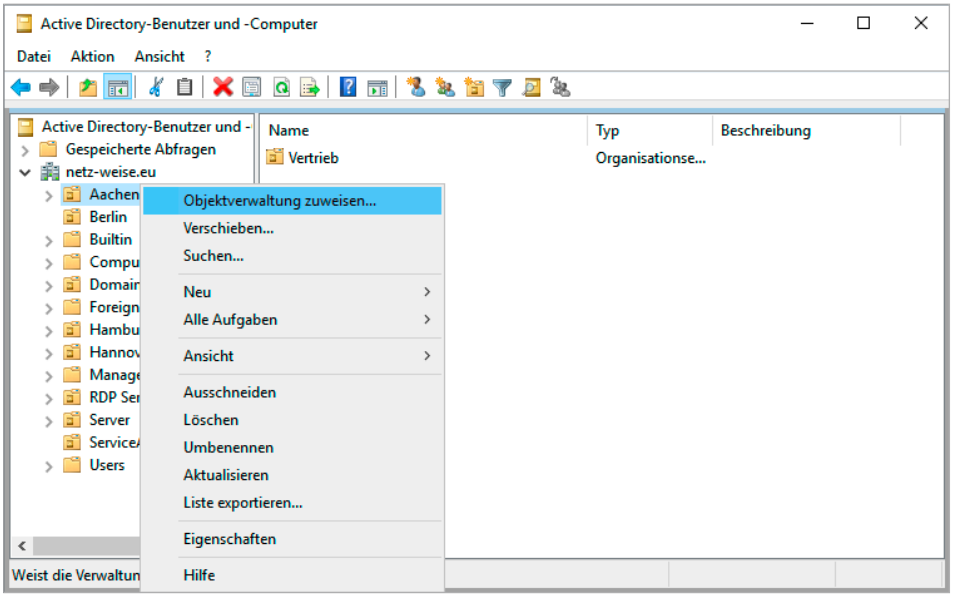


Bild 5.3 Wählen Sie in Active Directory-Benutzer und -Computer auf einer OU „Objektverwaltung zuweisen".

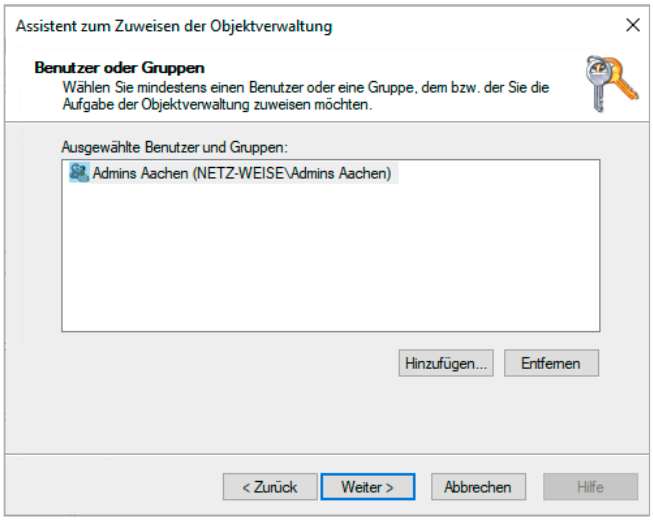


Bild 5.4 Wählen Sie eine Gruppe aus und vergeben Sie das Recht …

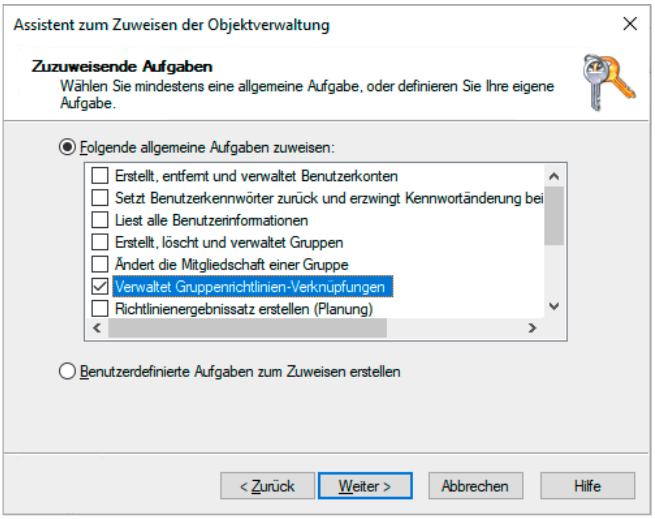


Bild 5.5 … „Verwaltet Gruppenrichtlinien-Verknüpfungen“.

Das setzt natürlich voraus, dass alle Benutzer, die gemeinsam administriert werden sollen, auch innerhalb der gleichen OU-Struktur liegen, im Beispiel also Aachen.

Schließlich können OUs auch verwendet werden, um Benutzer und Computer per Gruppenrichtlinien zu konfigurieren. Während die Berechtigungsvergabe und das „Sortieren“ von Ressourcen auch mit Containern passieren kann, können GPOs nur mit Organizational Units verknüpft werden. Das liegt daran, dass die GPOs auf der OU in einer Eigenschaft **gpLink** eingetragen werden, die auf Containern schlicht nicht existiert. (Mehr hierzu erfahren Sie in Kapitel 13, „Funktionsweise von Gruppenrichtlinien“.)

