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, Domänen-Objekte 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.

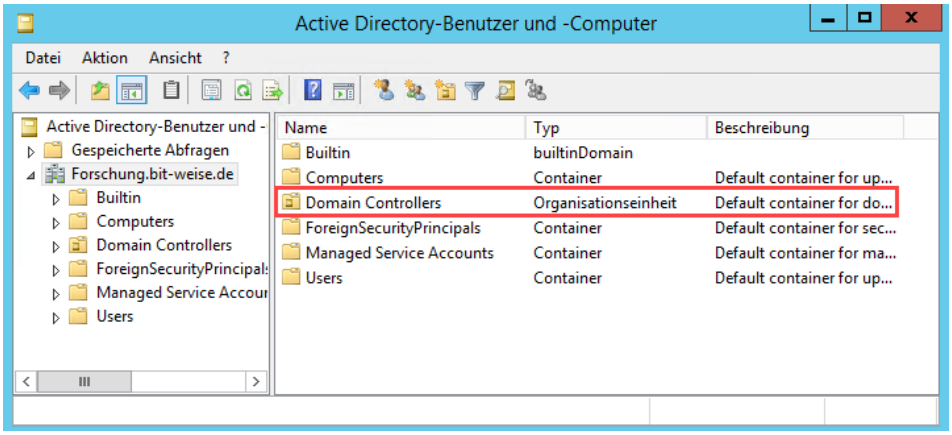

Bild 5.1 Ansicht einer neu installierten Domäne

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 Domänen-Controllern deutlich erhöhen (siehe Bild 5.2) – Domänen-Controller sind das Herz Ihres AD. Bekommt ein unberechtigter Benutzer Zugriff auf Ihr AD, 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.

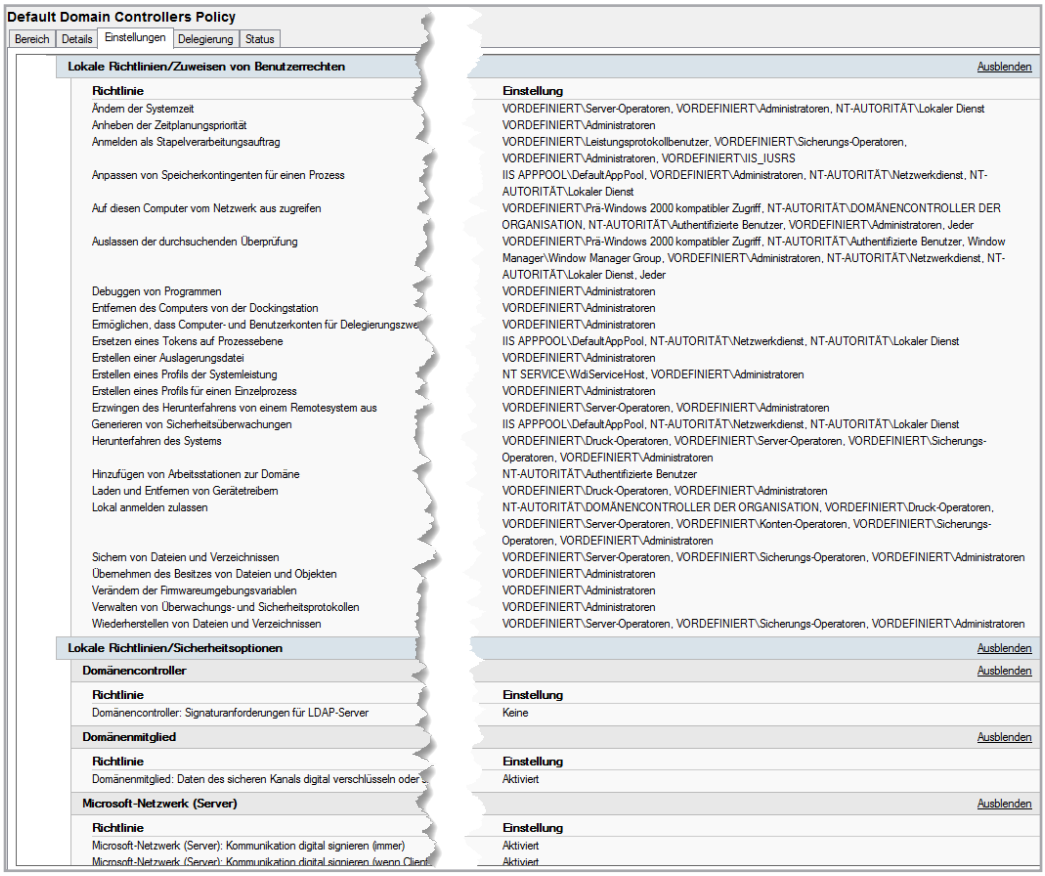

Bild 5.2 Die Default Domain Controllers Policy sichert DCs ab.

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 zurückzusetzen oder neue Gruppen anzulegen. Was Sie nicht können, ist, einem Benutzer das Recht zu geben, einen PC zu administrieren. Verstehen Sie mich an dieser Stelle nicht falsch, Sie können einen Benutzer in eine Gruppe aufnehmen, die auf einem PC das Recht hat, sich anzumelden, aber die Berechtigung wird auf dem PC vergeben.

