Thomas Bär/Frank-Michael Schlede

Know-how ist blau.

Windows 7
richtig administrieren

> So migrieren Sie alle Unternehmens-PCs von XP zu Windows 7

> Sicherheit mit Firewall, Benutzerkontrolle, Bitlocker und Applocker

> Automatisieren Sie Administrationsaufgaben mit Batch-Jobs und dem mächtigen Kommandozeilen-Tool PowerShell

> So steigern Sie die Performance Ihrer IT-Umgebung

So betreiben Sie Windows 7 im Unternehmen sicher und effizient!

FRANZIS

Vorwort und Dank

Wenn Sie diese Sätze lesen, ist das für uns Autoren eine gute Nachricht: Es bedeutet nämlich nicht nur, dass wir unser kleines Buch über Windows 7 im professionellen Einsatz fertig bekommen haben, sondern auch, dass wir Ihr Interesse dafür wecken konnten. Und obwohl wir im Vorfeld mit aller Kraft versucht haben, alles so genau wie möglich einzuplanen, sind wir ganz sicher, dass ohne Frage noch Teile von Windows 7 existieren, über die Sie gern mehr in diesem Buch gelesen hätten. Uns ging es bei diesem Buch vor allen Dingen um die Themen, von denen wir aus unserer langjährigen Erfahrung als Journalisten im IT-Umfeld wissen, dass sie für Administratoren wichtig und interessant sind.

Unser zweites Ziel bestand darin, unsere Leser an das vielfältige Feld der professionellen IT-Administration heranzuführen. Die »Berufung« zum Administrator ist ein sehr schönes, leider aber mitunter auch einsames Arbeitsfeld. Da es ja noch immer keinen offiziellen Berufszweig »Administrator« gibt, hoffen wir, dass auch viele Fachinformatikerinnen und Fachinformatiker (sie werden wohl am häufigsten diese Position ausfüllen) Gefallen an diesem Buch finden und dass sie unsere Tipps und Hinweise in ihrer täglichen Praxis einsetzen können.

Wir können ein solches Vorwort natürlich nicht ohne die entsprechenden Danksagungen abschließen, wobei unser größter Dank ohne Zweifel unseren Familien gilt, die, jede auf ihre Art, die IT-besessenen Männer und Papas aushält. Das gilt für die Bär-Familie Christina, George und Emelie ebenso wie für die Schledes Gabi, Markus, Simon und Frederik. Weiterer Dank geht an unseren Lektor Franz Graser beim Franzis Verlag. Er hat immer darauf vertraut, dass wir pünktlich abliefern, obwohl er selbst lang genug als IT-Journalist gearbeitet hat und das chronische Zeitproblem unseres Berufsstands nur zu gut kennt.

Stellvertretend für alle anderen Freunde und Bekannten, die uns direkt oder indirekt bei der Erstellung dieses Buches unterstützt haben, möchten wir Ines Gensinger und Frank Mihm-Gebauer vom Microsoft Presse-Service in Deutschland danken, die uns immer nach Kräften unterstützen und auch auf unsere noch so obskuren Fragen die entsprechenden Antworten fanden.

Schließlich sei noch der Musik der Bands Tocotronic, Porcupine Tree und Pink Floyd gedankt, deren Wohlklänge ebenfalls entscheidend zum Gelingen dieses Buches beigetragen haben.

Thomas Bär & Frank-Michael Schlede

Inhaltsverzeichnis

2 Konfiguration: Benutzer und Gruppen

Wie schon unter Windows Vista und XP kann ein Rechner auch unter Windows 7 Mitglied einer Arbeitsgruppe oder einer Windows-Domäne sein. Solange eine Workstation nur Mitglied einer Arbeitsgruppe ist, werden alle Konfigurationen, die sich auf die Zugriffsberechtigungen und die Sicherheit beziehen, auch direkt in den Einstellungen dieses Rechners vorgenommen.

Ist der Rechner hingegen an einer Windows-Domäne angemeldet, ist er also Mitglied dieser Domäne, so sind zwei verschiedene Ebenen für die Zugriffsrechte und die Sicherheit verantwortlich: die lokale Systemebene und die Ebene der Windows-Domäne. Wie unterscheiden sie sich? Geht es rein um die Zugriffe, die der Anwender auf dem lokalen Windows-7-System durchgeführen soll, können sie auch weiterhin auf der lokalen Systemebene eingerichtet werden. Wenn es allerdings darum geht, die Zugriffe und Einstellungen zu konfigurieren, die auch für andere Windows-Systeme und Ressourcen innerhalb der Active-Directory-Struktur gelten, müssen sie auch innerhalb des Verzeichnisdienstes konfiguriert und verwaltet werden.

2.1 Lokale Konten für Benutzer und Gruppen

Unter Windows 7 stehen Ihnen wie bei anderen Windows-Versionen sowohl Benutzerkonten als auch die sogenannten Gruppenkonten zur Verfügung. Während ein Benutzerkonto immer nur für einen Anwender angelegt und verwendet werden kann, können mehrere Benutzer in einer der Gruppen zusammengefasst werden. Natürlich ist es möglich und häufig auch sinnvoll, dass ein Anwender Mitglied in mehreren Gruppen auf dem Windows-System ist. Diese »Mehrfach-Mitgliedschaft« werden Sie besonders häufig bei Systembetreuern und Administratoren antreffen, die oft schon allein deshalb Mitglied mehrerer Gruppen sein müssen, um die entsprechenden Anwendungen richtig und mit allen Zugriffsrechten versehen betreuen und verwalten zu können.

Ein wichtiger Unterschied zwischen den Gruppenkonten und den eigentlichen Benutzerkonten: Nur mit einem Benutzerkonto können Sie sich sowohl an einem lokalen System als auch an einer Windows-Domäne anmelden – die Zuordnung eines Nutzers zu Gruppenkonten kann nur ein Administrator oder ein Anwender mit administrativen Rechten vornehmen. Wenn Sie die im Screenshot gezeigten Standardmöglichkeiten nutzen, um ein neues Nutzerkonto anzulegen oder die Einstellungen eines Kontos zu ändern, so unterliegen Sie ebenfalls einigen Einschränkungen: Windows 7 bietet Ihnen hier nur die Möglichkeit, ein Administratorkonto oder einen sogenannten Standard-

benutzer einzurichten. Wollen Sie es beispielsweise einem Benutzer ermöglichen, Mitglied in mehreren Gruppen zu sein und damit auch über die entsprechenden Rechte zu verfügen, oder wollen Sie gar auf Ihrem System eigene Gruppen einrichten und verwalten, so müssen Sie dazu auf die MMC (Microsoft Management Console) und die Computerverwaltung wechseln. Diese rufen Sie am schnellsten auf, indem Sie im Suchbereich des Startfeldes *Computerverwaltung* eingeben und anschließend darauf klicken.

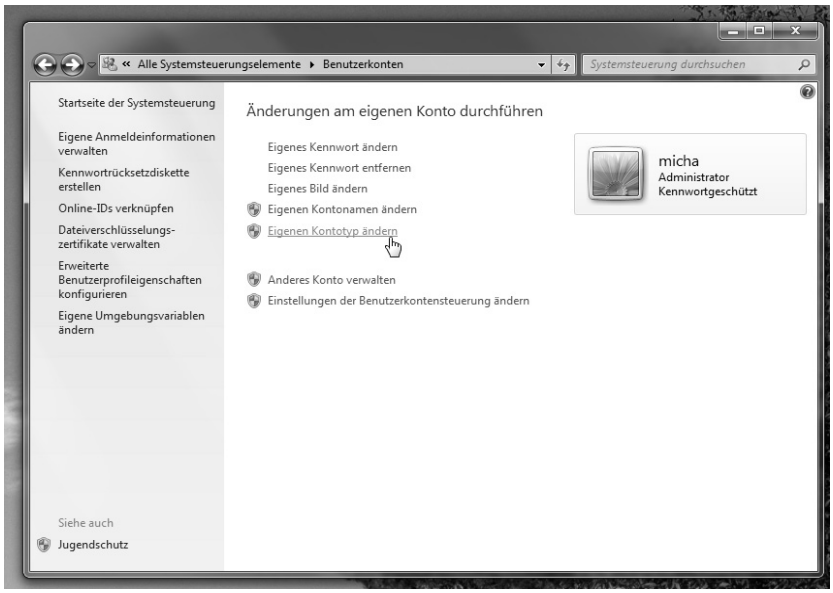

Bild 2.1: Der Standardweg, um Nutzer auf dem Windows-7-System einzurichten: In der Systemsteuerung können Konten angelegt und verändert werden.

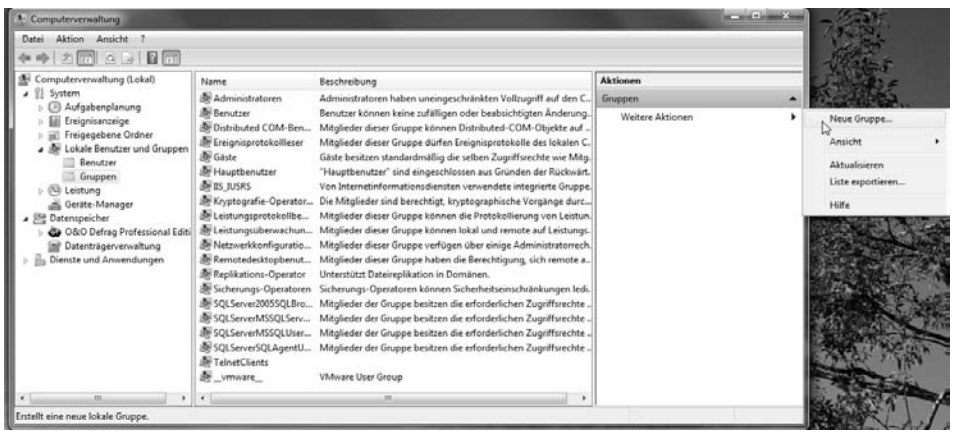

Bild 2.2: Neue Gruppen für das lokale Windows-7-System einrichten: Dies gelingt nur mit der Computerverwaltung in der Microsoft Management Console (MMC).

Sollte der Eintrag *Lokale Benutzer und Gruppen* auf Ihrem System in der MMC nicht zu finden sein, so müssen Sie das Snap-In manuell installieren. Dazu rufen Sie von der Kommandozeile oder durch Eingabe von `mmc` im Fenster *Ausführen* (Windows-Taste und »R«) eine leere Konsole auf.

Dort können Sie dann unter *Datei/Snap-In hinzufügen/entfernen* den Eintrag *Lokale Benutzer und Gruppen* auswählen und dieser Konsole hinzufügen. Danach sollten Sie diese Konsole für die spätere Verwendung unter einem entsprechenden Namen abspeichern.

Hinweis: Die Möglichkeit, mit dem MMC-Snap-In *Lokale Benutzer und Gruppen* die Nutzer- und Gruppenkonten lokal zu verwalten, steht erst mit der Professional-Version von Windows 7 zur Verfügung. Die Windows-7-Varianten Home und Home Premium enthalten diese Option nicht.

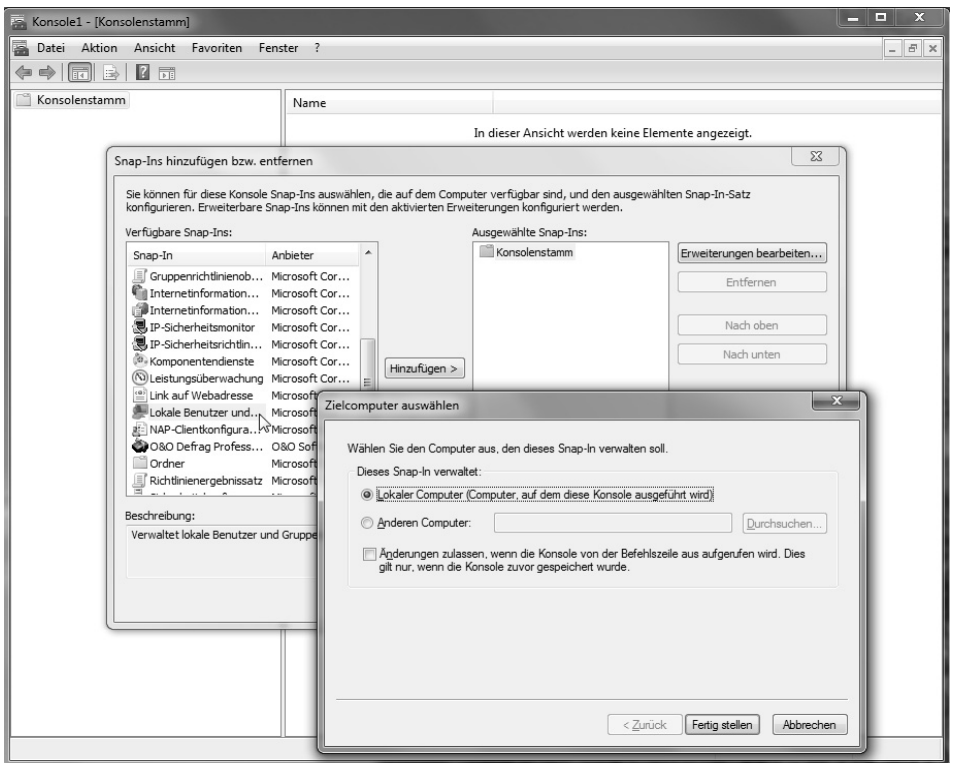

Bild 2.3: Die eigene Konsole: Ist das Snap-In für die lokalen Benutzer und Gruppen nicht installiert, kann der Administrator eine eigene Konsole anlegen.

2.1.1 Ein kurzer Ausflug zu den Domänenbenutzerkonten

Wie bereits in der Einleitung erwähnt, stehen Ihnen unter Windows 7 grundsätzlich zwei Arten von Benutzerkonten zur Verfügung: die lokalen Benutzerkonten und die Konten für Domänenbenutzer. Wir werden im Rahmen dieses Kapitels den Schwerpunkt auf die Einrichtung, Verwaltung und Betreuung der lokalen Benutzer- und Gruppenkonten legen. Die genaueren Konfigurations- und Verwaltungsgrundlagen der Nutzer und Gruppen in einer Domäne mittels Active Directory finden Sie in den Publikationen rund um die aktuellen Windows-Server.

Allerdings wollen wir in diesem Zusammenhang nicht vergessen zu erwähnen, dass Sie mittels eines entsprechenden Snap-Ins ebenfalls in der Lage sind, Domänenbenutzerkonten von einem Windows-7-System aus zu verwalten, das als Mitglied einer Active-Directory-Domäne angemeldet ist.

