holger **VOGES**
martin **DAUSCH**

GRUPPEN-RICHTLINIEN

IN WINDOWS SERVER 2016, 2012 UND 2008 R2

3. Auflage

Ein praktischer Leitfaden für die Windows-Verwaltung

HANSER

Mit großem Stichwortverzeichnis zum »Schnell-mal-Nachschlagen«

Voges/Dausch

Gruppenrichtlinien
in Windows Server 2016, 2012 und 2008 R2

Holger Voges
Martin Dausch

Gruppenrichtlinien in Windows Server 2016, 2012 und 2008 R2

Ein praktischer Leitfaden für die Windows-Verwaltung

3., erweiterte und aktualisierte Auflage

HANSER

Die Autoren:
Holger Voges, Hannover
Martin Dausch, Regensburg

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, Münster-Nienberge
Herstellung: Irene Weilhart
Umschlagdesign: Marc Müller-Bremer, München, www.rebranding.de
Umschlagrealisation: Stephan Rönigk
Gesamtherstellung: Kösel, Krugzell
Printed in Germany

Print-ISBN: 978-3-446-44564-2
E-Book-ISBN: 978-3-446-44914-5

Inhalt

Vorwort

Sie halten jetzt die dritte, stark überarbeitete und erweiterte Auflage dieses Buches in der Hand. Das Thema ist das gleiche geblieben, der Autor ist ein neuer.

Als der Hanser-Verlag mich angesprochen hat, ob ich Interesse hätte, die Neuauflage des Buches zu übernehmen, war ich hin- und hergerissen. Auf der einen Seite bin ich als Trainer und Berater für Windows-Systeme, SQL Server und PowerShell gut ausgelastet, auf der anderen Seite reizt mich das Thema doch sehr.

Ursprünglich hatte ich schon 2006 geplant, ein Buch über Windows-Gruppenrichtlinien zu schreiben, aber damals wollte sich kein Verlag (zumindest keiner, zu dem ich Kontakt hatte), an das Thema heranwagen. Ein Buch über Active Directory sollte es werden, mindestens 1000 Seiten. Heute bin ich sehr froh, dass ich mich auf das Abenteuer nicht eingelassen habe, denn jetzt weiß ich, wie viel Arbeit allein das Schreiben und Recherchieren für 200 Seiten neuen Inhalts macht.

Ich habe mich dann entschieden, den Mittelweg zu wählen und auf dem vorhandenen Inhalt aufzubauen, anstatt ein komplett neues Buch zu beginnen. Dabei habe ich mich natürlich an der Arbeit meines Vorautoren orientiert; hoffe aber, dass ich trotzdem in der Lage war, dem Buch meine eigene Prägung zu geben.

Sie finden in dem Buch vier vollständig neue Kapitel, sowie ein weiteres, das komplett überarbeitet wurde. Alle anderen Kapitel wurden aktualisiert und zum Teil stark ergänzt.

Ich möchte an dieser Stelle noch einmal ganz herzlich meiner Freundin danken, die es mit einer schier stoischen Ruhe ertragen hat, dass ich während unseres Urlaubs mit Laptop am Pool gesessen bin, um die letzten Kapitel des Buches fertig zu stellen, und trotzdem noch mit mir zusammen ist. Danke Isabelle, ohne dein Verständnis wäre dieses Buch vielleicht niemals fertig geworden. Außerdem vielen Dank an die Firma Specops, die mich tatkräftig dabei unterstützt hat, die letzten Fragen zu Specops Deploy zu klären, sowie meinen Mitarbeitern, allen voran meiner Schwester, die mir tagtäglich so viel Arbeitslast abnehmen. Und natürlich Ihnen, dass Sie dieses Buch gekauft haben.

Wenn Sie aus der Region Hannover kommen, möchte ich Sie ganz herzlich zur PowerShell Usergroup Hannover einladen. Die Usergroup trifft sich jeden dritten Freitag im Monat ab 18:30 Uhr in den Räumen meiner Firma Netz-Weise, um in gemütlicher Runde alle möglichen Bereiche von Windows PowerShell zu beleuchten. Mehr Informationen erhalten Sie unter *https://www.netz-weise.de/user-groups/powershell-user-group.html*.

Für Fragen, Korrekturen oder Anregungen senden Sie mir bitte eine E-Mail an *holger.voges@netz-weise.de*. Hier oder unter *https://www.netz-weise.de* können Sie mich auch erreichen, wenn Sie Interesse an Schulungen oder Beratung haben.

Und nun viel Spaß beim Lesen,

Holger Voges

Wissenwertes zu diesem Buch

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

Versionen

In dieser komplett überarbeiteten und erweiterten Neuauflage werden auch die relevanten Neuerungen der Gruppenrichtlinien unter Windows 10 und Windows Server 2016 beschrieben. Relevante Neuerungen sind durch das in der Randspalte dargestellte Symbol hervorgehoben.

Relevante Neuerungen unter Windows Server 2012 sind durch das nebenstehende Symbol hervorgehoben. Diese wirken sich insbesondere auf Clients unter Windows 8 aus, deren Konfiguration ohne entsprechende Gruppenrichtlinien nur eingeschränkt gelingt.

Inhalt

Dieses Buch ist in 18 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 Gruppenrichtlinienverwaltungskonsole (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 zu konfigurieren. Es werden Einstellungen für Window 7, Windows 8(.1) und Windows 10 behandelt.

In *Kapitel 9* werden Funktionen wie Ordnerumleitung gezeigt, die im Knoten „Windows-Einstellungen“ im Benutzer-Teil der Gruppenrichtlinien zu finden sind.

Administrative Vorlagen gibt es nicht nur für Computer, sondern auch für Benutzer. *Kapitel 10* zeigt, wieder am Beispiel einiger Einstellungen, welche Möglichkeiten Sie zur Konfiguration der Benutzerumgebung haben.

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 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 13, Verwalten von GPOs, geht auf die Verwaltungsaufgaben wie das Sichern und die Wiederherstellung von GPOs ein.

In *Kapitel 14* erfahren Sie, wie Gruppenrichtlinien-Vorlagen funktionieren, und wie Sie sie nutzen können, um GPOs für Ihre eigenen Zwecke zu erweitern.

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 fasst alle Themenbereiche rund um das Skripting zusammen. Sie erfahren, wie Sie mit Gruppenrichtlinien Start- und Anmeldeskripte ausführen können, wie Sie mit Hilfe von PowerShell viele Verwaltungsaufgaben automatisieren und auf welche Weise Sie mit Applocker die Ausführung von PowerShell einschränken oder verhindern können.

Zum Schluss soll Ihnen *Kapitel 18* einen Ausblick darauf geben, wie Sie die Konfiguration von Computern mit Hilfe von Desired State Configuration (DSC) erweitern oder Gruppenrichtlinien sogar ersetzen 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 unter *https://www.netz-weise-it.training/images/dokus/Scripte/GroupPolicyHelper.zip*. Das Modul wird ständig erweitert.

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). Mehr Informationen zu PowerShell-Modulen finden Sie in Kapitel 17.4 im Kasten „PowerShell-Module“.

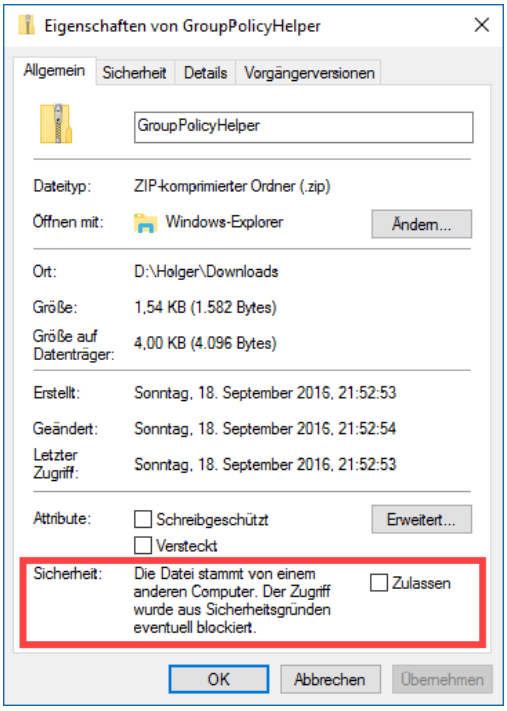

Bild 1
Aus dem Internet heruntergeladene Dateien müssen zugelassen werden

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*.