Das erlaubt es Ihnen auch, Standort-Administratoren zu definieren, die z. B. in Berlin 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).

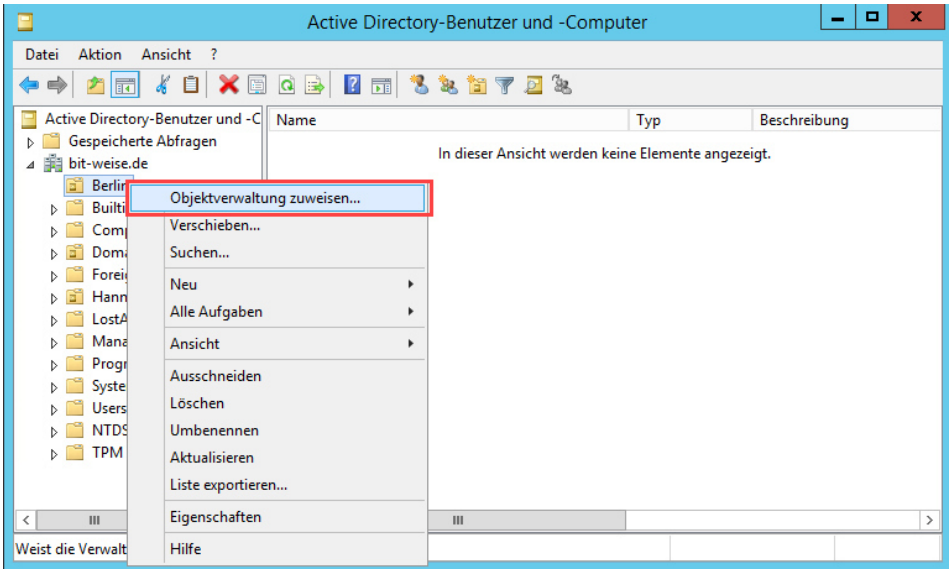

Bild 5.3 Wählen Sie in Active Directory-Benutzer und -Computer auf einer OU „Objektverwaltung zuweisen“.

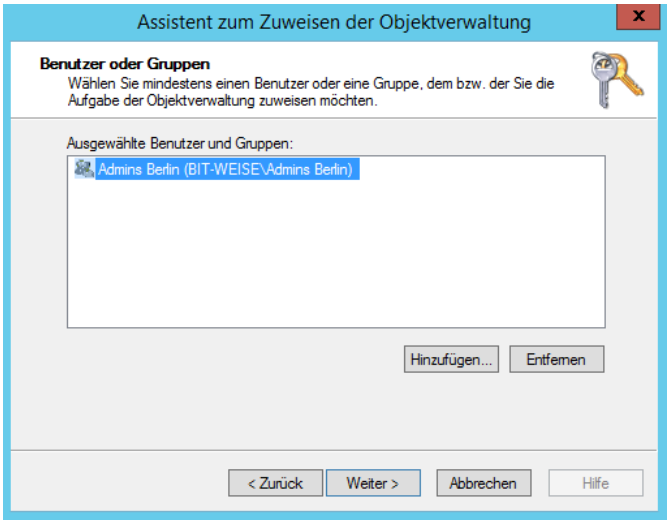

Bild 5.4 Wählen Sie eine Gruppe aus und vergeben Sie das Recht …

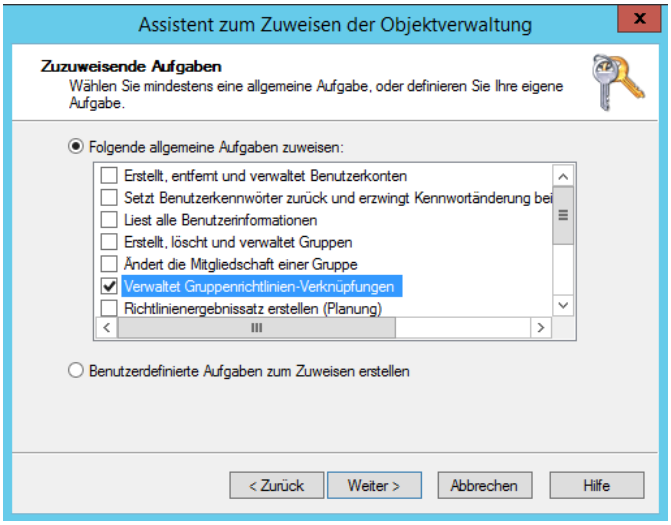

Bild 5.5 … „Verwaltet Gruppenrichtlinien-Verknüpfungen“.

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

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 12, 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 Benutzer 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 der „Authentifizierte Benutzer“ in die Liste „Sicherheitsfilter“ ein. Soll ein Benutzer oder Computer durch eine GPO betroffen werden, fügen Sie das Konto in die Gruppe ein.