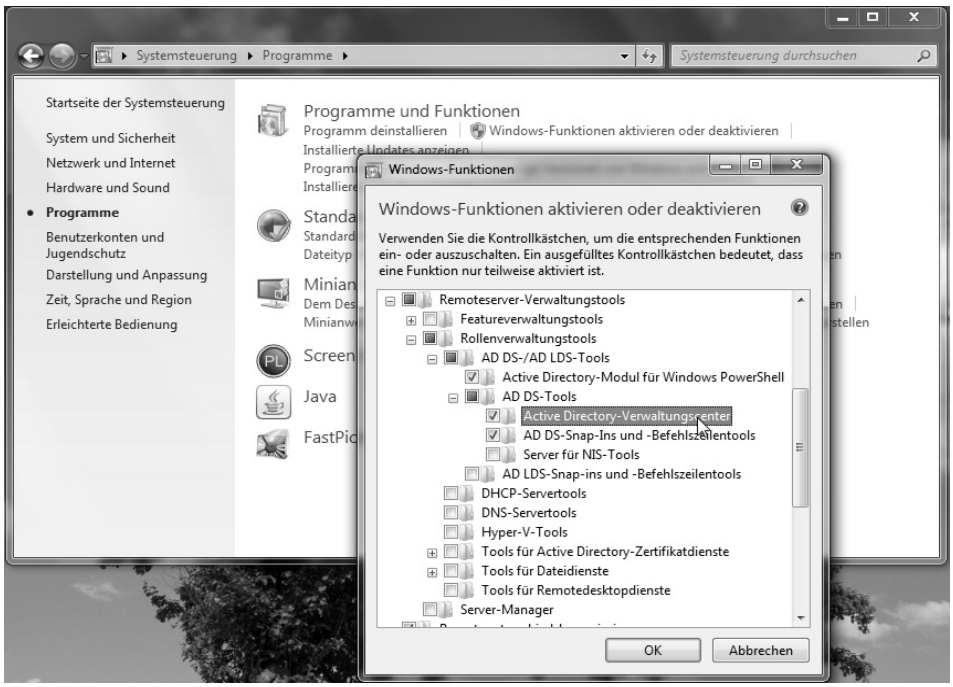

Bild 2.4: Konten der Domänennutzer von Windows 7 verwalten: Dazu muss das zusätzliche Softwarepaket *Remoteserver-Verwaltungstools* installiert sein.

Dazu müssen Sie zuvor allerdings die sogenannten *Remoteserver-Verwaltungstools* für Windows 7 von den Microsoft-Seiten herunterladen und auf dem System installieren. Danach können Sie unter *Systemsteuerung\Programme und Funktionen* im linken Panel den Bereich *Windows-Funktionen aktivieren oder deaktivieren* auswählen und dann wie im folgenden Screenshot gezeigt, die Verwaltungswerkzeuge auswählen, mit denen Sie auf Ihren Windows-Server zugreifen möchten. Diese Software steht in einer 32- und

einer 64-Bit-Version zur Verfügung und wird als Betriebssystem-Update auf das Windows-7-System installiert. Unter früheren Windows-Systemen bis zu Windows Vista war diese Software unter dem Namen *Windows Server Administrator Tools* oder einfach als *Adminpak.msi* bekannt.

⊡ Lesezeichen

http://bit.ly/aLIlmy
Downloadseite für die Remoteserver-Verwaltungstools

2.1.2 Die Grundlagen und Unterschiede der Benutzerkonten

Alle Benutzerkonten werden natürlich über einen Anmeldenamen identifiziert, der grundsätzlich immer aus zwei Teilen besteht: dem Benutzernamen und dem Namen des Computers oder der Domäne, an der sich der Nutzer anmeldet. Der vollständige Anmeldenamen eines Nutzers auf einem lokalen System oder an einer Domäne sieht im Prinzip immer so aus:

```
Legba7\hugo
company.local\hugo
```

Mit diesen beiden Beispielen wird die Anmeldung eines Nutzers *Hugo* einmal an einem lokalen System mit dem Namen *Legba7* und dann an einer Domäne mit dem Namen *company.local* gezeigt. Findet die Anmeldung ausschließlich am lokalen System statt, so kann der Name des Systems vor dem Nutzernamen wegfallen – ein Grund, warum vielen Anwendern, die nicht in einem Domänennetzwerk arbeiten, diese Art der Anmeldung zunächst ungewohnt erscheint. War Ihr System zuvor mit einer Domäne verbunden und haben Sie sich dort gegenüber dem Domänencontroller identifizert und melden sich dann wieder ab, so müssen Sie entsprechend den Namen des lokalen Computers angeben, wenn Sie sich beim nächsten Mal nur an diesem Windows-7-System anmelden wollen. Dann besitzen Sie natürlich auch keine Zugriffsrechte mehr auf die Ressourcen der Domäne. Weitere Informationen dazu finden Sie im Abschnitt 3.3 mit dem Titel »Windows 7 in der Domäne«.

Wenn es um die Anmeldung geht oder wenn Sie einen Blick auf die Benutzer- und Zugriffsrechte unter Windows 7 werfen, zeigt Ihnen das System immer den entsprechenden Namen des Anwenders an. Intern arbeitet es jedoch mit einer ganz anderen Kennzeichnung, der sogenannten Sicherheitskennung oder *SID* (*Security Identifier*). Dabei handelt es sich um eine eindeutige Kennzeichnung, die immer bei der Erstellung von sogenannten Sicherheitsprinzipalen angelegt wird.

Grundsätzlich werden alle Objekte, die auf einem Windows-System Berechtigungen zugewiesen bekommen, als Sicherheitsprinzipale verstanden: Dazu gehören neben dem Benutzernamen beispielsweise auch der Computername oder die Netzwerkadresse eines Systems. Jeder SID besteht aus einem Sicherheitskennungspräfix jeweils für die Domäne und für den Computer sowie einer Kennung für den Nutzer. Die SIDs kommen bei

vielen Gelegenheiten im Windows-Umfeld zum Einsatz, und gerade Administratoren kämpfen häufig mit den Problemen, die durch die absolute Einzigartigkeit dieser Kennung beispielsweise bei geklonten Systemen im Umfeld der Virtualisierung auftauchen.

Für das Umfeld der Benutzer- und Gruppenkonten stellen die SIDs auf jeden Fall sicher, dass der Name eines Nutzers eindeutig bleibt und der Nutzer auch dann seine Zugriffsrechte behält, wenn es ihm einfällt, seinen Benutzernamen zu ändern: Der neue Name wird mit dem SID verknüpft, sodass die Zugriffsrechte, die auf einer Abfrage dieser Kennung basieren, bestehen bleiben – der Nutzer hat weiterhin vollen Zugriff auf die Daten. Umgekehrt wird dadurch garantiert, dass er später zwar ein anderes Konto mit dem gleichen Namen anlegen kann, dieses durch den Namen aber nicht automatisch Zugriff auf die »alten« Dateien und andere Rechte erhält.

Die Nutzer eines Windows-Systems können neben den bekannten Kennwörtern auch durch Zertifikate geschützt werden. Während die Kennwörter einfach die Eingabe einer Zeichenfolge verlangen, was grundsätzlich auch bei komplexeren Passwörtern keinen hohen Sicherheitsanforderungen genügen kann, verlangt der Einsatz von Zertifikaten eine Kombination eines geheimen und eines öffentlichen Schlüssels: Während sich der Anwender wie üblich in einer interaktiven Sitzung am Windows-System anmeldet, wird die Authentifizierung erst durch den geheimen Schlüssel komplett. Diese ist dann entweder auf einer Smartcard oder einem USB-Stick sicher und verschlüsselt abgelegt. Durch diese doppelte Authentifizierung beim Anmelden am Windows-System wird eine weitaus höhere Sicherheit erreicht, als es mit normalen Kennwörtern je der Fall sein könnte.

Bei der Installation des Systems legt Windows 7 bereits eine Reihe von Standardkonten an, die gewisse Aufgaben im System haben. Dazu gehören:

- **Administrator:** Dieses vordefinierte Konto besitzt den kompletten Zugriff auf die Dienste, Dateien und Verzeichnisse sowie alle anderen Ressourcen auf dem Windows-7-System. Dies gilt bei einem lokalen Konto natürlich nur für dieses System, während sich die Rechte bei einem Domänenkonto auf die betreffende Domäne erstrecken. Es ist nicht möglich, dieses Konto zu löschen oder zu deaktivieren.
- **Gast:** Ein eingeschränktes Konto, das ursprüglich grundsätzlich für Nutzer vorgesehen war, die nur einmal oder sehr selten mit einem Windows-7-System arbeiten. Da durch ein solches allgemein bekanntes Konto auch bei eingeschränkten Rechten eine Sicherheitslücke entsteht, ist es nach der Installation grundsätzlich deaktiviert. Sie sollten das nicht ändern und dieses Konto nicht verwenden.

Neben diesen Konten, die auf einem System in der Praxis durch weitere Nutzerkonten ergänzt werden, besitzt ein Windows-7-System noch weitere Konten, die Sie aber nicht bei den Benutzerkonten finden. Diese Systemkonten, die oft auch als Pseudokonten bezeichnet werden, werden vom Betriebssystem dazu verwendet, seine Aufgaben auszuführen, ohne dass dazu ein Anwender mit entsprechenden Rechten angemeldet sein muss.

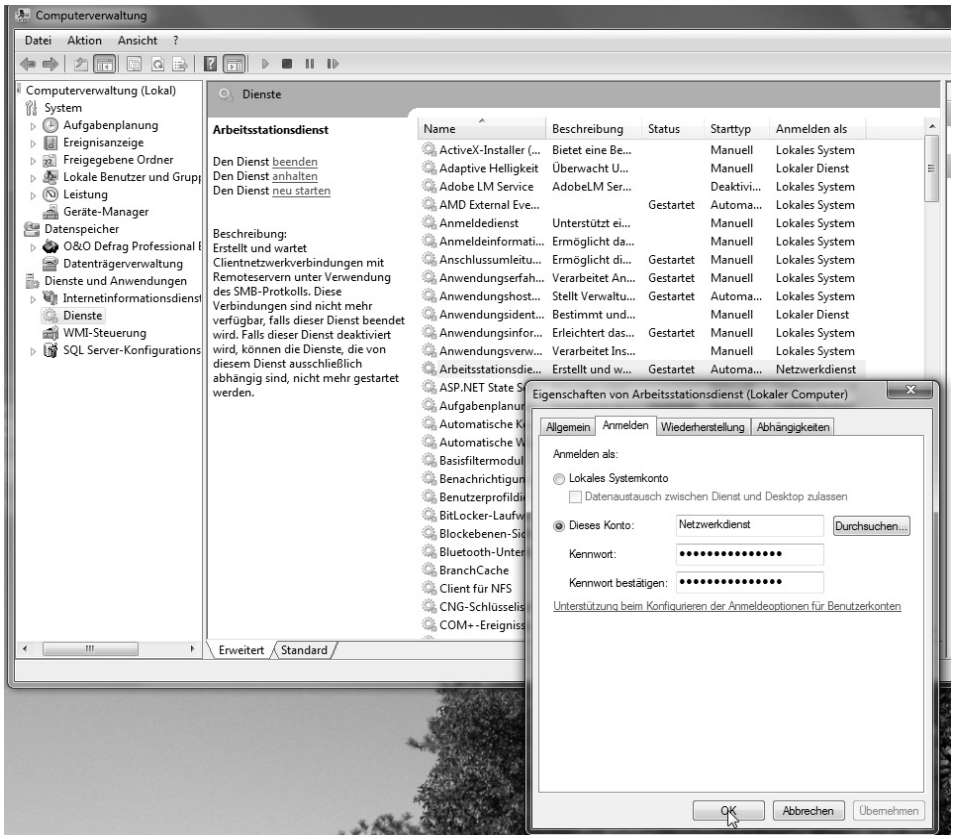

Bild 2.5: Die Übersicht der auf dem System aktiven Dienste zeigt es: Neben den normalen Benutzerkonten existieren noch System- oder Pseudokonten.

Diese Konten stehen ausschließlich auf dem lokalen System zur Verfügung, und es ist Ihnen nicht möglich, ihre Einstellungen mittels der Benutzerverwaltung zu ändern oder sich gar mit einer dieser Kennungen am System anzumelden. Zu diesen System- oder Pseudokonnten gehören:

- **Lokales System:** Mit der Kennung und den Rechten dieses Kontos führt das Windows-7-System die Systemprozesse und weitere Aufgaben auf Systemebene aus. Durch dieses Konto wird das Recht *Anmelden als Dienst* gewährt, sodass die meisten Services auch in seinem Kontext ausgeführt werden – das gilt vor allen Dingen für solche Dienste, die mit dem Desktop des Anwenders interagieren müssen. Benötigen Dienste nur geringere Rechte, werden sie zumeist unter dem Konto *Lokaler Dienst* oder auch unter *Netzwerkdienst* ausgeführt. Neben dem *Intelligenten Hintergrunddienst* werden auch der Computerbrowser, der Gruppenrichtlinien-Client und der Anmeldedienst unter diesem Konto ausgeführt.

- **Lokaler Dienst:** Ein Konto, das hauptsächlich für die Dienste zur Verfügung steht, die weniger Rechte benötigen. Dazu gehören unter anderem die Remote-Registrierung, der Web-Client und der Warndienst.
- **Netzwerkdienst:** Ebenfalls für Dienste gedacht, die weniger Rechte benötigen, dabei aber den Zugriff auf die Netzwerkressourcen brauchen. Zu den Diensten, die im Kontext dieses Kontos ablaufen, gehören beispielsweise der DNS-Client, die Leistungsprotokolle und Warnungen sowie der RPC-Locator. Gegenüber Remote-Systemen kann sich der Netzwerkdienst auch als Computerkonto authentifizieren.

2.1.3 Gruppenkonten vereinfachen die Verwaltung

Gruppenkonten dienen in erster Linie dazu, dem Systemverwalter die Arbeit zu erleichtern: Nutzer, die ähnliche Zugriffsrechte und Berechtigungen benötigen, können so zusammen und damit auch einfacher verwaltet werden. Grundsätzlich gilt: Ist ein Anwender Mitglied in einer Benutzergruppe, die das Recht besitzt, auf eine bestimmte Systemressource zuzugreifen, so besitzt dieser Anwender als Gruppenmitglied genau die gleichen Rechte. Eine Anmeldung an einem Windows-System mittels eines Gruppenkontos ist generell nicht möglich, dies funktioniert nur mit dem individuellen Benutzerkonto.

Ist ein System in verschiedenen Domänen tätig, kann es durchaus passieren, dass Gruppen mit gleichen Namen in unterschiedlichen Domänen oder eine Gruppe mit dem gleichen Namen in der Domäne und auf dem lokalen System existieren. Aus diesem Grund werden die Gruppen zumeist in der Form `Domäne\Gruppenname` oder `Computername\Gruppenname` angegeben, um so eine eindeutige Bezeichnung zu verwenden. Drei Arten von Gruppen kommen unter Windows 7 zum Einsatz:

- **Lokale Gruppen:** Sie werden auf den lokalen Systemen definiert und kommen ausschließlich dort zum Einsatz.
- **Verteilergruppen:** Diese Gruppen kommen für Verteilerlisten der E-Mail zum Einsatz. Sie werden in Active-Directory-Umgebungen definiert und verwendet.
- **Sicherheitsgruppen:** Auch diese Gruppen werden innerhalb einer Active-Directory-Domäne definiert und können mit Sicherheitsdeskriptoren verknüpft werden. Durch sie können einer solchen Gruppe Zugriffsrechte auf Dateien, Verzeichnisse, Freigaben und Netzwerkdrucker erteilt werden. Ebenso kann eine solche Sicherheitsgruppe die Berechtigung besitzen, bestimmte Objekttypen innerhalb einer Organisationseinheit (OU) im Active Directory zu verwalten.