Aktualisierungen

Administrative Vorlagen sind im Buch in drei 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. Das Dokument „Administrative Vorlagen in Windows 10“ in der Kategorie „Gruppenrichtlinien“ wird regelmäßig aktualisiert und enthält eine Beschreibung der wichtigsten administrativen Vorlagen unter Windows 10.

Nutzen Sie auch meinen Blog als Informationsquelle. Unter *https://www.Netz-Weise.de/weisheiten/tipps.html* schreibe ich regelmäßig über verschiedene IT-Themen, die mich beschäf-

tigen. 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 Begriff und Abkürzungen. Ich fürchte, dass auch in diesem Buch durch die Arbeit von 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 eine neue GPO erstellt, wird auch als Group Policy Container bezeichnet.
Gruppenrichtlinien-Einstellungen	Microsoft hat mit Windows Vista neue Einstellungsmöglichkeiten eingeführt, die im Englischen als „Group Policy Preferences“ bezeichnet werden. Im Deutschen wurde das zu „Gruppenrichtlinien-Einstellungen“ 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 einer 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 jeweils ca. vier Monaten Upgrades erhält, die neue Funktionen nachrüsten. Unternehmen können das verhindern, indem sie die LTSB-Version von Windows 10 nutzen – der sogenannte Long Term Service Branch. Die LTSB-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 einsetzen 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://technet.microsoft.com/en-us/itpro/windows/manage/group-policies-for-enterprise-and-education-editions?f=255&MSPPError=-2147217396*.

Um immer auf dem Laufenden zu bleiben, nutzen Sie auch meinen Blog.

1 Einleitung

Dieses Kapitel beantwortet folgende Fragen:

- 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 12, 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 Anmeldeskript-Aufgaben 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 Domänen-Objekts. 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.

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

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. So ließe sich etwa in der GPO „B-Standardbenutzer“ der Bereich Computerkonfiguration deaktivieren.

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

1.5 Wofür werden Gruppenrichtlinien am häufigsten verwendet?

Gruppenrichtlinien sind ein mächtiges Werkzeug, mit dem eine Fülle von Einstellungen und Anpassungen möglich sind. 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.

1.6 Muss man beim Ändern von Gruppenrichtlinien aufpassen?

Gruppenrichtlinien wirken, sobald eine Einstellung übernommen wurde. Wenn Sie nun 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.

1.7 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.

2 Die Gruppenrichtlinienverwaltung

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.

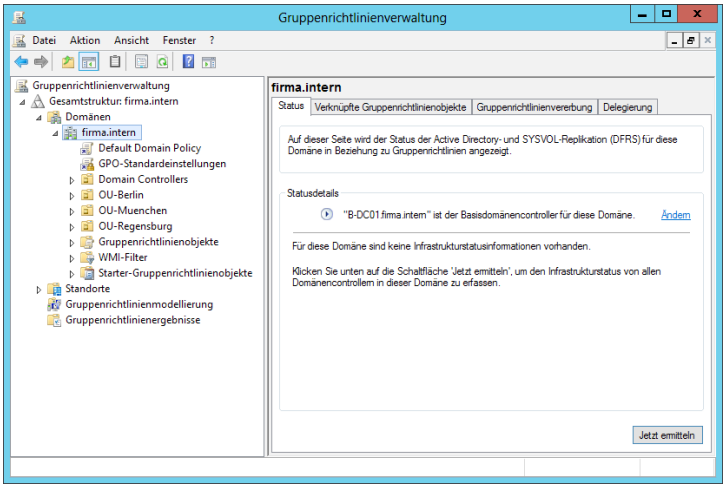

Bild 2.1
Die Gruppenrichtlinienverwaltungskonsole

Diese wird automatisch installiert, wenn Sie einen Server zum Domänencontroller machen. Wenn Sie die Gruppenrichtlinienverwaltung von einem anderen Rechner aus verwenden wollen, müssen Sie sie erst installieren.

2.2 Gruppenrichtlinienverwaltung installieren

Die Gruppenrichtlinienverwaltungskonsole ist bei Windows Server Teil des Betriebssystems und steht als Feature zur Verfügung. Sie müssen die Konsole nur über den Server-Manager nachinstallieren.

Unter Windows Server 2012 (R2) und Windows Server 2016

Öffnen Sie den Server-Manager und klicken Sie unter VERWALTUNG auf ROLLEN UND FEATURES HINZUFÜGEN.

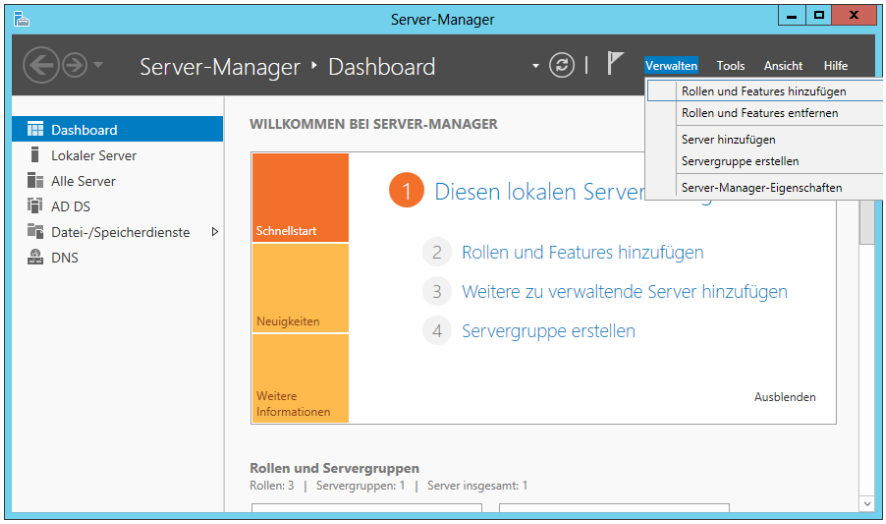

Bild 2.2 Features hinzufügen

Klicken Sie sich anschließend im Assistenten zum Hinzufügen von Rollen und Features bis zum Punkt „Features auswählen“, scrollen Sie unter FEATURES zum Punkt GRUPPEN RICHTLINIENVERWALTUNG und aktivieren Sie das entsprechende Kontrollkästchen.

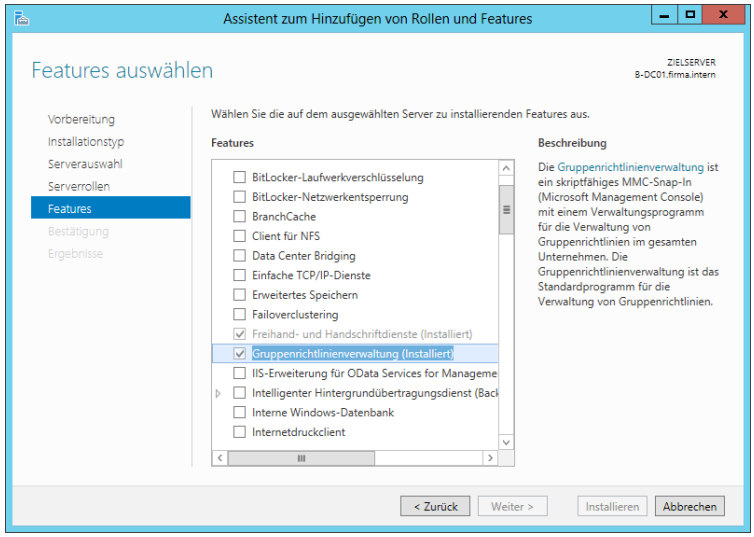

Bild 2.3 Feature Gruppenrichtlinienverwaltung auswählen

Klicken Sie nun auf 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.

2.3 Gruppenrichtlinienverwaltung erkunden

Klicken Sie auf dem Startbildschirm auf GRUPPENRICHTLINIENVERWALTUNG.