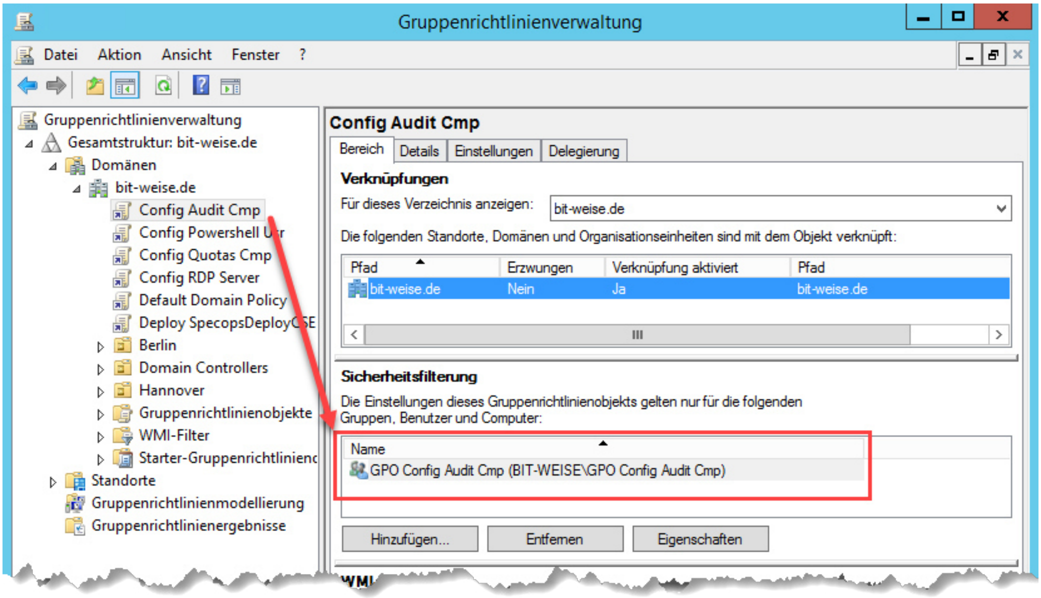

Bild 5.6 Die GPO sind unter der Domäne verknüpft, die Zuordnung erfolgt per Filter.

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 eine GPO einer OU zu, sehen Sie auf den ersten Blick, ob ein Benutzer von der 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.

Und zu guter Letzt hat Microsoft mit dem Patch MS16-072 gezeigt, was es bedeutet, zu viel an Sicherheitsfiltern herumzuspielen. Das Patch hat nämlich in vielen Unternehmen, die mit Sicherheitsfiltern gearbeitet haben, zu großem Chaos geführt, denn durch das Patch können nur noch GPOs vom Gruppenrichtlinienclient verarbeitet werden, die der Computer lesen kann. Entfernen Sie die authentifizierten Benutzer aus den Sicherheitsfiltern und erlauben den Domänencomputern das Lesen nicht wieder explizit, werden die Gruppenrichtlinien schlicht nicht mehr angewendet.

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 eine GPO?

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

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

Gegen „eine GPO pro Einstellung" spricht auf jeden Fall, dass Sie viel zu viele GPOs in Ihrer Domäne verwalten müssen. Es hat natürlich Vorteile, wenn man eine GPO hat, die „Kommandozeile deaktivieren" heißt. Haben Sie dann das Bedürfnis, einem Benutzer den Zugriff auf die Kommandozeile zu verweigern (BOfH lässt grüßen), weisen Sie ihm einfach die 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 1 GPO mit 20 Einstellungen. Wir reden hier allerdings von Verzögerungen im Millisekunden-Bereich pro GPO, sodass Sie nicht gleich panikartig alle Ihre GPOs in einer zusammenführen müssen.

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

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

- Zusammengehörige Sicherheitskonfigurationen gehören in eine GPO. Ein gutes Beispiel ist hier die „Default Domain Controllers Policy".
- RDP-Server-Einstellungen werden oft in einer GPO zusammengefasst.
- Sie haben einen Basissatz von Software, der auf jeden Client gehört? Ab in eine GPO.
- Logon-Einstellungen aus Gruppenrichtlinien-Einstellungen (Preferences) können in einer GPO stehen.
- Konfigurationseinstellungen, die für eine Gruppe von Computern oder Benutzern gelten sollen (Basiseinstellungen), können in einer 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. eine GPO, die den SQL-Server-Port öffnen soll, aber es gibt keine allgemeine 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 eine GPO GPO. Na klar ist eine GPO eine GPO, das weiß jeder und dazu muss man auch nicht mehr schreiben. Es gibt keine GPO in der GPMC, die keine GPO ist. Sie sagen ja auch nicht zu jedem Auto Auto. „Wow, guck mal, ein altes Auto Mercedes Silberpfeil." Der Sinn einer Namenskonvention ist es, wichtige Informationen in leicht erfassbarer Form abzulegen.

Grundsätzlich ist es wichtig, dass Sie Ihre GPOs kategorisieren (siehe Kapitel 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 Office
- Sicherheit Basis

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

- Konfiguration Basis Comp
- Installation BasisAnwendungen User
- Sicherheit Basis Comp

Wenn Sie eine spezifische GPO haben, die nur eine Einstellung betrifft, können Sie im Namen ruhig spezifischer werden.

- 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 der GPO aufzunehmen.

- 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.

- Conf Base Comp – HV
- Inst BaseApp User – HV
- 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 Conf Base Comp – HV
- HH Inst BaseApp User – 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/* und unter *http://www.gpanswers.com/a-clean-naming-convention-for-gpos/*.