Genau wie zuvor bei den Benutzerkonten geschildert, bekommen auch die Benutzergruppen SIDs, mit denen sie eindeutig identifiziert werden.

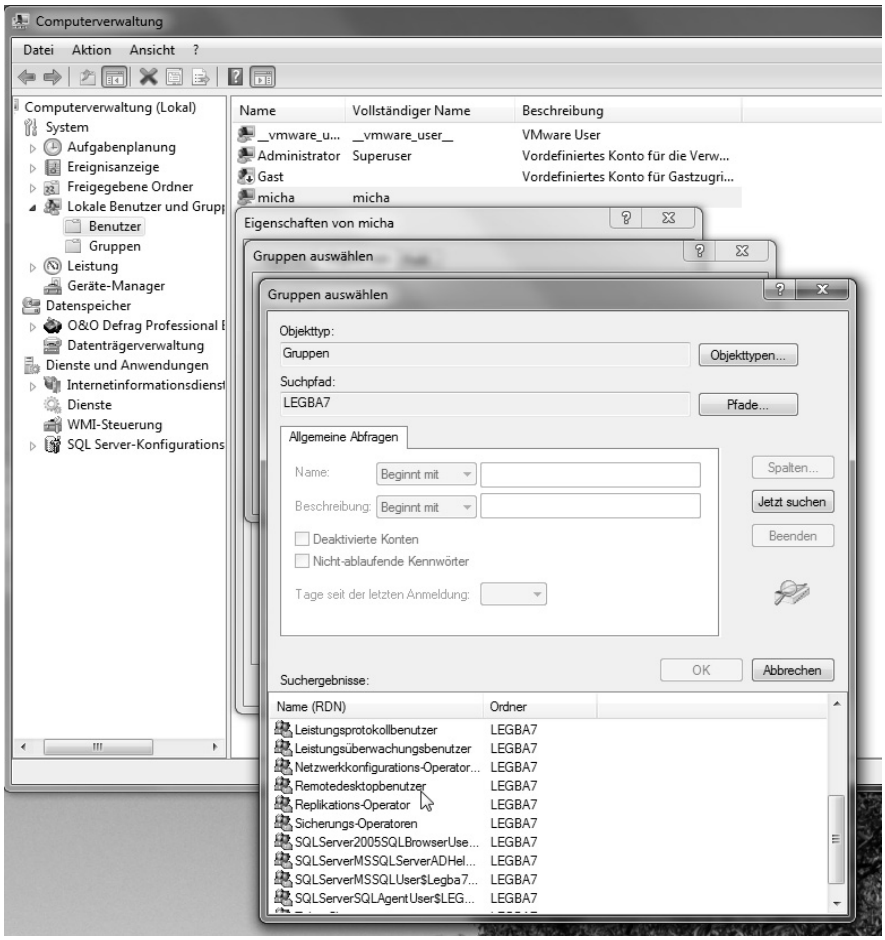

Bild 2.6: Windows stellt eine Reihe von vordefinierten Gruppen bereit: Diese Gruppen können dazu verwendet werden, bestimmte Zugriffsebenen zu definieren.

Wenn Sie daran gehen, mit Hilfe von Benutzergruppen bestimmte Ebenen von Zugriffen zu definieren und einzurichten, stehen unter Windows 7 bereits einige integrierte und vordefinierte Gruppen zur Verfügung:

- **Administratoren:** Hier finden Sie die lokalen Administratoren eines Systems, die den vollen Zugriff auf alle Ressourcen einer Workstation besitzen. Sie können sowohl neue Benutzerkonten einrichten als auch die Gruppenmitgliedschaften anderer Nutzer verändern und besitzen die vollständige Kontrolle über das lokale System. Aus diesem Grund sollten Sie sich sehr sorgfältig überlegen, welche Nutzer Sie in diese Gruppe aufnehmen.
- **Sicherungs-Operatoren:** Diese Gruppe ist berechtigt, Dateien und Verzeichnisse auf dem System zu sichern und wiederherzustellen. Sie sind auch in der Lage, Dateien

und Verzeichnisse zu sichern und wiederherzustellen, wenn sie keine Zugriffsrechte auf diese Dateien besitzen! Sie können dabei jedoch keine Zugriffsrechte dieser Daten verändern.

- **Kryptografie-Operatoren:** Sie verwalten die IP-Sicherheit (IPSec, siehe dazu auch Kapitel 6), die Konfiguration der Verschlüsselung sowie digitale Zertifikate und IDs.
- **Netzwerkkonfigurations-Operatoren:** Die Mitglieder dieser Gruppe sind in der Lage, die Netzwerkeinstellung der Workstation zu verwalten. Das schließt das Ändern der TCP/IP-Einstellungen und aller allgemeinen Netzwerkeinstellungen ein.
- **Leistungsprotokollbenutzer:** Sie verwalten die Leistungsprotokollierung und können Leistungsindikatoren sowohl verwalten als auch anzeigen lassen.
- **Systemmonitorbenutzer:** Die Mitglieder dieser Gruppe können Leistungsindikatoren und -protokolle lediglich anzeigen lassen.
- **Hauptbenutzer:** Diese Gruppe ist lediglich noch aus Kompatibilitätsgründen vorhanden: Sie besaß unter früheren Windows-Versionen vor Windows Vista zusätzliche Rechte, die beispielsweise die Installation von Programmen betrafen.
- **Remote-Desktopbenutzer:** Diese Anwender können sich via Terminaldienste oder über den Remote-Desktop (siehe dazu auch Kapitel 3.4) anmelden. Mitglieder der Gruppe Administratoren bekommen diese Berechtigung automatisch zugeteilt.
- **Replikations-Operator:** Die Benutzer dieser Gruppe sind in der Lage, die Datenreplikation auf dem lokalen System zu verwalten. Diese Technik kommt vornehmlich in Active-Directory-Domänen und auf den Windows-Servern zum Einsatz.
- **Benutzer:** Die Standardgruppe für »normale« Anwender, die der Administrator beim Anlegen neuer Nutzer auf dem lokalen System verwendet. Sie können sich lokal auf dem Windows-7-Rechner anmelden und dabei auch eine lokale Profildatei verwenden. Sie sind zudem in der Lage, diese Workstation zu sperren oder auch herunterzufahren.
- **Gäste:** Hier finden sich schließlich Nutzer mit stark eingeschränkten Rechten. Sie können zwar auch per Remote-Zugriff auf einem System mit seinen Ressourcen arbeiten, sind dabei aber extrem eingeschränkt.

Grundsätzlich werden Sie neue Anwender wahrscheinlich als Administratoren oder Benutzer anlegen. Kommt auf Ihrem Windows-7-System hauptsächlich moderne Software zum Einsatz, die schon für Windows Vista oder direkt für Windows 7 entwickelt wurde, so sollte ein solcher Anwender in den meisten Fällen über ausreichende Rechte verfügen, um seiner täglichen Arbeit nachzugehen. Nur wenn ältere Software aus XP-Zeiten oder davor verwendet wird, kann es nötig sein, dass bestimmte Programme oder Aufgaben ausschließlich mit den Rechten eines Administrators ausgeführt werden. Weitere Informationen dazu finden Sie im Abschnitt 4.1, in dem wir uns eingehend mit dem Thema Benutzerkontensteuerung (UAC – User Account Control) befassen.

2.2 Freigabe von Dateien und Ressourcen

Es gibt wenige Aspekte bei einem Windows-Betriebssystem, die so sicherheitsrelevant sind wie die Freigabe von Dateien und anderen Ressourcen wie beispielsweise Druckern. Denn durch die Freigabe solcher Systemressourcen bekommen andere Systeme direkten Zugriff auf einen Windows-7-Rechner. Deshalb gilt es in diesem Zusammenhang ganz besonders, dass ein Systemverwalter bei den Freigaben seiner Rechner immer die Sicherheitsaspekte im Auge haben und entsprechend verwalten muss.

Grundsätzlich stellt Ihnen das Windows-System drei unterschiedliche Verfahren zur direkten Freigabe von Dateien zur Verfügung:

- eine Freigabe öffentlicher Ordner,
- die gezielte Freigabe einzelner Ordner
- und die sogenannten Heimnetzgruppen.

Dabei ist natürlich der Einsatz der öffentlichen Ordner besonders einfach, da sie schließlich auf allen Windows-Systemen direkt zur Verfügung stehen. So kann jeder beliebige Anwender, der über ein Benutzerkonto und ein Kennwort auf einem Windows-Rechner verfügt, auch auf die öffentlichen Ordner Ihres Systems zugreifen. Damit wäre auch schon der eklatante Nachteil dieses Features genannt.

Wollen Sie gezielt definieren, welche Anwender oder Gruppen einen Zugriff auf bestimmte Dateien oder Ordner erhalten, kommen Sie nicht umhin, einzelne Dateien oder Ordner direkt freizugeben. Dieser größere Aufwand lohnt sich aber auf jeden Fall, denn auf diese Weise legen Sie exakt fest, wer die Dateien und Ordner anzeigen lassen oder sogar ändern darf.

Schließlich steht Ihnen mit Windows 7 ein weiteres, relativ einfaches Verfahren zur Verfügung, um Dateien freizugeben: die sogenannte Heimnetzgruppe. Eine Heimnetzgruppe steht ausschließlich auf Windows-7-Systemen zur Verfügung und besteht aus einer Gruppe von Windows-7-Rechnern, die Dokumente, Drucker, Bilder, Musik- und Videodateien gemeinsam nutzen können.

2.2.1 Dateifreigaben und die Sicherheit

Es sind zwei Faktoren, die ganz besonders den Grad der Sicherheit bestimmen, wenn es um Dateifreigaben auf modernen Windows-Systemen gebt: Neben dem ersten wichtigen Aspekt der Computereinstellungen sind es vor allem die Formate der Datenträger, auf denen sich die Dateien und Verzeichnisse befinden, die Sie freigeben möchten. In diesem Zusammenhang sei gleich auf einen wichtigen Unterschied zu früheren Windows-Systemen hingewiesen: Während es noch unter Windows XP nur möglich war, ganze Verzeichnisse freizugeben, führte Microsoft mit Windows Vista eine weitaus feinere Methode ein, die es Ihnen nun auch ermöglicht, einzelne Dateien im Netzwerk freizugeben.

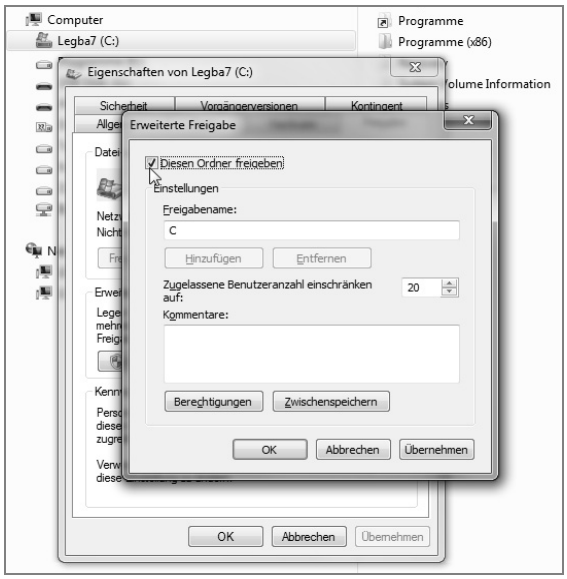

Bild 2.7: Das Format des Datenträgers ist entscheidend: Erst wenn NTFS zum EInsatz kommt, sind entsprechend fein granulierte Freigaben sicher möglich.

Geht es um die Sicherheit einer Dateifreigabe, hängt es entscheidend vom Format des lokalen Datenträgers ab, welche Optionen Sie hier verwenden können. So bietet Ihnen das alte FAT-Dateisystem weder in seiner FAT16- noch seiner etwas neueren FAT32-Ausprägung genügend Kontrolle über den Zugriff auf die Dateien und Verzeichnisse. Zwar sollten diese Dateisysteme nur noch in Ausnahmefällen zum Einsatz kommen, allerdings existieren noch genügend Installationen, in denen sie aus Gründen der Kompatibilität mit anderen Betriebssystemen weiterhin im Einsatz sind.

In einem FAT-Dateisystem können die Dateien grundsätzlich nur als *Schreibgeschützt*, *Verborgen* oder *System* eingestuft und gekennzeichnet werden. Obwohl diese Einstellungen jeweils sowohl für Dateien als auch für Ordner festgelegt werden können, besitzen sie einen gravierenden Nachteil: Jeder Anwender, der einen Zugriff auf ein Volumen (also ein Laufwerk) unter FAT hat, ist auch in der Lage, diese Einstellungen zu ändern oder gleich ganz außer Kraft zu setzen. So kann also in der Praxis jeder Nutzer beliebig auf jede Datei zugreifen, sie verändern oder auch löschen.

Kommt hingegen das Dateisystem NTFS zum Einsatz, so stehen Ihnen Berechtigungen zur Verfügung, mit deren Hilfe Sie sehr genau regeln können, ob der Zugriff auf einen Ordner oder eine Datei erlaubt oder verboten ist. Da diese Berechtigungen direkt mit dem Zugriffsmodell für die verschiedenen Anwender und Gruppen auf dem System verbunden sind, erhalten Sie hier eine sehr genaue Kontrolle darüber, wer auf bestimmte Dateien und Ordner zugreifen, sie anschauen oder auch verändern kann. Ab Windows Vista und damit auch unter Windows 7 unterstützen die Windows-Systeme zwei Freigabemodelle für die Daten:

- **Standardfreigabe:** Sie ermöglicht die Freigabe von Dateien aus jedem Ordner des Dateisystems. Die Benutzer erhalten hier nicht automatisch Zugriff auf die Dateien.

Die Sicherheitseinstellungen auf dem lokalen Datenträger legen fest, wer Zugang zu Dateien und Ordnern erhält.

- **Freigabe in öffentlichen Ordnern:** Ermöglicht die Freigabe von Dateien des Ordners, der unter *%SystemDrive%\Users\Public* zu finden ist. Auf deutschen Systemen kommt hier der Pfad *%SystemDrive%\Benutzer\Öffentlich* zum Einsatz. Die Zugriffsberechtigungen für diesen Ordner bestimmen, welche Nutzer und Gruppen auf öffentlich freigegebene Daten Zugriff erhalten und wie weit dieser reicht. Werden Dateien oder Ordner in diesen Ordner kopiert oder verschoben, so werden ihre Zugriffsrechte den Rechten des Ordners *Öffentlich* angepasst.

Unter Windows 7 ist es möglich, dass beide Freigabemodelle gleichzeitig zum Einsatz kommen. Es existiert zudem eine Gruppenrichtlinien-Einstellung, die festlegt, wie die Freigabe konkret geregelt wird. Um sie zu bearbeiten oder zunächst einmal zu aktivieren, müssen Sie den Editor für lokale Gruppenrichtlinien durch Eingabe von `gpedit.msc` in der Kommandozeile oder im Fenster *Ausführen* (Windows-Taste + »R«) aufrufen. Dort navigieren Sie im linken Panel der MMC in den Zweig *Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Netzwerkfreigabe*, wie es auch im folgenden Screenshot zu sehen ist. Die hier zur Verfügung stehenden Einstellungen kontrollieren, ob insbesondere im Ordner *%SystemDrive\Benutzer* eine Freigabe erlaubt ist oder nicht. Grundsätzlich wird hier festgelegt, ob und wie die Freigabe in Ordnern erlaubt ist, die einem bestimmten Nutzer-/Anwenderprofil auf dem System zugeordnet sind.