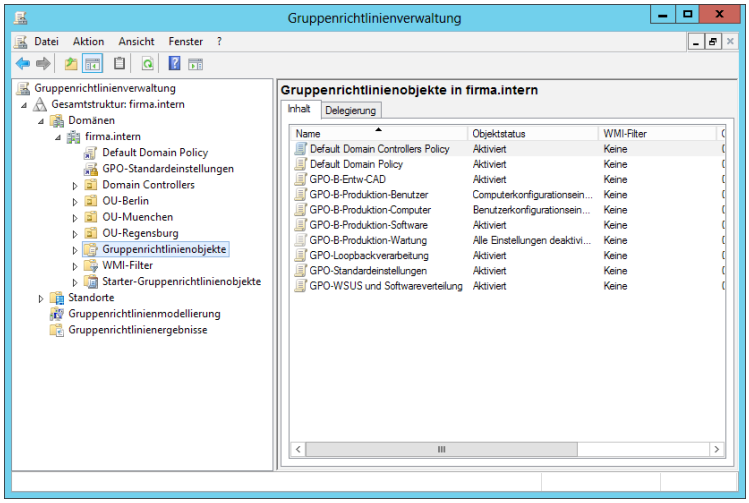

Bild 2.4 Gruppenrichtlinienverwaltung erkunden

Im linken Bereich der Gruppenrichtlinienverwaltung finden Sie die Baumansicht der Gesamtstruktur (Konsolenstruktur). Navigieren Sie in dieser zum Knoten „Gruppenrichtlinienobjekte“ unterhalb der Domäne. Hier ist der Speicherort der eigentlichen 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 der Gruppenrichtlinie „Default Domain Policy“ im rechten Fenster sehen Sie auf dem Symbol der „Default Domain Policy“ unterhalb des Domänennamens, dass dieses mit einem Pfeil versehen ist – es handelt sich um eine Verknüpfung.

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

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

2.5 Gruppenrichtlinienobjekte im Detail

Erweitern Sie nun den Knoten Gruppenrichtlinienobjekte und markieren Sie in der Konsolenstruktur die Default Domain Policy.

2.5.1 Register Bereich einer Gruppenrichtlinie

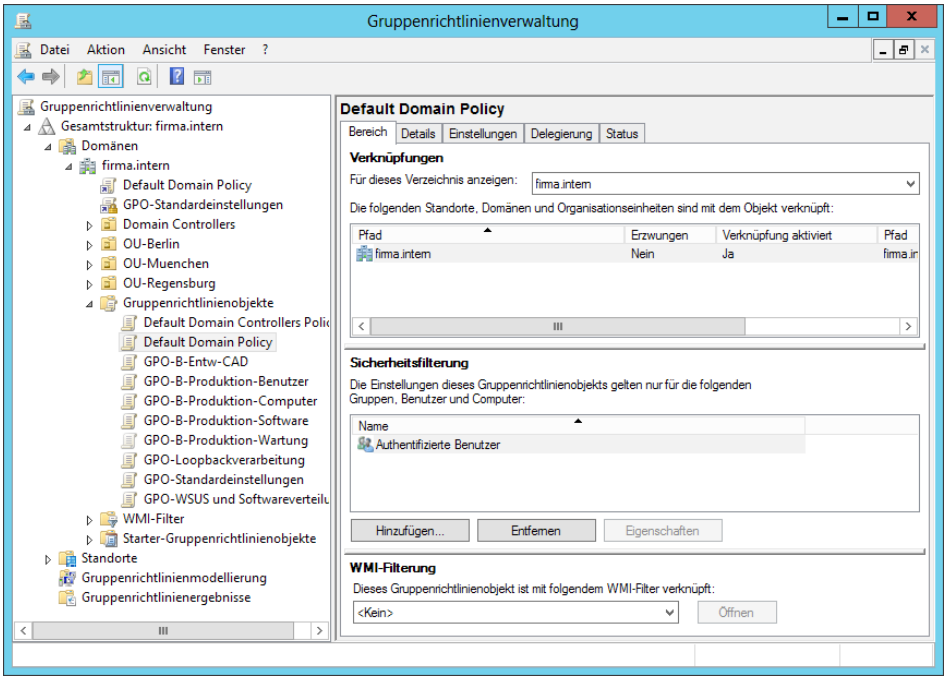

Bild 2.5 Register Bereich der Default Domain Policy

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

Daneben ist vermerkt, ob die Richtlinie erzwungen wird. Erzwingen bedeutet, die Einstellungen, die durch die Richtlinie vorgenommen werden, mit einem Schreibschutz zu versehen. Näheres dazu erfahren Sie in Abschnitt 4.5.1, „Erzwungen“, und in Kapitel 12, Funktionsweise von Gruppenrichtlinien.

Sie können hier auch sehen, ob die Verknüpfung aktiviert ist. Eine deaktivierte Verknüpfung würde bedeuten, dass die GPO-Verknüpfung nicht angewendet wird.

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 könnten hier auch andere Gruppen hinzufügen oder entfernen. In Abschnitt 4.5.5, „Gruppenrichtlinien filtern“, erhalten Sie mehr Details zur Wirkungsweise von Sicherheitsfilterung.

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

2.5.2 Register Details eines GPO

Klicken Sie nun auf das Register Details.

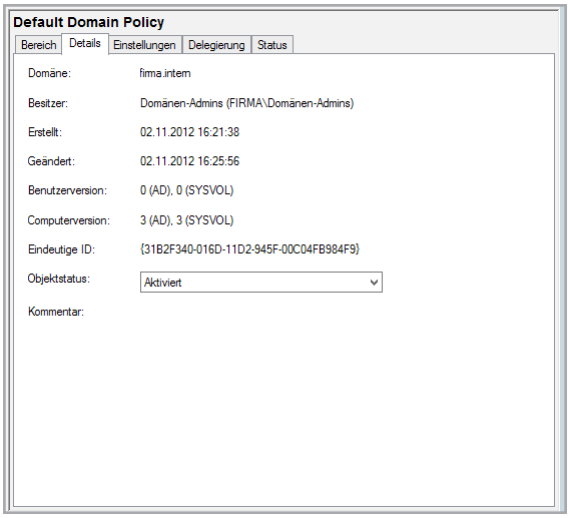

Bild 2.6
Register Details der Default Domain Policy

Im Register Details ist aufgeführt, wer der Besitzer der GPO ist, wann diese erstellt und geändert wurde, welche Benutzer- und Computerversion vorliegt und wie die eindeutige ID der Richtlinie lautet. Daneben können Sie hier die Richtlinie (nicht die Verknüpfung) ganz oder teilweise deaktivieren.

2.5.3 Register Einstellungen eines GPO

In der Registerkarte Einstellungen finden Sie einen Report über alle aktiven Einstellungen einer GPO. Diese Report ist vor allem dann wichtig, wenn Sie die Einstellungen, die in einer GPO gemacht wurden, überprüfen wollen. Im Group Policy Editor 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 unter Sicherheitseinstellungen und anschließend unter Kontorichtlinien/Kennwortrichtlinien auf Show. Sie können hier die einzelnen Einstellungen sehen, die in der Default Domain Policy im Knoten Kennwortrichtlinien vorgenommen wurden. Was diese Einstellungen bedeuten, erfahren Sie in Kapitel 7, „Windows-Einstellungen Computerverwaltung“.

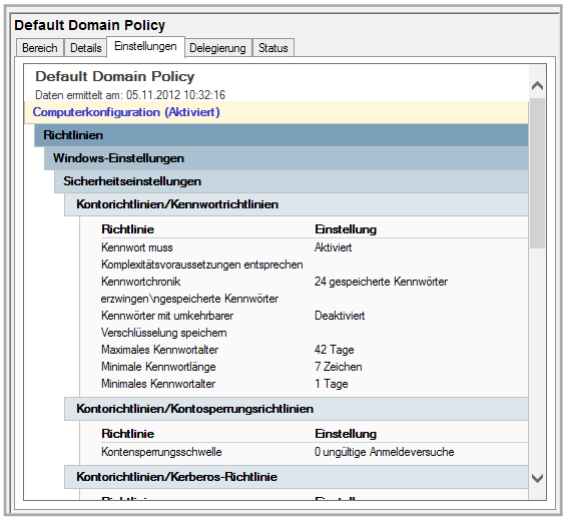

Bild 2.7
Register Einstellungen der Default Domain Policy

2.5.4 Register Delegierung einer GPO

Klicken Sie nun auf das Register Delegierung.