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 auch noch 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 eine GPO im Gruppenrichtlinienverwaltungs-Editor (GPE) und öffnen Sie in der Computerkonfiguration den `Knoten Richtlinien > Administrative Vorlagen > Windows Komponenten > Remotedesktopdienste > Remotedesktopsitzungs-Host > Verbindungen`. Öffnen Sie hier die Einstellung „Gleichmäßige CPU-Zeitplanung deaktivieren“.

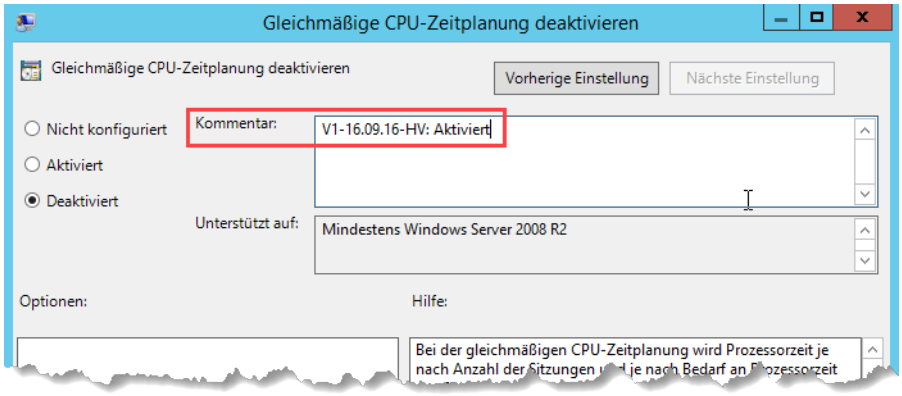

Bild 5.7 Administrative Vorlagen unterstützten Kommentare.

Sie finden in jeder Einstellung der administrativen Vorlagen ein Feld Kommentar, das in der GPO gespeichert wird. Tragen Sie hier bei jeder Änderung eine kurze Notiz mit Versionsnummer, Datum, Name des Bearbeiters und einer kurzen Änderungsbeschreibung ein. Wenn Sie mehrere Einstellungen in einem Rutsch vornehmen, sollten Sie die Versionsnummer für alle Einstellungen synchronisieren, damit man nachvollziehen kann, welche Einstellungen gemeinsam vorgenommen wurden.

Auch in Gruppenrichtlinien-Einstellungen finden Sie ein Kommentar-Feld. Sie finden es auf dem Register Gemeinsame Optionen.

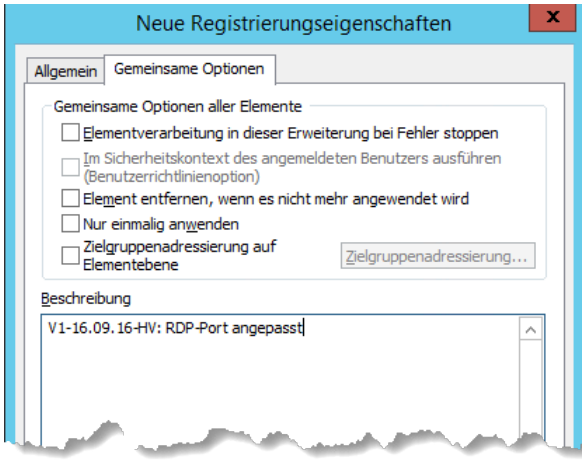

Bild 5.8 In den Einstellungen findet sich der Kommentar im zweiten Register.

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

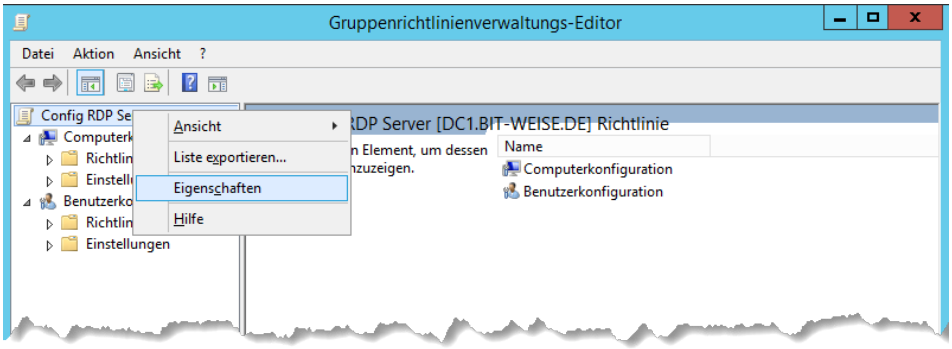

Bild 5.9 Öffnen Sie die GPO und dann die Eigenschaften.

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 der GPO das Kommentarfeld, und tragen Sie die Versionsnummer der Änderung, Datum, Name des Bearbeiters und alle Änderungen ein. Wenn Sie die Versionsnummer, die Sie hier verwalten, mit der Versionsnummer der vorher vorgenommenen Einträge abgleichen, können Sie so alle Einstellungen über den Kommentar der GPO wiederfinden.