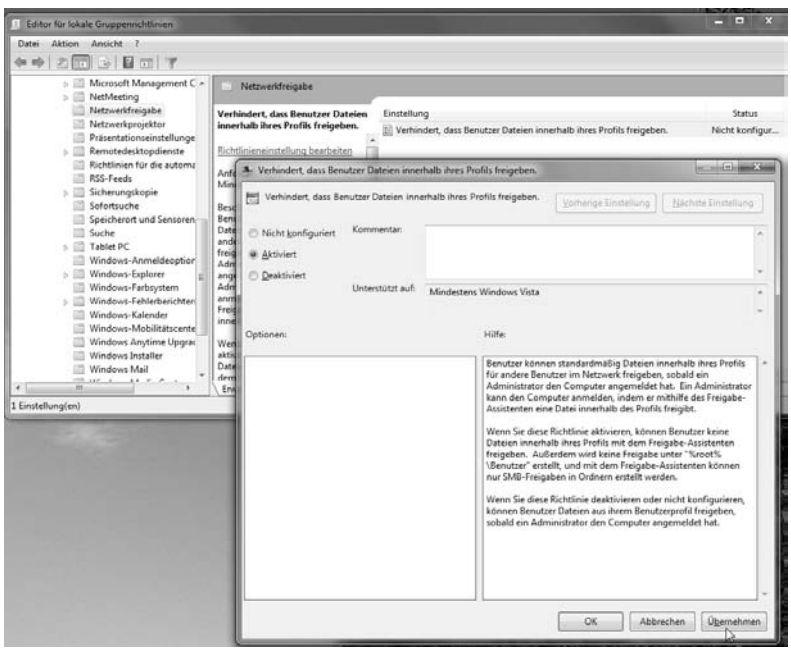

Bild 2.8: Wie die Freigabe geregelt wird: Eine Gruppenrichtlinie hat auf Windows-7-Systemen einen entscheidenen Einfluss auf diese Einstellungen.

Standardmäßig ist diese Richtlinie auf einem Windows-7-System nicht aktiv. In diesem Fall gilt, dass die Benutzer Dateien aus ihrem Benutzerprofil freigeben dürfen, sobald ein Nutzer mit Administratorrechten den Rechner für das Netzwerk freigegeben hat. Dazu muss er nichts weiter tun, als eine Datei aus seinem Profil freizugeben. Das gleiche Verhalten gilt auch, wenn die Richtlinie zwar konfiguriert, aber dann deaktiviert wurde.

Wurde die Richtlinie hingeben aktiviert, können die Nutzer keine Dateien aus ihrem Profil mit Hilfe des Freigabeassistenten freigeben. Der Freigabeassistent ist dann auch nicht in der Lage, Freigaben im Ordner *%SystemDrive\Benutzer* zu erteilen.

Grundsätzlich erscheint es zunächst am einfachsten, die öffentlichen Ordner für die Freigabe von Ordnern und Dateien zu verwenden. Unter Sicherheitsaspekten ist es aber auf jeden Fall vorzuziehen, die Standardfreigabe einzusetzen. Der etwas höhere Aufwand, der für Sie als Systemverwalter dadurch entsteht, wird durch den besseren Schutz und die genauere Kontrolle deutlich aufgewogen.

2.2.2 Kurze Anmerkungen zur Druckerfreigabe

Die Freigabe der Drucker unter Windows 7 unterscheidet sich nicht wesentlich von der Vorgehensweise, wie sie auch unter bisherigen Windows-Systemen üblich war: Freigegebene Drucker, die im Netzwerk-Explorer angezeigt werden, können – auch wenn sie unter älteren Windows-Systemen betrieben werden – auf einem anderem Windows-System im Netzwerk als Netzwerkdrucker eingebunden werden.

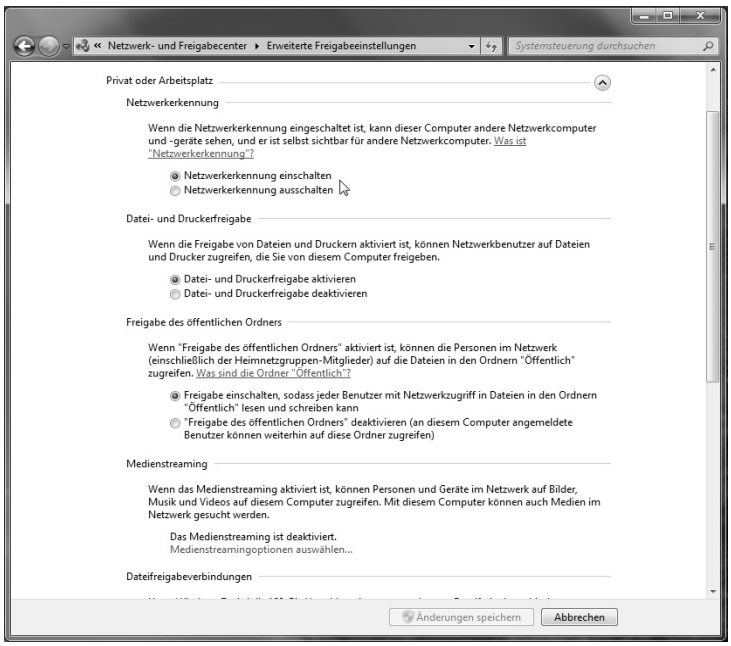

Bild 2.9: Wichtige Einstellung vor der Druckerfreigabe: Wenn im Netzwerk- und Freigabecenter die Netzwerkerkennung nicht freigegeben wurde, wird es nicht klappen.

Bevor Sie allerdings einen Drucker, der mit einem Windows-7-System verbunden ist, innerhalb des Netzwerks freigeben können, müssen Sie ein weiteres Mal das *Netzwerk- und Freigabecenter* aufsuchen. Dort wählen Sie im linken Panel den Eintrag *Erweiterte Freigabeeinstellungen* und anschließend das in diesem Fall gültige Netzwerkprofil aus. In diesem Profil sollten Sie dann, wie in unserem Screenshot zu sehen, sowohl den Punkt *Netzwerkerkennung einschalten* (erleichtert das Finden des Systems im Netzwerk) als auch *Datei- und Druckerfreigabe aktivieren* auswählen. Danach können Sie den Drucker Ihrer Wahl über sein Eigenschaftenmenü im Netzwerk freigeben.

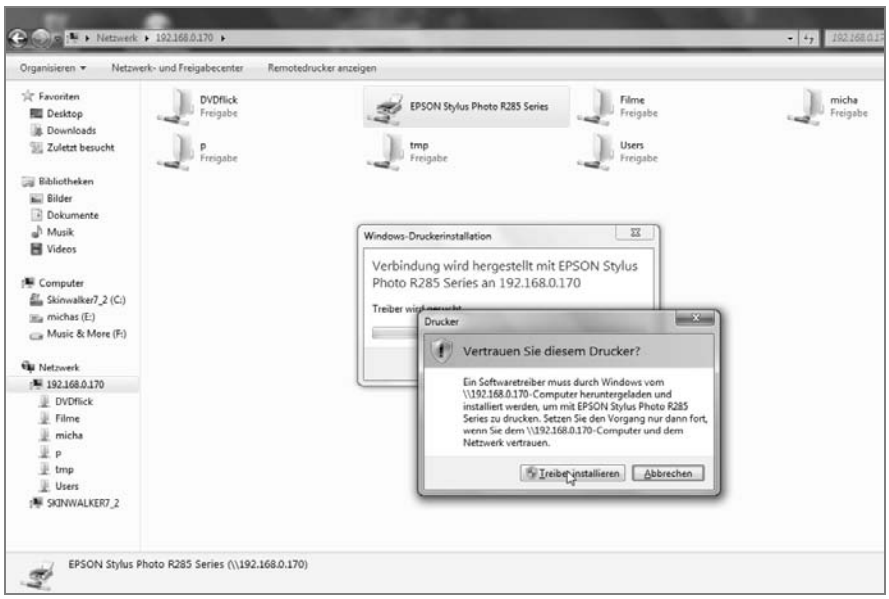

Bild 2.10: Der Zugriff auf den Drucker, der sich an einem Windows-7-System befindet, ist frei: Das System warnt noch einmal, dass nun Treiber von diesem System geladen werden.

Auch das Anbinden des Druckers erfolgt auf eine Art, die Sie höchstwahrscheinlich schon von anderen Windows-Systemen kennen: Wenn der Drucker an dem Windows-7-System freigegeben wurde, erscheint er im Netzwerk-Explorer des anderen Systems und kann dann problemlos eingebunden werden. Windows 7 warnt Sie noch einmal davor, dass Sie zum Betrieb des Druckers noch die entsprechenden Treiber vom Quellsystem herunterladen müssen – das sollten Sie natürlich nur bei Systemen tun, denen Sie vertrauen und von denen Sie sicher wissen, dass die Druckertreiber keine Fehler aufweisen oder in anderer Weise Probleme bereiten könnten.

5 Automatisierung und Scripting

Im Gegensatz zu Privatbenutzern haben es Administratoren in der Regel mit einer großen Anzahl von Computern zu tun. Deshalb stehen sie vor der Aufgabe, spezifische und gewünschte Systemanpassungen möglichst effektiv auf diese große Anzahl von Maschinen anzuwenden. Auf dem Markt existieren viele spezielle Programme von Drittherstellern für diese Problematik, die sogenannten System- und Service-Management-Lösungen, die auch als Client-Lifecycle-Management-Lösungen bekannt sind. Diese Programme setzen üblicherweise auf den Basisfähigkeiten des Windows-Betriebssystems auf und erweitern diese durch verbesserte Verwaltungsmöglichkeiten oder vereinfachen es, Änderungen zu steuern und zu überwachen.

Das Feld der Speziallösungen für mittlere und große Unternehmen überlässt Microsoft jedoch nicht ausschließlich Drittherstellern. Mit dem System Center Configuration Manager (SCCM) bietet der Hersteller selbst eine auf das Windows-Umfeld abgestimmte Verwaltungslösung für den professionellen Einsatz an.

Eine Vielzahl von Einstellungen und Verwaltungstätigkeiten lässt sich aber auch hervorragend mit den Bordmitteln von Windows erledigen, ohne dass Administratoren und Anwender auf solche erweiterten Zusatzprogramme zurückgreifen müssen. Soll ein Vorgang automatisiert und dann eventuell auf eine große Anzahl von Computern angewendet werden, so sind die grafischen Oberflächen zumeist nicht mehr das ideale Werkzeug: Hier können der Einsatz von Konsolen, Skripts und selbst die Verwendung einfachster Batch-Befehle große Vorteile bieten. Windows 7 stellt Ihnen eine ganze Reihe an Möglichkeiten für eine automatisierte und elegante Administration zur Verfügung, ohne dass unbedingt eine Verbindung zu einer Domäne existieren muss.

In diesem Kapitel stellen wir Ihnen deshalb die wichtigsten Grundlagen und Kommandos zu den Basistechniken der Windows-Automatisierung vor: die Eingabeaufforderung (CMD), die PowerShell als deutlich verbesserte und viel mächtigere Variante der Konsole und schließlich die auch über das Netzwerk verfügbare Windows Management Instrumentation (WMI).

5.1 Eingabeaufforderung

Die Eingabeaufforderung ist eine Funktion in Windows, die die Eingabe von Befehlen ermöglicht, zu denen beispielsweise nach wie vor die bekannten MS-DOS-Kommandos (Microsoft Disk Operating System) gehören. Die Konsole, die in der deutschen Win-

dows-Version stets als Eingabeaufforderung bezeichnet wird, erinnert an eine der ursprünglichsten Interaktionsmöglichkeiten zwischen Mensch und Maschine. Befehl eingeben – Befehl verarbeiten – Ergebnis ausgeben (im Fachjargon auch als EVA-Prinzip bezeichnet). Es gibt Befehle und Programme, die sich ausschließlich in der Eingabeaufforderung verwenden lassen, und andere Kommandos, für die keine Kommandozeilen-Version existiert.

5.1.1 Grundlagen der Konsole

Wird die Eingabeaufforderung (kurz CMD) gestartet, ohne dass zuvor über einen Rechtsklick *Als Administrator ausführen* gewählt wurde, so kann der Anwender in der Konsole gemäß dem erhöhten Sicherheitskonzept von Windows 7/Vista nur mit Standardrechten arbeiten. Es existiert eine Reihe von Systembefehlen, die nur mit den Rechten eines Administrators oder in einer Konsolensitzung im Administratorkontext arbeiten können. Noch unter Windows Vista musste der Anwender nach dem Starten der Konsole jedes Mal die Verwendung der erhöhten Rechte bestätigen, was unter Windows 7 glücklicherweise nicht mehr der Fall ist.

Starten der Konsole

Sie starten die Eingabeaufforderung, indem Sie auf *Startmenü/ Alle Programme/ Zubehör/Eingabeaufforderung* klicken oder in das Suchfeld des Startmenüs `cmd` eingeben und diese Eingabe mit der Eingabetaste bestätigen.

Tipp: Was ist aus dem Befehl *Ausführen* geworden?
Der Befehl *Ausführen* wird nicht mehr im Startmenü angezeigt. Das im Startmenü angezeigte Suchfeld bietet im Wesentlichen die gleiche Funktionalität wie der Befehl *Ausführen.* Falls Sie dennoch den gewohnten Befehl *Ausführen* verwenden möchten, können Sie ihn sich einblenden:

1. Rechtsklick in die Taskleiste, hier wählen Sie *Eigenschaften.*
2. Klicken Sie auf die Registerkarte *Startmenü* und dann auf *Anpassen.*
3. Aktivieren Sie in der Liste der Startmenüoptionen das Kontrollkästchen *Befehl "Ausführen"* und klicken Sie auf *OK.*

Sie können auch auf den Befehl *Ausführen* zugreifen, indem Sie die Windows-Taste und »R« drücken.

Eingabe von Befehlen

Befehle können in der Eingabeaufforderung sowohl in Groß- als auch in Kleinbuchstaben eingegeben werden. Befehlsoptionen können üblicherweise ebenfalls in Groß- und Kleinbuchstaben eingegeben werden. Leider haben sich nicht alle Entwickler an diese

Freiheit gehalten. Manche Optionen, typischerweise durch einen Schrägstrich eingeleitet, müssen in Großbuchstaben eingegeben werden. Und auch der Schrägstrich als Einleitung von Optionen ist nicht allgemeingültig – einige Optionen müssen mit einem vorangestellten Minuszeichen übergeben werden.

```
dir/w oder DIR/W
```

Auch die Reihenfolge der Optionen ist nicht einheitlich geregelt: Während manche Befehle die Optionen in einer genau vorgegebenen Reihenfolge erwarten, ist dies bei anderen Kommandos völlig gleichgültig. Im Zweifelsfall hilft ein Blick in die Onlinehilfe des jeweiligen Befehls, die mit `/?` ausgegeben wird.

Einzelne Parameter werden durch Kommas, Leerzeichen oder Strichpunkte voneinander getrennt. Es ist auch möglich, dass Befehle in einer Folgezeile fortgesetzt werden, sofern die vorherige Zeile durch das `^`-Zeichen beendet wurde. Das `^`-Zeichen verhindert darüber hinaus, dass eine Zeile durch die Eingabeaufforderung interpretiert wird. Diese Zeichen werden deshalb vielfach auch Maskenzeichen oder Escape-Zeichen genannt.