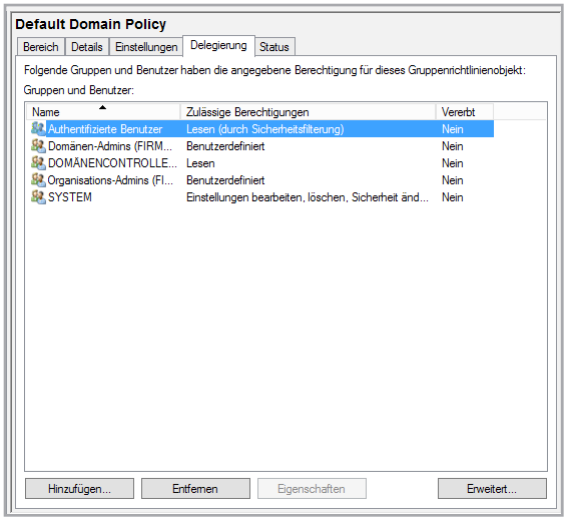

Bild 2.8
Register Delegierung der Default Domain Policy

Im Register Delegierung sind die einzelnen Gruppen und deren Berechtigungen auf das Gruppenrichtlinienobjekt differenziert aufgeführt. Hier können Sie auch die Sicherheitsfilterung der Richtlinie beeinflussen, wenn Sie negative Filterung verwenden wollen (vgl. Abschnitt 3.5, „Anpassungen der Verarbeitungsreihenfolge von Gruppenrichtlinien“). Außerdem können Sie hier festlegen, wer Zugriff auf die Richtlinieneinstellungen hat.

2.5.5 Register Status einer Gruppenrichtlinie

Klicken Sie nun auf das Register Status.

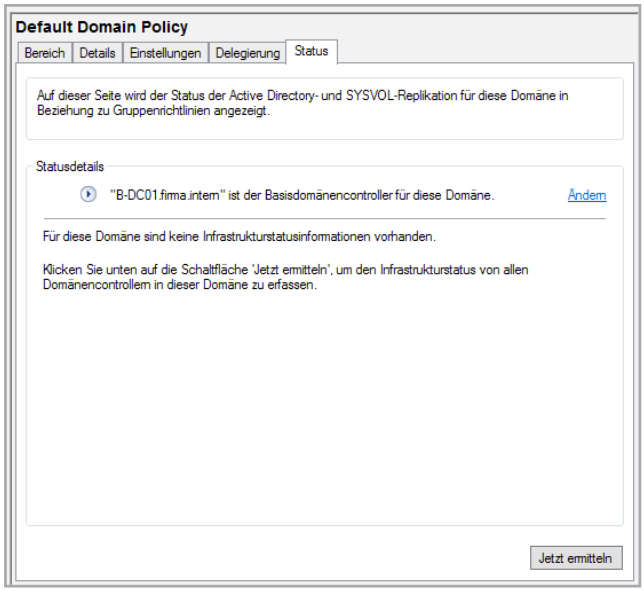

Bild 2.9 Register Status der Default Domain Policy

Im Register Status wird der aktuelle Replikationsstatus eines Gruppenrichtlinienobjekts dargestellt. Dazu wird durch Betätigen der Schaltfläche Jetzt ermitteln eine Abfrage an alle Domänencontroller gesendet und das Ergebnis anschließend wie folgt dargestellt.

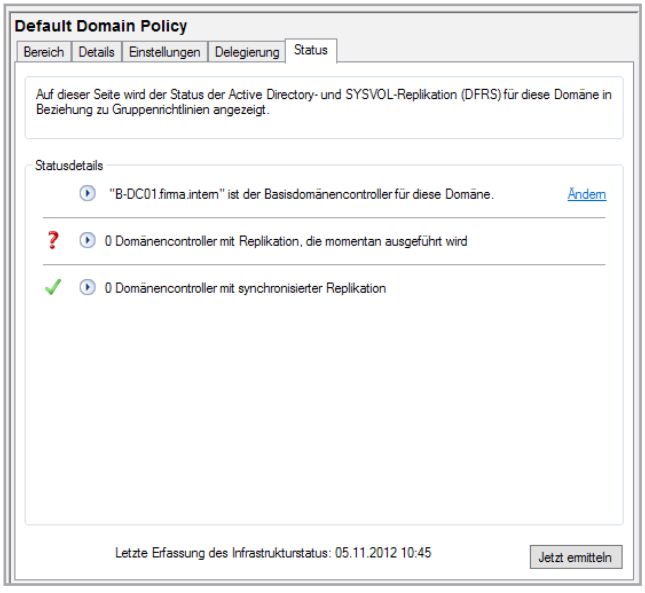

Bild 2.10 Register Status der Default Domain Policy (Ergebnis)

Unter „Statusdetails“ wird der Basisdomänencontroller der Domäne (Ursprung der Replikation) aufgeführt, mit Fragezeichen sind alle DCs aufgelistet, die gerade in einem Replikationsvorgang beteiligt sind, und mit einem grünen Häkchen werden die DCs mit erfolgreicher Replikation dargestellt.

2.6 Standorte und Gruppenrichtlinien

Gruppenrichtlinien können auch mit Standorten verknüpft werden. Dies setzt allerdings voraus, dass Sie Organisations-Admin sind. Domänenadministratoren haben nicht die Berechtigung, GPOs mit Standorten zu verknüpfen.

Um die Standorte anzuzeigen, wählen Sie im Kontextmenü von Standorte den Befehl STANDORTE ANZEIGEN... und anschließend die Standorte aus. Sie können auch mit den Schaltflächen ALLE AUSWÄHLEN oder AUSWAHL AUFHEBEN arbeiten. Bestätigen Sie Ihre Auswahl mit OK und erweitern Sie den Knoten Standorte.

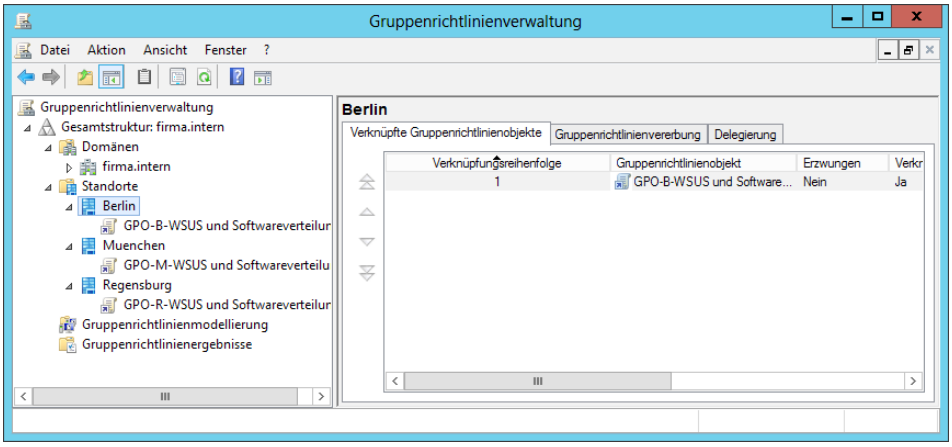

Bild 2.11 Standorte anzeigen

In diesem Beispiel wurden die drei Standorte Berlin, München und Regensburg ausgewählt und mit diesen exemplarisch eine jeweils standortspezifische Richtlinie für WSUS (Windows Server Update Services) und Softwareverteilung verknüpft. Dies entspricht der praktischen Verwendung lokaler Pfade für Updates, um die WAN-Verbindungen zu entlasten.

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 Tabelle 2.1 entnehmen können.

Tabelle 2.1 Übersicht über zusätzliche Elemente der Gruppenrichtlinienverwaltung

Element	Aufgabe
WMI-Filter	Dient der Verwaltung aller verfügbaren WMI-Filter. Diese werden hier gespeichert und können dann im Register Bereich mit einer GPO verknüpft werden.
Starter-Gruppenrichtlinienobjekte	Hierbei handelt es sich um Vorlagensammlungen, die verwendet werden können, um eine neue Gruppenrichtlinie mit Einstellungen für typische Situationen vorzukonfigurieren. Diese Vorlagen werden unter Starter-Gruppenrichtlinienobjekte gespeichert und verwaltet.
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 eine neue Gruppenrichtlinie im Knoten Gruppenrichtlinienobjekte. Klicken Sie dazu auf den Knoten Gruppenrichtlinienobjekte und wählen Sie im Kontextmenü den Befehl Neu. Geben Sie einen Namen für die Gruppenrichtlinie ein und entscheiden Sie, ob Sie aus einem Quell-Starter-Gruppenrichtlinienobjekt Einstellungen importieren möchten (lassen Sie im Moment die Auswahl auf (kein)).