Für Sie hat das zur Konsequenz, dass Sie bei der Planung Ihrer OU-Struktur vor allem drei Dinge einbeziehen müssen:

- Welche Benutzer sind räumlich und organisatorisch miteinander verbunden? Das bezieht sich auf den Standort genauso wie auf Abteilungen. Normalerweise erwartet man, dass sich Benutzer aus der gleichen Abteilung im AD auch in der gleichen OU befinden.
- Welche Benutzer sollen gemeinsam administriert werden? Dadurch, dass Sie im AD administrative Berechtigungen auf Konten vergeben können, macht es natürlich Sinn, alle Konten, die von den gleichen Administratoren verwaltet werden sollen, auch in den gleichen OUs anzulegen.
- Welche Benutzer sollen die gleiche Konfiguration erhalten? Dies bezieht sich z. B. auf zu installierende Software, aber auch auf Sicherheits- oder Clienteinstellungen. Die Konfiguration wird natürlich über Gruppenrichtlinien ausgeführt.

In den meisten Organisationen bilden diese drei Anforderungen eine gemeinsame Schnittmenge, was die Planung der OU-Struktur deutlich vereinfacht, denn dann brauchen Sie sich eigentlich nur noch einen Strukturplan Ihres Unternehmens herzunehmen und Ihre Abteilungen als OUs anzulegen.

Sollte sich Ihr Unternehmen allerdings nicht so einfach abbilden lassen, weil Sie über viele Standorte verfügen, Ihre Administratoren nicht standortweit arbeiten oder alle Ihre Benut-

zer individuelle Konfigurationen benötigen, sollten Sie sich für die Planung an eine goldene Regel halten: Das AD bietet Ihnen mithilfe der Delegierung und Gruppenrichtlinien zwei fantastische Werkzeuge, um sich viel Arbeit zu sparen. Diese Werkzeuge können Sie aber nur einsetzen, wenn Ihr AD das passende Design dafür aufweist. Das AD dient der Verwaltung Ihrer Benutzer und Ressourcen! Das Abbilden der Unternehmensstruktur hat also die mit Abstand geringste Priorität. Planen Sie nach Ihren administrativen Bedürfnissen, nicht danach, was sich mit dem wenigsten Aufwand umsetzen lässt. Wenn Sie alle Benutzer einer Abteilung anzeigen lassen wollen, können Sie im „Active Directory-Benutzer und -Computer“ beispielsweise mit gespeicherten Abfragen arbeiten und müssen sie nicht alle in einer OU verwalten.

Als Nächstes sollten Sie sich überlegen, welche Strukturen in Ihrem Unternehmen sich am seltensten ändern. Oft sind das Standorte. In manchen Unternehmen wird jede Abteilung einmal pro Jahr umstrukturiert, aufgelöst und durch neue ersetzt. Die Standorte bleiben aber häufig länger erhalten – schließlich ist es teuer, neue Gebäude zu mieten und die Mitarbeiter umzuziehen. Vielleicht sind Sie aber auch Administrator in einem Wanderzirkus, und feste Standorte kennen Sie gar nicht. Wo auch immer Sie sich wiedererkennen – die stabilsten Strukturen gehören in der AD-Struktur immer ganz nach unten, also direkt unterhalb der Domäne. Der Grund ist ganz einfach: Es ist deutlich einfacher, ein paar untergeordnete OUs zu verschieben oder umzustrukturieren als eine OU an der Wurzel eines Astes.

Speziell in Hinblick auf Gruppenrichtlinien ist es meist sinnvoll, noch einmal eine Trennung zwischen Benutzern, Computern und Servern durchzuführen, da es oft angebracht ist, Computereinstellungen und Benutzereinstellungen getrennt voneinander zu verwalten. Es kann, je nach Einsatzzweck der Computer, auch durchaus sinnvoll sein, die Computer alle gemeinsam in einer OU auf dem Standort zu verwalten, aber die Benutzer in ihren Abteilungen getrennt. Was für Sie am besten passt, hängt hauptsächlich davon ab, ob die Benutzer oder Computer die gleichen Einstellungen benötigen oder individuell konfiguriert werden müssen.

Fassen wir also noch einmal zusammen:

Für eine OU-Struktur ist es sinnvoll, an erster Stelle die administrativen Erfordernisse „Gruppenrichtlinien“ und „administrative Berechtigungen“ zu betrachten. Der Aufbau des Unternehmens lässt sich hierauf zwar oft abbilden, aber das muss nicht so sein.

Wenn Sie mit der Planung beginnen, identifizieren Sie zuerst die Strukturen, die sich am seltensten ändern. Die sollten auf der untersten OU-Ebene abgebildet werden. Meist sind dies die Standorte, gefolgt von Abteilungen. Wenn Ihre Benutzer alle die gleichen Einstellungen bekommen, kann es aber auch sinnvoll sein, sich die Abteilungen zu sparen. Versuchen Sie außerdem, Benutzer, Server und Computerkonten in getrennten OUs zu verwalten. Das ist sowohl aus administrativer als auch aus Gruppenrichtlinienverwaltungs-Sicht sinnvoll. Ein Mitarbeiter des UDH muss z. B. Benutzerkennwörter zurücksetzen können, aber deswegen benötigt er noch lange keine Berechtigungen auf dem Computerkonto des Benutzers (Achtung, wir reden hier wieder vom AD-Objekt, nicht vom PC!).

Ansonsten gilt: Unternehmensstrukturen sind oft fließend, und Ihre OU-Struktur sollte das auch sein. OUs sind nicht in Stein gemeißelt, und wenn Sie feststellen, dass eine OU-Struktur nicht Ihre Anforderungen erfüllt, dann ändern Sie sie! Mit ein bisschen Planung und PowerShell ist das Verändern einer OU-Struktur (natürlich abhängig von der Größe Ihrer Organisation) schnell erledigt. Haben Sie also keine Angst, dass Sie etwas falsch machen

könnten, man kann mit ein paar Vorsichtsmaßnahmen fast alles wieder rückgängig machen. Hauptsache, Sie machen regelmäßig ein Backup – und wissen auch, wie Sie es wiederherstellen können! ☺

5.2.2 GPOs und Sicherheitsfilterung

Ein weiterer Ansatz zur Implementierung ist die Zuweisung von GPOs über Sicherheitsfilter (siehe Kapitel 4, „Gruppenrichtlinien filtern“). Bei diesem Konzept verknüpfen Sie alle Ihre GPOs direkt unter der Domäne und ignorieren Ihre OUs komplett. Nun legen Sie für jede GPO eine Gruppe an und fügen diese anstatt „Authentifizierte Benutzer“ in die Liste „Sicherheitsfilter“ ein. Soll ein Benutzer oder Computer durch ein GPO konfiguriert werden, fügen Sie das Konto in die Gruppe ein.