Mithilfe des Ampersand-Zeichens `&` können Sie zudem die Befehle miteinander verknüpfen, sodass sie in der geschriebenen Reihenfolge ausgeführt werden. Setzen Sie das `&`-Zeichen zweimal hintereinander ein, wird der Folgebefehl nur dann ausgeführt, wenn der vorherige Befehl fehlerfrei abgearbeitet werden konnte. Das exakte Gegenteil bewirkt die Verwendung von `||`: Der nachfolgende Befehl wird nur ausgeführt, wenn der vorherige Befehl mit einem Fehler abgebrochen wurde:

```
dir c:/w&&dir d:/w
dir c:/w||dir d:/w
```

Die Ein- und Ausgaben der CMD-Befehle in der Eingabeaufforderung lassen sich problemlos umleiten, was besonders für automatisierte Befehlsabläufe interessant ist. Wollen Sie beispielsweise eine nächtliche Kopieraktion durchführen, so nützen Ihnen die protokollierten Ereignisse kaum etwas, wenn Sie sie nicht zu einem von Ihnen gewünschten Zeitpunkt kontrollieren können. Deshalb sollten Sie in solchen Fällen die Ausgabe des Kopierbefehls in eine Protokolldatei umlenken und sinnvollerweise einige Tage vorhalten. Wir stellen im Rahmen dieses Kapitels noch einen entsprechenden Batch-Job vor. Die folgende Tabelle zeigt die möglichen Optionen zum Umlenken der Ein- und Ausgaben der Kommandos:

Kommando	*Erläuterung*
`<Datei`	Liest Standardeingaben aus einer benannten Datei.
`>Datei`	Schreibt die Ausgabe in eine benannte Datei.
`>>Datei`	Hängt die Ausgabe an eine benannte Datei. Ist diese nicht vorhanden, wird sie erzeugt.

Umgebungsvariablen

Viele Werte hält Windows als sogenannte Umgebungsvariablen vor – das sind festgelegte Werte, die in der Eingabeaufforderung ausgelesen werden können. Wollen Sie zum Beispiel den Installationsort von Windows auslesen, so finden Sie diesen Wert in der Umgebungsvariablen mit der Bezeichnung `%windir%`. Der folgende Befehl zeigt einige der vorgestellten Möglichkeiten in der Praxis: Er gibt das komplette Inhaltsverzeichnis des Windows-Installationsordners in die Datei `dir.txt` aus, die im Temporär-Ordner (`%temp`) des System abgelegt wird. Daran anschließend öffnet sich diese Datei automatisch im Texteditor Notepad:

```
dir %windir% >%temp%dir.txt&&notepad %temp%dir.txt
```

Das wirft wiederum die Frage auf, woher das Betriebssystem eigentlich weiß, wo es den Editor (*notepad.exe*) zu suchen hat. Die Antwort auf diese Frage hat ebenfalls etwas mit den Umgebungsvariablen des Systems zu tun: In der Umgebungsvariablen `PATH` sind die Verzeichnisse aufgelistet, die das Windows-System auf der Suche nach einem Befehl oder einer ausführbaren Datei automatisch durchsucht.

Welche Verzeichnisse das im Detail sind, lässt sich entweder über den Befehl `SET` oder `PATH` ausgeben. Während `SET` alle definierten Umgebungsvariablen ausgibt, gibt `PATH` nur die Standardsuchpfade aus. Mit Hilfe des Befehls `SETX` können System- und Benutzervariablen auch dauerhaft geändert werden. Die Verwendung von Variablen in Skript- beziehungsweise Batch-Jobs hat den Vorteil, dass der Ablauf der kleinen Programme in verschiedenen Umgebungen und auch verschiedenen Betriebssystemen idealerweise unverändert möglich ist.

Alternativ können Sie sich die Umgebungsvariablen auch über die grafische Oberfläche von Windows ansehen und bearbeiten. Dazu ist ein Rechtsklick auf den Eintrag *Computer* im Startmenü und die Auswahl *Eigenschaften* erforderlich. Im linken Menü öffnet ein Linksklick die *Erweiterten Systemeinstellungen*. Dort können Sie im Register *Erweitert* unten im Fenster die Schaltfläche *Umgebungsvariablen* auswählen, um sie einzusehen beziehungsweise zu verändern.

5.1.2 Elementare Befehle

Die folgende Auflistung zeigt die elementaren Befehle, die in der Eingabeaufforderung von Windows zur Verfügung stehen. Alle hier genannten Befehle können unter Windows 7 direkt verwendet werden. Bei älteren Windows-Versionen hingegen ist mitunter die Installation des sogenannten Resource Kit erforderlich, ehe Sie alle diese Kommandos nutzen können.

Kommando	*Erläuterung*
`clip`	Überträgt die Ausgabe eines Befehls oder den Inhalt einer Datei in die Zwischenablage. z. B. `clip < %temp%dir.txt`
`cls`	Löscht die aktuelle Ausgabe im Programmfenster der Eingabeaufforderung.
`cmd`	Startet eine neue Eingabeaufforderung. Mit der Option `/k` bleibt der neue Interpreter auch nach Beendigung eines Befehls aktiv. Mit `/c` wird der neue Interpreter nach Abarbeiten des Befehls automatisch beendet. Die Option `/e:on` bzw. `/e:off` aktiviert bzw. deaktiviert die Erweiterungen des Befehlsinterpreters. Der Standardwert wird über die Registry *HKCU* oder *HKLM\Software\ Microsoft\Command Processor\Enable Extensions* gesteuert. Die Option `/d` deaktiviert die Autorun-Einträge der Registry und *HKCU* oder *HLKM\Software\Microsoft\Command Processor\Autorun*.
`comp`	`comp [Optionen] [Dateien 1] [Dateien 2]` Vergleicht Dateien identischer Größe in Dateigruppen miteinander. Unterschiede werden ausgegeben. Für den Vergleich unterschiedlich großer Dateien ist der Befehl `fc` zu nutzen.
`compact`	`compact [Optionen] [Dateien]` Verwaltet die NTFS-Dateikompression. Dateien und Ordner können komprimiert (`/c`) oder dekomprimiert (`/u`) werden. Mit der Option `/s[:Verzeichnis]` werden ein Verzeichnis und dessen Unterverzeichnisse selektiert. Die Option `/f` erzwingt die möglicherweise wiederholte Kompression bereits als komprimiert markierter Dateien (die ohne diese Option übergangen würden). Bei der Verwendung von `compact` ohne Parameter wird eine Übersicht der Komprimierung des aktuellen Verzeichnisses und der darin enthaltenen Dateien angezeigt. Mehrere Dateinamen und Platzhalter sind möglich. Zwischen den Parametern müssen Leerzeichen eingefügt werden.
`copy`	`copy [Optionen] [Quelle] [Ziel]` Kopiert eine oder mehrere Dateien an eine andere Position. Die Verwendung von regulären Ausdrücken ist zulässig. Hervorzuheben ist die Option `/L`: Wenn die Quelle eine symbolische Verknüpfung ist, wird die Verknüpfung anstelle der eigentlichen Datei, auf die die Verknüpfung zeigt, zum Ziel kopiert. Standardmäßig wird beim Überschreiben zum Bestätigen aufgefordert, außer wenn der `copy`-Befehl innerhalb einer Batch-Datei ausgeführt wird. Um Dateien aneinanderzuhängen, geben Sie eine einzelne Datei als Ziel an, aber mehrere Dateien als Quelle (unter Verwendung von Platzhaltern oder in der Form: Datei1 + Datei2 + Datei3).

Kommando	*Erläuterung*
`date`	Stellt das Datum des Computers. Die Option `/t` sorgt für eine Ausgabe des aktuellen Datums ohne Eingabemöglichkeit.
`del`	`del [Optionen] [Dateien]` Löscht Dateien. Die Option `/s` bewirkt eine Ausweitung auch auf Unterverzeichnisse. `/q` unterdrückt die Bestätigungsaufforderung. Mit Hilfe der Option `/f` wird das Löschen von schreibgeschützten Dateien erzwungen. Über `/a.[Attribut]` wird die Operation auf Dateien mit bestimmten Attributen beschränkt: H = versteckt S = System R = schreibgeschützt A = Archivbit gesetzt I = nicht indiziert L = Reparse Point, eine Datei oder ein Verzeichnis im NTFS-Dateisystem, die anzeigt, dass die Datei oder das Verzeichnis nicht innerhalb des Dateisystems liegt, sondern von einem speziellen Dateisystemtreiber behandelt wird und aus einer anderen Quelle stammt In Windows Vista und höher sind bisher zwei Arten von Reparse Points implementiert, Junctions und Symbolic Links, auch Softlinks genannt. Junctions sind jedoch schon seit Windows 2000 vorhanden.
`expand`	`expand -d {CAB-Datei}` Dekomprimiert Dateien aus CAB-Archivdateien.
`fc`	`fc [Optionen] [Dateien 1] [Dateien 2]` Vergleicht zwei Dateien oder zwei Sätze von Dateien und zeigt die Unterschiede zwischen ihnen an. Dieser Befehl hat eine sehr große Anzahl möglicher Optionen, die über `fc/?` ausgegeben werden.
`find`	`find [Optionen] "Zeichenfolge" [Dateien]` Sucht nach einer Zeichenfolge in einer Ausgabe oder Datei und gibt die Zeilen aus, in denen die Zeichenfolge gefunden wurde. Die Option `/v` zeigt nur die Zeilen an, in denen die gesuchte Zeichenfolge nicht vorkommt. `/i` sorgt für ein Ignorieren von Groß- und Kleinschreibung. Die Option `/c` zeigt nur die Anzahl übereinstimmender Zeilen an, und die Option `/n` zeigt vor jeder Zeile die entsprechende Zeilennummer.
`findstr`	`findstr [Optionen] [/c:Zeichenfolge] [/g:Datei / Zeichenfolgen] [Dateien]` Sucht in den angegebenen Dateien nach einer oder mehreren Zeichenfolgen bzw. regulären Ausdrücken und gibt die übereinstimmenden Zeilen aus. Dieser Befehl hat eine sehr große Anzahl möglicher Optionen, die über `findstr/?` ausgegeben werden können.

Kommando	*Erläuterung*
`format`	`format {LB}: [Optionen]` Formatiert das durch den Laufwerksbuchstaben LB benannte Volume. Mit der Option `/fs:{Typ}` wird der Dateisystemstyp (NTFS, UDF, FAT32 oder FAT) ausgewählt. Mit `/v {Name}` wird das Volume automatisch mit einer Bezeichnung versehen. Weitere Optionen, beispielsweise zur Definition von Clustergrößen oder Schnellformatierung, finden sich in der Onlinehilfe, die über `format/?` ausgegeben wird. Eine Formatierung des aktuellen Systemlaufwerks ist grundsätzlich nicht möglich.
`md`	`md {Pfad}` Erzeugt ein benanntes Verzeichnis (make directory).
`move`	`move [/] Quelle Ziel` Verschiebt Dateien in ein anderes Verzeichnis. Die Option `/y` unterdrückt die Bestätigungsaufforderung.
`nbtstat`	`nbtstat [Optionen]` Zeigt Namenstabellen und aktuelle Verbindungen des NetBIOS over TCP/IP an. Optionen: `-a` Computername: Zeigt die Namenstabelle des benannten Computers an. `-A` IP-Adresse: Zeigt die Namenstabelle der benannten IP-Adresse an. `-c` Zeigt den Inhalt der Remote-Cache-Namenstabelle an. `-n` Zeigt lokale NetBIOS-Namenszuordnungen an. `-r` Zeigt Namen an, die über WINS oder Broadcast aufgelöst wurden. `-R` Löscht die Namenstabelle und baut sie neu auf.
`now`	Gibt das aktuelle Datum und die Uhrzeit aus. Sehr praktisch bei der Erstellung von Logfiles.

`openfiles`	`openfiles /disconnect [Optionen]`
	Zeigt geöffnete Dateien an oder trennt sie.
	`openfiles /query [Optionen]`
	Zeigt die geöffneten Dateien an und gibt sie in einem gewählten Format aus. Mit `/fo {table/list/csv}` wird das Ausgabeformat als Tabelle, Liste oder CSV-Datei ausgewählt.
	Optionen:
	`/s` Computer
	`/u` Benutzer
	`/p` Passwort
	Dieser Befehl kann nur mit Administrationsrechten ausgeführt werden.

Kommando	*Erläuterung*
`path`	Gibt die Standardsuchpfade aus.
`recover`	`recover {Dateiname}` Versucht, eine Datei Sektor für Sektor einzulesen und wiederherzustellen.
`set`	Setzt den Wert einer Umgebungsvariablen nur für die aktuelle Sitzung des Interpreters. Wird die Eingabeaufforderung geschlossen, werden die gesetzten Werte verworfen. Sehr praktisch für »kurzlebige« Informationen, beispielsweise in Schleifenkonstrukten.
`setx`	Setzt den Wert einer Umgebungsvariablen für den angegebenen Benutzer, Computer oder entfernten Computer. Dieser Befehl hat eine sehr große Anzahl möglicher Optionen, die über `setx-?` ausgegeben werden können.
`sfc`	`sfc [Optionen]` Überprüft die geschützten Systemdateien von Windows und ersetzt möglicherweise falsche Versionen durch die korrekten Originaldateien von Microsoft. Die Option `/ScanNow` aktiviert eine sofortige Untersuchung und Reparatur aller Systemdateien. `/VerifyOnly` beschränkt den Vorgang auf eine reine Überprüfung. `/ScanFile={Dateiname}` beziehungsweise `/VerifyFile= {Filename}` beschränkt den Vorgang auf die benannte Datei. `/OFFBOOTDIR` gibt den Speichort des Offline-Startverzeichnisses für Offlinereparaturen an, `/OFFWINDIR` zeigt auf den Speichort des Offline-Windows-Verzeichnisses für Offlinereparaturen. Der Vorgang kann in Abhängigkeit von Systemauslastung und Geschwindigkeit einige Minuten Zeit in Anspruch nehmen und verlangt zwingend nach einer expliziten Anmeldung als Administrator.
`shutdown`	Herunterfahren eines Computers. `shutdown -f -s -t 0` sorgt für ein augenblickliches, erzwungenes Herunterfahren des lokalen Computers. `shutdown -s -m\\{Computer} -t 60 -c {"Kommentar"}` fährt den benannten Computer in einer Minute herunter und zeigt den im Kommentar benannten Text an. `shutdown -a` bricht das Herunterfahren des Computers wieder ab. Dieser Befehl hat eine unterschiedliche Syntax, in den Vorgängerversionen von Windows wird in der x86-Ausprägung möglicherweise anstelle von minus ein Schrägstrich verwendet.