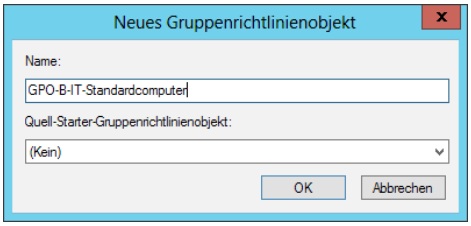

Bild 2.12
Neues Gruppenrichtlinienobjekt erstellen

Bestätigen Sie Ihre Konfiguration mit OK.

2.9 Gruppenrichtlinie verknüpfen

Wählen Sie nun eine Organisationseinheit aus, mit der Sie die neue Gruppenrichtlinie verknüpfen wollen. Wenn Sie noch keine Test-OU erstellt haben, können Sie auch auf die Domäne klicken und dort im Kontextmenü NEUE ORGANISATIONSEINHEIT aufrufen, einen Namen eingeben und diesen mit OK bestätigen.

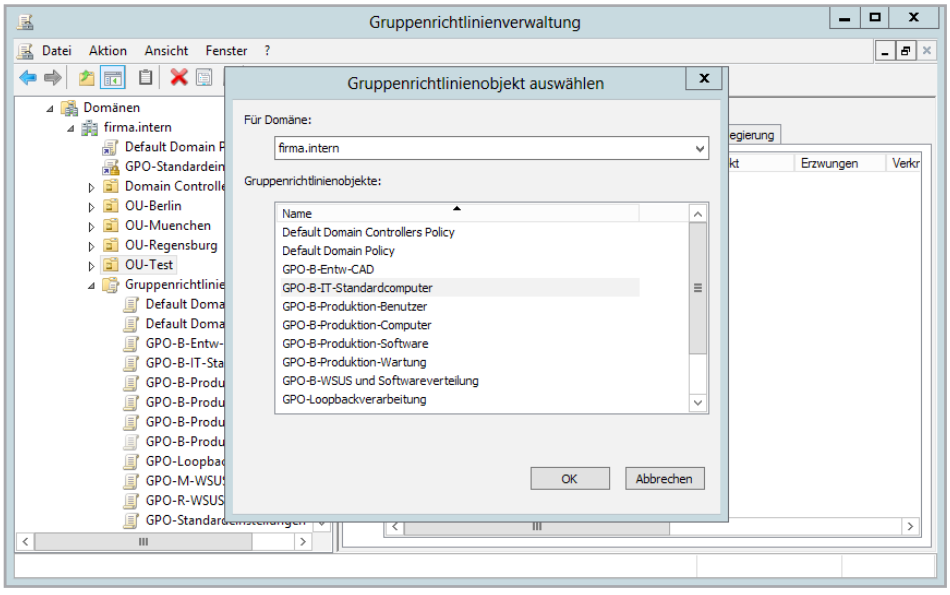

Bild 2.13 Vorhandenes GPO verknüpfen

Markieren Sie die Organisationseinheit und klicken Sie im Kontextmenü auf VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN. Wählen Sie nun im Assistenten „Gruppenrichtlinienobjekt auswählen“ die GPO aus, die Sie hier verknüpfen möchten, und bestätigen Sie Ihre Auswahl mit OK.

Sie können alternativ auch eine 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 der Praxis ist es nicht empfehlenswert, Gruppenrichtlinienobjekte direkt in der Produktivumgebung 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 die GPO auch Ihren Anforderungen entspricht, sollte es mit einer produktiven OU verknüpft werden.

2.10 Gruppenrichtlinie bearbeiten

Betätigen Sie im Kontextmenü einer Gruppenrichtlinie den Befehl BEARBEITEN, um den Gruppenrichtlinienverwaltungs-Editor für diese zu öffnen und Einstellungen zu konfigurieren.

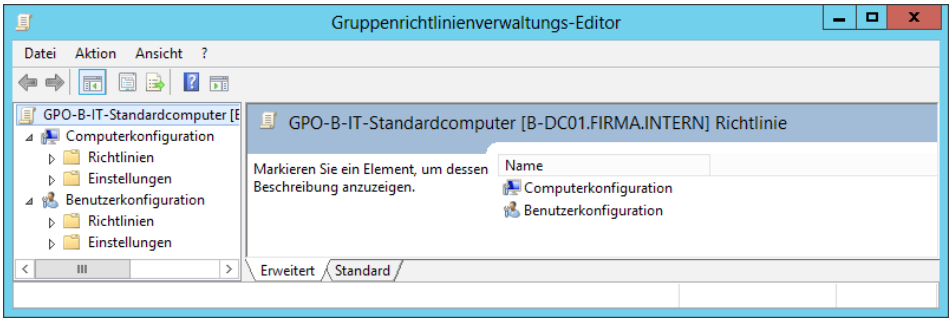

Bild 2.14 Gruppenrichtlinienverwaltungs-Editor

Der Gruppenrichtlinienverwaltungs-Editor ist im Konsolenbereich untergliedert in die Bereiche Computerkonfiguration und Benutzerkonfiguration. Diese sind wiederum in Richtlinien und Einstellungen untergliedert.

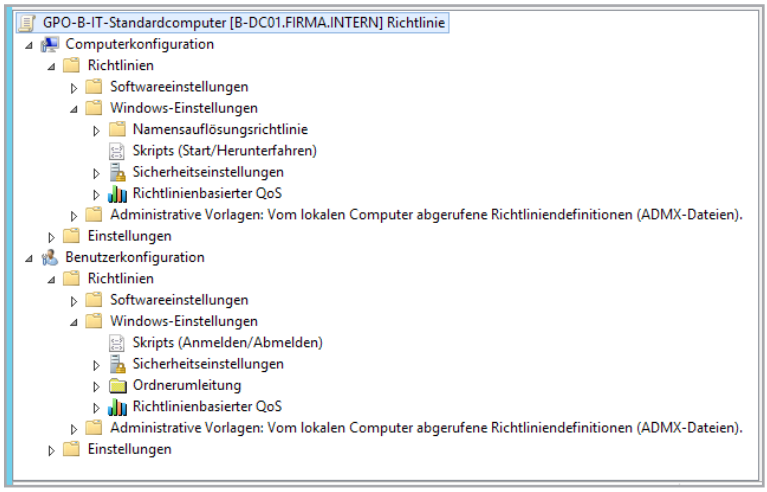

Bild 2.15 Übersicht über Richtlinien im Gruppenrichtlinienverwaltungs-Editor

Die Richtlinien sind jeweils unterteilt in die drei Bereiche: 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

Was passiert eigentlich genau, wenn eine Gruppenrichtlinie angewendet wird? Es werden Registrierungs-Schlüssel angewendet. Aber warum, in welcher Reihenfolge und welche Auswirkungen hat dies auf das System?

Ein tieferes Verständnis der Reihenfolge, in der Gruppenrichtlinien angewendet werden, ist ausschlaggebend für deren korrekten und effizienten Einsatz. Durch geschickten Umgang mit der Platzierung von Richtlinien lässt sich deren Anzahl minimieren und Änderungen können bei Bedarf schnell und effektiv eingepflegt werden. Darüber hinaus gibt es Methoden, mit denen Sie die Verarbeitungsreihenfolge beeinflussen können.

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 12, Funktionsweise von Gruppenrichtlinien.

3.2 Grundlagen der Gruppenrichtlinienverarbeitung

Gruppenrichtlinien werden von Windows seit Vista mithilfe eines eigenständigen Dienstes, des Gruppenrichtliniendiensts, verarbeitet. Der Gruppenrichtliniendienst 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.

Der Gruppenrichtlinienclient verarbeitet nur Einstellungen, 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

Eine 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 vorgenommen werden!

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

Wenn sich jetzt ein Benutzer am Computer anmeldet, dann startet der Gruppenrichtliniendienst das gleiche Prozedere. Er schaut nach, wo 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 auf den Benutzer an. Wenn sich der Benutzer und der PC nicht in der gleichen OU befinden, bedeutet dies aber, dass für den Benutzer und den Computer völlig unterschiedliche Gruppenrichtlinien gezogen wurden! Es gibt also faktisch eigentlich in jeder Gruppenrichtlinie immer zwei Gruppenrichtlinien – eine für Computer (Computerkonfiguration) und eine für Benutzer (Benutzerkonfiguration). Diese haben miteinander nichts zu tun!