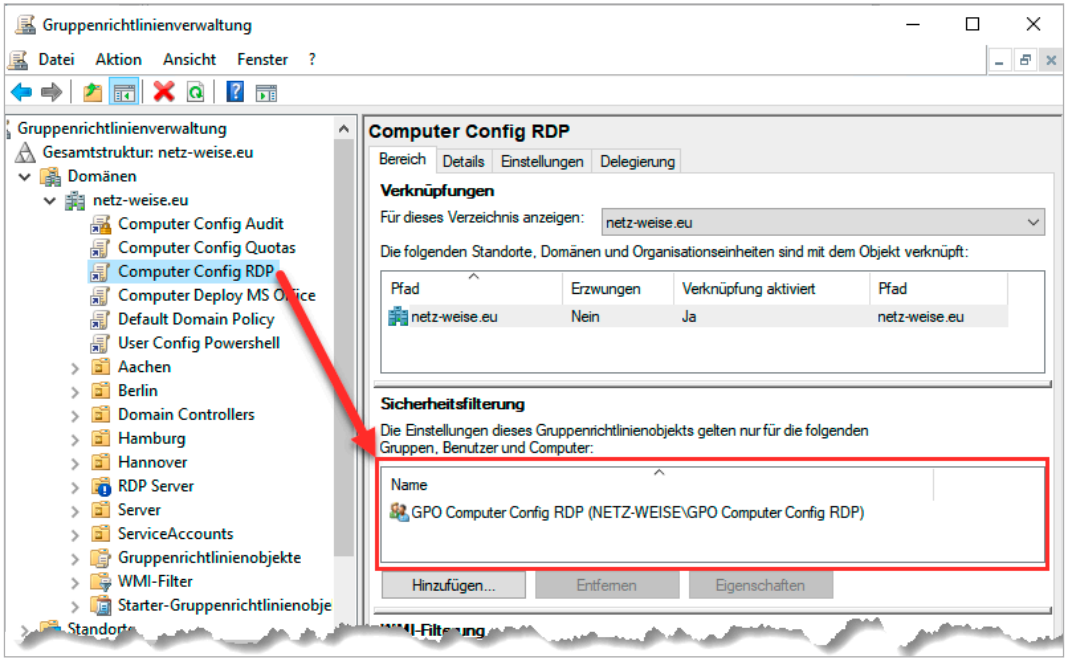


Bild 5.6 Die GPOs sind unter der Domäne verknüpft, die Zuordnung erfolgt per Filter.

Dieses Konzept ist weder von Microsoft noch von mir empfohlen, denn es hat mehrere Nachteile. Zum einen wird es schnell unübersichtlich, je mehr GPOs Sie verwalten müssen, denn alle GPOs liegen unterhalb der Domäne. Ordnen Sie ein GPO einer OU zu, sehen Sie auf den ersten Blick, ob ein Benutzer vom GPO betroffen ist oder nicht – Sie brauchen ja nur zu schauen, ob er sich in einer untergeordneten OU befindet. Benutzen Sie die Filterung, müssen Sie jedes Mal in die Gruppe schauen, die aber mit zunehmender Anwenderzahl auch immer unübersichtlicher wird.

Des Weiteren muss der Gruppenrichtlinienclient für jede einzelne Richtlinie überprüfen, ob sie angewendet werden muss, denn die Gruppenrichtlinien betreffen räumlich ja nun alle

Accounts der Domäne. Das kann den Anmeldevorgang bei einer großen Zahl von Gruppenrichtlinien verlängern.

Fazit: Versuchen Sie, Sicherheitsfilter so anzuwenden, wie Microsoft es vorgesehen hat – in Ausnahmefällen nämlich, wenn Sie Ihr Problem mit OUs nicht mehr oder nur sehr umständlich lösen können.

5.3 Wie viele Einstellungen gehören in ein GPO?

Eine häufige Frage ist, wie viele Gruppenrichtlinien man in einem GPO konfigurieren sollte. Für jede Einstellung ein GPO? Alle Einstellungen in ein GPO? Für Computer und für Benutzer jeweils ein eigenes GPO konfigurieren?

Wie üblich gibt es auf diese Frage keine eindeutige Antwort, nur Argumente für oder gegen jede Seite.

Gegen „ein GPO pro Gruppenrichtlinie“ spricht auf jeden Fall, dass Sie viel zu viele GPOs in Ihrer Domäne verwalten müssen. Es hat natürlich Vorteile, wenn man ein GPO hat, das „Kommandozeile deaktivieren“ heißt. Haben Sie dann das Bedürfnis, einem Benutzer den Zugriff auf die Kommandozeile zu verweigern (BofH[1] lässt grüßen), weisen Sie ihm einfach das GPO zu. Davon abgesehen, dass diese Konfiguration nur in Verbindung mit der Sicherheitsfilterung Sinn macht, die Sie ja eigentlich nur im Notfall einsetzen sollten, müssten Sie so eine Unmenge von GPOs verwalten. Es gibt auch einen zweiten Grund, der dagegen spricht, sehr viele GPOs zu verwenden, und das ist der Einfluss auf die Anmeldezeit. Das Verarbeiten von 20 GPOs mit 20 Einstellungen dauert länger als das Verarbeiten von einem GPO mit 20 Einstellungen. Wir reden hier allerdings von Verzögerungen im Millisekunden-Bereich pro GPO, sodass Sie nicht gleich panikartig alle Ihre GPOs zusammenführen müssen.