Kommando	Erläuterung
subst	subst [Laufwerksbuchstabe:] {Pfad} Erstellt ein virtuelles Laufwerk mit dem benannten Laufwerksbuchstaben. Mit der Option /d wird das Laufwerk wieder gelöscht. Beispielsweise wird mit subst u: c:\temp ein Laufwerk U: erzeugt, das auf C:\TEMP verweist. In der grafischen Datenträgerverwaltung von Windows werden die mit subst erzeugten Laufwerke nicht explizit ausgewiesen. Zudem gibt es einige Befehle in der Eingabeaufforderung, die mit diesen Laufwerken nicht zusammenarbeiten. Dazu zählen chkdsk, diskcomp, diskcopy, format, label und recover.
tree	tree {Verzeichnis} [Optionen] Gibt das benannte Verzeichnis in einer Baumansicht aus. Optionen: /a: Erzwingt die Ausgabe im ASCII-Zeichensatz /f: Zeigt ebenfalls die Dateinamen an.
type	type {Dateiname} Zeigt den Inhalt der benannten Datei an.
waitfor	Ein Befehl zur Steuerung voneinander abhängiger Aktionen mehrerer Computer in einem Netzwerk. Grundsätzlich werden zwei Varianten unterschieden: das Senden eines Signals und das Warten auf ein Signal. waitfor [/t {Timeout}] Signal Wartet auf das angegebene Signal. Die Option /t benennt eine maximale Wartezeit. Ein Signal ist eine maximal 225 Zeichen lange Zeichenkette, bestehend aus den ASCII-Zeichen mit den Codes zwischen 128 bis 255 (hier ist a–z, A–Z und 0–9 in jedem Fall enthalten). waitfor /si [/s Computer] Sendet ein Signal per Broadcast an alle Computer einer Domäne bzw. an den in der Option /s benannten Rechner.
where	where [/r Verzeichnis] Dateiname Sucht nach einer Datei im benannten Suchpfad und gibt den Speicherort der Datei aus. Ist kein Suchpfad angegeben, wird der Standardsuchpfad verwendet. Beispielsweise sucht where /r %userprofile% *.doc nach allen Word-Dokumenten im Benutzerpfad des aktuell angemeldeten Benutzers.

5.1.3 Einer der wichtigsten Befehle: net

Der Befehl net gehört ohne Zweifel zu den wichtigsten Befehlen, wenn es um die Arbeit mit und in Windows-Netzen geht. So wird jeder Administrator und IT-Profi bestätigen können, dass die Zuordnung von Netzlaufwerken und Netzdruckern zu seinen häufigs-

ten und wichtigsten Aufgaben gehört. Natürlich lassen sich Gruppenrichtlinien für diese Zuordnung einsetzen, doch der einfach einzusetzende Vorgänger `net` hat durchaus noch eine Daseinsberechtigung.

Kommando	*Erläuterung*
`net computer`	`net computer \\Computername [/add] [/del]` Fügt den angegebenen Computer einer Domäne hinzu bzw. entfernt ihn.
`net group`	Zeigt die globale Gruppe an und ändert sie. Die Verwendung der Option `/domain` sorgt für die Ausführung auf einem Domänencontroller anstatt auf dem lokalen System. `net group`: Zeigt den Namen der Gruppen in der aktuellen Domäne an. `net group Name [Benutzer] [/add] [/domain]`: Legt eine Gruppe an oder fügt Benutzer einer bereits existierenden Gruppe hinzu. Wird anstelle von `/add` die Option `/delete` verwendet, wird der Benutzer aus der Gruppe entfernt oder die Gruppe gelöscht.
`net localgroup`	Zeigt die lokale Gruppe an und ändert sie. Die Verwendung der Option `/domain` sorgt für eine Ausführung auf einem Domänencontroller anstatt auf dem lokalen System. Die Syntax entspricht der von `net group`.
`net use`	`net use [Gerät:] [\\Computer\Freigabe] [Passwort] [/user] [Optionen]` Ordnet dem lokalen PC eine Netzwerkressource zu. Hierbei kann es sich um einen Laufwerksbuchstaben oder einen Druckeranschluss handeln. Wird anstelle eines definierten Laufwerksbuchstabens ein Sternchen angegeben, wird der nächste zur Verfügung stehende Buchstabe gewählt. Wird kein Benutzer angegeben, wird der Name des aktuell angemeldeten Benutzers verwendet. Optionen: `/persistent:{yes/no}`: Erstellt eine dauerhafte Verbindung. `/home`: Ordnet den angegebenen Laufwerksbuchstaben dem Basisverzeichnis des Benutzers zu. `/delete`: Löscht die Zuordnung. `/savecred`: Speichert die verwendeten Anmeldeinformationen des Benutzers und das Passwort. Wird diese Freigabe künftig erneut verbunden, ist keine erneute Eingabe der Anmeldeinformationen notwendig.

Kommando	*Erläuterung*
`net user`	`net user [Benutzername] [Passwort *] [/add] [Optionen]` Erlaubt das Anlegen und Verändern von Benutzerkonten. Soll das Passwort direkt über die Eingabeaufforderung eingegeben werden, ohne dass es lesbar ist, so ist anstelle des Passworts ein Sternchen anzugeben. Mögliche Optionen des Befehls: `/active:{yes/no}`: Konto aktiv ja/nein `/add` oder `/delete` : Anlegen oder Löschen `/comment:[Zeichenfolge]`: Kommentar `/domain`: Führt Befehl auf Domänencontroller aus. `/fullname`: Benutzername `/expires: {Datum/never}`: Ablaufdatum des Kontos `/homedir`: Stammverzeichnis des Benutzers `/logonpasswordchg:{yes/no}`: Muss der Benutzer das Passwort nach der nächsten Anmeldung ändern oder nicht? `/passwordchg:{yes/no}`: Kann der Benutzer das Passwort ändern oder nicht? `/passwordreq:{yes/no}`: Muss ein Passwort vorhanden sein? `/profilepath:[Pfad]`: Profilpfad `/scriptpath:[Pfad]`: Pfad zum Anmeldeskript des Benutzers `/times:{all/Zeiten}`: Zulässige Anmeldezeiten für Benutzer `/workstations:[Liste]`: Beschränkt die Anmeldung des Benutzers auf die maximal acht benannten Computer in der Liste.
`net start` `net stop`	Möglichkeit, Dienste unter Windows zu starten oder zu stoppen. Wird nur `net start` eingegeben, so listet Windows alle aktuell gestarteten Dienste in der für das System gewählten Landessprache auf. Diese Bezeichnung ist für das Starten und Stoppen von Diensten leider nicht hilfreich, da der tatsächliche Dienstname gewählt werden muss. Am einfachsten sind diese Dienstnamen mit dem kleinen Zusatzprogramm PSTOOLS von Marc Russinovich ermittelbar. Mit `net stop wsearch` wird beispielsweise der Windows-Suchdienst auf dem lokalen PC beendet. Zur Ausführung des Befehls sind Administrationsrechte erforderlich. Ohne die entsprechenden Rechte gibt der Befehl als Fehlermeldung »Systemfehler 5« aus. Mit `net start wsearch` wird der Dienst wieder gestartet.
`net view`	`net view [Ziel]` Zeigt die Namen von Computern in einer Domäne oder einem Netzwerk an. Wird kein Ziel angegeben, werden alle Computer in der lokalen Domäne angezeigt.

6 Zusammenspiel im Netzwerk

Es gab einmal eine Zeit, in der Computer noch nicht über ein Netzwerk miteinander verbunden waren. Diese Zeit ist schon sehr lange vergangen: Spätestens seit dem Siegeszug des Internets in den neunziger Jahren gehört ein Kabel, das irgendwie mit einem Telefon- oder Netzwerksystem verbunden ist, zur Standardausrüstung.

Schon beim Design von Applikationen gehen die Entwickler heute davon aus, dass Ihr PC mit einem Netzwerk verbunden ist. Und wie auch immer die Anbindung aussieht, irgendein Kabel endet gewöhnlich mit einer Internetverbindung.

Ein Trend, der sich dabei immer deutlicher abzeichnet: Applikationen und Daten werden zunehmend direkt im Internet betrieben beziehungsweise dort gespeichert. Der eigene Desktop auf einem Windows-Computer wird möglicherweise eines Tages überhaupt nicht mehr erforderlich sein.

Noch geht es aber um Windows auf dem lokalen PC, und dieser ist mit einem Netzwerkkabel verbunden. In der klassischen Ausbaustufe für den professionellen Einsatz von Windows 7 treffen diese Client-Computer auf eine Active-Directory-Domäne, über die die Verwaltung der Benutzer-, Computer- und Datenobjekte zentralisiert betrieben wird.

Windows 7 bietet einige neue Funktionen für das Zusammenspiel mit Netzwerken, die außerordentlich beachtenswert sind. Der BranchCache ermöglicht ein intelligentes Vorhalten von Daten in verteilten Netzwerken auch auf Windows-7-PCs. Bei NAP handelt es sich nicht etwa um ein neues Dosenfutter für Hunde, sondern um die Etablierung einer sehr modernen Zugriffssicherheit, und Direct Access macht möglicherweise eine zusätzliche VPN-Umgebung in Ihrem Unternehmen überflüssig.

Alle in diesem Kapitel benannten Technologien sind eng mit dem Server-Betriebssystem Windows Server 2008 R2 verknüpft, einige sind ohne diese zentralen Komponenten überhaupt nicht einzusetzen. Aber auch ohne eine Active-Directory-Struktur sind die Funktionalitäten nicht nutzbar. Wir haben hier versucht, vor allen Dingen die Client-Aspekte dieser Techniken aufzuzeigen, und können die Seite der Server natürlich nur streifen.

Das betrifft sicher auch den vierten Abschnitt dieses Kapitels, in dem wir darauf eingehen, dass ein Windows-Client in einem Netzwerk heute sicher nicht nur auf andere Microsoft-Clients, sondern auch auf Linux-Systeme treffen wird – ein Umfeld, in dem sich Windows 7 ebenfalls sehr gut schlägt.

6.1 BranchCache

Microsoft beschreibt den BranchCache überaus blumig: »BranchCaching ist eine neue Funktion, die im Zusammenspiel von Windows Server 2008 R2 und Windows 7 zur Verfügung steht. Effiziente Ausnutzung von Ressourcen, zentrale Steuerung durch Gruppenrichtlinien und die Absicherung durch Verschlüsselung und Zertifikate ermöglichen sowohl für Webseiten als auch für Dateifreigaben ein Höchstmaß an Sicherheit und Effizienz bei einem Minimum an Komplexität in Ihrer Infrastruktur.«

Kurz gesagt: BranchCache ermöglicht die dezentrale »Pufferung« von Dateien auf Computern mit Windows 7. Sie brauchen dazu einen Windows Server 2008 R2, eine Domäne und Zertifikate. Wie das funktioniert, lesen Sie in diesem Abschnitt.

6.1.1 Grundüberlegung zu verteilten Netzwerken

Die Informationsdichte in den Netzwerken aller Unternehmen nimmt kontinuierlich zu. Diese Kernaussage wird jeder Administrator sicherlich ohne Zweifel unterschreiben. Verfügt ein Unternehmen über mehr als einen Standort, so dürfte sich allerorten Folgendes abgespielt haben: Was einst mit ein paar vernetzten PCs begann, wurde später durch lokale Server mit eigenen Domänen und eigener Dateiablage erweitert. Es folgte die Internetanbindung für jeden Standort – meist als Proxyserver realisiert.

Die Kosten für die Internetanbindungen sanken, und die einzelnen Netzwerke wurden zunächst für die Administration und dann für den sicheren Austausch von E-Mails miteinander verknüpft. Die einzelnen lokalen Domänen wurden aufgelöst und eine einzige große Domäne über alle Standorte gespannt. Die ersten Versuche einer zentralisierten Dateiablage schlugen bei vielen Unternehmen zunächst fehl, da sich die Zugriffsgeschwindigkeit über die WAN-Verbindung als zu träge erwies. Das Distributed File System (DFS) des Windows Server 2003 konnte zum Beispiel nur in Verbindung mit leistungsstarken WAN-Verbindungen gut eingesetzt werden.

Steht die Migration bei den Windows-Servern von Windows Server 2003 auf eine jüngere Version noch aus, so ist der verbesserte DFS-Dienst sicherlich eine zu prüfende Option. Das setzt aber erneut einen Windows-Server an jedem Standort voraus. Viele kleinere Dependancen ließen sich problemlos ohne Server vor Ort betreiben, sofern das Problem des schnelleren Dateizugriffs gelöst wäre. Die Sicherung aller Daten auf Bändern oder optischen Datenträgern zentralisiert am Hauptstandort wäre eine deutliche Vereinfachung in der IT-Administration.

In einem Konzept der Verschlankung der IT-Managementstruktur bietet sich grundsätzlich der Verzicht auf »kleinere Windows-Server« in den Außenstellen an. Die Stabilität und die Leistung der WAN-Verbindung zwischen Zentrale und Außenstelle sind jedoch bei allen Überlegungen stets mit höchster Priorität zu bedenken!

Je mehr Daten über eine WAN-Strecke geschickt werden, desto langsamer wird sie, das ist für jeden Benutzer spürbar. Ist beispielsweise eine Terminalserver-Applikation, die

zentral gehostet wird, Ihre primäre Anwendung, so werden Sie stets darauf achten wollen, dass diese Applikation gut funktioniert. Wird nun die Dateiablage von einem lokalen Server in einem Außenstandort auf die zentralen Filer verlegt, so wird die WAN-Leitung mit vielen Dateizugriffs-Operationen ausgelastet werden.

Sofern die Erhöhung der WAN-Leitungsgeschwindigkeit kein Problem darstellt, dürfte Sie dieser Umstand kaum erschrecken. Möglicherweise bietet sich die Methode BranchCache dazu an, dass Sie einerseits auf eine Serverlizenz und andererseits auf die Erhöhung der WAN-Geschwindigkeit verzichten können. Tatsächlich messbare Einsparungen im IT-Feld sind in der Praxis selten zu finden, möglicherweise ist BranchCache eine von diesen Seltenheiten.

Die Bedingungen sind ein Windows Server 2008 R2 auf dem Dateiserver, der die Daten üblicherweise bereitstellt, typischerweise ein Active Directory und Windows 7 als Client-Betriebssystem in den Versionen Enterprise oder Ultimate. Windows-XP- und -Vista-PCs profitieren von einem aktivierten BranchCache leider nicht.

Das primäre Einsatzgebiet für BranchCache ist die Beschleunigung des Zugriffs auf die Dateiablage. Inhalte von Webservern können per BranchCache ebenfalls beschleunigt bereitgestellt werden. Hierzu müssen Sie das BranchCache-Feature installieren und sicherstellen, dass der BranchCache-Dienst gestartet wurde, um die dadurch ermöglichte Beschleunigung von Inhaltsübertragungen durch einen Webserver mithilfe des BITS-Protokolls zu aktivieren. Weitere Schritte sind in diesem Fall nicht erforderlich.

6.1.2 Design und Komponenten für BranchCache

Wie bereits erwähnt, funktioniert BranchCache von Microsoft nur in Verbindung mit Client-Computern, die mit dem Betriebssystem Windows 7 Enterprise oder Ultimate installiert wurden. Die im Zusammenhang mit BranchCache aktiven Server müssen auf Basis von Windows Server 2008 R2 eingerichtet worden sein. Alle Varianten von Windows Server 2008 R2 werden unterstützt, mit Ausnahme von Server-Core-Installationen von Windows Server 2008 R2 Enterprise mit Hyper-V und Server-Core-Installationen von Windows Server 2008 R2 Datacenter mit Hyper-V. Die Einschränkung betrifft lediglich die Fähigkeit des Servers, als »Content-Server« zu fungieren. Das sind die File- und Webserver, die Informationen bereitstellen. Als sogenannte »Hosted Cache Server« (dazu später mehr) können alle Windows Server 2008 R2-Installationen verwendet werden.