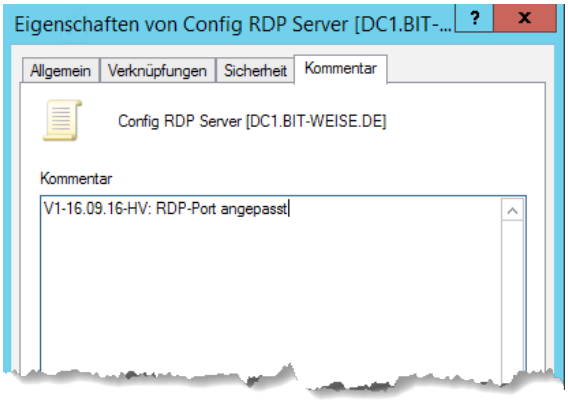

Bild 5.10
Kommentieren Sie Ihre GPOs!

Der Kommentar wird in einer eigenen XML-Datei in der GPO selbst gespeichert.

Den Kommentar der GPO können Sie sich jetzt in der GPMC anzeigen lassen, indem Sie das Register DETAILS der GPO öffnen.

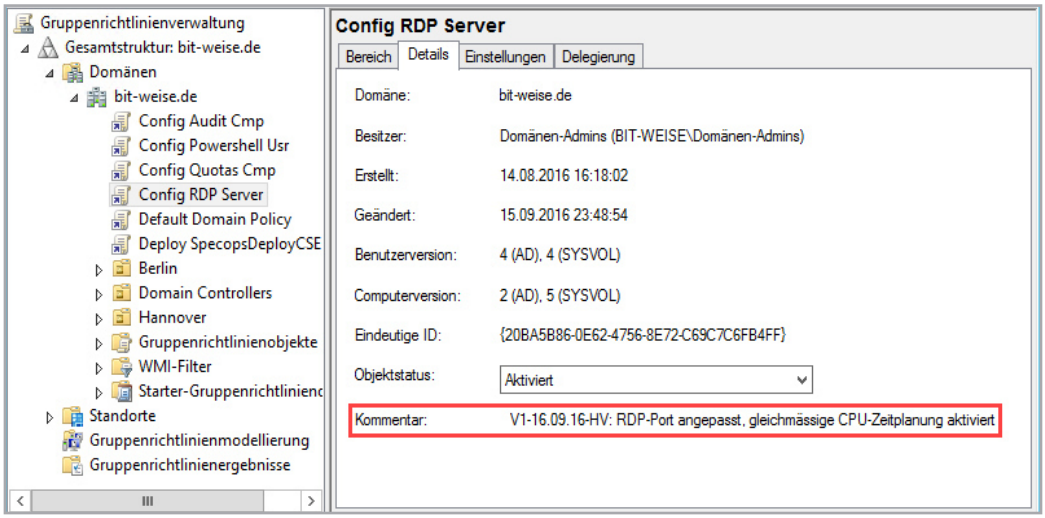

Bild 5.11 Der Kommentar wird in der GPMC unter Details angezeigt.

Sie können den Kommentar auch über PowerShell abrufen, indem Sie das Cmdlet `Get-GPO` aufrufen. Der Kommentar 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 Report, wenn Sie die Einstellungen der GPO aufrufen.

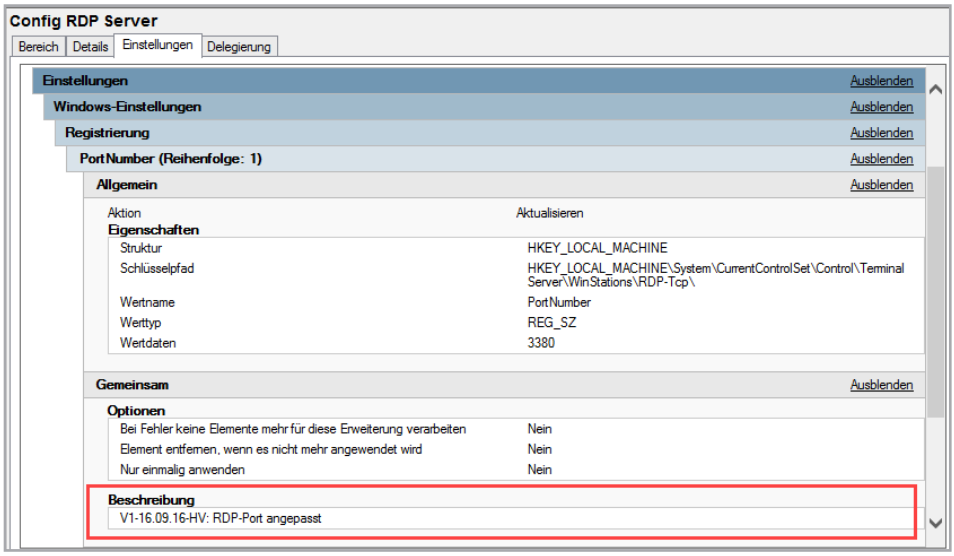

Bild 5.12 Im Report werden die Beschreibungen auch angezeigt.

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 13.3, Verwalten von Gruppenrichtlinienobjekten.