Auf der anderen Seite machen Sie sich extrem unflexibel, wenn Sie versuchen, möglichst viele Gruppenrichtlinien in einem GPO zu konfigurieren. Dadurch benötigen Sie letztlich wieder jede Menge GPOs, denn Sie müssen (leicht übertrieben) für jeden Benutzer ein eigenes GPO konfigurieren.

Der beste Weg befindet sich also wie üblich in der Mitte. Versuchen Sie, gemeinsame Einstellungen in einem GPO zu sammeln, die Sie dann an eine Gruppe von Benutzern verteilen können. Hier ein Vorschlag:

- Zusammengehörige Sicherheitskonfigurationen gehören in ein GPO. Ein gutes Beispiel ist hier die „Default Domain Controllers Policy“.
- RDP-Server-Einstellungen werden oft in einem GPO zusammengefasst.
- Sie haben einen Basissatz von Software, der auf jeden Client gehört? Ab in ein GPO.

[1] BofH: Bastard Administrator from Hell

- Logon-Einstellungen aus Gruppenrichtlinien-Einstellungen (Preferences) können in einem GPO stehen.
- Konfigurationseinstellungen, die für eine Gruppe von Computern oder Benutzern gelten sollen (Basiseinstellungen), können in einem GPO konfiguriert werden.

Zusammenfassend kann man sagen, dass sich fast alle Einstellungen auf Gruppen von Computern und Benutzern in Kategorien zusammenfassen lassen. Versuchen Sie, Ihre Kategorien zu identifizieren und daraus ein Schema zu entwickeln, an das Sie sich halten können. **Kombinieren Sie diese allgemeinen GPOs mit spezifischen Einstellungen, die Sie keiner Kategorie zuordnen können.** Haben Sie z. B. ein GPO, die den SQL-Server-Port öffnen soll, aber es gibt kein allgemeines GPO für SQL-Server, so ergänzen Sie Ihre allgemeinen GPOs durch spezifische GPOs.

5.4 Benennung von GPOs

Es gibt wohl kaum ein Thema, über das man so vortrefflich streiten kann wie über Namenskonventionen. Daher will ich Ihnen an dieser Stelle nur einen Vorschlag machen, wie Sie Ihre GPOs benennen können. Es gibt nicht **den** richtigen Weg. Es gibt nur verschiedene Ansätze, und Sie müssen den Ansatz finden, der zu Ihnen passt. Nur eins ist ganz sicher: Sie sollten auf jeden Fall eine Benennungskonvention festlegen, an die sich alle Kollegen halten müssen.

Zuerst eine Bitte: Versuchen Sie, Trivialitäten in Namen zu vermeiden. Nennen Sie eine OU nicht OU oder ein GPO nicht GPO. Na klar ist ein GPO ein GPO, das weiß jeder und deshalb ist diese Information überflüssig. Der Sinn einer Namenskonvention ist es, wichtige Informationen in leicht erfassbarer Form abzulegen.

Grundsätzlich ist es wichtig, dass Sie Ihre GPOs kategorisieren (siehe Abschnitt 5.3). Die Kategorien gehören sinnvollerweise in den Namen. Kategorien könnten z. B. sein:

- Konfiguration
- Installation
- Sicherheit
- Start
- Anmeldung

Die Kategorien können im Normalfall spezifiziert werden. Das kann z. B. ein Satz von Basiseinstellungen sein oder aber es sind spezifische Einstellungen. Übernehmen Sie diese in den Namen.

- Konfiguration Basis
- Konfiguration Firewall
- Konfiguration Applocker
- Installation BasisAnwendungen
- Installation MS Office
- Sicherheit Basis

Außerdem kann es sinnvoll sein anzugeben, ob das GPO Computer- oder Benutzereinstellungen vornimmt.

- Computer Konfiguration Basis
- User Installation BasisAnwendungen
- Computer Sicherheit Basis

Wenn Sie ein spezifisches GPO haben, das nur eine Einstellung betrifft, können Sie im Namen ruhig spezifischer werden.

- Computer Sicherheit Firewall SQL(1433) Eingehend offen

Wenn Sie mit mehreren Administratoren an GPOs arbeiten und jeder Admin seine eigenen GPOs anlegt, kann es auch sinnvoll sein, den Namen des Besitzers in das GPO aufzunehmen.

- Computer Sicherheit Firewall SQL(1433) Eingehend offen – Voges

Um die Übersichtlichkeit zu erhöhen, macht es Sinn, Abkürzungen einzufügen. Außerdem bin ich ein Freund der englischen Sprache bei der Benennung, aber das ist natürlich Geschmackssache, solange Sie nicht in einem global agierenden Konzern unterwegs sind.

- Comp Conf Base – HV
- Usr Inst BaseApp – HV
- Comp Sec FW SQL(1433) – HV

Wenn Sie GPOs haben, die nur an einen Ort gebunden sind, kann es Sinn machen, diesen ebenfalls mit anzugeben.

- H Comp Conf Base – HV
- HH Usr Inst BaseApp – HV

Natürlich können Sie die Informationen auch in beliebiger Reihenfolge angeben. Das Wichtigste ist, dass Sie überhaupt eine Namenskonvention haben, die eindeutig ist und die auch von allen verfolgt wird.

Weitere Diskussionen zur GPO-Benennung finden Sie unter *http://www.grouppolicy.biz/2010/07/best-practice-group-policy-design-guidelines-part-2/* oder kurz *https://bit.ly/2PcJWd7* und unter *http://www.gpanswers.com/a-clean-naming-convention-for-gpos/* oder kurz *https://bit.ly/2MRm90N*.