BranchCache ist ein passives Caching-Verfahren. Dabei werden nur die Daten vom Server auf den BranchCache-Computer übermittelt, die von einem Client-Computer angefordert wurden. Somit wird verhindert, dass über die WAN-Verbindung unnötige Datenmengen bewegt werden, die kontinuierlich synchron gehalten werden müssen. Grundsätzlich werden nur Leseanforderungen über diesen Cache-Speicher abgewickelt, während Schreibzugriffe direkt an den Fileserver geleitet werden. Ob eine Datei in einer noch gültigen Fassung im Cache vorliegt, ermittelt BranchCache über ein Hash-Verfahren.

BranchCache arbeitet transparent mit Secure Sockets Layer (SSL), Server Message Block (SMB) Signing und End-to-End-IPsec-Verschlüsselungen zusammen. Die Reduktion des Netzwerkverkehrs und die Beschleunigung des Netzwerkzugriffs haben somit keine negativen Auswirkungen auf die Sicherheit.

BranchCache-Betriebsmodus

BranchCache unterstützt zwei unterschiedliche Betriebsmodi – den *Hosted Cache* und den *Distributed Cache*. Für den Hosted Cache ist ein Windows Server 2008 R2 in der Zweigstelle erforderlich, über den die Windows-7-Client-Computer die zwischengespeicherten Daten beziehen.

Im Hosted-Modus sind einige zusätzliche Konfigurationsschritte erforderlich, da für den Hosted-Cache-Server ein Zertifikat erstellt werden muss. Dieses Zertifikat muss an alle zugreifenden Windows-7-Client-Computer verteilt werden. Die Daseinsberechtigung für den Hosted-Modus muss in aller Deutlichkeit infrage gestellt werden: Warum sollen zwischengespeicherte Daten verwendet werden, wenn mithilfe der DFS-Replikation auf die echten Daten zugegriffen werden kann?

In der zweiten Betriebsvariante, dem Distributed Cache, wird auf einen weiteren Server verzichtet. In dieser Konstellation gibt es keinen Host-Server in der Niederlassung, der die Aufgabe des Zwischenspeicherns für alle Client-Computer übernimmt, sondern die Windows-7-Computer rufen die Daten aus der Zentrale ab und speichern diese lokal zwischen.

Für jeden Client-Computer kann nur einer der beiden Betriebsmodi verwendet werden. Je nach Konfiguration ist mindestens ein Windows Server 2008 R2 erforderlich, der sogenannte Content-Server.

6.1.3 Installation und Konfiguration auf dem Content-Server

Bevor die anderen Konfigurationsschritte durchgeführt werden, gilt es zunächst, den Fileserver in der Zentrale, der die primäre Dateiablage in der Konstellation darstellt, für den BranchCache-Betrieb zu aktivieren. Diese Konfiguration ist unabhängig davon, welcher Betriebsmodus anschließend gewählt wird. Der Parallelbetrieb, beispielsweise Hosted Cache an einem größeren Standort und Distributed Cache in einer kleineren Außenstelle, sind möglich.

Auf dem zentralen Dateiserver muss der Rollendienst *BranchCache für Netzwerkfreigaben*, der zur Rolle *Dateidienste* gehört, installiert werden.

1. Öffnen Sie auf dem zentralen Dateiserver den Server-Manager.
2. Wählen Sie in der Baumstruktur den Eintrag *Rollen*.
3. Klicken Sie auf *Dateidienste*. Fehlt dieser Eintrag, so ist dieser Server noch nicht als Dateiserver installiert und konfiguriert.

4. Wähen Sie im unteren Bereich des Fensters den Befehl *Rollendienste hinzufügen.*
5. Wählen Sie im Fenster *Rollendienste hinzufügen* den Eintrag *BranchCache für Netzwerkdateien* ganz unten in der Auflistung aus und installieren Sie diesen Dienst.
6. Die Installation ist nach wenigen Sekunden abgeschlossen; Ihnen wird der Link zum *Konfigurieren der Offlineverfügbarkeit für einen freigegebenen Ordner* angezeigt.

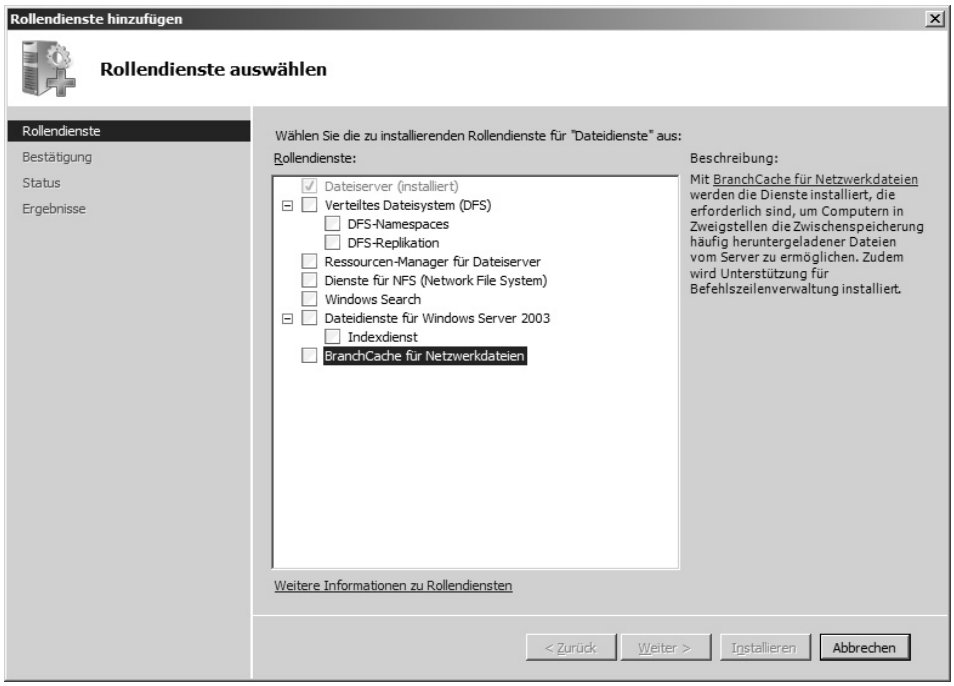

Bild 6.1: Auf dem zentralen Server muss der Rollendienst *BranchCache für Netzwerkdateien* installiert werden, ehe diese Funktion genutzt werden kann.

Nach der Installation ist der Rollendienst zwar grundsätzlich verfügbar, jedoch ist noch keine einzige Freigabe auf dem Server dahingehend konfiguriert worden, dass sie BranchCache überhaupt nutzt.

1. Sie nehmen die Einstellungen für jede Freigabe getrennt vor. Öffnen Sie dazu auf dem Dateiserver die *Freigabe- und Speicherverwaltung* im Startmenü unter *Verwaltung.*
2. Wählen Sie eine Freigabe aus, für die Sie Einstellungen für BranchCache aktivieren möchten. Öffnen Sie die gewünschte Freigabe mit einem Doppelklick. Wählen Sie im unteren Bereich des Dialogfensters die Schaltfläche *Berechtigung.*
3. Wählen Sie anschließend das zweite Register *Zwischenspeichern* aus, um Ihre Einstellungen vorzunehmen.

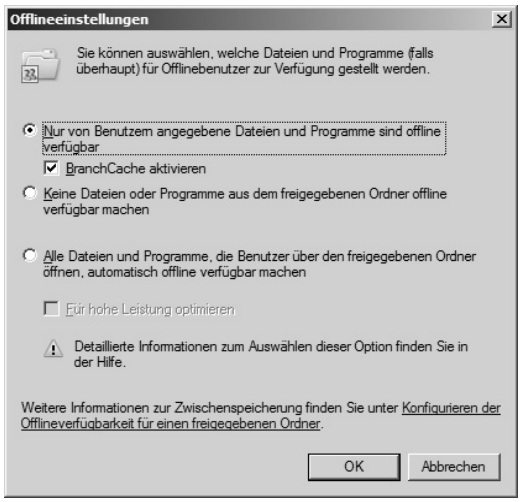

Bild 6.2: Ob eine Freigabe mit BranchCache genutzt werden kann oder nicht, wird für jede Freigabe separat auf dem Content-Server festgelegt.

4. Klicken Sie in diesem Fenster auf *BranchCache aktivieren*. Anschließend sind Client-Computer und Hosted-Cache-Server in der Lage, von dieser Freigabe zwischengespeicherte Informationen vorzuhalten.
5. Sie können den Editor für lokale Gruppenrichtlinien verwenden, um BranchCache auf einem einzelnen Server zu konfigurieren. In größeren Umgebungen mit mehreren Dateiservern empfiehlt sich die Verwaltung über eine Gruppenrichtlinie im Active Directory. Die Konfiguration des Hash-Werts ist in jedem Fall zu prüfen.

BranchCache-Gruppenrichtlinie für Content-Server:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole. Klicken Sie auf *Start*, zeigen Sie auf *Verwaltung* und klicken Sie dann auf *Gruppenrichtlinien-Verwaltungskonsole*.
2. Wählen Sie die Domäne aus, in der das Gruppenrichtlinienobjekt angewendet werden soll, oder wählen Sie eine *Richtlinie für Lokaler Computer* aus.
3. Klicken Sie im Menü *Aktion* auf *Neu*, um ein neues Gruppenrichtlinienobjekt zu erstellen.
4. Wählen Sie einen Namen für das Gruppenrichtlinienobjekt aus und klicken Sie auf *OK*.
5. Klicken Sie mit der rechten Maustaste auf das soeben erstellte Gruppenrichtlinienobjekt und wählen Sie *Bearbeiten*.
6. Klicken Sie auf *Computerkonfiguration*, zeigen Sie auf *Richtlinien*, dann auf *Administrative Vorlagen* und anschließend auf *Netzwerk* und klicken Sie dann auf *Lanman Server*.
7. Doppelklicken Sie auf *Hashveröffentlichung für BranchCache*.

8. Klicken Sie auf *Aktiviert.*
9. Wählen Sie unter *Optionen* eine der folgenden Aktionen unter *Aktionen zur Hashveröffentlichung* aus:
   - Hashveröffentlichung für alle freigegebenen Ordner zulassen
   - Hashveröffentlichung nur für freigegebene Ordner mit aktiviertem BranchCache zulassen
   - Hashveröffentlichung für keinen freigegebenen Ordner zulassen

6.1.4 BranchCache in der »Hosted Cache«-Konfiguration

Beim Hosted Cache kommt in der über die WAN-Verbindung angeschlossenen Niederlassung ein Windows Server 2008 R2 zum Einsatz, der zentral für alle Windows-7-Client-Computer den Cache in der Niederlassung darstellt. Für diesen Server muss im Zuge der Konfiguration ein Zertifikat erstellt werden, sodass sichergestellt werden kann, dass es sich bei den Daten von dem Server tatsächlich um die korrekte Maschine handelt.

Die Client-Computer greifen auf den Hosted-Cache-Server in der Niederlassung zu, um Daten der zentralen Server abzurufen. Benötigen Client-Computer Daten, die noch nicht auf dem Hosted-Cache-Server liegen, ruft dieser stellvertretend für den jeweiligen Client-PC die Daten vom Content-Server, dem Datei- oder Webserver in der Zentrale, ab.

Der Erstzugriff auf eine Datei, die noch nicht auf dem Hosted-Cache-Server gespeichert ist, verläuft somit im normalen, langsamen Zugriff der WAN-Verbindung. Spätere Zugriffe auf diese Daten laufen aber deutlich schneller ab. Leider gibt es noch keinen Befehl, der den Cache automatisch füllt. Am Ende dieses Kapitels finden Sie den Hinweis auf eine manuelle Methode, den Cache zu füllen.

Konfiguration von BranchCache als Hosted Cache

Die Einrichtung für den Hosted Cache besteht aus sechs Schritten:

1. Installieren des BranchCache-Features
2. Aktivieren des BranchCache-Features im Modus für gehostete Cache-Server
3. Erstellung eines Zertifikats für den gehosteten Cache
4. Verteilung des Zertifikats auf Client-Computer
5. Anpassung der Cachegröße
6. Konfigurierung des Client-Computers für die Verwendung des gehosteten Caches

Die Hosted-Cache-Konfiguration sieht einen Server in der Außenstelle vor, der für Client-Computer Dateien zwischenspeichert. Bei diesem Server muss es sich nicht um

einen dezidierten Datei- oder Webserver handeln. Auf dem Server muss als erster Schritt das Feature BranchCache installiert werden.

Gehen Sie dazu wie folgt vor:

1. Öffnen Sie durch einen Rechtsklick das Kontextmenü des Eintrags *Computer* im Startmenü auf dem Server in der Zweigstelle.
2. Wählen Sie *Verwalten* aus.
3. Öffnen Sie in der Baumstruktur am linken Fensterrand den Eintrag *Feature.*
4. Klicken Sie auf *Features hinzufügen.*
5. Wählen Sie *BranchCache.*
6. Klicken auf *Weiter* und schließen Sie den Vorgang durch die Installation des gewünschten Features ab.
7. Nach der Installation ist der BranchCache-Dienst zwar vorhanden und in der Startart auf *Automatisch* gesetzt, er ist jedoch noch nicht aktiv. Entweder wird der Server nun neu gestartet, oder der Dienst wird manuell gestartet.

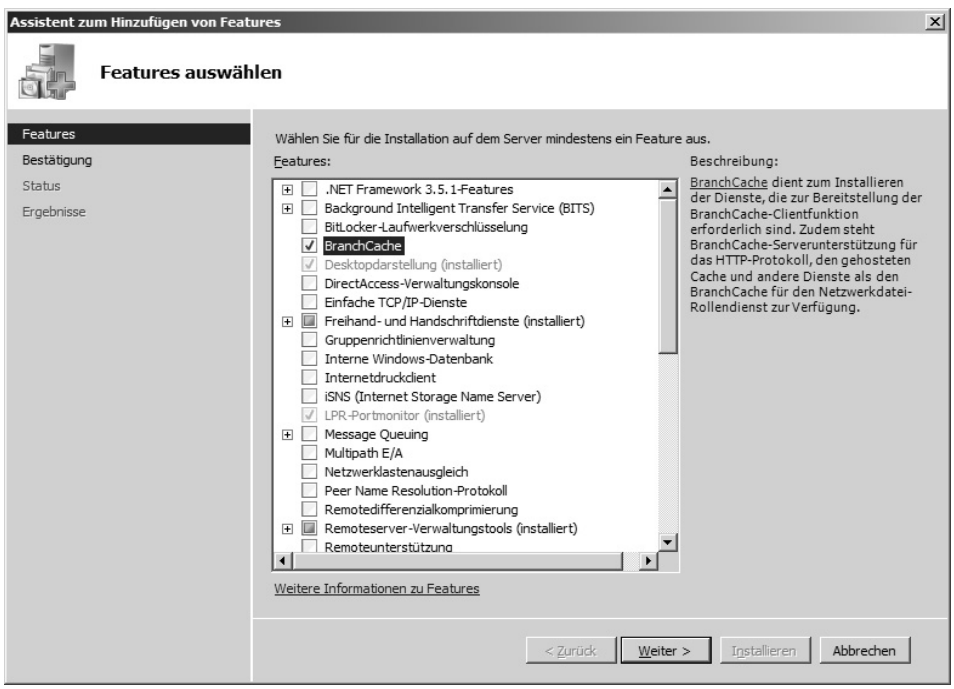

Bild 6.3: Der BranchCache wird über Features des Windows Server 2008 R2 hinzugefügt.