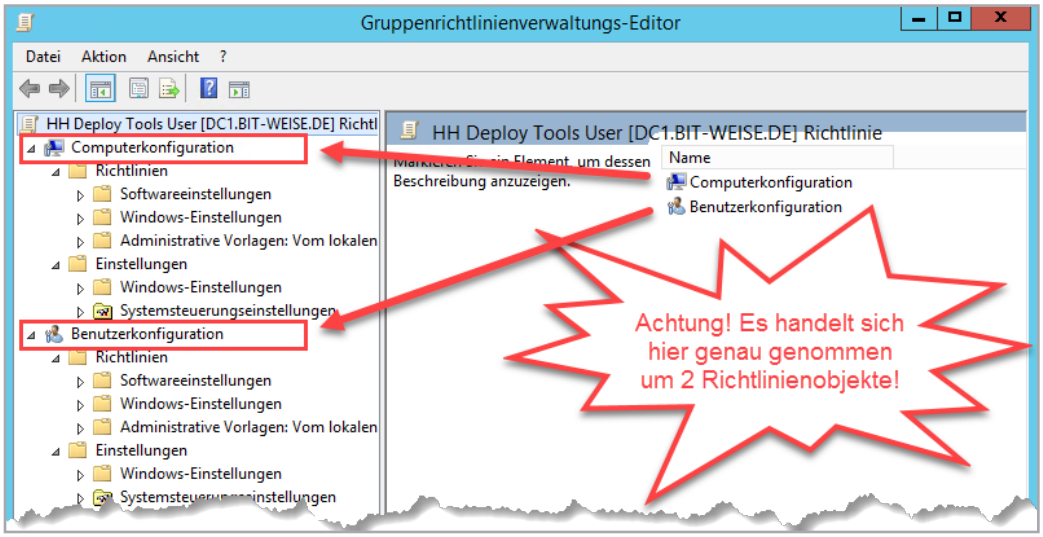

Bild 3.1 Computer- und Benutzerkonfiguration werden getrennt verarbeitet.

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.

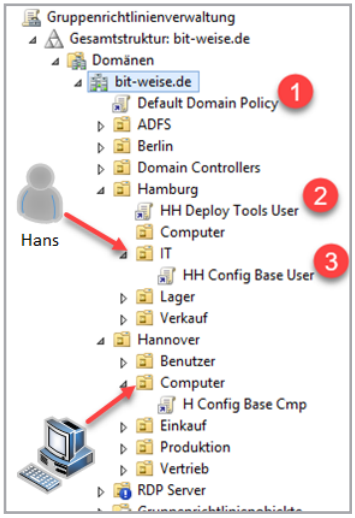

Bild 3.2
Der Benutzer kommt aus Hamburg, der Computer aus Hannover.

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?

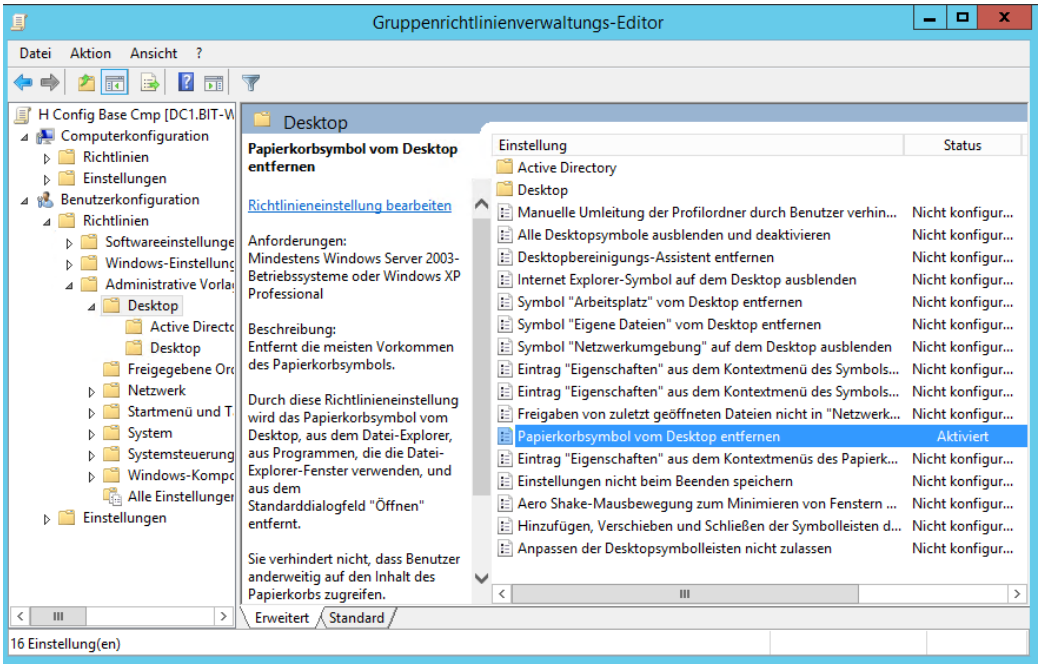

Bild 3.3 In dem GPO wird der Papierkorb für Benutzer vom Desktop ausgeblendet.

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

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 einer GPO festlegen, dass nur ein Teilbereich aktiviert werden soll. Dies kann entweder der Teilbereich Benutzerkonfiguration sein, der Teilbereich Computerkonfiguration oder beide Bereiche. Dann ist die gesamte Gruppenrichtlinie außer Funktion. Dies kann etwa sinnvoll sein, wenn eine 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 der GPO aus!

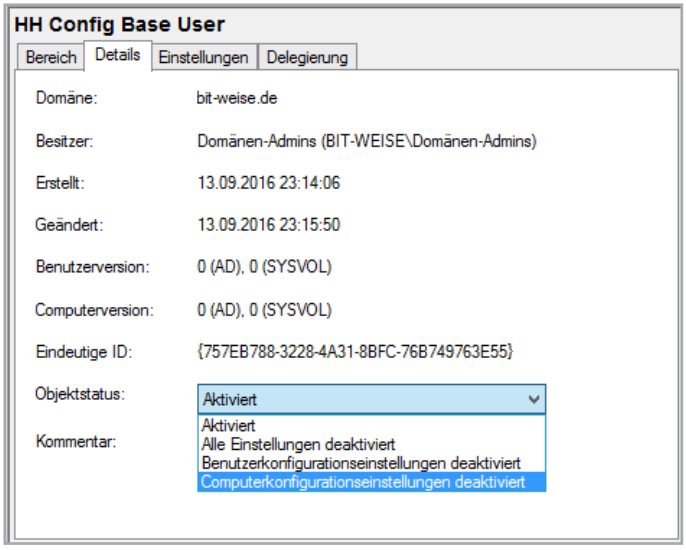

Bild 3.4 Bereiche einer GPO deaktivieren

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.

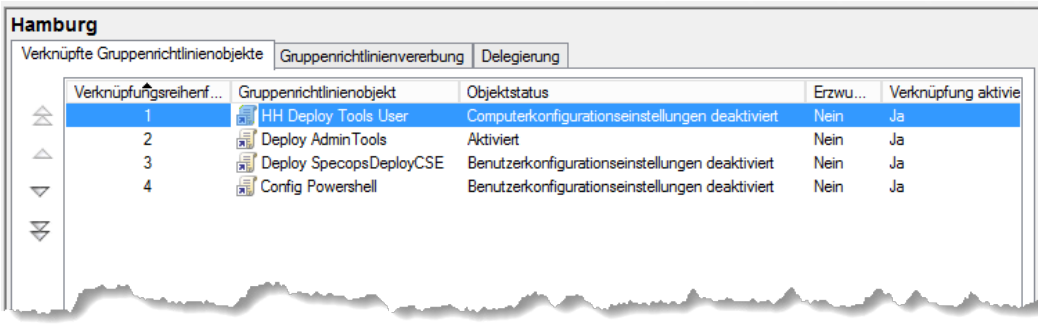

Bild 3.5 Objektstatus von GPOs prüfen

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.

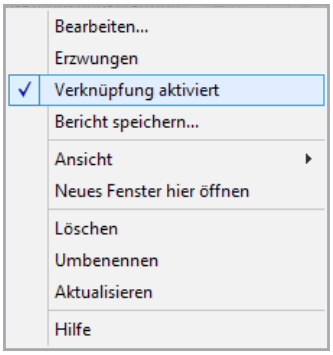

Bild 3.6
Verknüpfungseigenschaften bearbeiten

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.