5.5 Dokumentieren von GPOs

Es ist grundsätzlich immer eine gute Idee, alles zu dokumentieren, was Sie tun. Dummerweise haben Dokumentationen den Nachteil, dass sie Zeit kosten. Außerdem will eine Dokumentation gepflegt werden und man benötigt einen zentralen Ablageort.

Ich persönlich habe OneNote für mich als Dokumentationstool entdeckt. Das Tolle an OneNote ist, dass man Notizbücher auch freigeben und mit anderen Nutzern teilen kann. Dazu ist OneNote kostenlos und kann Notizbücher auch in SharePoint ablegen. Es gibt aber jede Menge Dokumentationstools da draußen, die bestimmt genauso gut sind. Und doch setzt sie

kaum jemand ein, weil es zusätzlichen Aufwand bedeutet, ein weiteres Tool zu öffnen, nachdem man Änderungen an einem System durchgeführt hat.

Die gute Nachricht ist, dass Sie seit Windows Server 2008 in der Lage sind, GPOs direkt in der GPMC zu dokumentieren. Zwar nicht alles, aber doch einiges.

Öffnen Sie hierfür in der Computerkonfiguration eines GPO den Knoten `Richtlinien > Administrative Vorlagen > Windows Komponenten > Remotedesktopdienste > Remotedesktopsitzungs-Host > Verbindungen` und dann die Richtlinie **Gleichmässige CPU-Zeitplanung deaktivieren**.

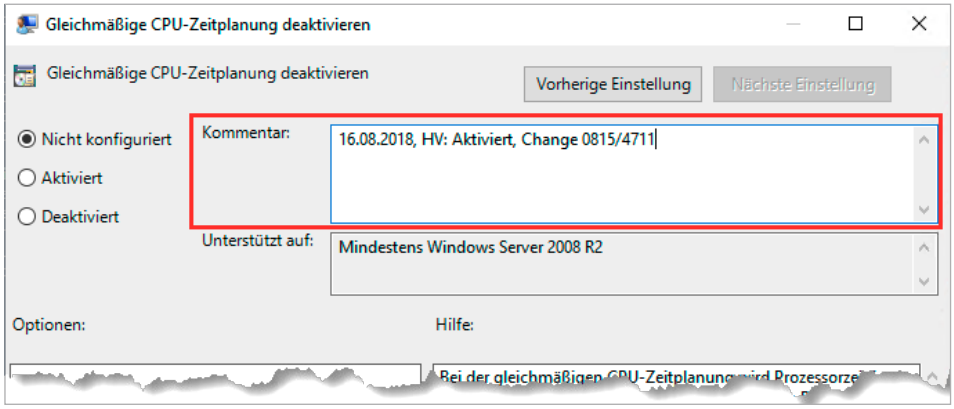


Bild 5.7 Administrative Vorlagen unterstützten Kommentare.

Sie finden in jeder Einstellung der administrativen Vorlagen ein Kommentarfeld, dessen Text im GPO gespeichert wird. Tragen Sie hier bei jeder Änderung eine kurze Notiz mit Datum, Name des Bearbeiters und einer kurzen Änderungsbeschreibung ein. Wenn Sie mehrere Einstellungen in einem Rutsch vornehmen, können Sie eine Versionsnummer führen, damit man nachvollziehen kann, welche Einstellungen gemeinsam vorgenommen wurden.

Auch in Gruppenrichtlinien-Einstellungen finden Sie auf der Registerkarte **Gemeinsame Optionen** ein Kommentarfeld.

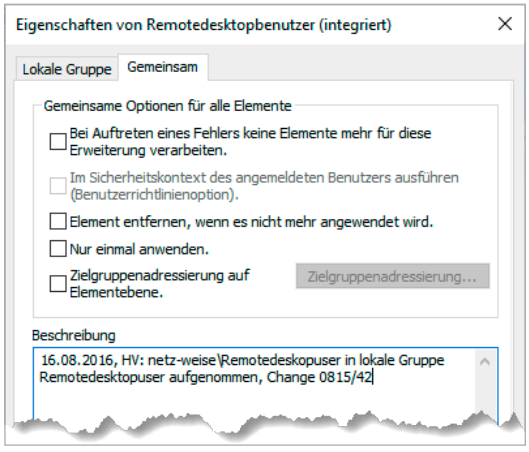


Bild 5.8
In den Einstellungen findet sich der Kommentar im zweiten Register.

Nun können Sie das GPO selbst kommentieren. Öffnen Sie hierfür im Editor das Kontextmenü des GPO, das Sie über den Namen des GPO erreichen (siehe Bild 5.9).

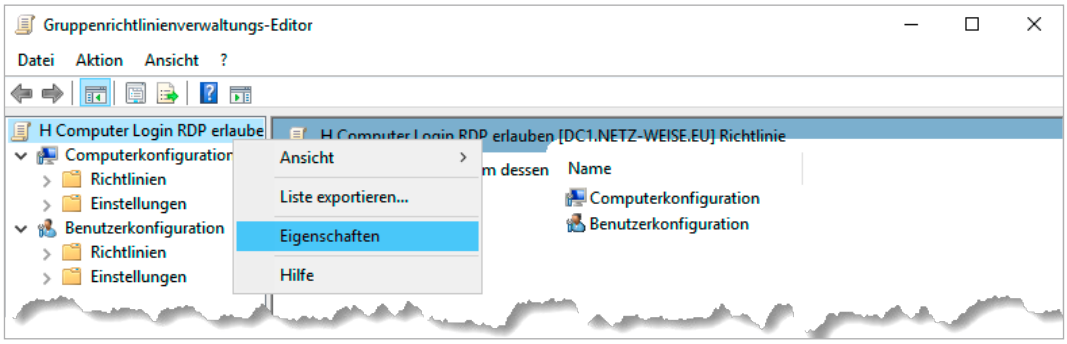


Bild 5.9 Öffnen Sie das GPO und dann die Eigenschaften.