Über das `netsh`-Kommando wird im zweiten Schritt die Konfiguration auf dem Hosted-Cache-Server fortgesetzt. Der Befehl aktiviert einerseits den Hosted-Cache-Modus,

andererseits wird die Firewall automatisch für die eingehenden Verbindungen auf Port 80 und 443 geöffnet. Domänenadministrationsrechte oder eine vergleichbare Berechtigung sind zur Durchführung erforderlich. Führen Sie die Eingabeaufforderung (`cmd.exe`) als Administrator aus:

```
netsh branchcache set service mode=SERVERNAME
```

Als `SERVERNAME` tragen Sie den voll qualifizierten Domänennamen (FQDN) des Servers ein. Befinden sich die Computer und der Server nicht in einer Active-Directory-Domäne, so fügen Sie `clientauthentication=NONE` an:

```
netsh branchcache {…} clientauthentication=NONE
```

Die Kommunikation der Client-Computer mit dem Hosted-Cache-Server wird über TLS (Transport Layer Security) abgewickelt. TLS arbeitet auf dem Server und den Client-Computern mit Zertifikaten. Auf dem Hosted-Cache-Server muss dazu ein Zertifikat zur Verfügung stehen, dem die Client-Computer vertrauen.

Sofern Sie über keine externen Zertifikate verfügen, arbeiten Sie dazu am einfachsten mit einer internen Zertifikatsstelle. Auf dem Hosted-Cache-Server wird ein Serverzertifikat installiert, dessen Zertifizierungsstelle die Client-Computer in der Außenstelle vertrauen müssen. Sollten Sie noch keine interne Zertifikatsstelle besitzen, so ist die Installation der Serverrolle *Active-Directory-Zertifikatsdienste* auf einem Windows Server 2008 erforderlich (weitere Informationen hierzu finden Sie im Internet unter dem Suchbegriff »Active-Directory-Zertifikatsdienste«).

⊡ Lesezeichen

http://bit.ly/beILpA
Informationen zu Active-Directory-Zertifikatsdiensten

Das Zertifikat muss zwingend im lokalen Computerkonto des Hosted-Cache-Servers abgelegt werden. Prüfen Sie im Zweifelsfall, ob dies bereits geschehen ist:

1. Geben Sie in das Suchfeld des Startmenüs den Suchbegriff `mmc` ein und starten Sie die Suche mit der Eingabetaste. Für das Aufrufen der Microsoft Management Console (MMC) sind Administrationsrechte erforderlich.
2. Klicken Sie auf *Snap-In hinzufügen* im Befehl *Datei*.
3. Wählen Sie in der Auflistung der möglichen Snap-Ins unten *Zertifikate* aus.
4. Stellen Sie sicher, dass im folgenden Dialog *Computerkonto* ausgewählt ist (siehe Bild 6.4).
5. Unter *Eigene Zertifikate / Zertifikate* muss das Zertifikat für den Server hinterlegt sein. Wenn sich das Serverzertifikat nicht findet, können Sie es über das Kontextmenü installieren.
6. Ist das Zertifikat bereits vorhanden, öffnen Sie es mit einem Doppelklick.

7. Wechseln Sie in das Register *Details*.
8. Klicken Sie auf den Eintrag *Fingerabdruck des Zertifikats* und kopieren Sie den Wert in eine Textdatei und anschließend in die Zwischenablage.

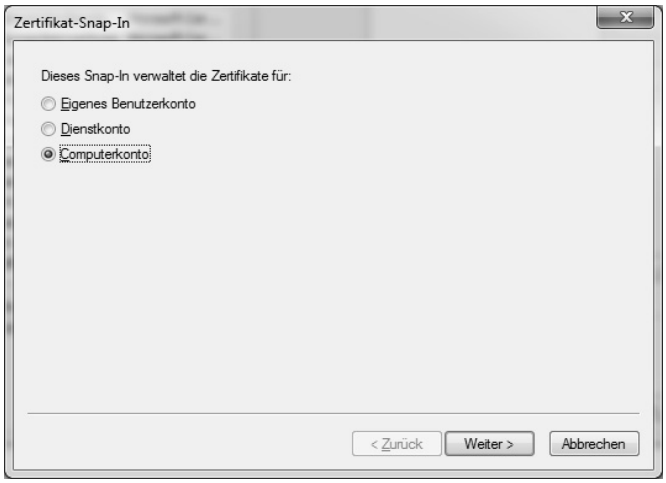

Bild 6.4: Das Zertifikat muss für das lokale Computerkonto des Hosted-Cache-Servers abgelegt werden.

Die weiteren Konfigurationsschritte werden in der Eingabeaufforderung unter Administrationsrechten auf dem Hosted-Cache-Server durchgeführt.

1. Öffnen Sie die Eingabeaufforderung mit Administrationsrechten.
2. Geben Sie folgenden Befehl in einer Zeile ein. Achten Sie darauf, dass der Fingerabdruck (hier ein Beispiel) des Zertifikats ohne Leerzeichen eingegeben wird. Die ID der Applikation ist fest vorgegeben und mit den geschweiften Klammern einzugeben. Als IP-Adresse wird 0.0.0.0 (`localhost`) verwendet:

```
netsh http add sslcert ipport=0.0.0.0 certhash=
1801c116554dc8b0b94b4649e142e66806e206cc
APPID={d673f5ee-a714-454d-8de2-492e4c1bd8f8}
```

3. Prüfen Sie nach der Eingabe mit folgendem Befehl, ob das Zertifikat mit der URL korrekt verbunden wurde:

```
netsh http show urlacl
```

4. Klicken Sie anschließend doppelt auf das Serverzertifikat in der Zertifikate-Konsole der MMC.
5. Prüfen Sie im Register *Erweitert*, ob das Zertifikat für Client-Authentifizierung und Server-Authentifizierung konfiguriert ist. Achten Sie darauf, dass die Client-Computer der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, vertrauen. Hierzu muss das Zertifikat der Stammzertifizierungsstelle bei den Client-Computern als vertrauenswürdig hinterlegt sein.

Anpassung der Cache-Größe

In der Standardeinstellung von Microsoft wird der Hosted-Cache-Server so eingerichtet, dass maximal fünf Prozent des Speicherplatzes auf den Festplatten als Zwischenspeicher für den BranchCache genutzt werden. Sollten Sie diesen Wert ändern wollen, so ist dies über die Eingabeaufforderung möglich:

1. Öffnen Sie die Eingabeaufforderung mit Administrationsrechten.
2. Geben Sie folgenden Befehl in einer Zeile ein. Der Wert ist als Prozentzahl ohne die geschweiften Klammern einzugeben:

```
netsh branchcache set cachesize size={WERT} percent=TRUE
```

Aktivierung des Hosted-Cache-Servers über CMD

Wird der Wert bereits über eine Gruppenrichtlinie gesteuert, können Sie ihn nicht mehr über die Eingabeaufforderung anpassen. Sie können den Hosted-Cache-Server jedoch auch über die Eingabeaufforderung aktivieren:

1. Öffnen Sie die Eingabeaufforderung mit Administrationsrechten.
2. Geben Sie folgenden Befehl in einer Zeile ein. Der Wert ist als Prozentzahl ohne die geschweiften Klammern einzugeben:

```
netsh branchcache set service mode=HOSTEDSERVER
```

BranchCache über Gruppenrichtlinien steuern

Die Konfiguration des Hosted-Cache-Servers erfolgt über Gruppenrichtlinien oder über NETSH-Kommandos. In größeren Umgebungen ist der Einsatz von Gruppenrichtlinien im Sinne der besseren Administration und Nachvollziehbarkeit der Konfiguration zu bevorzugen.

1. Öffnen Sie über das Suchfeld oder das Feld *Ausführen* auf dem Windows Server 2008 R2 den Editor für die lokale Gruppenrichtlinie über die Eingabe `gpedit.msc` und bestätigen Sie die Eingabe mit der Eingabetaste.
2. Öffnen Sie die *Computerkonfiguration*.
3. Öffnen Sie *Administrative Vorlagen*.
4. Öffnen Sie *Netzwerk*.
5. Klicken Sie in der Baumstruktur auf *BranchCache*, um auf der rechten Seite des Fensters die Einstellungsmöglichkeiten für den Server zu sehen. Eine weitere Einstellung finden Sie unter *LanMan-Server*.

Beachten Sie, dass Sie den Rollendienst *BranchCache für Netzwerkdateien* auf dem zentralen Server, dem sogenannten Content-Server, in jedem Fall installiert haben müssen. Der Hosted Cache kann nur funktionieren, wenn überhaupt Daten für das Caching vom zentralen Server zur Verfügung gestellt werden.

Die Client-Konfiguration erfolgt über die Einstellungen unter *BranchCache*. Die Einrichtung einer Hosted-Cache-Umgebung ist komplett unabhängig von der Definition von Standorten im Active Directory. Wie BranchCache in Ihrer Netzwerkumgebung eingerichtet wird, hängt somit ausschließlich an den hier vorgenommenen Einstellungen.

Roundtrip-Einstellung für BranchCache

Die wichtigste Einstellung in diesem Zusammenhang ist die Roundtrip-Netzwerklatenz. Mit diesem Wert wird der Standardwert für die Roundtrip-Netzwerklatenz geändert, oberhalb dessen Netzwerkdateien von Client-Computern in der Niederlassung zwischengespeichert werden.

Netzwerkdateien werden standardmäßig in der Zweigstelle zwischengespeichert, sofern die Roundtrip-Netzwerklatenz der WAN-Verbindung über 80 ms liegt. Um die auf die Zweigstellencomputer heruntergeladenen Netzwerkdateien immer zwischenzuspeichern, legen Sie den Wert für die Netzwerklatenz auf 0 fest. Um das Zwischenspeichern von Netzwerkdateien in Zweigstellen zu deaktivieren, legen Sie die Latenz auf einen sehr hohen Wert fest.

Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden Netzwerkdateien vom Client-Computer gemäß der Dokumentation zwischengespeichert, wenn der Wert für die Roundtrip-Netzwerklatenz der WAN-Verbindung über 80 ms liegt.

6.1.5 BranchCache in der »Distributed Cache«-Konfiguration

In kleineren Niederlassungen, in denen kein Windows Server 2008 R2 zur Verfügung steht, aber Windows-7-Client-Computer verwendet werden, kann der BranchCache in der Konfiguration Distributed Cache eingesetzt werden.

In dieser Konstellation gibt es keinen Host-Server in der Niederlassung, der die Aufgabe des Zwischenspeicherns für alle Client-Computer übernimmt, sondern die Windows-7-Computer rufen die Daten aus der Zentrale ab und speichern sie lokal zwischen.

Andere Windows-7-Rechner in derselben Niederlassung können auf diese zwischengespeicherten Daten zugreifen, ohne die Informationen erneut über die WAN-Leitung anzufordern. So lassen sich die Vorteile von BranchCache auch ohne einen Server in der Niederlassung nutzen. Diese Technik funktioniert jedoch nur innerhalb eines einzelnen Subnetzes. Wird ein Client-Computer, der zwischengespeicherte Daten bereitstellt, heruntergefahren, so steht diese Pufferung nicht mehr zur Verfügung. In diesem Fall fordern die anderen Client-Computer in der Niederlassung die Daten über den regulären Weg über die WAN-Verbindung direkt vom Server an.

Thomas Bär/Frank-Michael Schlede

Windows 7
richtig administrieren

In den meisten Unternehmen ist nicht Vista, sondern erst Windows 7 der Nachfolger des altehrwürdigen Windows XP. Die beiden erfahrenen Praktiker und Fachautoren Thomas Bär und Frank-Michael Schlede zeigen Ihnen, wie Sie Windows 7 auf Unternehmens-PCs effizient, erfolgreich und sicher betreiben. Sie lernen die Hürden der Migration von XP zu 7 zu meistern und den XP-Modus zu nutzen, um besonders störrische Programme weiter zu verwenden. Auch die Themen Sicherheit, Automatisierung und Linux-Integration kommen nicht zu kurz.

Upgrade und Konfiguration von Windows 7

Die Uhr von Windows XP läuft ab. Dieses Buch zeigt Ihnen, wie Sie schmerzfrei auf das moderne PC-Betriebssystem Windows 7 migrieren und wie Sie das System optimal auf den Unternehmens-PCs verbreiten. Für alle Anwendungen, die noch das alte Windows benötigen, finden Sie Tipps, wie Sie den XP-Modus der Profi-Versionen von Windows 7 einsetzen. Sie erfahren, wie Sie Anwender und Benutzergruppen anlegen, ihnen über Gruppenrichtlinien Rechte zuweisen und ihnen Dateien und Systemressourcen wie Drucker zur Verfügung stellen. Darüber hinaus zeigen Ihnen die Autoren, wie Sie Administrationsaufgaben per Skript automatisieren. Sie lernen, wie Sie die Eingabeaufforderung für Skripte nutzen, und erhalten eine Einführung in das mächtige Kommandozeilen-Tool PowerShell.

Maximale Sicherheit

Die Firewall und die Benutzerkontensteuerung bilden zwei herausragende Security-Features von Windows 7. Die Autoren zeigen Ihnen, wie Sie beide Elemente konfigurieren müssen, um größtmögliche Sicherheit bei gleichzeitigem Benutzerkomfort zu erhalten. Darüber hinaus erfahren Sie, wie Sie die Festplattenverschlüsselung Bitlocker im Unternehmen zielführend einsetzen und unerwünschte Software im Netz mit dem Applocker blockieren. Mit den Tipps dieses Buches wird das Erstellen der dafür notwendigen Richtlinien und Regeln zum Kinderspiel.

Zusammenspiel im Netzwerk

Auch wenn die frühen Windows-Systeme auf Einzelplatzrechner ausgelegt waren, macht Windows 7 im Netzwerk und auch im Zusammenspiel mit Linux-Rechnern eine gute Figur. Die Autoren zeigen, wie Sie mit Hilfe von BranchCache den Datenverkehr in einem Wide Area Network minimieren und damit die Performance Ihrer IT steigern. Darüber hinaus beleuchten sie die Network Access Protection, mit der Sie sicherstellen, dass alle Rechner im Netz über die wichtigsten Sicherheits-Patches verfügen. Zudem erfahren Sie, wie Sie Windows- und Linux-Rechner nebeneinander in einem Netz betreiben.

Aus dem Inhalt:

Über die Autoren:

Thomas Bär ist Leiter der Klinischen IT der Bezirkskliniken Schwaben. Seit zehn Jahren arbeitet er darüber hinaus als Fachautor zu IT- und Computerthemen.

Frank-Michael Schlede blickt auf über zwanzig Jahre Erfahrung als IT-Fachjournalist zurück, unter anderem war er Chefredakteur der Zeitschriften UnixOpen und Windows IT Pro.

30,– EUR [D]
ISBN 978-3-645-60056-9