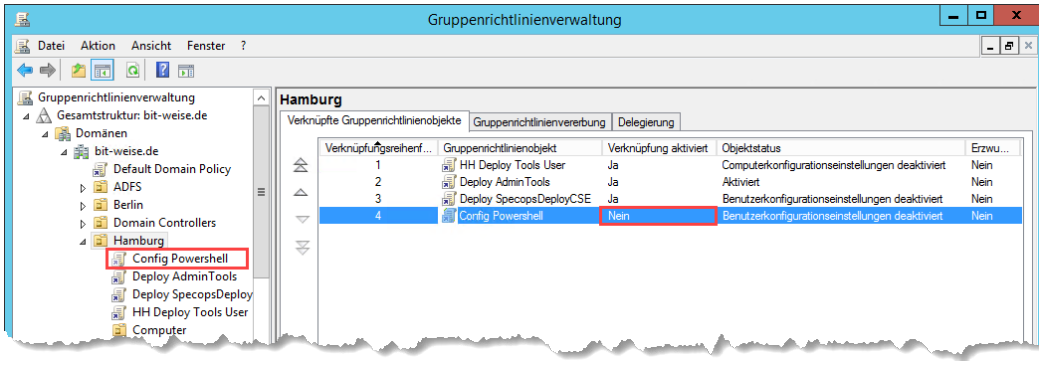

Bild 3.7 Verknüpfungsstatus überprüfen

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!

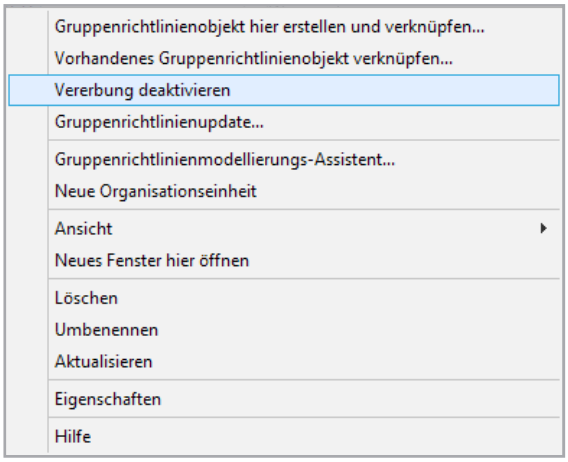

Bild 3.8 Vererbung deaktivieren

Um die Vererbung von Gruppenrichtlinien für eine Organisationseinheit zu deaktivieren, navigieren Sie in der Konsolenstruktur auf die Organisationseinheit, öffnen Sie das Kontextmenü und klicken Sie auf VERERBUNG DEAKTIVIEREN. Die Organisationseinheit ist nun mit einem Ausrufezeichen in einem blauen Kreis gekennzeichnet.

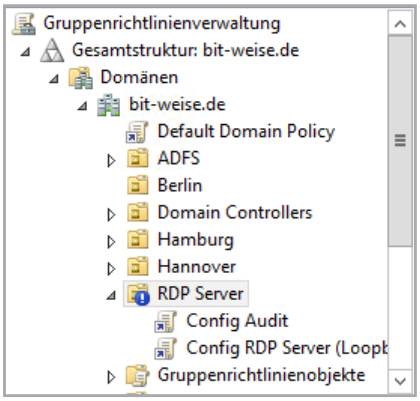

Bild 3.9
Organisationseinheit mit deaktivierter Vererbung

3.4.4 Erzwingen von GPOs

Wenn Sie sicherstellen möchten, dass die Einstellungen einer 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.

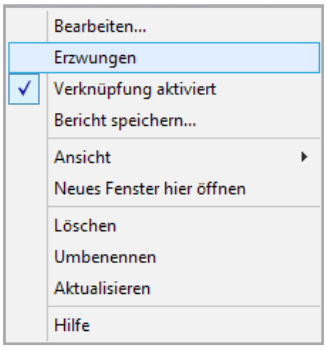

Bild 3.10
Kontextmenübefehl Erzwungen

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

Achten Sie darauf, dass eine erzwungene GPO schreibgeschützt ist und von einer tiefer liegenden, ebenfalls erzwungenen GPO nicht überschrieben werden kann. Erzwingen dreht effektiv also die Priorität der GPOs um.

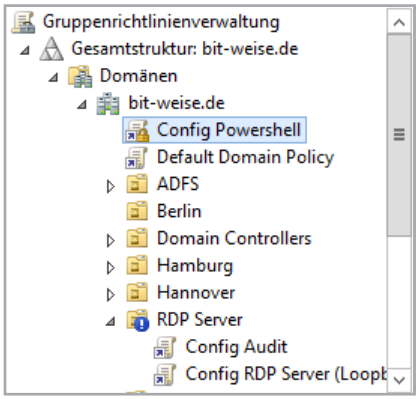

Bild 3.11
Erzwungene Gruppenrichtlinienverknüpfung

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 im AD – Sie vergessen hinterher (ich wette um eine Kiste Bier), die Einstellung wieder rückgängig zu machen, und beim nächsten Mal müssen Sie eine weitere 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.

3.4.5 Gruppenrichtlinien filtern

Standardmäßig werden Gruppenrichtlinien bei der Erstellung mit der Berechtigung Gruppenrichtlinie übernehmen für die Gruppe „Authentifizierte Benutzer“ angelegt.

Wenn Sie nur bestimmten Gruppen von Benutzern oder Computern das Übernehmen von Gruppenrichtlinieneinstellungen erlauben wollen, können Sie die Gruppenrichtlinie filtern:

- Sie können positive Filter verwenden, wenn nur die Mitglieder einer ausgewählten Gruppe die Einstellungen übernehmen sollen.
- Mit negativen Filtern verweigern Sie den Mitgliedern einer ausgewählten Gruppe die Anwendung der GPO.

3.4.5.1 Positive Sicherheitsfilterung

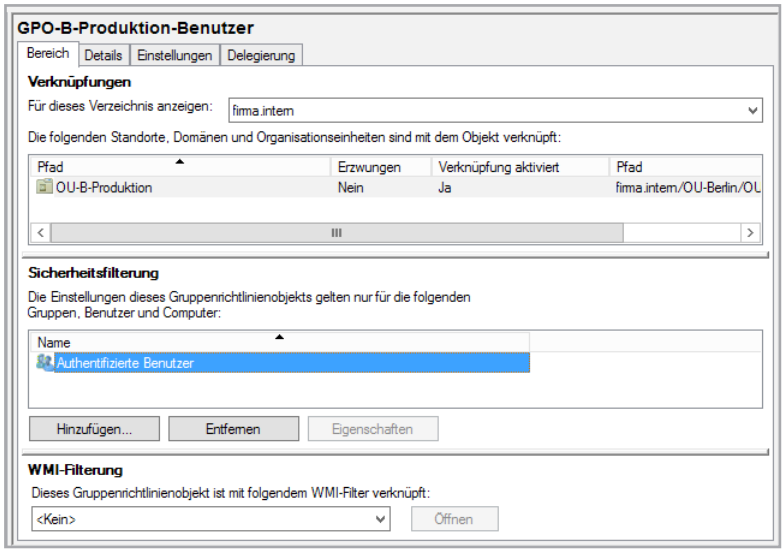

Bild 3.12 Sicherheitsfilterung einer Gruppenrichtlinie

Die positive Sicherheitsfilterung können Sie anpassen, indem Sie im Register Bereich einer Gruppenrichtlinie unter Sicherheitsfilterung auf die Schaltfläche Hinzufügen klicken und dann wie gewohnt eine Gruppe auswählen. Dies ergibt jedoch nur einen Sinn, wenn Sie die Gruppe „Authentifizierte Benutzer“ entfernen, da alle Benutzer (und Computer) zu den Authentifizierten Benutzern gehören.