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)

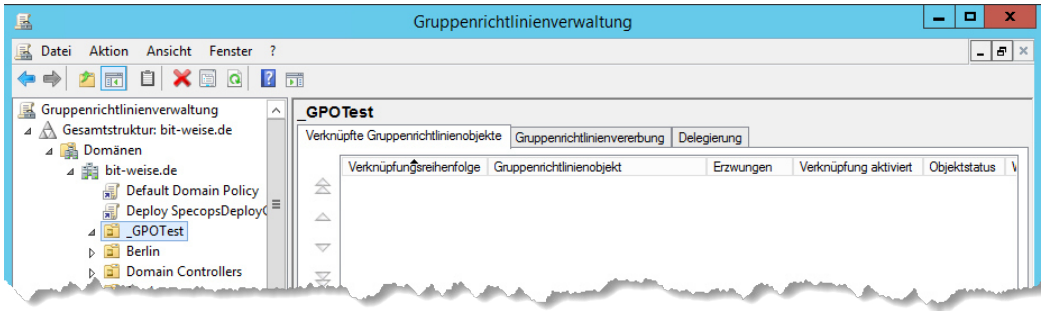

Bild 5.13 Die Test-OU ist direkt unter der Domäne aufgehängt.

In der Abbildung Bild 5.13 habe ich die Test-OU „_GPOTest“ genannt. Der Unterstrich dient dazu, die Test-OU gleich am Anfang der Liste in Active Directory-Benutzer und -Computer 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 GPOs 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 die GPO hinterher verknüpft werden soll, und dort den Register Vererbung aufrufen (siehe Bild 5.14).

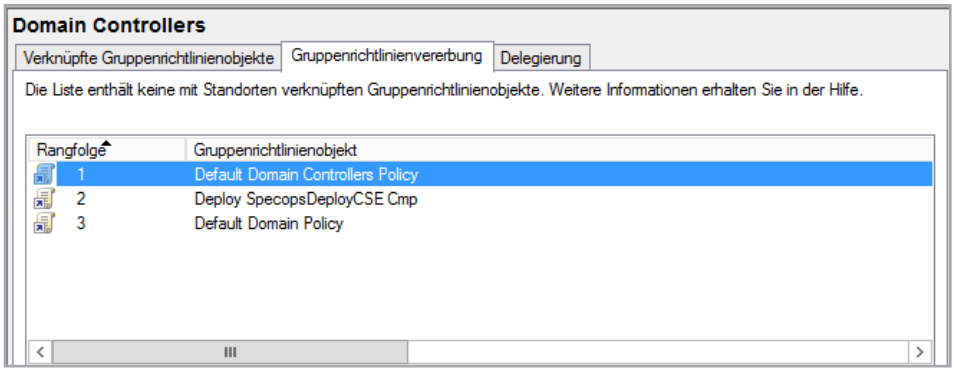

Bild 5.14 In dieser Reihung müssen die GPOs auf der Test-OU verknüpft werden.

Alternativ können Sie auch das PowerShell-Cmdlet Get-GPInheritance verwenden.

```
> (Get-GPInheritance -Target "ou=Domain Controllers,DC=bit-Weise,DC=de").
InheritedGpoLinks

GpoId       : 6ac1786c-016f-11d2-945f-00c04fb984f9
DisplayName : Default Domain Controllers Policy
Enabled     : True
Enforced    : False
Target      : OU=Domain Controllers,DC=bit-weise,DC=de
Order       : 1
GpoId       : 6c7327e8-55d6-4402-80c7-6691f89c80e3
DisplayName : Deploy SpecopsDeployCSE Cmp
Enabled     : True
Enforced    : False
Target      : DC=bit-weise,DC=de
Order       : 1
GpoId       : 31b2f340-016d-11d2-945f-00c04fb984f9
DisplayName : Default Domain Policy
Enabled     : True
Enforced    : False
Target      : DC=bit-weise,DC=de
Order       : 2
```

Wenn Sie eine neue GPO testen wollen, erstellen Sie diese ganz einfach auf der Test-OU, aber vergessen Sie nicht, den Status im Namen festzuhalten. Solange die 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 der GPO!

Wenn Sie eine bestehende 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 der GPO, die Sie bearbeiten möchten, und wählen Sie Kopieren. Nun öffnen Sie das Kontextmenü des Containers „Gruppenrichtlinienobjekte“ und wählen Einfügen.