Wählen Sie **Eigenschaften** aus, öffnet sich das Eigenschaften-Fenster, das bis auf das Register **Kommentar** nur Einstellungen erlaubt, die Sie über die GPMC schneller erledigen können. Den Kommentar allerdings können Sie nur hier bearbeiten. Öffnen Sie einfach nach jeder Änderung in dem GPO das Kommentarfeld, und kopieren Sie die individuellen Einträge der Änderungen hinein.

Bild 5.10 Kommentieren Sie Ihre GPOs!

Der Kommentarverlauf wird in einer eigenen XML-Datei in dem GPO gespeichert. Sie können sich die Kommentare in der GPMC anzeigen lassen, indem Sie das Register **Details** des GPO öffnen.

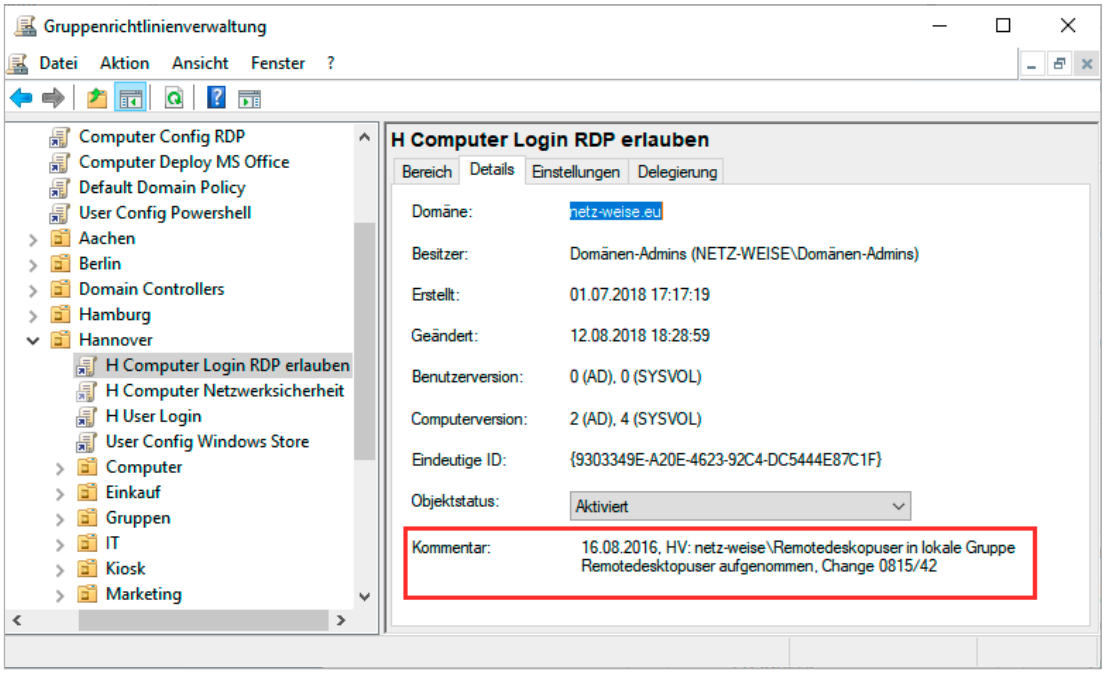


Bild 5.11 Der Kommentar wird in der GPMC unter „Details“ angezeigt.

Sie können den Kommentar auch über PowerShell abrufen, indem Sie das Cmdlet `Get-GPO` aufrufen. Er wird unter „Description“ angezeigt.

Listing 5.1 Auch PowerShell zeigt den Kommentar an.

```
> get-gpo -name "Config Rdp Server"
DisplayName      : Config RDP Server
DomainName       : bit-weise.de
Owner            : BIT-WEISE\Domänen-Admins
Id               : 20ba5b86-0e62-4756-8e72-c69c7c6fb4ff
GpoStatus        : AllSettingsEnabled
Description      : V1-16.09.16-HV: RDP-Port angepasst, gleichmässige CPU-Zeitplanung
aktiviert
CreationTime     : 14.08.2016 16:18:02
ModificationTime : 16.09.2016 01:34:12
UserVersion      : AD Version: 4, SysVol Version: 4
ComputerVersion  : AD Version: 5, SysVol Version: 5
WmiFilter        : Speicher größer 2GB
```

Die Kommentare, die Sie in den Einstellungen direkt hinterlegt haben, finden Sie im Gruppenrichtlinien-Report, wenn Sie die Einstellungen des GPO aufrufen.