ACHTUNG! Am 15. Juni 2016 hat Microsoft das Sicherheits-Patch MS16-072 verteilt, das eine Man-in-the-Middle Attack verhindern soll und bei einigen Firmen zu großem Chaos geführt hat, die mit Sicherheitsfilterung arbeiten. Das Patch MS16-072 soll verhindern, dass ein Angreifer Ihren Clients falsche GPOs unterjubelt. Dafür hat Microsoft das Verhalten des Gruppenrichtlinienclients so umgestellt, dass er sich jetzt mit dem Computerkonto am Domänencontroller anmeldet und nicht mehr wie bisher mit dem Benutzerkonto des Benutzers, der gerade verarbeitet wird. Haben Sie die Gruppe authentifizierte Benutzer aus der Sicherheitsfilterung entfernt und dem Computerkonto keine Berechtigungen gegeben, kann der Gruppenrichtlinienclient die GPOs nicht mehr vom Server abrufen und anwenden! Um dieses Problem zu lösen, müssen Sie den Computerkonten zumindest Lese-Rechte auf die GPOs geben. Dies geschieht über das Register Delegierung – siehe den folgenden Abschnitt „Negative Sicherheitsfilterung“.

Mehr Infos finden Sie unter *https://support.microsoft.com/en-us/kb/3163622* und beim GPO-Guy: *https://sdmsoftware.com/group-policy-blog/bugs/new-group-policy-patch-ms16-072-breaks-gp-processing-behavior/*

3.4.5.2 Negative Sicherheitsfilterung

Die negative Sicherheitsfilterung stellt eine komplexere Aufgabe dar. Um sie auszuführen, müssen in den erweiterten Sicherheitsberechtigungen der Gruppe explizite Einstellungen vorgenommen werden. Verfahren Sie dazu wie folgt.

Öffnen Sie das Register DELEGIERUNG der Gruppenrichtlinie und klicken Sie auf die Schaltfläche ERWEITERT.

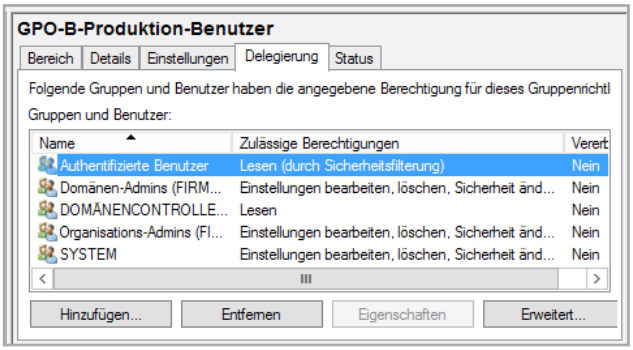

Bild 3.13 Einrichten negativer Sicherheitsfilterung

Wählen Sie nun die Gruppe aus, für die Sie die Sicherheitsfilterung einrichten möchten, und markieren Sie bei „Gruppenrichtlinie übernehmen“ das Kontrollkästchen für VERWEIGERN. Bestätigen Sie Ihre Konfiguration mit ÜBERNEHMEN.

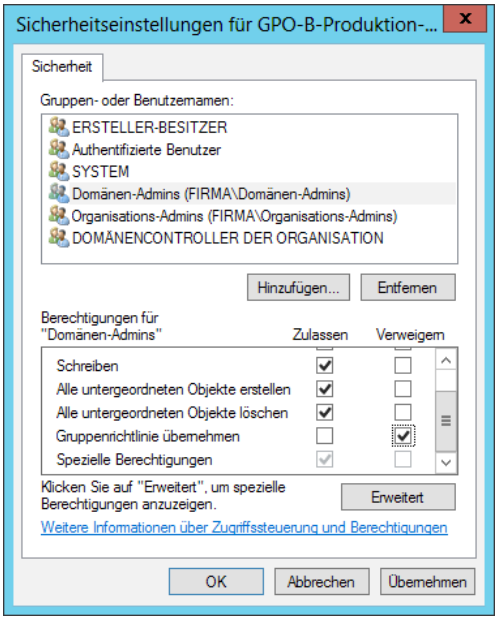

Bild 3.14
Übernehmen verweigern

Sie erhalten nun eine Warnmeldung, die besagt, dass Zugriffsverweigerungen stets Vorrang haben. Setzen Sie den Vorgang mit JA fort.

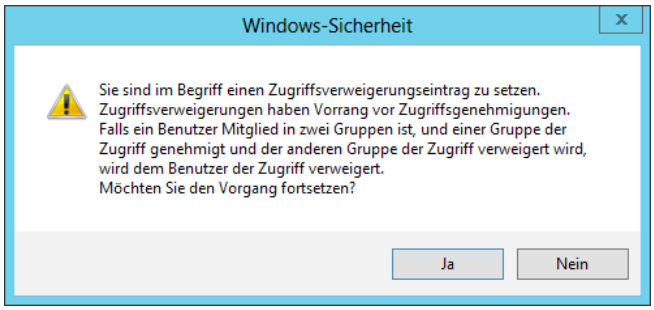

Bild 3.15
Warnung vor Zugriffsverweigerung

Wenn Sie mit der Sicherheitsfilterung arbeiten, können Sie hier auch der Gruppe „Domänencomputer“ die Berechtigung Lesen vergeben, um die Probleme von Fix MS16-072 zu beheben.

3.5 Praktisches Beispiel für die Verarbeitungsreihenfolge von Gruppenrichtlinien

Das folgende Beispiel verdeutlicht, wie in der Praxis mit Gruppenrichtlinien gearbeitet wird und welche Rolle dabei die Reihenfolge der Richtlinienverarbeitung spielt. Sie administrieren das Netzwerk eines mittelständischen Unternehmens in der Metallverarbeitung. Das Unternehmen hat zwei Standorte, die Hauptniederlassung in Berlin und eine Außenstelle in München. An beiden Standorten sind Produktionsabteilungen, in denen unter anderem CAD-Systeme eingesetzt werden. Mobile Mitarbeiter setzen tragbare Rechner an beiden Standorten ein.

Betrachten Sie zur Verdeutlichung die OU-Struktur in Bild 3.16.

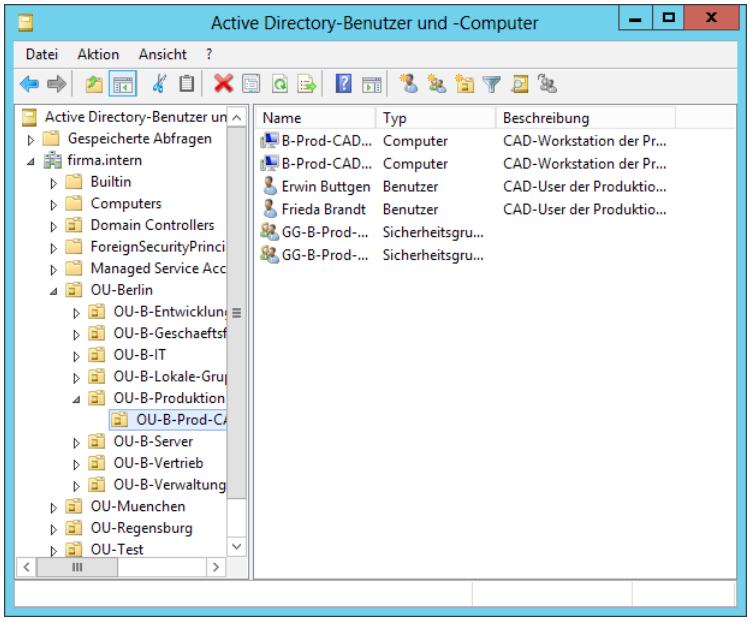

Bild 3.16 OU-Struktur der Beispielfirma

Sie möchten nun die in Tabelle 3.1 dargestellten Einstellungen mittels Gruppenrichtlinien realisieren.

Tabelle 3.1 Anforderungen für Gruppenrichtlinien

▪ Kennwörter sollen mindestens neun Zeichen lang sein und müssen den Komplexitätsanforderungen entsprechen.
▪ Alle Rechner sollen einen lokalen WSUS-Server für die Verarbeitung von Softwareupdates verwenden. Dies betrifft auch die mobilen Rechner.
▪ Standardbenutzer dürfen die Bildschirmauflösung nicht ändern.
▪ CAD-Benutzer dürfen die Bildschirmauflösung ändern.
▪ Wartungs-Ingenieure dürfen auf alle Funktionen der Systemsteuerung zugreifen. Wartungs-Ingenieure sind zugleich Standardbenutzer der Produktionsabteilung.
▪ Standardsoftware soll an alle Benutzer der Produktionsabteilung verteilt und auf jedem Rechner installiert werden, an dem sich die Benutzer anmelden.
▪ Softwareverteilung der Produktionssoftware soll nur an Produktionsserver erfolgen, nicht an andere Rechner der Produktionsabteilung.