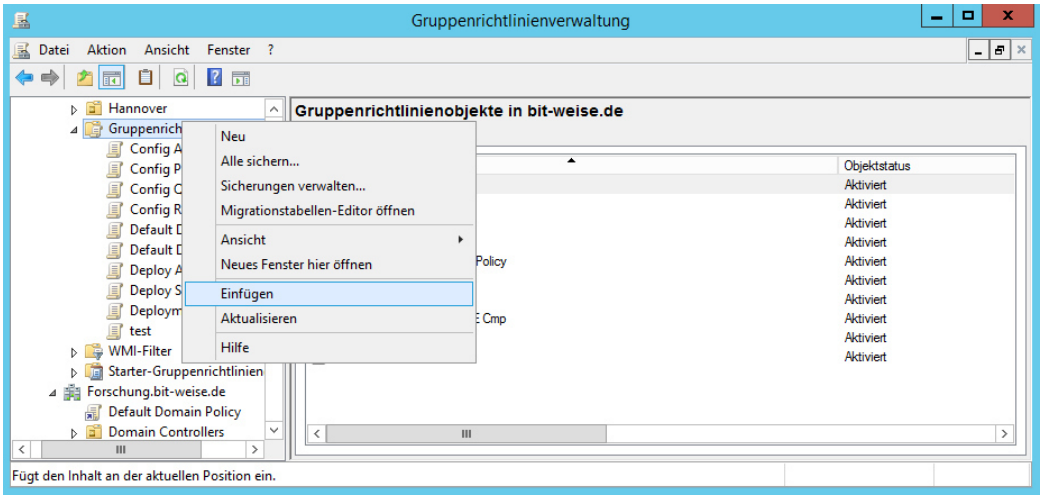

Bild 5.15 Eine kopierte GPO wird über „Gruppenrichtlinienobjekte“ eingefügt.

Die GPMC fragt Sie jetzt noch, ob Sie auch die Berechtigungen übernehmen möchten („Vorhandene Berechtigungen beibehalten“), was Sie bestätigen.

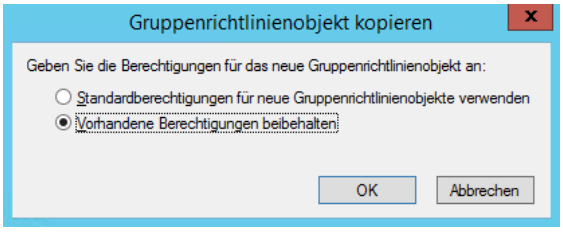

Bild 5.16
Übernehmen Sie die Berechtigungen.

Die Kopie heißt jetzt „Kopie von <Originalname>“. Benennen Sie die GPO nun so um, dass man die Test-GPO sofort wiedererkennt. AGPM verwendet z. B. eckige Klammern um die GPO (siehe Kapitel 16, Advanced Group Policy Management). Mein Vorschlag: Verwenden Sie spitze Klammern. Sollten Sie auf AGPM umsteigen, haben Sie keine Namenskonflikte, aber die spitzen Klammern fallen auf und führen außerdem dazu, dass alle Test-GPOs immer oben im Container „Gruppenrichtlinienobjekte“ angezeigt werden. Vergessen Sie nicht, wieder ein Datum und den Verursacher in den Namen der GPO einzufügen. Nun können Sie die Kopie der Produktions-GPO auf der Test-OU verlinken, indem Sie die Test-OU aufrufen und im Kontextmenü VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN auswählen. Achten Sie auf die richtige Verknüpfungsreihenfolge, die Sie in der GPMC einstellen können, wenn Sie eine OU aufrufen und das Register VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE auswählen. Je weiter die GPO in der Liste oben steht (je niedriger ihre Verknüpfungsreihenfolge ist), desto höher ist ihre Priorität.

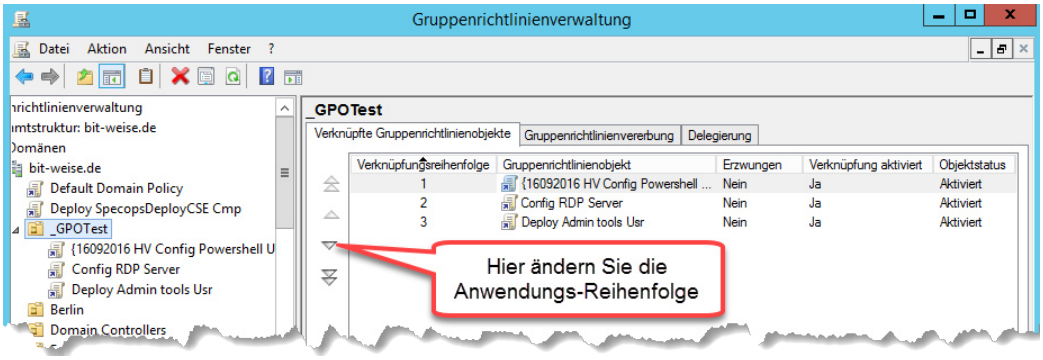

Bild 5.17 Legen Sie die richtige Anwendungsreihenfolge fest.

Den Kopiervorgang können Sie natürlich auch wieder von PowerShell erledigen lassen.

Listing 5.2 Kopieren einer GPO

```
Copy-GPO -SourceName "Config Audit Cmp" -TargetName "{16092016 HV Config Audit cmp}"
-CopyACL
```

In der Test-OU können Sie jetzt die Auswirkungen Ihrer neuen GPOs ausgiebig testen. Da Sie die Original-GPOs alle mit verknüpft haben, haben Sie im Prinzip eine vollständige Simulation Ihrer Umgebung.

5.7 Empfohlene Vorgehensweisen

Es gibt eine Reihe von Erfahrungswerten – oder Best Practices, wie es auf Neudeutsch heißt –, die ich Ihnen an dieser Stelle gerne noch ans Herz legen möchte. Versuchen Sie, sie zu beherzigen, es sei denn, Sie haben einen wirklich richtig guten Grund.