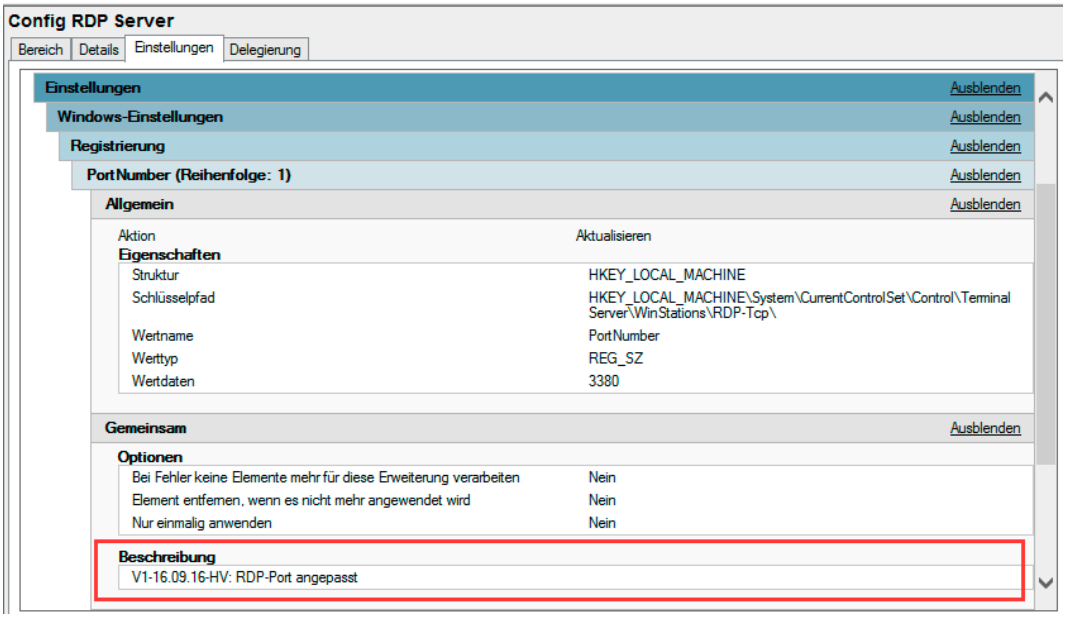


Bild 5.12 Im Report werden die Beschreibungen auch angezeigt.

5.6 Testen von GPOs

Es kann nicht oft genug gesagt werden, und ich werde es im Laufe des Buches noch öfter tun: Testen Sie alle GPOs, bevor Sie sie auf Ihre Produktivumgebung loslassen. GPOs sind gefährlich! GPOs sind wie Atomkraft (aber ohne den Müll) – unglaublich nützlich, aber wenn Sie nicht aufpassen, haben Sie einen GAU. Ich habe es in meinem Leben bisher zwei Mal geschafft, mithilfe von GPOs eine Domäne komplett funktionsunfähig zu machen – in kontrollierten (Schulungs-)Umgebungen. Zum Glück gibt es in der virtuellen Welt die Möglichkeit, im abgesicherten Modus zu arbeiten, ein Konzept, das der Schöpfer unseres Universums leider nicht vorgesehen hat.

Grundsätzlich gibt es drei Ansätze, um Ihre GPOs zu testen – einen Test Forest (vorzugsweise virtuell), eine Testdomäne in Ihrem Produktiv Forest oder, wenn Ihnen die Mittel dazu fehlen, eine Test-OU. Ich stelle Ihnen hier kurz Test-Forest- und Test-OU-Ansätze vor. Die Testdomäne entspricht weitestgehend dem Test Forest.

Wenn Sie mit einem Test Forest arbeiten, sollten Sie Ihre Live-Umgebung so gut wie möglich in einer virtuellen Umgebung abbilden. Duplizieren Sie also die wesentlichen Teile Ihrer OU-Struktur sowie alle GPOs in die Testumgebung, und legen Sie sich außerdem eine Reihe von Testbenutzern und Computern mit unterschiedlichen Berechtigungen an. Speziell wenn Sie mit Sicherheitsfilterung arbeiten, ist das besonders wichtig, denn Sie müssen ja nach Möglichkeit alle Auswirkungen simulieren können.

Am besten versuchen Sie, Ihre Testumgebung komplett zu isolieren. Dann können Sie einfach einen virtuellen Domänencontroller Ihrer Live-Umgebung sichern und in Ihrer Testumgebung wieder einspielen. Achten Sie dann aber darauf, dass Ihre Testumgebung keine Verbindung zur Live-Umgebung herstellen kann, ansonsten bekommen Sie eventuell echte Probleme! Wenn Sie über keine virtuellen Domänencontroller verfügen, können Sie auch einen neuen Domänencontroller in Ihrer Domäne aufsetzen, eine vollständige Replikation erzwingen und den Domänencontroller dann von Ihrer Domäne trennen. Achten Sie darauf, den Domänencontroller hinterher wieder aus Ihrer Produktivdomäne zu entfernen. Das funktioniert mithilfe des Kommandozeilentools `ntdsutil.exe` am besten. Eine Beschreibung zum Vorgang finden Sie bei Microsoft unter *https://technet.microsoft.com/de-de/library/cc816907(v=ws.10).aspx*. Der Transfer von GPOs kann über Sichern und Wiederherstellen der GPOs durchgeführt werden. Microsoft stellt für den Transfer von GPOs zwischen Domänen auch gleich noch Migrationstabellen bereit, die z. B. Gruppennamen zwischen Domänen automatisch anpassen können. Mehr hierzu finden Sie in Kapitel 14.3, „Einstellungen importieren und migrieren“.

Wenn Ihnen die Mittel fehlen, einen Test Forest zu erstellen, tut es meist auch eine Test-OU. Eine Test-OU hat den Vorteil, dass man sie einfach erstellen und mit ein wenig Aufwand auch alles bombensicher testen kann. Der Nachteil an einer Test-OU ist allerdings, dass Sie in der Produktion rumpfuschen. Die richtigen Vorsichtsmaßnahmen vorausgesetzt ist das zwar ungefährlich, aber es wirkt trotzdem ein bisschen wie das Experimentieren mit gefährlichen Erregerstämmen – wenn die Vorsichtsmaßnahmen versagen und doch mal etwas in die Umwelt gelangt, haben Sie ein Problem. Machen Sie sich daher am besten einen Ablaufplan, den Sie beim Testen von GPOs einhalten.