- Planen Sie Ihre Gruppenrichtlinien im Vorfeld. Es ist keine gute Idee, Ihre Gruppenrichtlinien nach dem Prinzip Try and Error zu implementieren. Glauben Sie mir, Sie sparen sich keine Zeit, aber auf Dauer kostet es Sie einfach nur Zeit und Nerven.
- Versuchen Sie, Ihre OU-Struktur an Ihre GPO-Bedürfnisse anzupassen, denn genau dafür sind OUs da.
- Verknüpfen Sie Gruppenrichtlinien mit OUs und setzen Sie Sicherheitsfilterung nur in Ausnahmefällen. Sicherheitsfilter funktionieren zwar gut, aber Sie verlieren schnell die Übersicht.
- Vermeiden Sie das Erzwingen von GPOs. Erzwingen sollte nur als Sicherheitsfunktion eingesetzt werden – also zur Durchsetzung von Sicherheitseinstellungen auf allen Computern. Erzwingen ist ganz sicher kein Troubleshooting-Feature!
- Verwenden Sie Vererbungsblockierung („Vererbung deaktivieren“) nur in Ausnahmefällen. Die Vererbungsblockierung kann z. B. sinnvoll sein, wenn Sie eine eigenständige OU für RDP-Server anlegen oder wenn Sie mehrere Standorte haben, die unabhängig admi-

nistriert werden sollen. Als Faustregel gilt: Wenn nicht schon in der Planungsphase aufgefallen ist, dass Vererbungsblockierung verwendet werden soll, ist es vermutlich wirklich nicht notwendig.

- Verknüpfen Sie Ihre GPOs immer so nah am zu konfigurierenden Objekt wie möglich.
- Spielen Sie nicht in der Produktionsumgebung an GPOs herum. Alle GPO-Änderungen müssen vorher in einer Testumgebung überprüft werden, bevor sie zum Einsatz kommen, denn oft haben GPOs Nebenwirkungen, die man nicht erwartet, oder es kommt zu Kreuzwirkungen mit anderen GPOs.
- Versuchen Sie, Gruppenrichtlinien zu kategorisieren und in GPOs zusammenzufassen. Eine Einstellung pro GPO ist keine gute Idee, weil es die Anmeldung verlangsamt und Ihnen eine Riesensammlung von GPOs beschert, die nicht mehr durchschaubar ist.
- Versuchen Sie, doppelte Einstellungen zu vermeiden. Wenn die gleiche Einstellung in mehreren GPOs vorkommt, wird der Gruppenrichtlinienclient nicht die letzte anwenden, sondern alle hintereinander. Das kostet Zeit!
- Vermeiden Sie die Einstellung „Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten“. Diese Einstellung sorgt dafür, dass der Benutzer seinen Anmeldebildschirm immer erst sieht, wenn die Computer-GPOs abgearbeitet sind (synchrone Verarbeitung, siehe Kapitel 12, Funktionsweise von Gruppenrichtlinien). Die Einstellung sorgt zwar dafür, dass sich GPOs vorhersagbarer verhalten, aber sie verlangsamt den Anmeldevorgang.
- Erstellen Sie Computerkonten, bevor Sie den Computer in die Domäne aufnehmen (auch Pre-Staging genannt), oder verwenden Sie `RedirCmp.exe`, um den Standardcontainer für neue Computerobjekte zu ändern. Standardmäßig werden neue Computerkonten im Container „Computers“ angelegt, auf dem aber keine Gruppenrichtlinien verknüpft werden können. Sie verschenken damit die wertvolle Möglichkeit, alle Computerkonten bereits bei Aufnahme in die Domäne mit Basiseinstellungen zu versehen.
- Vermeiden Sie Anmeldeskripte zur Konfiguration der Benutzerumgebung (siehe Kapitel 17, Gruppenrichtlinien verwalten mit PowerShell). Verwenden Sie stattdessen Gruppenrichtlinien-Einstellungen (Group Policy Preferences). Diese sind einfacher einzurichten und können im Fehlerfall besser behandelt werden.
- Vermeiden Sie Änderungen an den zwei vorkonfigurierten Gruppenrichtlinien „Default Domain Policy“ und „Default Domain Controllers Policy“, die über das Anpassen der Kennwortrichtlinien hinausgehen. Erstellen Sie für neue Einstellungen neue GPOs und stellen Sie die neuen GPOs in der Verarbeitungs-Rangfolge einfach vor die Default Policy (siehe Bild 5.17). Änderungen in den Default Policies erschweren die Fehlersuche und Behebung. Wenn Sie schon eine vollständig veränderte Policy haben, können Sie diese einfach kopieren, die Kopie in der Verarbeitungsreihenfolge vor die Default-Policy setzen und per `dcgpofix.exe` die Originaleinstellungen wiederherstellen.
- Halten Sie die Menge der Benutzer mit Berechtigungen auf GPOs so gering wie möglich – Sie wissen ja: Viele Köche verderben den Brei.
- Und zu guter Letzt: Wenn alles schiefläuft, ist Ihre letzte Rettung ein Backup! Wie Sie Backups von GPOs automatisiert erstellen können, erfahren Sie in Kapitel 17, Gruppenrichtlinien verwalten mit PowerShell.