Eine Test-OU funktioniert eigentlich ganz prima. Was Sie zum Testen benötigen, sind eigentlich nur:

- eine Test-OU unterhalb der Domäne
- einen oder mehrere virtuelle Test-PCs (je nach Konfiguration und Anzahl der Betriebssysteme, die bei Ihnen im Einsatz sind)
- einen oder mehrere Testbenutzer (echte oder Dummys, echte sind natürlich besser)

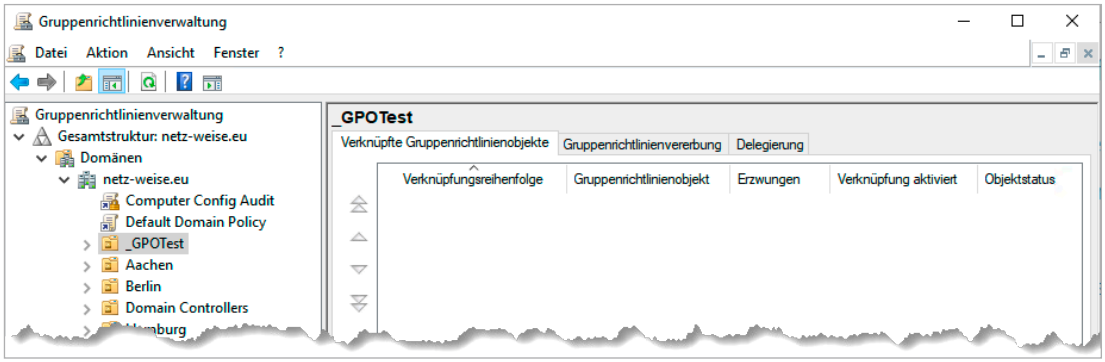


Bild 5.13 Die Test-OU ist direkt unter der Domäne aufgehängt.

In Bild 5.13 heißt die Test-OU **_GPOTest**. Der Unterstrich dient dazu, die Test-OU gleich oben in der GPMC anzuzeigen.

Verschieben Sie jetzt Ihre Testcomputer- und Testbenutzerkonten in die Test-OU. Wenn Sie mehrstufige GPOs testen wollen (also mehrere GPOs, die sich über mehrere OUs vererben), bilden Sie zuerst die OU-Struktur ab. Nun verknüpfen Sie alle bestehenden GPOs in der Reihenfolge der tatsächlichen Anwendung mit Ihrer Test-OU. Die Reihenfolge können Sie sehen, wenn Sie sich die OU nehmen, auf der das GPO hinterher verknüpft werden soll, und dort das Register **Vererbung** aufrufen (siehe Bild 5.14).

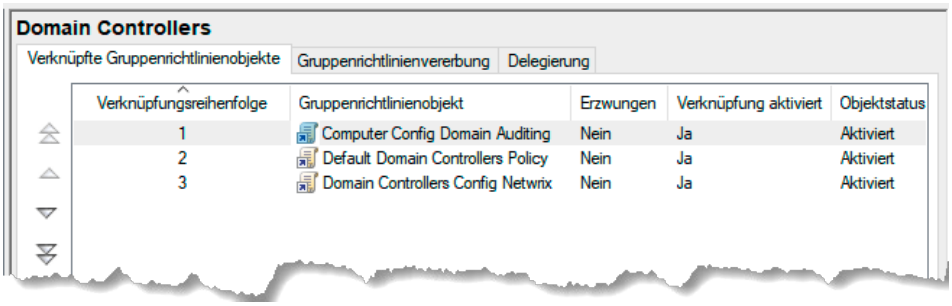


Bild 5.14 In dieser Reihenfolge müssen die GPOs auf der Test-OU verknüpft werden.

Alternativ können Sie auch das PowerShell-Cmdlet `Get-GPInheritance` verwenden, um die Vererbung abzurufen. Auf seiner Basis finden Sie im GroupPolicyHelper-Modul zum Buch das Cmdlet `New-GphTestOU`. Das Cmdlet hat zwei wichtige Parameter, `-OUName` und `-CopyInheritanceFrom`. Damit ist es möglich, eine neue TestOU anzulegen und alle Gruppenrichtlinienverknüpfungen zu kopieren. Geben Sie keinen OU-Namen an, legt das Cmdlet automatisch eine neue OU „_GPOTest“ im Domänenstamm an.

Listing 5.2 Anlegen einer Test-OU mit allen Group Policy-Verknüpfungen

```
New-GphTestOU -CopyInheritanceFrom "OU=Computer,OU=Hannover"
```

Wenn Sie ein neues GPO testen wollen, erstellen Sie dieses ganz einfach auf der Test-OU, aber vergessen Sie nicht, den Status im Namen festzuhalten. Solange das GPO nicht produktionsreif ist, sollte man das am Namen ersehen, am besten mit einem Datum, damit man alte Test-GPOs wiederfindet, und einem Verursacher (Namenskürzel). Nutzen Sie auch hier die Kommentarfunktion des GPO!

Auch zum Anlegen eines Test-GPO stellt Ihnen das GroupPolicyHelper-Modul ein Cmdlet zur Verfügung, `New-GphTestGPO`. `New-GphTestGPO` legt Ihnen automatisch ein neues Test-GPO an und verlinkt es mit Ihrer OU. Mit dem Parameter `-NoLink` können Sie das Verknüpfen mit Ihrer Test-OU verhindern und nur ein GPO anlegen, mit `-OUPath` geben Sie den Pfad zur OU an, mit der die Verknüpfung erfolgen soll.

Listing 5.3 Eine neue Test-GPO anlegen

```
New-GphTestGPO -OUPath 'OU=Test,OU=Hannover"
```

Wenn Sie ein bestehendes GPO bearbeiten wollen, erstellen Sie eine Kopie. Das geht ganz einfach, ist aber ein wenig versteckt. Öffnen Sie hierfür den Container „Gruppenrichtlinienobjekte“ in Ihrer GPMC, öffnen Sie das Kontextmenü des GPO, das Sie bearbeiten möchten, und wählen Sie **Kopieren**. Nun öffnen Sie das Kontextmenü des Containers „Gruppenrichtlinienobjekte“ und wählen **Einfügen**.